5.1.2.e

Van: 5.1.2.e <5.1.2.e @minvws.nl>
Verzonden: woensdag 12 februari 2020 13:03
Aan: Functionaris gegevensbescherming
Onderwerp: RE: datalek Tweede Kamer

Beste 5.1.2.e

Het nummer van de melding die ik heb gedaan is: 5.1.2.i

Voor wat betreft het voorstel om nader kennis te maken. Daar sta ik volledig achter. Ik ga komende zaterdag op vakantie en ben begin maart weer terug.
Past een kopje koffie in de tweede week maart in jullie agenda? Maandag 9 maart om 15.00 of woensdag 11 maart om 11 uur?

Vriendelijke groeten,

5.1.2.e

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: woensdag 12 februari 2020 11:19
Aan: 5.1.2.e <5.1.2.e @minvws.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: datalek Tweede Kamer

Beste 5.1.2.e

Dank voor de informatie van zojuist! Ik dacht; ik mail je. Dan heb je mijn contactgegevens! Ik wacht het kenmerknummer van jullie melding af.
Inmiddels is ook de cache bij google verwijderd.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	03-01-2020 16:12:50
Uniek nummer	5.1.2.i
	5.1.2.i

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Tweede Kamer der Staten-Generaal

Inbreuk op de vertrouwelijkheid van de gegevens	Ja
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Ja

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Persoonsgegevens per ongeluk gepubliceerd

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

Betrokken burger heeft op 18 juli 2019 o.a. aan de vaste Kamercommissie voor onderwijs een klachtbrief gestuurd (klacht over een school). Verzocht werd zorgvuldig met de persoonsgegevens om te gaan (geheimhouding). De vaste Kamercommissie heeft op 11 september 2019 per brief aan de minister van onderwijs gevraagd om een kopie van zijn antwoord aan betrokkene. Deze brief bevatte abusievelijk de volledige naam van betrokkene. Deze brief is op 11 september 2019 op de website van de Tweede Kamer gepubliceerd. De brief van 18 juli 2019 --welke als bijlage werd meegestuurd met de brief van 11 september-- is niet op de website gepubliceerd. Het gaat derhalve alleen om de volledige naam van betrokkene. Op 2 januari 2019 heeft betrokkene het datalek ontdekt en contact opgenomen met de Kamer.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Ja
Geslacht, geboortedatum en/of leeftijd	Nee

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Nee
Klanten (huidig en potentieel)	Ja
Leerlingen of studenten	Nee
Patiënten	Nee
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Onder 'klant' wordt verstaan: een burger die de Kamer benadert met een probleem/klacht

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	1
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	1

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op	Nee

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Ja
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Nee
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Nee

Andere gevolgen, namelijk:

Betrokkene + gezin zijn bang voor represaillemaatregelen en voor smaad en laster

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Ja
Wanneer heeft u het datalek gemeld aan de betrokkenen?	03-01-2020

Wat is de inhoud van de melding aan de betrokkenen?

Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?

9. Overig

Is naar uw mening deze melding compleet?

Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

5.1.2.e

Van: Functionaris gegevensbescherming
Verzonden: dinsdag 7 januari 2020 14:59
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: RE: melding Autoriteit Persoonsgegevens

Beste 5.1.2.e

Onderstaande mail aan 5.1.2.e en jou sluit ik af met het noemen van een aantal actiepunten. Graag doe ik in dit verband een beroep op jou.

1. onderzoeken of betrokkene nader geïnformeerd moet worden;

De mail die je al hebt gestuurd, lijkt me op zich voldoende. Heb je hierop nog een reactie ontvangen? Te overwegen valt betrokkene nog een keer te mailen of te bellen met de vraag of een en ander voor haar nu voldoende beantwoord is. Daarbij kunnen we dan melden dat ook de Kamer het incident heeft gemeld bij de Autoriteit Persoonsgegevens (AP). Ook kan betrokkene dan geïnformeerd worden over de uitkomsten van onderstaande actiepunten.

2. onderzoeken of de desbetreffende informatie door anderen daadwerkelijk is geraadpleegd op de website van de Kamer en hoeveel dit keer betrof;

Weet jij of nagegaan kan worden hoeveel keer en wanneer de desbetreffende informatie op de website is geraadpleegd? Dan hebben we op zich een idee hoeveel keer anderen kennis hebben kunnen nemen van de naam van betrokkene.

3. welke organisatorische maatregelen er getroffen moeten (of kunnen) worden om herhaling te voorkomen.

Dit betreft een belangrijk onderdeel van het gemeld hebben van datalekken. Indien en voor zover de AP vragen gaat stellen naar aanleiding van de melding zullen deze zeker betrekking hebben op dit onderwerp. Wellicht ook omdat de vorige melding betrekking had om eenzelfde proces. Ik weet dat er de nodige aandacht is voor de naleving van de AVG bij de GC's en dat het incidenten betreft die niet met een 100%-garantie uit te sluiten zijn. Maar Toch de volgende (belangrijke) vragen:

- Kan jij aangeven of de procedure is aangepast danwel dat deze wordt aangepast?
- Bestaat er wellicht software dat gebruikt kan worden om namen en/of andere persoonsgegevens etc. op te sporen?

Met vriendelijke groet,

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

-----Oorspronkelijk bericht-----
Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 3 januari 2020 16:40
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: melding Autoriteit Persoonsgegevens

Dank 5.1.2.e goede formulering lijkt me

Met vriendelijke groet,
drs. 5.1.2.e
5.1.2.e
Cultuur en Wetenschap
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
5.1.2.e @tweedekamer.nl

-----Oorspronkelijk bericht-----
Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 3 januari 2020 16:35
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: melding Autoriteit Persoonsgegevens

Beste 5.1.2.e en 5.1.2.e

Het Datelekteam ontving vanmiddag een melding van een datalek. Het lek is inmiddels 'gedicht' en er is al contact geweest met de persoon die het lek heeft gemeld (=tevens de persoon over wie gegevens zijn gelekt). Deze persoon heeft inmiddels ook een klacht ingediend bij de Autoriteit Persoonsgegevens. De Kamer is verplicht om binnen 72 uur na bekendwording (van het lek) melding hiervan te doen bij de Autoriteit Persoonsgegevens. Dat heb ik inmiddels gedaan (zie bijlage). In het kort: het datalek betreft:

"Betrokken burger heeft op 18 juli 2019 o.a. aan de vaste Kamercommissie voor onderwijs een klachtbrief gestuurd (klacht over een school). Verzocht werd zorgvuldig met de persoonsgegevens om te gaan (geheimhouding). De vaste Kamercommissie heeft op 11 september 2019 per brief aan de minister van onderwijs gevraagd om een kopie van zijn antwoord aan betrokkene. Deze brief bevatte abusievelijk de volledige naam van betrokkene. Deze brief is op 11 september 2019 op de website van de Tweede Kamer gepubliceerd. De brief van 18 juli 2019 --welke als bijlage werd meegestuurd met de brief van 11 september-- is niet op de website gepubliceerd. Het gaat derhalve alleen om de volledige naam van betrokkene. Op 2 januari 2019 heeft betrokkene het datalek ontdekt en contact opgenomen met de Kamer".

De naam is inmiddels vervangen door initiatalen. Met betrokkene is contact opgenomen en excuses aangeboden.

Verdere actie zal bestaan uit:

1. onderzoeken of betrokkene nader geïnformeerd moet worden; 2. onderzoeken of de desbetreffende informatie door anderen daadwerkelijk is geraadpleegd op de website van de Kamer en hoeveel dit keer betrof; 3. welke organisatorische maatregelen er getroffen moeten (of kunnen) worden om herhaling te voorkomen.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR

Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Docnr4

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 28 januari 2020 08:12
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: RE: melding datalek
Bijlagen: melding verkeerde documenten in P-Direkt personeelsdossier; documenten in verkeerd personeelsdossier

Opvolgingsvlag: Opvolgen
Vlagstatus: Met vlag

Dag 5.1.2.e
Ja, beiden zijn geïnformeerd zoals ik destijds ook al heb aangegeven. Zie bijlagen ter info.
Met vriendelijke groet,
5.1.2.e

Adviseur HR - Stafdienst HR
Tweede Kamer der Staten-Generaal

Aanwezig: dinsdag tot en met vrijdag
(oneven weken: dinsdag tot en met donderdag)
Postbus 20018, 2500 EA Den Haag
T (+5.1.2.e | M 5.1.2.e
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl
Vanaf 2 januari 2019 is de Tweede Kamer aangesloten op P-Direkt. Het shared service center voor de Rijksoverheid op het gebied van personeels– en salarisadministratie. U kunt als ambtenaar van de Tweede Kamer hier uw personeelszaken regelen, zoals verlof registreren, IKB aanvragen en uw personeelsdossier inzien. Ook kunt u vanaf deze datum op Rijksportaal veel wet- en regelgeving en andere handige informatie terugvinden, die u eerst aantrof in het personeelshandboek.
Op Plein2 (http://plein2/personeelszaken) vindt u informatie over de aansluiting bij P-Direkt, zoals de veelgestelde vragen en een wegwijzer voor het P-Direkt portaal.

Van: 5.1.2.e
Verzonden: maandag 27 januari 2020 11:04
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: melding datalek
Beste 5.1.2.e
Zie onderstaand bericht van jou over datalek:
Hierbij meld ik een data lek.
Door een medewerker - de heer 5.1.2.e - is geconstateerd dat er in zijn P-Direkt personeelsdossier documenten voorkomen die van een andere medewerker zijn, namelijk de heer 5.1.2.e Dit is mij, 5.1.2.e 5.1.2.e door de heer 5.1.2.e heden gemeld.
Stappen tot nu toe:

- *Ik heb onderzocht om welke documenten het gaat. In deze situatie betreft het een vijftal documenten betreffende diploma's en certificaten.*
- *Contact met P-Direkt opgenomen en verzocht de documenten zo spoedig mogelijk te verwijderen uit het dossier van de heer 5.1.2.e en op de juiste plaats in het dossier van de heer 5.1.2.e onder te brengen.*
- *Zowel de heer 5.1.2.e als de heer 5.1.2.e worden na het verzenden van deze mail direct per mail hiervan door mij op de hoogte gesteld.*

Indien nodig word ik graag geïnformeerd over vervolgstappen die door mij dienen te worden gezet.
Kun je ons laten weten of betrokkenen zijn geïnformeerd, zodat wij deze melding kunnen afsluiten?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Tweede Kamer der Staten-Generaal
5.1.2.e of 5.1.2.e

Postbus 20018, 2500 EA Den Haag
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Alle informatie over de Tweede Kamer is te vinden op www.tweedekamer.nl. U kunt de Tweede Kamer ook volgen op Facebook en Twitter. Download ook de gratis Tweede Kamer vergaderagenda app in de Apple of Android store.

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 5 februari 2020 08:06
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: FW: I2001 0975 - TOPdesk melding

Ha 5.1.2.e

Gisteren heb ik met 5.1.2.e en 5.1.2.e afgesproken dat verlies/diefstal van telefoons en andere gegevensdragers zoals laptop of ipad een standaardbehandeling krijgen die bestaat uit:

- Melding verlies/diefstal bij servicedesk (persoonlijk of telefonisch)
- Invullen meldformulier datalek
- Persoon moet in geval van diefstal aangifte doen bij politie en pv inleveren
- Servicedesk stelt de bekende vragen zoals beveiliging gegevensdrager met pincode etc etc. en noteert dit in TopDesk
- Incident wordt doorgegeven aan Datalekteam
- Datalekteam kijkt of servicedesk alle afgesproken en noodzakelijke acties heeft uitgevoerd. Als er verder geen bijzonderheden zijn gemeld door SD constateert datalekteam dat er geen nadere acties meer nodig zijn.
  Datalekteam meld incident gereed.
- Incident is opgenomen in het datalekregister.

Ik stel voor dat wij de volgende standaardtekst toevoegen aan alle incidenten die wij ontvangen over vermissing/diefstal van een gegevensdrager:
Het datalekteam constateert dat de Servicedesk (SD) alle afgesproken en noodzakelijke acties heeft uitgevoerd. Er zijn geen nadere bijzonderheden gemeld door SD. Datalekteam concludeert dat er geen acties meer nodig zijn en meldt het incident gereed.

Ben je het hiermee eens?
Zo ja, dan kunnen we dit gelijk toevoegen aan I2001 0975, het incident dat gisteren aan ons is doorgestuurd.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Tweede Kamer der Staten-Generaal
5.1.2.e of 5.1.2.e

Postbus 20018, 2500 EA Den Haag
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Alle informatie over de Tweede Kamer is te vinden op www.tweedekamer.nl. U kunt de Tweede Kamer ook volgen op Facebook en Twitter. Download ook de gratis Tweede Kamer vergaderagenda app in de Apple of Android store.

Van: 5.1.2.i <5.1.2.i@tweedekamer.nl>
Verzonden: dinsdag 4 februari 2020 14:58
Aan: 5.1.2.e 5.1.2.e tweedekamer.nl>; 5.1.2.e <5.1.2.e@tweedekamer.nl>; 5.1.2.e

5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2001 0975 - TOPdesk melding

Geacht Datalekteam

Melding met nummer: I2001 0975 is aan u overgedragen.

Het betreft : [unresolved: incident_specid]
Verloren iPad

04-02-2020 14:57 5.1.2.e
@Datalekteam: Aanmelder meldt op 24 januari dat ze haar iPad (TABL2114) verloren heeft. Er is door 5.1.2.i een Selective Wipe uitgezet, maar deze is nog niet doorgekomen. Het apparaat is de afgelopen 18 dagen niet online geweest. Mevrouw geeft aan dat haar ontgrendelcode niet makkelijk te raden is (dus niet 0000 of 1234).

I2001 0975.PNG

04-02-2020 14:53 5.1.2.e
Aanmelder is maandag niet langs geweest. iPad heeft Selective Wipe nog niet uitgevoerd.

Aanmelder meldt dat ze geen makkelijk te raden unlock code heeft en komt morgen langs voor de iCloud wipe.

24-01-2020 16:52 5.1.2.e
Mevrouw meldt dat zij haar TK iPad verloren is, TABL2114.
Selective Wipe request gestuurd, maar door het afsluiten van Citrix is het niet duidelijk of deze aankomt.
Selective wipe was requested at 24-1-20 16:53:00. This operation is carried out upon device connection.
Mevrouw komt maandag langs de balie, er wordt een poging gedaan een wipe uit te voeren via iCloud.

24-01-2020 16:49 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de

daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. GEEN spaties)
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i' of '5.1.2.h + 5.1.2.i')?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

Tweede Kamer
DER STATEN-GENERAAL

Oplegnotitie ALGEMENE VERORDENING GEGEVENSBESCHERMING
AVG verantwoording en speerpunten 2021

5.1.2.e
2513 5.1.2.e
T 5.1.2.e
M 5.1.2.e
5.1.2.e @tweedekamer.nl

Aard van de bespreking

- Dit onderwerp is ook op 31 mei 2021 in het MT geagendeerd en behandeld. De besluiten van het MT zijn in deze oplegnotitie verwerkt en geel gearceerd.
- De functionaris voor gegevensbescherming en de Privacy-officer zullen het jaarverslag toelichten. Daarbij zal ook het factsheet 'kennis en bewustwording' aan de orde komen.
- De vraag over de investering om het AVG-register wel op orde te krijgen, wordt ter vergadering toegelicht. Daarover vindt nog een overleg plaats met de CIO.

Beknopte samenvatting

Door middel van bijgaande 'woordwolk' en feitenoverzichten wordt het MT verslag gedaan van de AVG-activiteiten in 2019 en 2020 en geïnformeerd over de speerpunten 2021. Tijdens de vergadering zullen eerst de onderwerpen waaraan een beslispunt is gekoppeld worden toegelicht. Dat betreft: het AVG-register, datalekken, privacy by design, privacy by default en governance. Het MT zal daarna gevraagd worden over welke woorden in de woordenwolk een toelichting gewenst is.

Beslispunten/aanbevelingen

1. AVG-register: de stafdiensten en de Beveiligingsdienst aan te sporen het AVG-register met betrekking tot hun verwerkingen van persoonsgegevens voor 1 september 2021 in orde te maken;

   Besluit MT 31 mei 2021: het MT stemt in met beslispunt 1 met inachtneming van een gewijzigde datum 31 december 2021 (i.p.v. 1 september 2021).

2. Datalekken: bewustwording vergroten en de diensthoofden aan te sporen datalekken in de werkoverleggen te bespreken en vooral ook datalekken te melden (leren van fouten);

   Besluit MT 31 mei 2021: het MT stemt in met beslispunt 2.

3. Privacy by design: het is verplicht om bij alle diensten en projecten waarbij persoonsgegevens worden verwerkt standaard advies in te winnen bij de FG en de PO;

   Besluit MT 31 mei 2021: het MT stemt in met beslispunt 3.

4. Privacy by default: bij alle applicaties dient de standaardinstelling privacy vriendelijk te zijn ingesteld, derhalve er dient eerst specifiek door de gebruikers instemming verleend te worden voor de verwerking van gegevens (het vinkje staat niet standaard aan);

   Besluit MT 31 mei 2021: het MT stemt in met beslispunt 4.

5. Governance: diensthoofden gaan door middel van de PDCA-cyclus rapporteren over de naleving van de AVG (nadat een format is aangeleverd). De MT-leden zullen met regelmaat in de directie-overleggen en bila's aandacht vragen voor en informeren naar de naleving van de AVG binnen de ambtelijke organisatie.

   Governance: Het MT gaat na waar de AVG-verantwoordelijkheden liggen in het geval de verwerking van een persoonsgegeven niet ligt bij de ambtelijke organisatie ligt.

   Besluit MT 31 mei 2021: ten aanzien van beslispunt 6 gaat hHR na waar de verantwoordelijkheden liggen

Eerder behandeld in MT

Financiële consequenties

Geen

Personele consequenties

geen

Communicatieve consequenties

ICT-consequenties

Zie beslispunten 5 en 6

Advies hHR

Advies hFEZ

Advies hCOM

Advies CIO

Doorgeleiding

Ondernemingsraad

- Informatie
- Advies
- Instemming

Docnr15


Escalatie
Coaching
Escaperoom
Functie elders
Privacy-by-design
Eigenaarschap
Advisering
Privacy shield
Datalekken
DPIA
Persoonsgegevens
AVG-register
Groningen
Naturalisatie
Governance
Rechtszaak
Persoonsgegevens
Burgerinitiatieven
Bewustwording
25-mei-18
Rekkelijk
Handig
Contactpersonen
Prioriteiten/risico's
AP
ADR
Norgen
AVG
E-learning
AVG

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 21 februari 2020 14:01
Aan: Functionaris gegevensbescherming
Onderwerp: FW: Datalek vanwege weggewaaide documenten in afvalcontainer

Dag 5.1.2.e

Onderstaande situatie is operationeel vanuit de FD opgepakt naar de RSO toe. In het verlengde hiervan heb ik de situatie nog besproken met 5.1.2.e In hoeverre dit formeel (on)voldoende is kan ik niet inschatten. Om nu te voorkomen dat er diverse lijntjes gaan lopen vanuit deze situatie, vraag ik me wel af wat nu wijsheid is. Als in: ligt er voor iemand nog een te nemen actie?

Groeten,
5.1.2.e

5.1.2.e

hoofd Services
Facilitaire Dienst
Tweede Kamer der Staten-Generaal

Postbus 20018
2500 EA Den Haag
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

---

Van: 5.1.2e <5.1.2.e@tweedekamer.nl>
Verzonden: maandag 17 februari 2020 10:15
Aan: 5.1.2.e 5.1.2.e <5.1.2.e@tweedekamer.nl>
Onderwerp: FW: Datalek vanwege weggewaaide documenten in afvalcontainer

Goedemorgen 5.1.2.e

Wil jij dit verder oppakken s.v.p.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Facilitaire Dienst
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e
M +(5.1.2.e
E 5.1.2.e@tweedekamer.nl
I www.tweedekamer.nl

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: dinsdag 11 februari 2020 12:55

Aan: 5.1.2e 5.1.2e @tweedekamer.nl>
Onderwerp: FW: Datalek vanwege weggewaaide documenten in afvalcontainer

Beste 5.1.2e

Ik las onderstaande melding in het verslag van het MT. Ik ben benieuwd welke actie het MT hierop heeft ondernomen en wat de aard en strekking van de genoemde documenten zijn. Het betreft in ieder geval een potentieel datalek dat volgens het beleid van de Kamer bij de FG gemeld moet word. Zou jij kunnen bevorderen dat die melding plaatsvindt via http://plein2/datalekken. Het is wellicht ook een punt van informatiebeveiliging.

5.1.2e

Verslag Managementteam

vergaderdatum 3 februari 2020
deelnemers 5.1.2e (Griffier), 5.1.2e 5.1.2e 5.1.2e
5.1.2e], 5.1.2e 5.1.2e 5.1.2e

1. Opening en actualiteiten

hCOM meldt dat door een te volle afvalcontainer in het we
weggewaaid. Sommige daarvan zijn geretourneerd. Het is
deze documenten zijn.

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 4 juni 2020 14:05
Aan: 5.1.2.e
Onderwerp: RE: twee lopende incidentmeldingen datalekken

Twee akkoord

Dank

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e 5.1.2.e
Verzonden: donderdag 4 juni 2020 12:55
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: twee lopende incidentmeldingen datalekken

Ha 5.1.2.e

Er zijn twee incidentmeldingen naar het datalekteam gestuurd:

I2006 0002, zie bijlage. Gaat over vermissing GSM. Ik wil dit datalek gereedmelden. SD heeft noodzakelijke info verzameld en wipe uitgevoerd. Melding wordt aan datalekregister toegevoegd. Ben je akkoord?

I2006 0003, zie bijlage. Gaat over WhatsApp fraude. Een kamerlid heeft een 'bedel-bericht' ontvangen van een oud-kamerlid. Ik vraag mij af of dit een datalek is of een informatiebeveiligingsincident. Dit soort meldingen zijn niet eerder naar het datalekteam gestuurd, terwijl dit vaak voorkomt.
Ik stel voor dat wij dit geen incident voor het datalekteam vinden en de incidentmelding terugleggen bij het security-team. Wat vind jij?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Tweede Kamer der Staten-Generaal
5.1.2.e of 5.1.2.e

Postbus 20018, 2500 EA Den Haag
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Alle informatie over de Tweede Kamer is te vinden op www.tweedekamer.nl. U kunt de Tweede Kamer ook volgen op Facebook en Twitter. Download ook de gratis Tweede Kamer vergaderagenda app in de Apple of Android store.

Docnr8

5.1.2.e

Van: Functionaris gegevensbescherming
Verzonden: woensdag 24 juni 2020 14:44
Aan: '5.1.2.e'
CC: Functionaris gegevensbescherming
Onderwerp: RE: Datalek P-direkt

Beste 5.1.2.e

Dank voor onderstaand bericht.
Ik zou het graag telefonisch met jou willen bespreken. Kun je mij bellen?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Tweede Kamer der Staten-Generaal
5.1.2.e of 5.1.2.e

Postbus 20018, 2500 EA Den Haag
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Alle informatie over de Tweede Kamer is te vinden op www.tweedekamer.nl. U kunt de Tweede Kamer ook volgen op Facebook en Twitter. Download ook de gratis Tweede Kamer vergaderagenda app in de Apple of Android store.

Van: 5.1.2.e <5.1.2.e@p-direkt.minbzk.nl>
Verzonden: woensdag 24 juni 2020 14:34
Aan: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: Datalek

Hallo,

Maandag 22 juni kwam mij een datalek onder ogen waarbij gegevens zijn gelekt van een oud-medewerker van de Tweede Kamer, vandaar dat ik u informeer. Het betreft een specificatie arbeidsongeschiktheidsuitkering. Het document had moeten worden geplaatst in het personeelsdossier van de oud-medewerker werkzaam bij de Tweede Kamer, maar is geplaatst in het personeelsdossier van een andere medewerker werkzaam bij de Tweede Kamer. Het document is verwijderd uit het verkeerde personeelsdossier. De medewerker waarvan de gegevens zijn gelekt is niet meer werkzaam bij de Tweede Kamer. Een HR-adviseur van de Tweede Kamer heeft het datalek geconstateerd en gemeld bij P-Direkt.

Hieronder vermeld ik de door mij geregistreerde gegevens:

Op welke datum geconstateerd?	Op welke datum is het datalek	Wat is er gebeurd?	Welke gegevens betreft het?	Welke partijen betrokken?	Wat is het gevolg?	Wat is de opvolging?	Wat heeft het datalek v

	ontstaan?						
12-jun 2020	Datum van document 16-10-2018	Er is een document in een verkeerd personeelsdossier geplaatst. Het betreft twee medewerkers met dezelfde achternaam.	Het betreft een document over specificatie arbeidsongeschiktheid suitkering/ ziekteverloop.	Document is in het dossier van een medewerker van de Tweede Kamer geplaatst. De gegevens die gelekt zijn zijn van een oud-medewerker Tweede Kamer. Datalek is geconstateerd en gemeld door HR-adviseur Tweede Kamer.	De medewerker van de Tweede Kamer heeft kennis kunnen nemen van de gegevens van de oud-medewerker.	Het document is verwijderd uit het dossier van de medewerker van de Tweede Kamer en geplaatst in juiste dossier.	De oorzaak van het data bekend.

Mocht u nog aanvullende informatie nodig hebben dan is dat uiteraard geen enkel probleem.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Medewerker Security en Kwaliteit
.....
P-Direkt
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schenkkade 100 | 2595 AS | Den Haag | 4e verdieping
Postbus 20011 | 2500 EA | Den Haag
.....
M 5.1.2.e
E 5.1.2.e @p-direkt.minbzk.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard

ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

5.1.2.e

Van: Functionaris gegevensbescherming
Verzonden: donderdag 3 september 2020 16:07
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming; 5.1.2.e
Onderwerp: datalek

Beste 5.1.2.e

Via een mail van 5.1.2.e en 5.1.2.e (zie hieronder) vernam ik het incident. Door de drukte op het werk ben je vast nog niet toegekomen aan het doen van de melding van het datalek. Weet dat ik daar begrip voor heb. Zodra dat kan, ontvangen wij graag de melding. Dan kunnen we nagaan of en zo ja welke stappen verder genomen moeten worden.

Dank en groet,

5.1.2.e

We hebben de werkwijze griffies commissie bij inzagerecht bekeken, heldere beschrijving! We hebben nog een paar kleine suggesties en vragen die je als het goed is terug kunt zien in het bestand. Wanneer schikt het jullie om hierover verder te praten?

V.w.b. het onderwerp brieven derden, zouden wij nog een terugkoppeling geven van het overleg met de 3 hGC's. Bijgevoegd de meest recente versie van de notitie die met hen besproken is. Kort gezegd kunnen zij zich vinden in de notitie. We hebben de vraagpunten die daarin worden opgenomen besproken en geconcludeerd dat er geen noodzaak is om adresgegevens op te vragen als er een emailadres bekend is. De huidige werkwijze moet dus worden aangepast. Hiermee gaan we aan de slag, door een handleiding te maken voor de nieuwe werkwijze. Die zullen we t.z.t. naar jullie sturen.

Daarnaast werd ik (5.1.2.e) afgelopen zaterdag gebeld door een burger waarvan morgen een burgerinitiatief plenair wordt behandeld. Op de website van de TK was haar e-mail gepubliceerd als bijlage van een Kamerbrief. In deze e-mail stond haar telefoonnummer. Dit is dus een datalek. Ik heb hier zaterdag contact over gehad met 5.1.2.e Zij zou een melding datalek doen. Is dit inmiddels ook bij jullie terechtgekomen?

We horen van jullie.

Groeten,
5.1.2.e en 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 4 september 2020 15:27
Aan: 5.1.2.e ; Functionaris gegevensbescherming
Onderwerp: Re: datalek

Top, dank je wel.

Begrijp ik goed dat het telefoonnummer inmiddels niet meer zichtbaar is online?

Jij ook heel fijn weekend toegewenst,

5.1.2.e

Op 4 sep. 2020 om 14:55 heeft 5.1.2.e <5.1.2.e @tweedekamer.nl> het volgende geschreven:

Hallo 5.1.2.e

Bijgaand het ingevulde formulier melding datalek.

Fijn weekend alvast!

Met vriendelijke groet,

5.1.2.e

5.1.2.e
5.1.2.e
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | F +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: donderdag 3 september 2020 16:18
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Fwd: datalek

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

> **Van:** Functionaris gegevensbescherming <fg@tweedekamer.nl>
> **Datum:** 3 september 2020 om 16:07:22 CEST
> **Aan:** "5.1.2.e" <5.1.2.e @tweedekamer.nl>

Kopie: Functionaris gegevensbescherming <fg@tweedekamer.nl> 5.1.2.e
5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: datalek

Beste 5.1.2.e

Via een mail van 5.1.2.e en 5.1.2.e (zie hieronder) vernam ik het incident. Door de drukte op het werk ben je vast nog niet toegekomen aan het doen van de melding van het datalek. Weet dat ik daar begrip voor heb. Zodra dat kan, ontvangen wij graag de melding. Dan kunnen we nagaan of en zo ja welke stappen verder genomen moeten worden.

Dank en groet,

5.1.2.e

We hebben de werkwijze griffies commissie bij inzagerecht bekeken, heldere beschrijving! We hebben nog een paar kleine suggesties en vragen die je als het goed is terug kunt zien in het bestand. Wanneer schikt het jullie om hierover verder te praten?

V.w.b. het onderwerp brieven derden, zouden wij nog een terugkoppeling geven van het overleg met de 3 hGC's. Bijgevoegd de meest recente versie van de notitie die met hen besproken is. Kort gezegd kunnen zij zich vinden in de notitie. We hebben de vraagpunten die daarin worden opgenomen besproken en geconcludeerd dat er geen noodzaak is om adresgegevens op te vragen als er een emailadres bekend is. De huidige werkwijze moet dus worden aangepast. Hiermee gaan we aan de slag, door een handleiding te maken voor de nieuwe werkwijze. Die zullen we t.z.t. naar jullie sturen.

Daarnaast werd ik (5.1.2.e) afgelopen zaterdag gebeld door een burger waarvan morgen een burgerinitiatief plenair wordt behandeld. Op de website van de TK was haar e-mail gepubliceerd als bijlage van een Kamerbrief. In deze e-mail stond haar telefoonnummer. Dit is dus een datalek. Ik heb hier zaterdag contact over gehad met 5.1.2.e Zij zou een melding datalek doen. Is dit inmiddels ook bij jullie terechtgekomen?

We horen van jullie.

Groeten,
5.1.2.e en 5.1.2.e

<formulier_melding_datalek.docx>

Docnr11

5.1.2.e

Van: Functionaris gegevensbescherming
Verzonden: dinsdag 8 september 2020 10:22
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming; 5.1.2.e
Onderwerp: RE: datalek

Beste 5.1.2.e

Mooi dat het snel opgelost is! Ik zie dit incident niet als een meldingswaardig incident zodat er geen melding hoeft te worden gemaakt bij de Autoriteit Persoonsgegevens. Volgens bestaand beleid (verantwoordingsplicht) kunnen we dit incident pas afmelden zodra de betrokkene een berichtje heeft gekregen (brief of mail) waarbij een samenvatting van het incident –en de oplossing daarvan-- wordt gegeven en waarbij excuses voor het ongemak wordt aangeboden. Ook resteert mij de vraag of er nog verdere mogelijkheden zijn om het proces zo in te richten dat herhaling voorkomen kan worden. Graag ontvangen wij een kopie van het berichtje aan betrokkene/melder. Als je wilt, kan een van ons uiteraard mee- of tegenleen

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 4 september 2020 15:52
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: Re: datalek

Hallo 5.1.2.e

Dat klopt. Vorige week zaterdag is het stuk al uit Parlis verwijderd en daarmee van de website van de Kamer. Maandag jl. is het stuk ook van overheid.nl verwijderd!

Met vriendelijke groet,
5.1.2.e
5.1.2.e

Op 4 sep. 2020 om 15:27 heeft 5.1.2.e <5.1.2.e @tweedekamer.nl> het volgende geschreven:

Top, dank je wel.

Begrijp ik goed dat het telefoonnummer inmiddels niet meer zichtbaar is online?

Jij ook heel fijn weekend toegewenst,

5.1.2.e

Op 4 sep. 2020 om 14:55 heeft 5.1.2.e <5.1.2.e @tweedekamer.nl> het volgende geschreven:

Hallo 5.1.2.e

Bijgaand het ingevulde formulier melding datalek.

Fijn weekend alvast!

Met vriendelijke groet,

5.1.2.e

5.1.2.e
5.1.2.e
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | F +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: donderdag 3 september 2020 16:18
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Fwd: datalek

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

> **Van:** Functionaris gegevensbescherming <fg@tweedekamer.nl>
> **Datum:** 3 september 2020 om 16:07:22 CEST
> **Aan:** " 5.1.2.e " <5.1.2.e @tweedekamer.nl>
> **Kopie:** Functionaris gegevensbescherming <fg@tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>
> **Onderwerp: datalek**
>
> Beste 5.1.2.e
>
> Via een mail van 5.1.2.e en 5.1.2.e (zie hieronder) vernam ik het incident. Door de drukte op het werk ben je vast nog niet toegekomen aan het doen van de melding van het datalek. Weet dat ik daar begrip voor heb. Zodra dat kan, ontvangen wij graag de melding. Dan kunnen we nagaan of en zo ja welke stappen verder genomen moeten worden.

Dank en groet,

5.1.2.e

We hebben de werkwijze griffies commissie bij inzagerecht bekeken, heldere beschrijving! We hebben nog een paar kleine suggesties en vragen die je als het goed is terug kunt zien in het bestand. Wanneer schikt het jullie om hierover verder te praten?

V.w.b. het onderwerp brieven derden, zouden wij nog een terugkoppeling geven van het overleg met de 3 hGC's. Bijgevoegd de meest recente versie van de notitie die met hen besproken is. Kort gezegd kunnen zij zich vinden in de notitie. We hebben de vraagpunten die daarin worden opgenomen besproken en geconcludeerd dat er geen noodzaak is om adresgegevens op te vragen als er een emailadres bekend is. De huidige werkwijze moet dus worden aangepast. Hiermee gaan we aan de slag, door een handleiding te maken voor de nieuwe werkwijze. Die zullen we t.z.t. naar jullie sturen.

Daarnaast werd ik (5.1.2.e) afgelopen zaterdag gebeld door een burger waarvan morgen een burgerinitiatief plenair wordt behandeld. Op de website van de TK was haar e-mail gepubliceerd als bijlage van een Kamerbrief. In deze e-mail stond haar telefoonnummer. Dit is dus een datalek. Ik heb hier zaterdag contact over gehad met 5.1.2.e Zij zou een melding datalek doen. Is dit inmiddels ook bij jullie terechtgekomen?

We horen van jullie.

Groeten,
5.1.2.e en 5.1.2.e

<formulier_melding_datalek.docx>

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 15 september 2020 09:26
Aan: Functionaris gegevensbescherming; Schellart, D.
Onderwerp: RE: datalek melding I2007 0679
Bijlagen: Datalek van brief

Hallo 5.1.2.e

Zie bijlage. Excuses dat het zo lang heeft moeten blijven liggen.
Hopelijk is dit voldoende en hebben wij nu alles behandeld.

Groeten,
5.1.2.e

Medewerker Personeelsbeheer
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T (+ 5.1.2.e
E 5.1.2.i tweedekamer.nl
I www.tweedekamer.nl

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: dinsdag 8 september 2020 15:45
Aan: 5.1.2.i D. <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: datalek melding I2007 0679

Beste collega's,

Er staat nog een melding datalek open in ons meldingenregister. Het betrof een incident waarbij sprake was van een personeelsdocument van iemand anders. In de eerste plaats wil ik wijzen op de procedure (had ik eerder moeten doen). Een datalek moet altijd gemeld worden via het daartoe bestemde formulier. Zie voor procedure Plein2 en de e-learning datalekken. Verder valt in de terugkoppeling aan de melder op dat niet uitgelegd wordt wat er precies fout is gegaan. Ook valt op dat degene (5.1.2.e) van wie een formulier in het dossier van de melder was gevoegd niet geïnformeerd is over het incident. Ik vind dat dit alsnog –conform het beleid van en de praktijk bij de Kamer -- gedaan moet worden (accountability) . Verder nog een voorstel: zullen we binnenkort een C&B- overleg plannen over de AVG?

Graag ontvang ik een afschrift van de mail met uitleg aan 5.1.2.e Dan meld ik het incident gereed.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 30 september 2020 12:39
Aan: Functionaris gegevensbescherming
Onderwerp: Re: datalek

5.1.2.e !

Met vriendelijke groet,
5.1.2.e
5.1.2.e

Op 30 sep. 2020 om 08:11 heeft Functionaris gegevensbescherming <fg@tweedekamer.nl> het volgende geschreven:

Beste 5.1.2.e

Dank voor je bericht en acties! Ik meld het 'incident' als gereed in ons register van datalekmeldingen.

5.1.2.e

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 29 september 2020 14:29
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek

Hallo 5.1.2.e

Zie onderstaande mail van de griffier van de commissie J&V inzake het datalek. Zij hebben vandaag een mail aan betrokkene gestuurd. Ik hoop dat dit afdoende is.

Voor wat betreft jouw vraag of het proces zo kan worden ingericht dat herhaling voorkomen kan worden kan ik het volgende zeggen. Wij proberen altijd een check te maken in de ontvangen stukken of er onbedoeld privacygevoelige gegevens in voorkomen, maar in de honderden stukken die wij per week ontvangen komt het helaas wel eens voor dat er iets tussendoor glipt. Het blijft mensenwerk..

Met vriendelijke groet,

5.1.2.e

5.1.2.e
5.1.2.e
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | F +(5.1.2.e
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e (5.1.2.e) <5.1.2.e@tweedekamer.nl>
Verzonden: dinsdag 29 september 2020 13:58
Aan: 5.1.2.e <5.1.2.e@tweedekamer.nl>; 5.1.2.e <5.1.2.e@tweedekamer.nl>
CC: 5.1.2.e (5.1.2.e) <5.1.2.e@tweedekamer.nl>
Onderwerp: RE: datalek

Beste 5.1.2.e

Aan betrokkene is per mail medegedeeld dat haar e-mailadres en daarmee ook haar telefoonnummer is verwijderd van de Website van de TK, die als bijlage was gepubliceerd bij een Kamerbrief. Wij hebben hier ook onze excuses voor aangeboden.
De mailwisseling van een maand geleden is echter niet bewaard gebleven.
Dit is alles wat ik daarover kan zeggen, hoop dat het afdoende is.

Met vriendelijke groet,

5.1.2.e (5.1.2.e)

5.1.2.e
GC Bestuur en Onderwijs
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

---

Van: 5.1.2.e <5.1.2.e@tweedekamer.nl>
Verzonden: dinsdag 29 september 2020 13:05
Aan: 5.1.2.e <5.1.2.e@tweedekamer.nl>; 5.1.2.e 5.1.2.e) <5.1.2.e@tweedekamer.nl>
Onderwerp: RE: datalek

Super. Dank jullie wel!

Met vriendelijke groet,

5.1.2.e

5.1.2.e
5.1.2.e
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | F +(5.1.2.e
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 29 september 2020 12:24
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl> 5.1.2.e (5.1.2.e)
<5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek

Ha 5.1.2.e

De betreffende mail is nog niet aan betrokkene verstuurd. We gaan dit vandaag doen en zullen je een afschrift sturen, zodat 5.1.2.e vervolgens geïnformeerd kan worden.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
GC Bestuur en Onderwijs
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 28 september 2020 16:05
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e (5.1.2.e)
<5.1.2.e @tweedekamer.nl>
Onderwerp: Fwd: datalek

Hoi 5.1.2.e en 5.1.2.e

Zie de onderstaande mail van 5.1.2.e Ik heb jullie op 9 en 15 september al een mail hier over gestuurd. Ik begreep van 5.1.2.e dat 5.1.2.e dit na haar vakantie zou oppakken. Kunnen jullie mij een afschrift sturen van de mail aan betrokkene zodat ik 5.1.2.e kan informeren? Dank!

Met vriendelijke groet,
5.1.2.e
5.1.2.e

Begin doorgestuurd bericht:

> **Van:** Functionaris gegevensbescherming <fg@tweedekamer.nl>
> **Datum:** 28 september 2020 om 15:48:35 CEST
> **Aan:** " 5.1.2.e " <5.1.2.e @tweedekamer.nl>
> **Onderwerp: FW: datalek**
>
> Beste 5.1.2.e
>
> Deze mail is vast aan je aandacht ontsnapt. Graag een korte update.
>
> 5.1.2.e
>
> Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

Van: Functionaris gegevensbescherming
Verzonden: dinsdag 8 september 2020 10:22
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>; Leeuwen van 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek

Beste 5.1.2.e

Mooi dat het snel opgelost is! Ik zie dit incident niet als een meldingswaardig incident zodat er geen melding hoeft te worden gemaakt bij de Autoriteit Persoonsgegevens. Volgens bestaand beleid (verantwoordingsplicht) kunnen we dit incident pas afmelden zodra de betrokkene een berichtje heeft gekregen (brief of mail) waarbij een samenvatting van het incident –en de oplossing daarvan-- wordt gegeven en waarbij excuses voor het ongemak wordt aangeboden. Ook resteert mij de vraag of er nog verdere mogelijkheden zijn om het proces zo in te richten dat herhaling voorkomen kan worden. Graag ontvangen wij een kopie van het berichtje aan betrokkene/melder. Als je wilt, kan een van ons uiteraard mee- of tegenleen

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 4 september 2020 15:52
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: Re: datalek

Hallo 5.1.2.e

Dat klopt. Vorige week zaterdag is het stuk al uit Parlis verwijderd en daarmee van de website van de Kamer. Maandag jl. is het stuk ook van overheid.nl verwijderd!

Met vriendelijke groet,
5.1.2.e
5.1.2.e

Op 4 sep. 2020 om 15:27 heeft 5.1.2.e
<5.1.2.e @tweedekamer.nl> het volgende geschreven:

Top, dank je wel.

Begrijp ik goed dat het telefoonnummer inmiddels niet meer zichtbaar is online?

Jij ook heel fijn weekend toegewenst,

5.1.2.e

> Op 4 sep. 2020 om 14:55 heeft 5.1.2.e
> <5.1.2.e @tweedekamer.nl> het volgende geschreven:
>
> Hallo 5.1.2.e
>
> Bijgaand het ingevulde formulier melding datalek.
>
> Fijn weekend alvast!
>
> Met vriendelijke groet,
>
> 5.1.2.e
>
> 5.1.2.e
> 5.1.2.e
> Tweede Kamer der Staten-Generaal
>
> Postbus 20018, 2500 EA Den Haag
> T +(5.1.2.e | F +(5.1.2.e
> E 5.1.2.e @tweedekamer.nl | I
> www.tweedekamer.nl
>
> **Van:** 5.1.2.e <5.1.2.e @tweedekamer.nl>
> **Verzonden:** donderdag 3 september 2020 16:18
> **Aan:** 5.1.2.e <5.1.2.e @tweedekamer.nl>;
> 5.1.2.e
> <5.1.2.e @tweedekamer.nl>
> **Onderwerp:** Fwd: datalek
>
> Verstuurd vanaf mijn iPhone
>
> Begin doorgestuurd bericht:

Van: 5.1.2.e 5.1.2.e <fg@tweedekamer.nl>
Datum: 3 september 2020 om 16:07:22 CEST
Aan: "5.1.2.e" <5.1.2.e @tweedekamer.nl>
Kopie: Functionaris gegevensbescherming <fg@tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: datalek

Beste 5.1.2.e

Via een mail van 5.1.2.e en 5.1.2.e (zie hieronder) vernam ik het incident. Door de drukte op het werk ben je vast nog niet toegekomen aan het doen van de melding van het datalek. Weet dat ik daar begrip voor heb. Zodra dat kan, ontvangen wij graag de melding. Dan kunnen we nagaan of en zo ja welke stappen verder genomen moeten worden.

Dank en groet,

5.1.2.e

We hebben de werkwijze griffies commissie bij inzagerecht bekeken, heldere beschrijving! We hebben nog een paar kleine suggesties en vragen die je als het goed is terug kunt zien in het bestand. Wanneer schikt het jullie om hierover verder te praten?

V.w.b. het onderwerp brieven derden, zouden wij nog een terugkoppeling geven van het overleg met de 3 hGC's. Bijgevoegd de meest recente versie van de notitie die met hen besproken is. Kort gezegd kunnen zij zich vinden in de notitie. We hebben de vraagpunten die daarin worden

opgenomen besproken en geconcludeerd dat er geen noodzaak is om adresgegevens op te vragen als er een emailadres bekend is. De huidige werkwijze moet dus worden aangepast. Hiermee gaan we aan de slag, door een handleiding te maken voor de nieuwe werkwijze. Die zullen we t.z.t. naar jullie sturen.

Daarnaast werd ik (5.1.2.e) afgelopen zaterdag gebeld door een burger waarvan morgen een burgerinitiatief plenair wordt behandeld. Op de website van de TK was haar e-mail gepubliceerd als bijlage van een Kamerbrief. In deze e-mail stond haar telefoonnummer. Dit is dus een datalek. Ik heb hier zaterdag contact over gehad met 5.1.2.e 5.1.2.e Zij zou een melding datalek doen. Is dit inmiddels ook bij jullie terechtgekomen?

We horen van jullie.

Groeten,
5.1.2.e en 5.1.2.e

<formulier_melding_datalek.docx>

Feitenoverzichten AVG-beleid Tweede Kamer periode 2019-2020

Doel	Stavaza	Risico
Alle verwerkingen van persoonsgegevens moeten staan in het digitale AVG-register van de Tweede Kamer. • Om aan te kunnen tonen dat zorgvuldig wordt omgegaan met de bescherming van persoonsgegevens; • Incidenten (datalekken) snel en adequaat te behandelen; • Op verzoek te tonen aan de toezichthouder (Autoriteit Persoonsgegevens). Het AVG-register wordt door elke dienst zelf gevuld. Het diensthoofd geeft per verwerking een definitief akkoord.	Kritieke diensten (met veel en gevoelige persoonsgegevens) nog niet volledig op orde: Stafdienst HR, Beveiligingsdienst, FEZ en DA.	AVG-register is het fundament waarop de maatregelen van de AVG rusten. Wanneer dit fundament onvoldoende op orde is kan niet verder gebouwd worden aan het noodzakelijke privacybeleid. Het bemoeilijkt het tijdig en adequaat voldoen aan bv inzageverzoeken. En diensthoofden kunnen onvoldoende monitoren wat hun AVG-verantwoordelijkheid is.

Doel	Stavaza	Risico
Alle medewerkers binnen de Tweede Kamer moeten zich bewust zijn van de rechten en plichten van de AVG.	Via het opgebouwde netwerk van AVG-contactpersonen komt langzaam de bewustwording op gang. Ook is de AVG meegenomen in de brede campagne “werken met informatie – Hoe doe je dat?”.	AVG-kennis bijspijkeren is niet voldoende. Bewustwording is een continu proces, om de aandacht niet te laten verslappen. Bewustwording is de belangrijkste troef voor de bescherming van persoonsgegevens. Medewerkers moeten ervan doordrongen zijn dat zij altijd en overal zorgvuldig omgaan met persoonsgegevens.

Datalek (artikelen 33 en 34 AVG)

Er is sprake van een datalek wanneer er iets fout gaat in de omgang met persoonsgegevens. Voorbeelden:

- onbeveiligd gevoelige persoonsgegevens versturen;
- verlies van een fysiek dossier of telefoon/iPad/usb-stick waardoor iemand mogelijke toegang heeft tot persoonsgegevens;
- wanneer bepaalde persoonsgegevens per ongeluk zijn vernietigd of onjuist blijken te zijn
- wanneer persoonsgegevens onbevoegd of onbedoeld zijn ingezien door personen;
- wanneer gegevens door ransomware of systeemstoring niet meer toegankelijk zijn

Datalekken moeten verplicht worden geregistreerd in een datalekregister. De Tweede Kamer gebruikt hiervoor TopDesk.

Doel datalekregister	Stavaza	Risico
Het doel van het registreren in het datalekregister is dat ervan kan worden geleerd, om datalekken in de toekomst zo veel mogelijk te voorkomen. Een ander doel is dat daarmee aan de Autoriteit Persoonsgegevens kan worden aangetoond dat datalekken daadwerkelijk worden gemonitord en opgevolgd.	Er is een datalekprocedure ingericht[1] en een op maat gemaakte e-learning datalekken beschikbaar.	Er worden binnen de Tweede Kamer nauwelijks datalekken gemeld. Het meest voorkomende datalek is het verlies van telefoon of iPad. Het niet melden van datalekken is een overtreding van de AVG (kans op boete). Belangrijker risico is dat er binnen de Tweede Kamer niet wordt geleerd van de fouten, waardoor de rechten en vrijheden van personen niet gewaarborgd zijn.

[1] Zie Plein2 voor de procedure datalekken, http://plein2/node/23736

Overzicht aantallen en soorten datalekken in2019	aantal	%
Verloren/gestolen/gevonden gegevensdrager (telefoon, Ipad, laptop, usb-stick)	22	42%
P-documenten in verkeerd p-dossier	7	13%
Foutieve machtigingen	6	12%
verkeerde geadresseerde/ontvanger email	6	12%
Datalek fractie	5	10%
Geen datalek Tweede Kamer	2	4%
Hack wervingsapplicatie HR	1	2%
document uit verkeerde printer	1	2%
Geen datalek want geen persoonsgegevens	1	2%
per abuis publicatie op internet	1	2%
Totaal in 2019	**52**	100%
Overzicht aantallen en soorten datalekken in 2020	**aantal**	**%**
Verloren/gestolen/gevonden gegevensdrager (telefoon, Ipad, laptop, usb-stick)	16	41%
P-documenten in verkeerd p-dossier	4	10%
Geen datalek Tweede Kamer	4	10%
WhatsApp hack	4	10%
Telefoonoplichting (spoofing)	4	10%
per abuis publicatie op internet	2	5%
Foutieve machtigingen	1	3%
verkeerde geadresseerde/ontvanger email	1	3%
document uit verkeerde printer	1	3%
Documenten uit papiercontainer op straat gewaaid	1	3%
Geen datalek want geen persoonsgegevens	1	3%
Totaal in 2020	**39**	100%

Aandachtspunten:

- In 2021 tot nu toe 0 datalekmeldingen. Dat is zorgelijk omdat dit niet realistisch is.
- Via MT en diensthoofden medewerkers laten weten dat zij datalekken moeten melden bij 5.1.2.i zodat de organisatie leert van fouten en verbeteringen kan aanbrengen aan processen en systemen.
- Datalekprocedure toevoegen aan de lopende campagne "Veilig werken met informatie. Hoe doe je dat?"

AVG-rechten van betrokkenen

Doel procedure rechten betrokkenen	Stand van zaken	risico
Mensen hebben AVG-rechten om controle te houden over hun persoonsgegevens. De Tweede Kamer moet zorgen dat de systemen, processen en interne organisatie is ingericht op deze rechten. Alle medewerkers moeten op de hoogte zijn van hoe binnen de Tweede Kamer het proces ingericht is om te voldoen aan de rechten van betrokkenen.	De FG is contactpersoon en zorgt ervoor dat betrokkenen hun rechten kunnen uitoefenen. En hij bewaakt de wettelijke procedure en termijnen. Op intranet en internet moet duidelijk en transparant worden gecommuniceerd hoe betrokkenen hun rechten kunnen uitoefenen. In 2021 zal deze informatie door FG en PO worden geëvalueerd en geactualiseerd.	Onbekendheid procedure Rechten betrokkenen binnen diensten, waardoor verzoeken niet conform de AVG in behandeling worden genomen. Inmiddels is door de Privacy Officer i.s.m. griffie commissies en FG een conceptproces opgesteld om binnen de griffies commissies te kunnen voldoen aan binnengekomen AVG-verzoeken. Daarnaast is in samenwerking met DIA een proces ingericht om te kunnen voldoen aan verwijderingsverzoeken in het kader van oude Naturalisatiewetten. In 2021 worden overige diensten via de AVG-contactpersonen gewezen op de procedure.

De Tweede Kamer heeft inmiddels een aantal inzageverzoeken en verwijderingsverzoeken ontvangen. Elk verzoek betrof een unieke situatie, waar met maatwerk gehoor aan is gegeven.
Bij behandeling van de verzoeken bleken processen onvoldoende ingericht te zijn om tijdig aan de rechten van betrokkenen te kunnen voldoen. De behandelingstermijn is hierdoor langer geweest dan toegestaan.

Onderstaand meerjarig overzicht laat een constant beeld zien.

Overzicht aantal en soort verzoeken betrokkenen in 2018, 2019 en 2020:

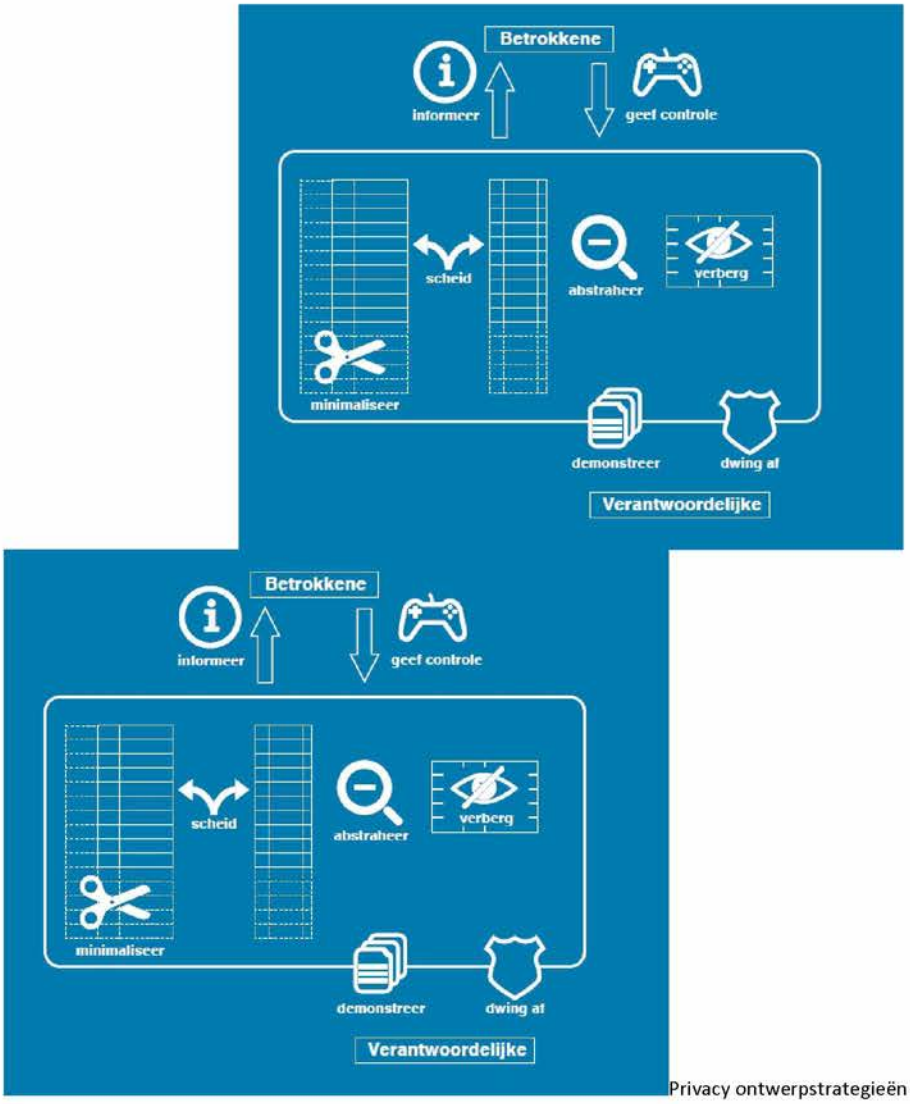
jaartal	aantal	soort	kenmerk	Afhandeling	bijzonderheden
2018	2	Verwijdering	AVG2018VV101	afgehandeld 2 juni 2020	naturalisatiewet - procedure met KOOP ingericht
			AVG2018VV102	afgehandeld 12 mei 2020	naturalisatiewet - procedure met KOOP ingericht
2019	3	Inzage	AVG2019VI101	afgehandeld december 2019	betrokkenheid advocaat betrokkene. Dossier BVA
			AVG2019VI102	afgehandeld 18 december 2020	betrokkenheid Landsadvocaat en Rechtbank Den Haag
			AVG2019VI103	afgehandeld binnen termijn 4 weken	concept-procedure met griffie commissie opgesteld
2020	3	Verwijdering	AVG2020VV101	afgehandeld 4 maanden na indiening verzoek	naturalisatiewet - aanvullende procedure met KOOP
			AVG2020VV102	afgehandeld 3 maanden na indiening verzoek	naturalisatiewet - aanvullende procedure met KOOP
			AVG2020VV103	afgehandeld binnen 1 week na indiening verzoek	publicatie op internet, brief onterecht niet geanonimiseerd

Klachten over gebruik persoonsgegevens

In 2019 en 2020 heeft de FG een tweetal klachten ontvangen over gebruik persoonsgegevens door de Tweede Kamer.

1. Een burger beklaagde zich over het gebruik van zijn persoonsgegevens in een onderzoek van de vaste commissie voor Economische Zaken en Klimaat. Dit betreft het Onderzoek naar schadevergoeding NAM. De Tweede Kamer wil weten of betrokken burgers tevreden zijn over de afhandeling. De burger beklaagt zich dat de Tweede Kamer zonder zijn toestemming in bezit is gekomen van zijn persoonsgegevens.
2. Een oud-senator meldt dat zijn huisadres vindbaar is op internet. Hij verwijst met een link naar de vindplaats. Het betreft een Kamerstuk uit 2004, toen privéadressen van Tweede Kamerleden desgewenst werden gepubliceerd in een Kamerstuk.

Privacy by design en privacy by default (artikel 25 AVG)



Privacy ontwerpstrategieën door 5.1.2.e

<u>Privacy by design</u>:

Doel	Stand van Zaken	Risico
Houdt in dat bij het ontwerpen van producten en diensten zo vroeg mogelijk aandacht wordt besteed aan de bescherming van persoonsgegevens	Privacy by design wordt nog niet automatisch meegenomen in startdocument. Hiervoor is aandacht gevraagd bij CIO-office. Functioneel beheerders zijn geïnformeerd over de eis van Privacy by design en by default.	Wanneer in processen en aanschaf van systemen geen rekening wordt gehouden met de AVG is het moeilijk om de AVG volledig toe te passen. Zoals de mogelijkheid om gegevens te verwijderen, inzage te verlenen in verwerking persoonsgegevens, passende organisatorische en technische beveiliging

Mooi voorbeeld Privacy by design:
De Facilitaire dienst heeft bij de vervanging van de printers de bescherming van persoonsgegevens is meegenomen bij de aanschaf van de huidige multifunctionele printers (MFP's).

Met de huidige huidige MFP's:

- worden vertrouwelijke documenten beschermd door deze alleen aan de juiste gebruikers vrij te geven en;
- wordt de veiligheid van netwerkprinters verbeterd door een accurate wijze van verificatie van deze gebruikers.

Hierdoor worden datalakken en inbreuken op informatiebeveiliging beter voorkomen.

Aanbeveling

Aanbevolen wordt de verplichting in te stellen dat bij alle nieuwe diensten en projecten waarbij persoonsgegeven worden verwerkt standaard advies wordt ingewonnen bij de FG en/of de PO.

Privacy by default

Doel	Stand van Zaken	Risico
houdt in dat de standaardinstellingen van een product of dienst rekening houden met de bescherming van persoonsgegevens, en er niet vooraf hokjes of velden zijn aangevinkt. 'Locatiegegevens bijhouden' moet standaard uitstaan op een telefoon, je moet hiervoor een actieve handeling uitvoeren.	Nog onduidelijk of de instellingen van formulieren die Tweede Kamer gebruikt standaard op privacy vriendelijk staan. FG en PO bespreken dit in 2021/2022 met alle diensten en met name met functioneel beheerders.	Wanneer de standaardinstellingen niet privacy vriendelijk zijn ingesteld, is het mogelijk dat persoonsgegevens worden verwerkt die niet noodzakelijk zijn voor het specifieke doel.

De zes grondslagen van de AVG (artikel 6, lid 1 a t/m f AVG):

- Toestemming
- Vitale Belangen
- Wettelijke Verplichting
- Overeenkomst
- Algemeen Belang
- Gerechtvaardigd Belang

Elke verwerking van persoonsgegevens is een inbreuk op de privacy van de mensen over wie het gaat. Daarom mogen persoonsgegevens alleen worden verwerkt als het echt niet anders kan om een doel te bereiken. Bovendien moet het gebruik van de persoonsgegevens gebaseerd zijn op één van de zes grondslagen die de AVG noemt. Deze lijst is limitatief, dat wil zeggen dat er geen andere gronden kunnen worden aangevoerd.

De rechtsgrond moet je zelf bepalen vóórdat de verwerking van persoonsgegevens begint. En je moet zorgen dat goed wordt onderbouwd waarom de grondslag is gekozen.

De grondslag voor elke verwerking moet op de volgende plekken worden vermeld:

1. In de privacyverklaring. Zo weten de mensen van wie u gegevens verwerkt waarom u dit mag. En komen zij niet voor verrassingen te staan. Dit kan u helpen om aan uw informatieplicht te voldoen.
2. In het privacybeleid. Dat helpt voor het voldoen aan de verantwoordingsplicht.
3. In het verwerkingsregister.

In 2021 en 2022 worden alle verwerkingen door FG en PO gecontroleerd op voldoen aan de informatieplicht AVG.

Welke partijen (intern en extern) zijn betrokken bij de gegevensverwerking?
Welke rol en verantwoordelijkheid heeft elke partij?

Voor de AVG worden binnen de Tweede Kamer onderstaande partijen en rollen onderscheiden:

Wie	**Rol**
Griffier van de Tweede Kamer	Verwerkingsverantwoordelijke
Ambtelijke diensten	Voeren het intern beheer uit van de gegevensverwerking
Diensthoofd/leidinggevende	Is verantwoordelijk voor alle gegevensverwerkingen die binnen de dienst plaatsvinden (eigenaarschap
AVG-contactpersoon	a. fungeren als 'adviesloket' bij vragen binnen de eigen dienst over de AVG; b. inventariseren, beoordelen, bijhouden en melden van verwerkingen persoonsgegevens; c. aanspreekpunt voor de FG bij incidenten (waaronder datalekken) en privacy verzoeken; d. zorgen dat de AVG blijvend onder de aandacht is van de medewerkers van de eigen dienst en draagt zo bij aan het privacy bewustzijn van de Tweede Kamer.
Leverancier van dienst of IT-systeem	Nagaan wat de rol van de leverancier is. Verwerker of verwerkings-verantwoordelijke, of gezamenlijk verwerkingsverantwoordelijk. Op basis van de bepaalde rol nagaan welke afspraken gemaakt moeten worden over verwerking persoonsgegevens
Kamerleden/Kamerfractie	Elk Kamerlid en elke Kamerfractie is verwerkingsverantwoordelijk voor de eigen gegevensverwerkingen.
FG Tweede Kamer	Houdt intern onafhankelijk toezicht op de naleving van de AVG door de ambtelijke organisatie, is contactpersoon voor de rechten van betrokkenen, adviseert op uitgevoerde DPIA's en is contactpersoon voor de AP
Privacy Officer	Adviseert en ondersteunt de ambtelijke organisatie bij AVG-taken en vragen. Adviseert bij afspraken met leveranciers, zorgt voor uitvoering DPIA's en begeleidt de AVG-contactpersonen van de diensten.

Aanbevelingen:

- Management moet top-down met regelmaat aandacht vragen voor en informeren naar de naleving van de AVG binnen de ambtelijke organisatie. En diensthoofden laten rapporteren over de stand van zaken binnen de diensten.

- Het is de taak van elk diensthoofd om regelmatig met de eigen AVG-contactpersoon te bespreken wat de stand van zaken is van de AVG. Dit helpt bij borgen van het AVG gedachtengoed en initiëren van verbeteracties die voor de eigen dienst prioriteit hebben.
- In 2021 zal door de FG en PO in overleg worden getreden over de reeds lopende PDCA-cyclus en nagegaan worden hoe de AVG aan deze cyclus kan worden toegevoegd.
- Aandacht voor verduidelijking over wie AVG-verzoeken afhandelt indien dit niet of niet geheel betrekking heeft op de ambtelijke organisatie.

Een DPIA is:

- Een systematische beschrijving van de gegevensverwerking
- Een beoordeling van de privacy risico's
- Maatregelen om die risico's aan te pakken
- Specifiek: is de gegevensverwerking rechtmatig?

Een DPIA is niet:

- instrument om vast te stellen of een voorgenomen gegevensverwerking in lijn is met de privacyregelgeving (compliance)
- vaste vorm of vragenlijst

Een DPIA is verplicht, namelijk wanneer er waarschijnlijk sprake is van een hoog risico. Vaak betreft het dan gevoelige of bijzonder persoonsgegevens. Ook wanneer er geen verplichting is kan het raadzaam zijn om een DPIA uit te voeren om zicht te krijgen op mogelijke privacy risico's.

Een DPIA wordt binnen de Tweede Kamer om verschillende redenen uitgevoerd.
- zorgvuldigheidsredenen (gaswinning)
- aard, hoeveelheid of complexiteit van de persoonsgegevens (IAM, cameratoezicht)
- verplichting (biometrisch systeem)

Aandachtspunten:

- Een DPIA uitvoeren is geen eenmalige exercitie, maar een continu proces. Het is de taak van de betreffende dienst om te monitoren of de gegevensverwerking verandert. Bijvoorbeeld wanneer een nieuwe technologie gebruikt wordt, of dat de persoonsgegevens voor een ander doel of op een andere locatie gebruikt gaan worden (zoals straks B67).
- Een DPIA moet periodiek worden uitgevoerd, ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld 1 keer per 3 jaar. In de DPIA-rapportage wordt afgesproken wanneer de DPIA herhaald moet worden.
- Monitoring door diensthoofd op de naleving van de besluiten van de DPIA.

Meerjarig overzicht DPIA's Tweede Kamer periode 2019-2021:

Jaartal	**DPIA over**
2019	Bezoekersregistratiesysteem (Lange Poten)
2019	Beheer camerabeelden van het Pelco Camera Observatie Systeem Beveiligingsdienst
2019	IAM
2021	Biometrisch systeem B67
2021	Parlementaire Enquête Aardgaswinning Groningen (5 onderzoeksfases zoals bepaald in het onderzoeksvoorstel. Opheffing van de commissie en de archivering van de informatie.

Bewaartermijnen en Archiefwet

Doel	Stand van zazen	Risico
Persoonsgegevens mogen gebruikt worden als identificeerbaar gegeven, voor zolang als het nodig is voor de doeleinden waarvoor de gegevens verzameld zijn. Dit heet het beginsel van opslagbeperking. Wanneer persoonsgegvens niet meer noodzakelijk zijn voor het doel moeten ze worden vernietigd of gearchiveerd.	Nog niet alle ambtelijke diensten hebben voor de AVG de termijn bepaald hoelang persoonsgegevens noodzakelijk zijn om te gebruiken. Inmiddels beschikt de Tweede Kamer over een selectielijst waarin is aangegeven welke archiefbescheiden voor vernietiging of voor blijvende bewaring in aanmerking komen.	Wanneer persoonsgegevens te lang bewaard worden is er een grotere inbreuk op de persoonlijke levenssfeer van de betrokkenen. En wordt niet voldaan aan de AVG. Gegevens die je niet meer hebt hoef je niet te verantwoorden of te beschermen met passende maatregelen.

Speerpunten FG en PO voor het jaar 2021

A. Speerpunten Functionaris voor de Gegevensbescherming en Privacy Officer

1. privacy by default: in hoeverre staan de applicaties bij de Tweede Kamer standaard op veilig?
2. in hoeverre is voldaan aan de AVG-informatieplicht?
3. Inbedden AVG in werkprocessen: Inkoop

B. Speerpunten Functionaris voor de Gegevensbescherming voor 2021:

4. Ontwikkelen vormgeving AVG-rapportage voor MT (PDCA-cyclus)
5. Steekproef stand van zaken AVG-register: bijzondere gegevens

C. Speerpunten Privacy Officer voor 2021:

6. Reactiveren AVG-contactpersonen en begeleiden nieuwe contactpersonen
7. Meer bekendheid geven aan procedure AVG-rechten, procedure datalekken, informatieplicht
8. Uitvoeren DPIA's, waaronder CCTV, IAM en TCS
9. Beslisboom verwerker/verwerkingsverantwoordelijke, modelverwerkersovereenkomst/ verwerkersafspraken/onderlinge regeling, evalueren en waar nodig aanpassen i.s.m. Inkoop en zorgen voor inbedding en borging binnen de Tweede Kamerorganisatie

Docnr17

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 22 juni 2021 10:06
Aan: TK-diensthoofden
CC: 5.1.2.e ; 5.1.2.e
Onderwerp: AVG-stukken MT 21 juni 2021
Bijlagen: Feiten bij de woordwolk 2019-2020.docx; Oplegnotitie bespreking stavaza AVG in MT 21 juni 2021.docx; Woordwolk bij terugblik 2019 en 2020 tbv MT.docx

Geachte diensthoofden,

Tijdens het MT van 21 juni 2021 is afgesproken dat de AVG-jaarverslagen van 2019 en 2020 ter informatie worden verzonden aan de diensthoofden. Hierbij ontvangt u de desbetreffende documenten.

Met vriendelijke groet,

5.1.2.e

5.1.2.e MT
Staf Griffier
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA, Den Haag
T 5.1.2.e | 5.1.2.e@tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Van: Griffier Tweede Kamer
Verzonden: dinsdag 31 augustus 2021 17:21
Aan: Functionaris gegevensbescherming
CC: 5.1.2.e
Onderwerp: RE: datalek TK

Beste 5.1.2.e

Naar aanleiding van je onderstaande mail willen we je vragen dit op te nemen met 5.1.2.e voor verdere afhandeling.

Ik bericht je dit mede namens 5.1.2.e Ik zet hem in de cc.

Groet,
5.1.2.e
Tst. 5.1.2.e

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: dinsdag 31 augustus 2021 09:12
Aan: Griffier Tweede Kamer <Griffier@tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.1.e <5.1.2.e @tweedekamer.nl>
Onderwerp: datalek TK

Beste 5.1.2.e en 5.1.2.e

Met betrekking tot het datalek bij de TK dienen er nog een tweetal acties verricht te worden. Als FG meld ik dat dit incident nog formeel afgehandeld dient te worden. Nu weet ik dat er vanuit de Kamer al een brief (met blik stoopwafels) is verstuurd. Ik wil graag een kopie van die brief zodat ik daarop de formele reactie kan afstemmen. Navraag bij Comm leverde niets op. Weet dat inmiddels het datalek bij de Autoriteit Persoonsgegevens is gemeld. Ook dient er nog een brief aan de KvK opgesteld te worden, wij lezen graag mee op deze brief. Ter verdere informatie het volgende: de PvD had op hun website nog de desbetreffende informatie staan met daarop de persoonsgegevens van betrokkene vermeld. 5.1.2.e heeft hierover contact opgenomen, zij bedankten voor de informatie en wij gaan er vanuit dat de persoonsgegevens worden gelakt.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 6 september 2021 13:22
Aan: Functionaris gegevensbescherming
Onderwerp: FW: datalek TK
Bijlagen: Re: bezorging boeket twv 25 euro

5.1.2.e

Naar aanleiding van het datalek bij griffie plenair heb ik op verzoek van Vz/Griffier en 5.1.2.e telefonisch contact opgenomen met de familie 5.1.2.e Van te voren heb ik met een woordvoerder overlegd over de woordvoeringslijn die hij had gehanteerd naar de journalist van het NRC.

Aangezien wij geen telefonische gegevens hadden hebben wij het telefoonnummer gekregen via woordvoerder Rutte (met toestemming van de familie 5.1.2.e).

Ik sprak met de moeder van 5.1.2.e over het voorval. Het was een prettig gesprek.

Tijdens dat gesprek heb ik haar gevraagd of ik hun adres mocht hebben (adres was inmiddels van internet verdwenen) om te gebruiken voor het sturen van een bloemetje en attentie.

Bijgevoegd de opdracht naar 5.1.2.e en tekst op het kaartje. Ook bij de attentie voor 5.1.2.e zat een kaartje met een tekst van gelijke strekking.

Hartelijke groet,

5.1.2.e

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: woensdag 1 september 2021 11:43
Aan: Wensem, P. van <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek TK

Beste 5.1.2.e

Zie onderstaande mailwisseling. Kan jij me verder helpen?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

Van: Griffier Tweede Kamer <Griffier@tweedekamer.nl>
Verzonden: dinsdag 31 augustus 2021 17:21
Aan: Functionaris gegevensbescherming <fg@tweedekamer.nl>

CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek TK

Beste 5.1.2.e

Naar aanleiding van je onderstaande mail willen we je vragen dit op te nemen met 5.1.2.e voor verdere afhandeling.

Ik bericht je dit mede namens 5.1.2.e Ik zet hem in de cc.

Groet,
5.1.2.e
Tst. 5.1.2.e

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: dinsdag 31 augustus 2021 09:12
Aan: Griffier Tweede Kamer <Griffier@tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl> 5.1.1.e <5.1.2.e @tweedekamer.nl>
Onderwerp: datalek TK

Beste 5.1.2.e en 5.1.2.e

Met betrekking tot het datalek bij de TK dienen er nog een tweetal acties verricht te worden. Als FG meld ik dat dit incident nog formeel afgehandeld dient te worden. Nu weet ik dat er vanuit de Kamer al een brief (met blik stoopwafels) is verstuurd. Ik wil graag een kopie van die brief zodat ik daarop de formele reactie kan afstemmen. Navraag bij Comm leverde niets op. Weet dat inmiddels het datalek bij de Autoriteit Persoonsgegevens is gemeld. Ook dient er nog een brief aan de KvK opgesteld te worden, wij lezen graag mee op deze brief. Ter verdere informatie het volgende: de PvD had op hun website nog de desbetreffende informatie staan met daarop de persoonsgegevens van betrokkene vermeld. 5.1.2.e heeft hierover contact opgenomen, zij bedankten voor de informatie en wij gaan er vanuit dat de persoonsgegevens worden gelakt.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 13 september 2021 15:52
Aan: Functionaris gegevensbescherming
Onderwerp: Aanvullende informatie betreft datalek brief van 5.1.2.e
Bijlagen: 2021D32987.docx; 2021D32990.pdf; 2021D32988.pdf; 2021D32989.pdf; 2021D32995.docx

Beste 5.1.2.e

Zoals je weet, heeft een datalek vandaag helaas plaatsgevonden met betrekking tot een brief van een burger (5.1.2.e). De commissie had in Parlis een brief van de heer 5.1.2.e met datum 9 september (2021D32995) geprobeerd te koppelen als bijlage aan een andere brief (2021D32987) die hij al eerder naar de Kamer had verstuurd op 8 september. Omdat men niet de juiste procedure had gevolgd bij het registreren van de laatste brief van de heer 5.1.2.e (2021D32995), is deze brief zichtbaar geweest op verschillende websites (o.a. tk.nl en 1848.nl). Het document 2021D32995 is al verwijderd van Parlis, zoals je weet.

De heer 5.1.2.e heeft aan de commissie nu gevraagd om zaak 2021Z15390 en zijn brief 2021D32987 van afgelopen woensdag 8 september ook te laten verwijderen van Parlis, inclusief zijn 3 bijlagen: 2021D32990, 2021D32988 en 2021D32989. Telefonisch hebben we met elkaar afgesproken dat ik deze documenten nog niet van Parlis ga verwijderen totdat de behandeling van deze datalek afgehandeld is. Ik heb wel de documenten in kwestie op concept gezet, op deze manier zijn ze nu alleen intern te openen door de muterende medewerkers van Parlis.

Voor de duidelijkheid: de brief 2021D32987 van afgelopen woensdag 8 september en zijn 3 bijlagen 2021D32990, 2021D32988 en 2021D32989 waren correct geregistreerd in Parlis en zijn niet gelekt naar de websites. De datalek betreft alleen de brief van 9 september 2021D32995.

Ik stuur je met deze e-mail alle documenten voor de zekerheid. Ik hoor graag van je wanneer ik de brief 2021D32987 van afgelopen woensdag 8 september en zijn 3 bijlagen 2021D32990, 2021D32988 en 2021D32989 van Parlis mag verwijderen.

Met vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 13 september 2021 14:45
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: spoed verzoek zaak laten vervallen

Beste 5.1.2.e

Bijgaand een verzoek om zaak 2021Z15390 uit Parlis te verwijderen. Dit is op verzoek van de afzender.

5.1.2.e d.d. 08-09-2021

Met vriendelijke groet,

5.1.2.e

medewerker registratie
Griffie Plenair - Bureau Wetgeving
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(31)70-318 | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.1.e E. <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 13 september 2021 14:17
Aan: Registratie-Griffie <5.1.2.i @tweedekamer.nl>
Onderwerp: spoed verzoek zaak laten vervallen

Kunnen jullie onderstaande zaak laten vervallen?
De afzender trekt zijn brief graag in

2021Z15390 Reactie m.b.t. situatie van kwetsbare Afghanen

Met vriendelijke groet,

5.1.2.e

Commissie assistent
commissie Buitenlandse Zaken, contactgroep Frankrijk
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 14 september 2021 09:26
Aan: 5.1.2.e ; Functionaris gegevensbescherming
Onderwerp: FW: datalek TK
Bijlagen: FW: datalek TK

Concept:

Geachte mevrouw 5.1.2.e

De persoonsgegevens van uw dochter waren van 20 augustus 2021 tot en met 23 augustus 2021 onbedoeld zichtbaar op internet. Over dit incident heeft een medewerker van de Kamer reeds met u contact opgenomen. Ter aanvulling daarop informeer ik u als volgt. De Tweede Kamer heeft naar aanleiding van het incident het datalek gemeld bij de Autoriteit Persoonsgegevens (AP) vanwege het feit dat uw dochter minderjarig is en omdat het incident negatieve gevolgen met zich mee kan brengen. De AP bestudeert alle meldingen en kan besluiten tot een nader onderzoek. Naast de melding bij de AP heeft de Kamer de procedure voor het publiceren van ontvangen brieven intern en extern weer onder de aandacht gebracht. Als functionaris voor de gegevensbescherming van de Tweede Kamer zal ik in overleg treden met de betrokken diensten om te zien of deze procedures aangescherpt moeten of kunnen worden.

I2108 0447 Datalek Parlis – vermelding privéadres burger op internetsite Tweede Kamer
23 augustus om 21:02 is melding gedaan van datalek in TopDesk. Hierbij is de volgende informatie meegestuurd:

Beste Servicedesk,
Bij deze wil ik graag een melding doen over een datalek:

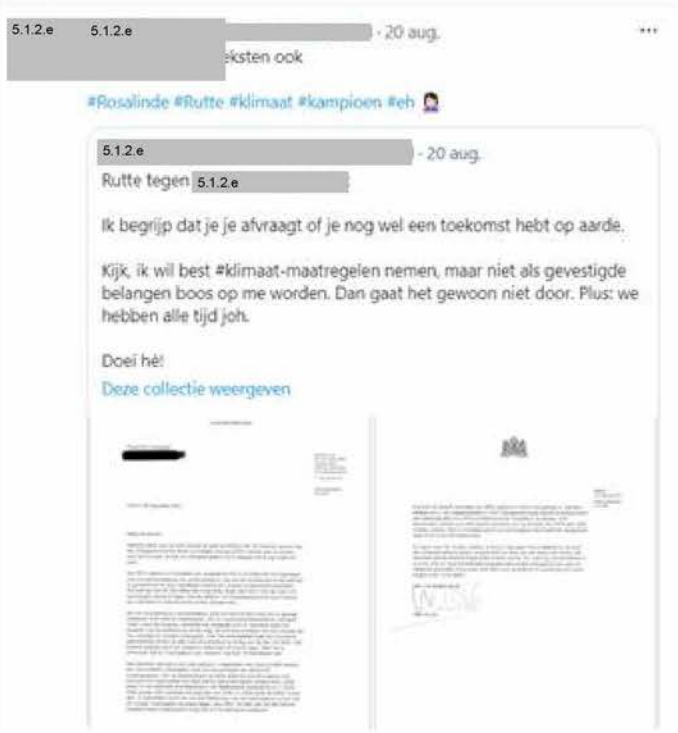
- *Op 20 augustus 2021 is in Parlis een antwoord geregistreerd (2021D30810) met een bijlage (2021D30811) door de Griffie plenair. Dit is een antwoord van de minister-president op schriftelijke vragen gesteld door het Kamerlid Ouwehand (zie 2021D30379).*
- *De volledige naam van een burger (5.1.2.e) werd vermeld in beide documenten (antwoord en bijlage). In de bijlage werd het privéadres van 5.1.2.e ook vermeld. NB: de bijlage in kwestie is een afschrift van een brief die Mark Rutte aan 5.1.2.e heeft verzonden.*
- *Beide documenten (antwoord en bijlage), inclusief de volledige naam en het adres van de burger, waren helaas ook zichtbaar op TK.nl sinds 20 augustus door de koppeling die Parlis en de website TK.nl met elkaar delen.*
- *Vandaag, 23 augustus, is de naam "5.1.2.e " in beide documenten geanonimiseerd[1] door de Griffie plenair (vervangen door initialen). En haar privé adres is ook van de bijlage verwijderd. Door deze correctie uitgevoerd in het systeem Parlis toont de website TK.nl deze privégegevens ook niet meer.*

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
5.1.2.e
5.1.1.e
Griffie plenair/Bureau Wetgeving
5.1.1.e

Nader onderzoek door Privacy Officer:

- Op 13 augustus 2021 heeft het lid Ouwehand schriftelijke vragen gesteld aan de MP, zie Deze vragen zijn opgenomen in Parlis, zie Document.
- De Partij voor de Dieren heeft deze schriftelijke vragen opgenomen op haar website, zie Vragen Ouwehand over de bezorgde brief van de 14-jarige 5.1.2.e aan de minister-president - Partij voor de Dieren . In deze vragen verzoekt Ouwehand om de brief van 5.1.2.e openbaar te maken.
- Griffie commissie/ Griffie Tweede Kamer heeft de vragen van het lid Ouwehand zonder anonimiseren/pseudonimiseren doorgestuurd naar ministerie AZ.
- 20 augustus 2021 stuurt de MP de brief van 5.1.2.e met zijn antwoord aan 5.1.2.e in afschrift naar de Tweede Kamer. De persoonsgegevens van 5.1.2.e zijn niet weggelakt door het ministerie van AZ en de brief plus bijlage wordt mét de persoonsgegevens, waaronder het privéadres, op de internetpagina van de Tweede Kamer geplaatst, zie Detail 2021D30810 | Tweede Kamer der Staten-Generaal
- Zaterdag 21 augustus twitterde 5.1.2.e over het antwoord van Rutte en zij voegde de complete antwoordbrief (mét het privéadres) in haar twitterbericht (inmiddels is dit privéadres weggelakt. Door wie?) .



- De ouders van 5.1.2.e zagen het bericht van Ouwehand en tot hun schrik dat het privéadres niet was weggelakt. Toen waren de eerste haatberichten al verstuurd (via Twitter? Post?)
- Vanaf vrijdag 20 augustus heeft moeder geprobeerd contact te krijgen met de Tweede Kamer. Onduidelijk is naar welk nummer zij heeft gebeld.
- Volgens artikel in NRC zou de Beveiliging van de Tweede Kamer hebben geadviseerd om de politie in te schakelen en te vragen een extra rondje te rijden.
  BVA is niet gebeld. Navraag bij 5.1.2.e

- Maandag 23 augustus heeft moeder contact gehad met de griffie plenair, 5.1.2.e 5.1.2.e heeft actie ondernomen en de persoonsgegevens gepseudonimiseerd in R.L. zowel in Parlis als op de website TK.
- Maandag 23 augustus heeft een journalist van NRC gebeld met stafdienst Communicatie. 5.1.2.e heeft e.e.a. uitgezocht door navraag bij griffie plenair. Zij heeft de journalist laten weten dat er onbedoeld een menselijke fout is gemaakt en dat deze inmiddels hersteld is. Vervolgens heeft zij de Voorzitter geïnformeerd, en daarna de Griffier.

- Maandag 23 augustus om 21:05 uur is er vanuit TopDesk een melding gestuurd naar het Datalekteam.

Wat moet er gebeuren?

1. Informeren betrokkene met officiële brief
2. Datalek melden aan AP
3. Nagaan waarom de datalekprocedure niet is gevolgd (meenemen in de evaluatie datalekprocedure). Immers pas 23 aug om 21:05 is datalekteam geïnformeerd. Toen waren reeds verschillende acties uitgevoerd.
4. Met contactpersonen Griffies commissie en griffie plenair het gebruik van persoonsgegevens in schriftelijke vragen bespreken. Immers, zij checken de vragen op inhoud en redactioneel.
5. Informatie over AVG en FG op website Tweede Kamer meenemen in de evaluatie. Is deze info voldoende duidelijk en vindbaar?
6. Taakverdeling datalekteam meenemen in de evaluatie datalekprocedure. Maandag 23 augustus is CISO door stafdienst Communicatie telefonisch geïnformeerd over het datalek, de FG niet (klopt dat?)
7. Partij voor de dieren informeren over gebruik persoonsgegevens op internet, nav twitterbericht Ouwehand.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 10 september 2021 12:31
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek TK

Hi 5.1.2.e

Bijgevoegd mijn antwoord van maandag jl.

Met vriendelijke groet,

5.1.2.e

Stafdienst Communicatie
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 10 september 2021 12:18
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek TK

Hi 5.1.2.e

Onderstaand bericht is vast aan je aandacht ontsnapt. Zou je me de brief alsnog kunnen toesturen. Dan kan ik ook het incident AVG-technisch afsluiten.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: Wensem, P. van <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 1 september 2021 13:01
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek TK

Ha 5.1.2.e en 5.1.2.e

Willen jullie even contact opnemen met 5.1.2.e om hem te informeren wanneer en op welke wijze in contact is getreden met de ouders en wat met welk begeleidend schrijven is opgestuurd aan de jongedame zelf.

Met vriendelijke groet,

5.1.2.e

5.1.1.e
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | M +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: woensdag 1 september 2021 11:43
Aan: 5.1.1.e 5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek TK

Beste 5.1.2.e

Zie onderstaande mailwisseling. Kan jij me verder helpen?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

Van: Griffier Tweede Kamer <Griffier@tweedekamer.nl>
Verzonden: dinsdag 31 augustus 2021 17:21
Aan: Functionaris gegevensbescherming <fg@tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek TK

Beste 5.1.2.e

Naar aanleiding van je onderstaande mail willen we je vragen dit op te nemen met 5.1.2.e voor verdere afhandeling.

Ik bericht je dit mede namens 5.1.2.e Ik zet hem in de cc.

Groet,
5.1.2.e
Tst. 5.1.1.e

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: dinsdag 31 augustus 2021 09:12
Aan: Griffier Tweede Kamer <Griffier@tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>; 5.1.1.e <5.1.2.e @tweedekamer.nl>
Onderwerp: datalek TK

Beste 5.1.2.e en 5.1.2.e

Met betrekking tot het datalek bij de TK dienen er nog een tweetal acties verricht te worden. Als FG meld ik dat dit incident nog formeel afgehandeld dient te worden. Nu weet ik dat er vanuit de Kamer al een brief (met blik stoopwafels) is verstuurd. Ik wil graag een kopie van die brief zodat ik daarop de formele reactie kan afstemmen. Navraag bij Comm leverde niets op. Weet dat inmiddels het datalek bij de Autoriteit Persoonsgegevens is gemeld. Ook dient er nog een brief aan de KvK opgesteld te worden, wij lezen graag mee op deze brief. Ter verdere informatie het volgende: de PvD had op hun website nog de desbetreffende informatie staan met daarop de persoonsgegevens van betrokkene vermeld. 5.1.2.e heeft hierover contact opgenomen, zij bedankten voor de informatie en wij gaan er vanuit dat de persoonsgegevens worden gelakt.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | | www.tweedekamer.nl

[1] Noot van de Privacy Officer: Vermelding van initialen is geen anonimiseren.

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 20 september 2021 10:52
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: FW: datalek

Ha 5.1.2.e

5.1.2.e heeft het adres van de familie op een enveloppe gezet. Ik heb de brief geprint en in de enveloppe gestopt. Deze enveloppe ligt in jouw postvakje op de 7e etage (kamer 5.1.1.e e.a.).
Wil jij de brief tekenen en versturen?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e@tweedekamer.nl>
Verzonden: maandag 20 september 2021 09:58
Aan: Functionaris gegevensbescherming <fg@tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e@tweedekamer.nl>
Onderwerp: RE: datalek

5.1.2.e

ik heb haar contactgegevens ook niet. Ik heb deze mevrouw namelijk via de telefooncentrale te woord gestaan.

Met vriendelijke groet,

5.1.2.e

inhoudelijk medewerker
Griffie Plenair - Bureau Wetgeving
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

---

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: vrijdag 17 september 2021 10:42
Aan: 5.1.2.e <5.1.2.e@tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>; 5.1.2.e

<5.1.2.e @tweedekamer.nl>
Onderwerp: datalek

Beste 5.1.2.e

Dank voor de input. Zou jij namens mij onderstaand bericht aan mevrouw 5.1.2.e kunnen sturen. Ik heb haar contactgegevens niet en ik vid het ook niet nodig dat ik daarover beschiok.

Alvast veel dank!

Geachte mevrouw 5.1.2.e

De persoonsgegevens van uw dochter waren van 20 augustus 2021 13.30 uur tot en met 23 augustus 2021 11.30 uur onbedoeld zichtbaar op internet. Over dit incident heeft een medewerker van de Kamer reeds met u contact opgenomen. Ter aanvulling daarop informeer ik u als volgt. De Tweede Kamer heeft naar aanleiding van het incident het datalek gemeld bij de Autoriteit Persoonsgegevens (AP) vanwege het feit dat uw dochter minderjarig is en omdat het incident negatieve gevolgen met zich mee kan brengen. De AP bestudeert alle meldingen en kan besluiten tot een nader onderzoek. Naast de melding bij de AP heeft de Kamer de procedure voor het publiceren van ontvangen brieven intern en extern nogmaals onder de aandacht gebracht.

5.1.2.e
Functionaris gegevensbescherming

Docnr23

Tweede Kamer
DER STATEN-GENERAAL

aan 5.1.2.e

Postbus 20018
2500 EA Den Haag

5.1.2.e

Prinses Irenepad 1
2595 BG 's-Gravenhage

M 5.1.2.e
5.1.2.e @tweedekamer.nl

datum 21 september 2021
betreft Datalek
pagina 1/1

Geachte mevrouw 5.1.2.e

De persoonsgegevens van uw dochter waren van 20 augustus 2021 13.30 uur tot en met 23 augustus 2021 11.30 uur onbedoeld zichtbaar op internet. Over dit incident heeft een medewerker van de Kamer reeds met u contact opgenomen. Ter aanvulling daarop informeer ik u als volgt.

De Tweede Kamer heeft naar aanleiding van het incident het datalek gemeld bij de Autoriteit Persoonsgegevens (AP) vanwege het feit dat uw dochter minderjarig is en omdat het incident negatieve gevolgen met zich mee kan brengen. De AP bestudeert alle meldingen en kan besluiten tot een nader onderzoek. Naast de melding bij de AP heeft de Kamer de procedure voor het publiceren van ontvangen brieven intern en extern nogmaals onder de aandacht gebracht.

Tenslotte verzoek ik u met mij contact op te nemen in het geval u vragen hebt over deze / m.f of over het datalek.

Met vriendelijke groet,

5.1.2.e

Functionaris gegevensbescherming

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 22 september 2021 17:57
Aan: Functionaris gegevensbescherming; StafdienstHR
Onderwerp: RE: datalekmelding

Ha 5.1.2.e
Ik heb 5.1.2.e inmiddels gesproken en het is afgehandeld.

Met vriendelijke groeten,

5.1.2.e

5.1.2.i
Tweede Kamer der Staten-Generaal

Kamer 5.1.2.e Bezuidenhoutseweg 67, Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | M 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

---

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Verzonden: donderdag 2 september 2021 12:52
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; StafdienstHR <5.1.2.i tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: RE: datalekmelding

Ha 5.1.2.e

Dank voor je felicitatie ☺.
En dank voor onderstaande informatie. Ik wacht nadere berichtgeving van 5.1.2.e via jou, af.

Fijne dag!

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 1 september 2021 22:09
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; StafdienstHR <5.1.2.i tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: RE: datalekmelding

Dag jarige 5.1.2.i !
5.1.2.e heeft bij een controle op een p-dossier (Of het id bewijs er inzat) gezien dat een document in het verkeerde dossier zat. Ze heeft daarvan melding gemaakt, p-direkt verzocht het te corrigeren, de belanghebbenden geïnformeerd en is daarna ziek haar zwangerschapsverlof in gegaan. Ik weet niet of het hiermee is afgehandeld. Ik zal het 5.1.2.e vragen.
Een fijne verjaardag nog!
Groet
5.1.2.e

Verzonden vanaf mijn Galaxy

-------- Oorspronkelijk bericht --------
Van: "5.1.2.e" <5.1.2.e@tweedekamer.nl>
Datum: 01-09-21 15:02 (GMT+01:00)
Aan: StafdienstHR <5.1.2.i tweedekamer.nl>
Cc: "5.1.2.e <j5.1.2.e@tweedekamer.nl>, Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: datalekmelding

Beste collega's van HR,

Beste collega's van HR,

Het datalekteam heeft op 5 augustus jl. onderstaande melding ontvangen van 5.1.2.e over een datalek.

Wij hebben meer informatie nodig om de melding te behandelen en de benodigde stappen uit te zetten. Wie kan mij hier vandaag meer informatie over geven?
Ik voeg het formulier datalekken bij, dat bij een melding van een datalek ingevuld naar 5.1.2.i moet worden gestuurd.
Tevens stuur ik jullie de link naar de datalekpagina op Plein2 waar meer informatie is te vinden over de datalekprocedure van de Tweede Kamer en de e-learning Datalekken is te vinden.

5.1.2.e 5.1.2.e

Date sent: Aug 5, 2021 3:57 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Melding datalek

Ha collega's,

Hierbij wil ik graag een datalekmelding maken die vandaag ontdekt is bij Stafdienst HR. Er wordt ook een melding gemaakt bij P-dir herstellen. Tevens worden desbetreffende personen geinformeerd door Stafdienst HR.

Met vriendelijke groet,
5.1.2.e
Medewerker stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
M +(5.1.2.e)
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Aanwezig op maandag, dinsdag en donderdag

Ik hoor graag van één van jullie!

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Formulier melding datalek

Tweede Kamer
DER STATEN-GENERAAL

Dit formulier is bedoeld om een melding te maken van een (mogelijk) datalek. De Algemene Verordening Gegevensbescherming (AVG) verplicht de Tweede Kamer om datalekken binnen de organisatie te registreren en te melden. Een datalek is een incident waarbij persoonsgegevens, waarvoor de Tweede Kamer verantwoordelijk is, zijn gelekt naar personen of instanties die geen toegang mogen hebben tot deze gegevens. Ook het verloren gaan of beschadigen van persoonsgegevens valt datalekken.

Melding
Meld het datalek zo snel als mogelijk door dit formulier in te vullen en per e-mail te sturen naar 5.1.2.i @tweedekamer.nl.

Let op!
Stuur geen overige correspondentie of stukken mee met dit formulier. Deze worden (wanneer nodig) door het datalekteam bij jou opgevraagd . Het datalekteam bestaat uit: Functionaris Gegevensbescherming, CISO en Security Officer.

Melder

1a. Naam:	5.1.2.e - 5.1.2.e
1b. Afdeling:	Programmabureau Tijdelijke Huisvesting

Over het incident

2a. Op welke datum vond het incident plaats?

Op ☐
Tussen ☐ en ☐
☒ Nog niet bekend

2b. Welke ongeoorloofde actie heeft plaatsgevonden?

☐ Lezen/inzien	☐ Veranderen	☐ Diefstal of verlies
☐ Kopiëren	☐ Vernietiging	☒ Nog niet bekend

2c. Welk type gegevensdrager(s) zijn betrokken?

☐ Laptop	☐ Tablet	☐ Smartphone
☐ E-mail	☐ Brief	☐ Fax
☐ SharePoint	☐ Netwerkschijf	☐ Papieren stuk
☐ Website	☐ Social media:	
☐ Overige:	oa usb sticks en CD's	

2d. Wat is de oorzaak?

☐ Diefstal van gegevensdragers	☐ Verkeerd geadresseerd
☐ Verlies van gegevensdragers	☐ Te veel geadresseerden
☐ Onveilig vernietigen/wegwerpen	☐ Verkeerd bezorgd
☐ Scherm niet vergrendeld	☐ Niet aangekomen
☐ Onbeheerd achterlaten stukken	☐ Verkeerde autorisaties
☐ Indringer in het pand	☐ Dataverlies zonder back-up
☐ Te veel gegevens geleverd	☐ Digitale inbraak, hacking
☐ Verkeerde gegevens geleverd	☐ Phishing (e-mail, telefonisch)
☐ Overige:	bij de verhuizing zijn spullen in ladeblokken achter gelaten

2e. Korte beschrijving van het incident:	de overgedragen ladenblokken zijn door DJI geleegd, daar lagen nog een aantal usb sticks en cd in. De gegevendragers zijn overhandigd aan de Tweede Kamer en worden vernietigd. De overige ladeblokken die zijn afgevoerd worden voor overdracht gecontroleerd om eventuele lekken te voorkomen.

Over de gegevens

3a. Om welk type persoons-gegevens gaat het?	☐ Naam, adres- en woonplaatsgegevens ☐ Telefoonnummers ☐ E-mailadressen of gebruikersnamen op social media ☐ Toegangsgegevens (bijv. inlognaam/wachtwoord ☐ Financiële gegevens (bijv. rekeningnummer) ☐ Dossiernummer ☐ Burgerservicenummer (BSN) ☐ Kopieën van legitimatiebewijzen (bijv. paspoort, rijbewijs ☐ Geslacht, geboortedatum en/of leeftijd ☐ Bijzondere persoonsgegevens (bijv. ras, etniciteit, religie, politieke overtuiging, vakbondslidmaatschap, criminele gegevens, seksuele leven, medische gegevens) ☒ Overige onbekend, de usb sticks en cd's zijn niet uitgelezen
3b. Van hoeveel personen zijn persoonsgegevens betrokken bij het incident? (schatting)	Minimaal: 1 Maximaal: 30
3c. Bevat de groep mensen van wie de gegevens zijn gelekt:	☐ Minderjarigen ☐ Overige kwestbare groepen
3d. Omschrijf de groep mensen van wie de gegevens zijn gelekt:	
3e. Welke gevolgen kan het datalek hebben voor de persoonlijke levenssfeer van de betrokkenen?	☐ Stigmatisering of uitsluiting ☐ Schade aan de gezondheid ☐ Blootstelling aan (identiteit)fraude ☐ Blootstelling aan spam of phishing ☒ Overige: onbekend
3f. Waren de gegevens versleuteld, gehasht of op andere wijze onbegrijpelijk of ontoegankelijk gemaakt?	☐ Nee ☐ Ja, op de volgende wijze: ☐ Deels, op de volgende wijze: onbekend

5.1.2.e

Van: Functionaris gegevensbescherming
Verzonden: woensdag 10 november 2021 12:37
Aan: 5.1.2.i
CC: Functionaris gegevensbescherming; 5.1.2.e 5.1.2.e
Onderwerp: FW: formulier_melding_datalek ladeblokken
Bijlagen: formulier_melding_datalek ladeblokken.docx

Beste collega´s van de helpdesk,

Kunnen jullie een datalekmelding in topdesk zetten en hierbij bijgaand formulier bij opnemen?

Dank

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 9 november 2021 14:51
Aan: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: formulier_melding_datalek ladeblokken

5.1.2.e

Bijgaand het gevraagde formulier. Is dit zo voldoende?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Programmabureau / Facilitaire Dienst
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 22 november 2021 12:05
Aan: 5.1.2.e
Onderwerp: evaluatie aanpak datalekken Tweede Kamer

Ha 5.1.2.e

Dit jaar wil ik de procedure en aanpak datalekken binnen de Tweede Kamer evalueren. Op de teamsite heb ik een evaluatie-voorstel geplaatst en een voorzet gedaan voor de collega's die in bij de evaluatie wil betrekken. zie
https://teamsite/project/AVG/AVGDocumenten/Instrumenten%20van%20de%20AVG/Datalekken/Evaluatie%20datalekken/Evaluatie%20aanpak%20datalekken%20Tweede%20Kamer.docx?Web=1

Wil jij het document doorlezen en mij jouw reactie laten weten?

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 20 maart 2023 16:51
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: concept voorstel script voor SD met betrekking tot datalekken
Bijlagen: 0230301 SD en script datalekken.docx

Ha 5.1.2.e

Hierbij stuur ik jou mijn conceptvoorstel voor een nieuw script voor Datalekken.
Wil jij het doorlezen?
Laat mij weten wanneer we het samen kunnen bespreken, bij voorkeur op een maandag of dinsdag (mijn agenda is actueel bijgewerkt).

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Rapportage van de evaluatie Aanpak datalekken binnen de Tweede Kamerorganisatie
Looptijd 1 december 2021 – eind februari 2022

1. Inleiding

Per 1 januari 2016 is de 'Wet Meldplicht Datalekken' in werking getreden. Op grond van deze wet zijn organisaties (zowel ondernemingen als overheden) verplicht om direct melding te doen bij de Autoriteit Persoonsgegevens (AP) van een 'inbreuk in verband met persoonsgegevens' (hierna: datalek). Zo'n datalek moet ruim worden geduid. Het betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of er passende technische of organisatorische beschermingsmaatregelen waren getroffen of niet. Een datalek kan zich in beide situaties voordoen en doet zich sneller voor dan vaak gedacht. Een datalek kan bestaan uit een gerichte inbreuk door hackers of een technisch beveiligingsprobleem, maar er is ook sprake van een datalek indien een laptop, telefoon, tablet, USB-stick of andere gegevensdrager is verloren of gestolen. Er is mogelijk ook sprake van een datalek indien op een gegevensdrager een of andere 'malware' wordt aangetroffen. Deze en andere voorvallen dienen alle te worden gemeld bij de Autoriteit Persoonsgegevens, indien deze (mogelijk) leiden tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het is aan de organisatie zelf om te bepalen of dat het geval is.
Het is nu zes jaar na het van kracht zijn van de Wet Meldplicht datalekken. Een goed moment om te evalueren hoe de Tweede Kamer het proces rondom datalekken heeft ingericht en of dit (nog steeds) voldoet aan de eisen van de Avg.

2. Doel en opzet van het onderzoek evaluatie datalekken

Het doel van deze evaluatie is om te evalueren hoe de aanpak datalekken binnen de Tweede Kamer werkt en of deze aanpak (nog steeds) voldoet aan de wettelijke eisen. De aanbevelingen en verbeterpunten die voortvloeien uit deze evaluatie zullen in de resterende maanden van 2022 worden opgepakt.

De evaluatie is uitgevoerd door 5.1.2.e en 5.1.2.e en bestaat uit de volgende stappen:

- (Individuele) interviews van maximaal 45 minuten met sleutelfiguren;
- Terugkoppeling van de interviewresultaten naar de geïnterviewden met als doel gezamenlijk trekken van conclusies en formuleren van aanbevelingen;
- Aanbevelingen voorzien van tijdspad en actiehouder;
- Actualiseren van de informatie over datalekken o.a. op Plein2 en in TopDesk. En sleutelfiguren en Avg-contactpersonen trainen op het geactualiseerde proces.

In de evaluatie komen de volgende onderwerpen aan de orde:

1. <u>Kennis over datalekken binnen de Tweede Kamerorganisatie</u>
   Is er voldoende kennis binnen de diensten van de Tweede Kamer over wat een datalek is? Weet men de informatie op Plein2 te vinden en toe te passen? Welke middelen/platforms gebruiken we om de kennis en bewustwording te borgen?

2. <u>Stappenplan datalekken Tweede Kamer</u>

3. Samenstelling en rollen datalekteam
   Gekeken wordt naar samenstelling en rollen binnen het datalekteam.
   Het huidige datalekteam bestaat uit zeven personen. Welke rollen zijn te onderscheiden?

4. Analyse van de administratie van datalekken
   Datalekken moeten verplicht worden geregistreerd in het datalekregister. De Tweede Kamer heeft een datalekregister ingericht in TopDesk. Hoe functioneert dit datalekregister? Voldoet het datalekregister aan de verplichtingen van de AVG? Wordt het register gebruikt voor analyse om trends en ontwikkelingen te signaleren? Maakt de FG gebruikt van het register?

3. Bevindingen en aanbevelingen

Er zijn in totaal 10 interviews met verschillende sleutelfiguren afgenomen. Voor de lijst met geïnterviewde personen, zie bijlage 1.
In deze paragraaf worden per onderwerp de aanbevelingen en verbeterpunten weergegeven die in de interviews naar voren zijn gekomen.

3.1 Kennis over datalekken binnen de Tweede Kamerorganisatie

De geïnterviewden geven in ruime meerderheid aan dat het belangrijk is dat iedereen binnen de Tweede Kamerorganisatie weet wat een datalek is en vervolgens weet hoe gehandeld moet worden. Zo geeft de Service Desk (SD) van de Tweede Kamer aan dat melders van verlies of diefstal van apparatuur als telefoon, laptop of tablet zich niet bewust zijn dat dit een datalek is. Verlies of diefstal wordt gemeld om een nieuw apparaat te krijgen en niet als datalek.
Qua kennis en bewustwording is in de afgelopen jaren zeker vooruitgang geboekt. Ook het datalekteam heeft inmiddels meer kennis en ervaring opgedaan over datalekken. Op Plein2 is informatie over datalekken te vinden en staat een op maat gemaakte e-learning. Het is niet duidelijk hoe vindbaar deze informatie is voor medewerkers van de Tweede Kamer en of deze geraadpleegd wordt bij vragen. Er is behoefte aan meer duiding en voorbeelden van datalekken die kunnen voorkomen binnen de Tweede Kamer. Dit zal de herkenbaarheid van datalekken aanzienlijk kunnen vergroten.

Belangrijk aandachtspunt is dat er jaarlijks maar weinig datalekken worden gemeld[1]. Dit kan komen doordat men een gemaakte fout liever onder de pet houdt en/of zich niet bewust is dat het belangrijk en verplicht is het melden. Het is reëel te veronderstellen dat er jaarlijks (veel) meer datalekken plaatsvinden binnen de Tweede Kamer, zoals bijvoorbeeld verkeerde emailadressering, ongeautoriseerde toegang tot informatie en langer bewaren van persoonsgegevens dan noodzakelijk. Tot slot wordt aangegeven dat er behoefte is aan een toelichting op de verschillende rollen binnen de Avg. Zoals: wie is waar aanspreekbaar op en/of verantwoordelijk voor bij Avg-vragen, in het bijzonder in geval van datalekken.

Aanbevelingen

- Kennis over en bewustwording van potentiële datalekken is een onderwerp waar blijvend aandacht voor moet zijn.
- Via sleutelfiguren zoals het MT van de Tweede Kamer, diensthoofden, Avg-contactpersonen, medewerkers SD, Security Awareness Officer en Servicemanagers Dienst kennis delen over

[1] In 2019 – 52 gemelde datalekken; In 2020 – 39 gemelde datalekken; In 2021 - 49 gemelde datalekken; t/m maart2022 - 7 gemelde datalekken.

datalekken die zich hebben voorgedaan, evenals de maatregelen die zijn genomen om herhaling van deze datalekken te voorkomen.

- Zorgen dat bovengenoemde sleutelfiguren een goed beeld hebben van het soort datalekken binnen de Tweede Kamer en wat de impact is.
- Daarnaast via e-learning, quiz op Plein2, escaperoom met het thema Datalekken in de centrale hal kan de kennis over datalekken worden verhoogd en blijvende aandacht worden gegeven aan datalekken.
- Het aantal bij de SD gemelde datalekken is niet realistisch. Via MT en diensthoofden moeten medewerkers worden aangemoedigd om datalekken bij 5.1.2.i te melden. Een ludieke actie als het uitloven van een taart bij elk 10e datalek kan daarbij als aansporing helpen.

3.2 Stappenplan datalekken Tweede Kamer

De SD is de eerste lijn waar datalekken moeten worden gemeld. Daar wordt een inschatting gemaakt of het om een potentieel datalek gaat. De SD zet gemelde potentiele datalekken door naar het datalekteam. De SD maakt hierbij gebruik van een sjabloon, bestaande uit een aantal standaardvragen. Het sjabloon moet worden geëvalueerd om na te gaan of alle noodzakelijke informatie/toelichting bij de verschillende stappen is opgenomen. Om een goede beoordeling te kunnen geven of een melding een datalek betreft zou meer informatie moeten worden uitgevraagd.

SD geeft aan dat het meldformulier Datalekken dat door de melder moet worden ingevuld, erg uitgebreid is. Dit leidt tot geringe bereidheid het formulier in te vullen. Wellicht te verbeteren door er een webformulier van te maken en het aantal vragen te verminderen. Na vaststelling dat het een datalek is kan er immers altijd nadere informatie worden opgevraagd.
Er wordt geopperd dat ~~een~~ het stroomschema “Wat is een datalek” en “Wat moet je doen” bij kan dragen aan de verhoging van de kennis en aan verdere bewustwording. Ook terugkoppeling van soort datalekken aan sleutelfiguren[2] binnen de Tweede Kamer kan hierbij helpen. Het belang van het aanpakken van beveiligingsincidenten en datalekken is voor de organisatie gelijk. De huidige werkwijze is dat eerst team Beveiligingsincidenten aan de slag gaat bij een melding en vervolgens het Datalekteam. Hierdoor is het mogelijk dat datalekken te laat worden onderkend en gemeld. Een mogelijke oplossing is aansluiting bij het Team Beveiligingsincidenten. Voor medewerkers is de melding bij de SD en het dichten van het datalek meestal de belangrijkste stap. Aandachtspunt is te zorgen dat de andere (verplichte!) stappen ook voldoende aandacht krijgen, zoals wel/niet melden bij de AP, wel/niet melden bij de betrokkene, registratie van het datalek en terugkoppeling naar de melder. In paragraaf 3.4 wordt hier nader op ingegaan.

Tot slot wordt opgemerkt dat voor de meldingen beveiligingsincidenten en datalekken eenzelfde systeem wordt gebruikt, te weten TopDesk. Per incident kan echter maar één oplosgroep aan het incidenten worden gehangen. Dit zorgt voor vertraging en kan leiden tot overschrijding van wettelijke termijnen die gelden voor melding Datalekken.

Niet elk datalek hoeft aan de AP te worden gemeld. Melding hoeft slechts te worden gedaan indien een datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als daarop een aanzienlijke kans bestaat. Indien aannemelijk is dat de inbreuk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de persoon op wie deze gegevens betrekking hebben, moet de inbreuk ook aan de betrokken personen worden gemeld. Voorbeelden van datalekken

[2] Sleutelfiguren zoals het MT van de Tweede Kamer, diensthoofden, Avg-contactpersonen, medewerkers SD, Security Awareness Officer en Servicemanagers Dienst Automatisering

binnen de Tweede Kamer kan bijdragen aan het sneller en beter herkennen van datalekken en zorgen voor hoger aantal meldingen van datalekken bij 5.1.2.i

Het is nog niet altijd duidelijk op basis van welke criteria de Tweede Kamerorganisatie een datalek meldt bij de AP en/of betrokkene. Opstellen van duidelijke criteria en voorbeelden van datalekken die zich binnen de Tweede Kamer hebben voorgedaan kunnen hier zeer behulpzaam bij zijn en zullen zorgen voor meer uniformiteit.

Aanbevelingen

- Evalueren welke informatie bij de datalekmelding door de SD wordt uitgevraagd. Is dit voldoende informatie? Welke informatie ontbreekt?
- Meldformulier datalekken evalueren op duidelijkheid en bruikbaarheid
- Stroomschema opstellen voor herkennen datalek
- Team beveiligingsincidenten en Datalekteam integreren, zodat bij incidentmelding bij de SD gezamenlijk wordt bepaald wie welke actie moet ondernemen. Dit zorgt voor tijdswinst en voorkomt mogelijke overschrijding wettelijke termijn meldplicht bij AP
- Criteria en voorbeelden opstellen van datalekken die bij AP en/of betrokkene moeten worden gemeld
- Regelmatig terugkoppelen aan sleutelfiguren welke datalekken zich hebben voorgedaan binnen de Tweede Kamer, zodat zij een goed beeld hebben van het soort datalekken binnen de Tweede Kamer en wat de impact is op betrokkenen

3.3 Samenstelling en rollen datalekteam

Het datalekteam bestaat momenteel uit zeven personen[3]. Dit aantal is in de loop van de tijd zo gegroeid zonder benoemde reden voor het toevoegen van deze personen aan het datalekteam. Zo is onduidelijk waarom BVA, Security Officer, Security Architect en CISO deel uitmaken van het team. Daarnaast wordt geconstateerd dat er binnen het datalekteam niet altijd urgentie is bij alle leden om te reageren op een melding. Hierdoor worden datalekmeldingen niet altijd (tijdig) afgesloten. Voorgesteld wordt om bij de eerste incidentmelding te schakelen met een klein kernteam, bestaande uit FG, PO en aangevuld met een medewerker privacy-ondersteuning. Dit kernteam bepaalt of er sprake is van een datalek en naar welke oplosgroep het datalek moet worden opgeschaald, en wie deel moet uitmaken van die oplosgroep. De ondersteuner zorgt hierbij voor de praktische uitvoering, zoals bijeenroepen oplosgroep en de noodzakelijke documentatie en communicatie. Deze werkwijze met een klein kernteam volgt de beproefde aanpak van het Team Beveiligingsincidenten. De behandeling en afhandeling van datalekken zal met deze aanpak veel efficiënter verlopen en het risico op overschrijding van wettelijke termijnen (zoals het binnen 72 uur melden van een datalek bij de AP) aanzienlijk doen verminderen. Ook wordt voorgesteld om beide kernteams te integreren bij elke incidentmelding, om in het vroegst mogelijke stadium te weten of er naast een beveiligingsincident ook sprake is van een datalek.

Aanbevelingen

- Beperk het datalekteam tot een kern van drie personen, bestaande uit FG, PO en medewerker privacy-ondersteuning
- Integreer het Datalekteam met Team Beveiligingsincidenten (zie aanbevelingen onder 3.3)

[3] 5.1.2.e (FG), 5.1.2.e 5.1.2.i 5.1.2.e 5.1.2.i 5.1.2.e (5.1.2.i , 5.1.2.e (5.1.2.i , 5.1.2.e 5.1.2.i) en 5.1.2.e (5.1.2.i

3.4 Analyse van de administratie van datalekken

De Avg verplicht organisaties om alle datalekken, ongeacht of deze moeten worden gemeld aan de AP en/of betrokkenen, te documenteren. Het is gebruikelijk om datalekken te documenteren in een datalekregister. Het doel van het registreren is dat ervan kan worden geleerd, om datalekken in de toekomst zo veel mogelijk te voorkomen. Een ander doel is dat daarmee aan de Autoriteit Persoonsgegevens kan worden aangetoond dat datalekken daadwerkelijk worden gemonitord en opgevolgd.
Ook wordt het datalekregister gebruikt door de FG van de Tweede Kamer om te rapporteren aan het MT en diensthoofden over welke datalekken zich hebben voorgedaan. Uit de jaarlijkse rapportage kunnen trends en ontwikkelingen worden gehaald en de rapportage kan worden vergeleken met de jaarrapportage die de AP maakt over datalekken.

De administratie van de datalekken vindt binnen de Tweede Kamer plaats in TopDesk. In de praktijk blijkt het een arbeidsintensieve en tijdrovende klus om het register goed bij te houden.
Bekeken moet worden wie de administratie van het datalekregister bij kan houden. Daarnaast moet bekeken worden of de opzet van het register, zoals nu vormgegeven is in TopDesk, voldoet aan de verplichtingen van de Avg[4].

Tot slot is opgemerkt dat nog niet optimaal gebruik wordt gemaakt van de informatie die te halen is uit het datalekregister. Het register kan efficiënter worden ingezet voor rapportage, analyse en informatiedeling met FG, Avg-contactpersonen, MT, diensthoofden en andere sleutelfiguren. Zo wordt er momenteel niet tot nauwelijks samen met securitymensen teruggekeken naar datalekken die zich hebben voorgedaan. Datalekken komen altijd voort uit een security-incident en daarom is het goed om regelmatig met security te bespreken wat er gebeurd is en welke maatregelen breed genomen zouden moeten worden.

Aanbevelingen

- Bepalen wie het datalekregister gaat bijhouden
- Met de FG bespreken of het datalekregister voldoet aan de verplichtingen van de Avg
- Afspreken hoe het datalekregister binnen de Tweede Kamer efficiënter kan worden ingezet voor analyse, rapportage en informatiedeling

[4] De volgende informatie over een datalek moet worden gedocumenteerd:

- Een korte omschrijving van het datalek
- Datum waarop het datalek plaatsvond
- Wat er met de gegevens is gebeurd (zijn ze verloren gegaan, of door een onbevoegde ingezien, gekopieerd of gewijzigd?)
- Van welke groep(en) personen er gegevens gelekt zijn, en om hoeveel personen het gaat
- Om welke soorten gegevens het gaat
- De (mogelijke) gevolgen van de inbreuk (bijvoorbeeld een risico op identiteitsfraude of reputatieschade)
- De maatregelen die zijn genomen naar aanleiding van het lek. Welke actie is ondernomen om schade te voorkomen of zo veel mogelijk te beperken (bijvoorbeeld het op afstand wissen van gegevens, of het wijzigen van wachtwoorden. Maar ook: wat heeft u gedaan om te zorgen dat het niet nog een keer kan gebeuren?)

Bijlage 1 – Lijst van geïnterviewde personen

17 januari 2022 - 5.1.2.e 5.1.2.e en 5.1.2.e – Service Desk van de Dienst Automatisering

18 januari 2022 - 5.1.2.e – 5.1.2.i

18 januari 2022 - 5.1.2.e – 5.1.2.i

18 januari 2022 - 5.1.2.e – 5.1.2.i

18 januari 2022 - 5.1.2.e – 5.1.2.i

19 januari 2022 - 5.1.2.e en 5.1.2.e - Servicemanagers bij Dienst Automatisering

19 januari 2022 - 5.1.2.e 5.1.2.i en 5.1.2.e (SD)

20 januari 2022 - 5.1.2.e - 5.1.2.i

20 januari 2022 - 5.1.2.e - 5.1.2.i
5.1.2.e

25 januari 2022 - 5.1.2.e – Functionaris voor de 5.1.2.i

27 januari 2022 - 5.1.2.e – Beveiligingsambtenaar (BVA)

Planning van het onderzoek

1e helft december	Versturen uitnodigingen interviews aan sleutelfiguren
2e helft dec 2021 – 1e helft 2022	Afname interviews
eind januari 2022	Bespreken interview resultaten, groepssessie geïnterviewden 1e
helft februari 2022	Formuleren conclusies en vervolgstappen
eind februari 2022	Presentatie eindrapport aan FG, CISO en CIO
maart 2022 – december 2022	Actiepunten en verbeterpunten uitvoeren

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 28 maart 2022 10:13
Aan: 5.1.2.e
Onderwerp: RE: Rapportage Evaluatie datalekken maart 2022
Bijlagen: Rapportage evaluatie datalekken maart 2022.docx

Goedemorgen 5.1.2.e
Mooi geschreven rapportage! Alles staat erin wat we hebben besproken met de geïnterviewden. Ik heb twee (kleine) dingetjes aangepast (zie bijlage).

Met vriendelijke groet,

5.1.2.e

Managementassistente Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e M +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

---

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 23 maart 2022 17:26
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Rapportage Evaluatie datalekken maart 2022

Ha 5.1.2.e

Hierbij de rapportage van de evaluatie. Omwille van de tijd laat ik de bespreking met alle geïnterviewden vervallen. In plaats daarvan wil ik de rapportage aan hen voorleggen met de vraag of ze de bevindingen en aanbevelingen herkennen en onderschrijven.
Wil jij het verslag kritisch doorlezen en jou op- en aanmerkingen toevoegen?
Alvast bedankt.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 6 april 2022 15:37
Aan: 5.1.2.i
Onderwerp: RE: Rapportage evaluatie datalekken

Ha 5.1.2.e

Dank voor je snelle en positieve reactie. En dank voor de redactionele wijzigingen. Die pas ik aan.

Groet,
5.1.2.e

Van: 5.1.2.i 5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 6 april 2022 15:32
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: Rapportage evaluatie datalekken

Ha 5.1.2.e

Goed verhaal, vlot geschreven met een duidelijke lijn en opbouw ☺ (ik heb het wel anders gezien in de TK).

Kleine taaltechnische correcties:

- Ik zou AVG overal met hoofdletters schrijven (conform de schrijfwijze op https://autoriteitpersoonsgegevens.nl/nl);
- FG zal niet voor iedereen een bekende afkorting zijn, ik zou dat bij de eerste vermelding op blz. 2 één keer voluit schrijven;
- Een kleine spelfout: op bladzijde 5 eerste paragraaf staat “beoordeeld”, dat moet zijn “beoordeelt”;
- In de volgende paragraaf: “privacy medewerker” schrijf je in principe aan elkaar: “privacymedewerker” (zie https://onzetaal.nl/taaladvies/engels-woord-in-een-nederlandse-samenstelling). Alternatief is een streepje ertussen.

Met vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 6 april 2022 14:59
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl> 5.1.2.i 5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e J. <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Rapportage evaluatie datalekken

Beste collega’s,

In januari jl. zijn jullie geïnterviewd over de aanpak van datalekken binnen de Tweede Kamer.

Bijgaand stuur ik jullie de rapportage die een weergave is van ieders input in deze interviews. Voor elk van de vier thema's die zijn besproken heb ik aanbevelingen geformuleerd.

Aan ieder van jullie het verzoek om de rapportage kritisch door te lezen. Herken je de weergave en kun je de aanbevelingen ondersteunen?
Na jullie kritische blik wordt de rapportage aangeboden aan de CIO (5.1.2.e s), FG (5.1.2.e) en CISO (5.1.2.e 5.1.2.e).

Ik hoor het graag uiterlijk maandag 11 april a.s.. Je kunt je feedback in de tekst weergeven d.m.v. een opmerking of tekstvoorstel.
Alvast bedankt voor de medewerking.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e@tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 11 april 2022 11:59
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Rapportage evaluatie datalekken

Ha 5.1.2.e

Dank voor de feedback. Goed punt dat ik zeker meeneem in de rapportage.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 8 april 2022 14:59
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: Rapportage evaluatie datalekken

Ha 5.1.2.e en 5.1.2.e

Ik heb één suggestie opgenomen in bijgaand document, hoop dat jullie daar nog iets mee kunnen voor het eindverslag. Een meer algemene opmerking; en ik denk niet dat jullie daar nog iets mee kunnen, omdat de interviews al afgerond zijn; is dat het mij opvalt dat er vooral gesproken is met collega's die 'dagelijks' bezig zijn met datalekken/meldingen (Service desk, CISO, DA etc.), maar dat het perspectief van de overige collega's minder is meegenomen, bijv. AVG-contactpersonen bij andere diensten communicatie, DIA, HR etc.

Prettig weekend alvast!

Met vriendelijke groet,

5.1.2.e

5.1.2.i
Vaste commissie voor Digitale Zaken
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
M 5.1.2.e

E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 6 april 2022 14:59
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e R. <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.i 5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2. <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Rapportage evaluatie datalekken

Beste collega's,

In januari jl. zijn jullie geïnterviewd over de aanpak van datalekken binnen de Tweede Kamer.
Bijgaand stuur ik jullie de rapportage die een weergave is van ieders input in deze interviews. Voor elk van de vier thema's die zijn besproken heb ik aanbevelingen geformuleerd.

Aan ieder van jullie het verzoek om de rapportage kritisch door te lezen. Herken je de weergave en kun je de aanbevelingen ondersteunen?
Na jullie kritische blik wordt de rapportage aangeboden aan de CIO (5.1.2.e), FG (5.1.2.e) en CISO (5.1.2.e 5.1.2.e).

Ik hoor het graag uiterlijk maandag 11 april a.s.. Je kunt je feedback in de tekst weergeven d.m.v. een opmerking of tekstvoorstel.
Alvast bedankt voor de medewerking.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 11 april 2022 14:46
Aan: 5.1.2.e
Onderwerp: RE: Rapportage evaluatie datalekken

Opvolgingsvlag: Opvolgen
Vlagstatus: Voltooid

5.1.2.e 5.1.2.e

Met belangstelling heb ik jouw rapportage "Evaluatie datalekken "gelezen en ik kan mij geheel vinden in de presentatie en terugkoppeling van de meest majeure issues van de evaluatie. Ook de door jouw gedane aanbevelingen kunnen mijn goedkeuring wegdragen. Veel succes met het vervolg!

Met hartelijke groet,

5.1.2.i 5.1.2.i

Beveiligingsambtenaar
Staf Griffier
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e |
E 5.1.2.e @tweedekamer.nl |
I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 6 april 2022 14:59
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl> 5.1.2.i 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i <5.1.2.e @tweedekamer.nl>; 5.1.2.i 5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2.i 5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Rapportage evaluatie datalekken

Beste collega's,

In januari jl. zijn jullie geïnterviewd over de aanpak van datalekken binnen de Tweede Kamer.
Bijgaand stuur ik jullie de rapportage die een weergave is van ieders input in deze interviews. Voor elk van de vier thema's die zijn besproken heb ik aanbevelingen geformuleerd.

Aan ieder van jullie het verzoek om de rapportage kritisch door te lezen. Herken je de weergave en kun je de aanbevelingen ondersteunen?
Na jullie kritische blik wordt de rapportage aangeboden aan de CIO (5.1.2.e), FG (5.1.2.e) en CISO (5.1.2.e 5.1.2.e).

Ik hoor het graag uiterlijk maandag 11 april a.s.. Je kunt je feedback in de tekst weergeven d.m.v. een opmerking of tekstvoorstel.
Alvast bedankt voor de medewerking.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e@tweedekamer.nl | | www.tweedekamer.nl

5.1.2.e

Onderwerp: Aanbieding verslag Evaluatie aanpak datalekken binnen de Tweede Kamer
Locatie: D3 koffiepleintje of kamer 5.1.2.e

Begin: do 14-4-2022 10:15
Einde: do 14-4-2022 10:30
Tijd weergeven als: Voorlopig

Terugkeerpatroon: (geen)

Vergaderingsstatus: Nog niet gereageerd

Organisator: 5.1.2.e
Verplichte deelnemers: 5.1.2.e 5.1.2.e ; 5.1.2.e ; 5.1.2.e

Beste 5.1.2.e en 5.1.2.e

Graag wil ik morgen het verslag van de Evaluatie aanpak datalekken binnen de Tweede Kamer aan jullie aanbieden. Het rapport voeg ik alvast als bijlage bij.
Ik hoop dat dit op deze korte termijn lukt.

Helaas is er geen zaaltje beschikbaar, daarom stel ik voor dit te doen op D3 koffiepleintje, of indien mogelijk op de kamer 5.1.2.e

Als dit tijdstip morgen niet uitkomt zal ik een moment na het meireces plannen.

Ik hoor graag van jullie.

Groet,
5.1.2.e

Aan : 5.1.2.i 5.1.2.i en 5.1.2.e
Van : 5.1.2.e en 5.1.2.e
d.d. : 14 april 2022
Betr. : Evaluatie aanpak datalekken binnen de Tweede Kamer

Beknopte samenvatting

Hierbij bieden wij jullie de Evaluatie aanpak datalekken binnen de Tweede Kamer aan.
Deze evaluatie is intern uitgevoerd middels interviews met een aantal sleutelfiguren binnen de Tweede Kamer. De interviews zijn afgenomen in de maand januari 2022.

Het doel van deze evaluatie is na te gaan in hoeverre de aanpak datalekken binnen de Tweede Kamer werkt en of deze aanpak (nog steeds) voldoet aan de wettelijke eisen. De aanbevelingen en verbeterpunten die voortvloeien uit deze evaluatie 5.1.2.e bedoeld om de aanpak waar nodig te verbeteren.

Uit de gesprekken met sleutelfiguren komt naar voren dat de kennis over en bewustwording van datalekken zeker is toegenomen in de afgelopen jaren. De geïnterviewden wijzen er echter op dat het heel belangrijk dat de kennis en bewustwording blijvend onder de aandacht blijft van alle ambtenaren binnen de Tweede Kamer. Zodat men een datalek weet te herkennen en ook weet hoe te handelen. Daarnaast geven geïnterviewden aan het belangrijk te vinden regelmatig geïnformeerd te worden over het soort datalekken dat zich heeft voorgedaan binnen de Tweede Kamer en de acties die zijn genomen.

De evaluatie heeft zich gericht op een viertal onderwerpen, te weten:

1. Kennis over datalekken binnen de Tweede Kamerorganisatie
2. Stappenplan datalekken Tweede Kamer
3. Samenstelling en rollen datalekteam
4. Analyse van de administratie van datalekken

In onderstaande rapportage komen deze vier onderwerpen achtereenvolgens aan de orde en worden per onderwerp een aantal aanbevelingen gedaan.

Deze aanbevelingen zullen in de periode april – december 2022 door het datalekteam worden opgepakt en omgezet in concrete acties. In de AVG jaarrapportage 2022 zullen de resultaten van deze acties worden meegenomen. (Geïnterviewde) sleutelfiguren zullen bij de uitwerking van de aanbevelingen worden betrokken.

Rapportage van de evaluatie Aanpak datalekken binnen de
Tweede Kamerorganisatie
Looptijd 1 december 2021 – eind februari 2022

1. Inleiding

Per 1 januari 2016 is de 'Wet Meldplicht Datalekken' in werking getreden. Op grond van deze wet zijn organisaties (zowel ondernemingen als overheden) verplicht om direct melding te doen bij de Autoriteit Persoonsgegevens (AP) van een 'inbreuk in verband met persoonsgegevens' (hierna: datalek). Zo'n datalek moet ruim worden geduid. Het betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens. Het is daarbij niet van belang of er passende technische of organisatorische beschermingsmaatregelen waren getroffen of niet. Een datalek kan zich in beide situaties voordoen en doet zich sneller voor dan vaak gedacht. Een datalek kan bestaan uit een gerichte inbreuk door hackers of een technisch beveiligingsprobleem, maar er is ook sprake van een (mogelijk) datalek indien een laptop, telefoon, tablet, USB-stick of andere gegevensdrager is verloren of gestolen. Er is ook sprake van een (mogelijk) datalek indien op een gegevensdrager een of andere 'malware' wordt aangetroffen. Deze en andere voorvallen dienen alle te worden gemeld bij de Autoriteit Persoonsgegevens, indien deze (mogelijk) leiden tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het is aan de organisatie zelf om te bepalen of dat het geval is.

Het is nu zes jaar na het van kracht zijn van de Wet Meldplicht datalekken. Een goed moment om te evalueren hoe de Tweede Kamer het proces rondom datalekken heeft ingericht en of dit (nog steeds) voldoet aan de eisen van de AVG.

2. Doel en opzet van het onderzoek evaluatie datalekken

Het doel van deze evaluatie is om te evalueren hoe de aanpak datalekken binnen de Tweede Kamer werkt en of deze aanpak (nog steeds) voldoet aan de wettelijke eisen. De aanbevelingen en verbeterpunten die voortvloeien uit deze evaluatie zijn bedoeld voor het datalekteam ter verbetering van de aanpak. Het onderzoek moet tevens aanbevelingen doen om de informatievoorziening over datalekken richting de sleutelfiguren binnen de Tweede Kamer te verbeteren.

De eindrapportage zal worden aangeboden aan de CIO, Functionaris Gegevensbescherming (FG) en CISO van de Tweede Kamer, die allen vanuit hun eigen rol een verantwoordelijkheid dragen voor datalekken binnen de Tweede Kamer.

De evaluatie is uitgevoerd door 5.1.2.e en 5.1.2.e en bestaat uit de volgende stappen:

- (Individuele) interviews van maximaal 45 minuten met sleutelfiguren;
- Formuleren aanbevelingen en verbeterpunten voortkomend uit de (individuele) interviews;
- Actualiseren van de informatie over datalekken o.a. op Plein2 en in TopDesk.
- Sleutelfiguren en AVG-contactpersonen trainen op het geactualiseerde proces.

In de evaluatie komen de volgende onderwerpen aan de orde:

1. Kennis over datalekken binnen de Tweede Kamerorganisatie
   Is er voldoende kennis binnen de diensten van de Tweede Kamer over wat een datalek is? Weet men de informatie op Plein2 te vinden en toe te passen? Welke middelen/platforms gebruiken we om de kennis en bewustwording te borgen?

2. Stappenplan datalekken Tweede Kamer
   De Autoriteit Persoonsgegevens heeft een praktisch stappenplan opgesteld dat moet worden doorlopen bij een (potentieel) datalek. Aan de orde komen vragen als.: worden alle noodzakelijke stappen doorlopen indien er binnen de Tweede Kamer sprake is van een (potentieel) datalek? Is voldoende duidelijk welke informatie door wie bij elke stap moet worden opgevraagd en geanalyseerd? Wie zorgt voor de noodzakelijke maatregelen om het datalek te dichten? Welke criteria hanteert de Tweede Kamer bij het wel/niet melden bij de AP en/of betrokkene? Wie doet de daadwerkelijke melding bij AP en/of betrokkene? Wie zorgt voor het opnemen van de meldingen van (potentiële) datalekken in het datalekregister?

3. Samenstelling en rollen datalekteam
   Het Datalekteam van de Tweede Kamer komt in actie zodra er een incident wordt gemeld bij 5.1.2.i (Service Desk (SD)) waar persoonsgegevens bij zijn betrokken. Gekeken wordt naar samenstelling, grootte en rollen binnen het datalekteam. Het huidige datalekteam bestaat uit zeven personen. Welke rollen zijn te onderscheiden binnen het datalekteam, en welke rollen zijn noodzakelijk? Hoe verloopt de samenwerking en communicatie tussen SD, SET en datalekteam?

4. Analyse van de administratie van datalekken
   Datalekken moeten verplicht worden geregistreerd in het datalekregister. De Tweede Kamer heeft een datalekregister ingericht in TopDesk. Voldoet het datalekregister van de Tweede Kamer aan de verplichtingen van de AVG? Biedt het huidige datalekregister voldoende kennis en inzichten om trends en ontwikkelingen te signaleren? Wordt de administratie ook voor dit doel gebruikt, bijvoorbeeld door de FG? Wie is verantwoordelijk voor het bijhouden van het datalekregister?

Planning van het onderzoek

1e helft december	Versturen uitnodigingen interviews aan sleutelfiguren
2e helft dec 2021 – 1e helft 5.1.2.e 2022	Afname interviews
eind januari 2022	Bespreken interview resultaten, groepssessie geïnterviewden 1e
helft februari 2022	Formuleren conclusies en vervolgstappen
eind februari 2022	Presentatie eindrapport aan FG, CISO en CIO
maart 2022 – december 2022	Aanbevelingen nader uitwerken en verbeterpunten uitvoeren

3. Bevindingen en aanbevelingen

Er zijn in totaal 10 interviews met verschillende sleutelfiguren afgenomen. Voor de lijst met geïnterviewde personen, zie bijlage 1. Hieronder worden per onderwerp de aanbevelingen en verbeterpunten weergegeven die uit deze interviews naar voren zijn gekomen.

3.1 Kennis over datalekken binnen de Tweede Kamerorganisatie

De geïnterviewden geven in ruime meerderheid aan dat het belangrijk is dat iedereen binnen de Tweede Kamerorganisatie weet wat een datalek is en tevens weet hoe gehandeld moet worden. Zo geeft de Service Desk (SD) van de Tweede Kamer aan dat melders van verlies of diefstal van apparatuur als telefoon, laptop of tablet zich meestal niet bewust zijn dat dit een datalek is. Verlies of diefstal wordt gemeld om een nieuw apparaat te krijgen en niet omdat er sprake is van een (potentieel) datalek.
Qua kennis over en bewustwording van datalekken is in de afgelopen jaren zeker vooruitgang geboekt. Ook het datalekteam heeft inmiddels meer kennis en ervaring opgedaan over (potentiële) datalekken. Op Plein2 is informatie over datalekken te vinden en staat een op maat gemaakte e-learning. Het is onduidelijk hoe vindbaar deze informatie is voor medewerkers van de Tweede Kamer en hoe vaak deze informatie geraadpleegd wordt. Geïnterviewden geven aan dat er behoefte is aan meer duiding en voorbeelden van datalekken die kunnen voorkomen binnen de Tweede Kamer. Zij geven aan dat dit de herkenbaarheid van datalekken aanzienlijk zal verhogen.

Belangrijk aandachtspunt voor de Tweede Kamer is dat er jaarlijks maar weinig datalekken worden gemeld[1]. Geïnterviewden denken dat dit komt omdat men zich niet bewust is dat het belangrijk en verplicht is een datalek te melden. Men richt zicht vooral op het herstellen van het datalek.

Het is echter reëel te veronderstellen dat er jaarlijks (veel) meer datalekken plaatsvinden binnen de Tweede Kamer, zoals bijvoorbeeld verkeerde emailadressering, ongeautoriseerde toegang tot informatie en langer bewaren van persoonsgegevens dan noodzakelijk. Het risico van het niet registreren/melden van datalekken is dat dit kan leiden tot een boete van de AP en reputatieschade voor de Tweede Kamer.

Het jaarlijkse aantal gemelde datalekken binnen de Tweede Kamer laat dus een dalende trend zien. Dit is tegengesteld aan de ontwikkeling die de AP laat zien in de jaarlijkse rapportage datalekken. Bovendien wordt binnen de Tweede Kamer vooral melding gedaan van vermiste/gestolen apparaten, terwijl de AP in de jaarlijkse rapportages aangeeft dat de meest voorkomende datalekken ontstaan door menselijke fouten, zoals een e-mail verstuurd aan de verkeerde ontvanger. Dit soort datalekken worden bij de Tweede Kamer sporadisch gemeld.

Het verdient aanbeveling om de Kamerambtenaren via de sleutelfiguren aan te sporen om datalekken te melden bij 5.1.2.i Een ludieke actie als het uitloven van een taart bij elk 10e gemelde datalek zou daarbij als aansporing kunnen helpen. Daarnaast kan de kennis over datalekken via een e-learning, een quiz op Plein2 of een escaperoom met het thema datalekken blijvend onder de aandacht worden gebracht en bijdrage aan hoger aantal meldingen.

Aanbevelingen

- Kennis over en bewustwording van (potentiële) datalekken moet blijvend aandacht krijgen.
- Actuele kennis over datalekken die zich hebben voorgedaan regelmatig delen met sleutelfiguren zoals het MT van de Tweede Kamer, diensthoofden, AVG-contactpersonen, medewerkers SD, Security Awareness Officer en de Servicemanagers Dienst Automatisering.
- Hetzelfde geldt voor de technische en/of organisatorische maatregelen die zijn genomen om herhaling van deze datalekken te voorkomen.

[1] In 2019 – 52 gemelde datalekken; In 2020 – 39 gemelde datalekken; In 2021 - 49 gemelde datalekken; t/m maart2022 - 7 gemelde datalekken.

3.2 Stappenplan datalekken Tweede Kamer

De SD is de eerste lijn waar datalekken moeten worden gemeld. Daar wordt een inschatting gemaakt of het om een potentieel datalek gaat. De SD zet gemelde potentiele datalekken vervolgens door naar het datalekteam. De SD maakt hierbij gebruik van een sjabloon, bestaande uit een aantal standaardvragen. De SD geeft aan dat de kennis van SD-medewerkers over datalekken vooral is gericht op IT-meldingen en digitale datalekken. De SD wil het sjabloon samen met de PO/FG evalueren op duidelijkheid, juistheid en volledigheid.

De SD geeft aan dat de gevraagde informatie op het meldformulier Datalekken erg uitgebreid is. Dit leidt tot geringe bereidheid om dit formulier in te vullen. De SD vraagt zich af of het webformulier vereenvoudigd kan worden. Na de melding bij de SD kan immers indien nodig nadere informatie worden opgevraagd bij de melder. Voorts oppert de SD dat een stroomschema "Wat is een datalek" en "Wat moet je doen bij een datalek" bij kan dragen aan de verhoging van de kennis en aan verdere bewustwording. Ook terugkoppeling van de categorieën datalekken aan sleutelfiguren2 kan hierbij helpen.

Een ander punt dat geïnterviewden aangeven is dat het belang van de aanpak van beveiligingsincidenten en datalekken voor de Tweede Kamerorganisatie gelijk is. De huidige werkwijze is echter dat eerst team Beveiligingsincidenten aan de slag gaat en daarna het Datalekteam. Dit leidt tot het risico dat een datalek mogelijk te laat worden onderkend en vervolgens te laat gemeld wordt bij de AP. Nauwere samenwerking en directere communicatie met team Beveiligingsincidenten kan dit risico verkleinen. Het verdient aanbeveling te onderzoeken welke nadere samenwerking mogelijk is tussen team Beveiligingsincidenten en het Datalekteam.

Voor medewerkers van de Tweede Kamer is de melding van een (potentieel) datalek bij de SD meestal de belangrijkste stap. De SD zorgt er (mede) voor dat het datalek wordt gedicht. Het is van belang dat de andere (verplichte!) stappen ook voldoende aandacht krijgen, zoals het wel/niet melden bij de AP, het wel/niet melden aan de betrokkene, de registratie van het datalek en de terugkoppeling naar de melder. In paragraaf 3.4 wordt hier nader op ingegaan.

Niet elk datalek hoeft aan de AP en/of betrokkene te worden gemeld. Melding bij de AP hoeft slechts te worden gedaan indien een datalek leidt tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als daarop een aanzienlijke kans bestaat. Melding aan betrokkene moet worden gedaan indien aannemelijk is dat de inbreuk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de persoon op wie deze gegevens betrekking hebben. Het is niet altijd duidelijk wat voor de Tweede Kamerorganisatie de criteria zijn om een datalek te melden bij AP en/of betrokkene. Dit moet nader worden uitgewerkt en geformuleerd.

Tot slot wordt door een geïnterviewde opgemerkt dat voor de meldingen van beveiligingsincidenten en datalekken eenzelfde systeem wordt gebruikt, te weten TopDesk. Per incident kan echter maar één oplosgroep aan het incidenten worden gehangen, terwijl een datalek altijd ook een beveiligingsincident is. Mogelijke gevolgen zijn o.a. langs elkaar heen werken, dubbel werk en overschrijding van de wettelijke termijn voor het melden van een datalek bij de AP.

[2] Sleutelfiguren zoals het MT van de Tweede Kamer, diensthoofden, Avg-contactpersonen, medewerkers SD, 5.1.2.i Awareness Officer en Servicemanagers Dienst Automatisering

Aanbevelingen

- Evalueer samen met de SD het sjabloon dat de SD gebruikt bij de eerste inschatting of er sprake is van een (potentieel) datalek. Wordt alle noodzakelijke informatie uitgevraagd?
- Evalueer het meldformulier datalekken Wordt er voldoende informatie uitgevraagd? Welke informatie ontbreekt? Nodigt het formulier de melder uit om in te vellen?
- Stel een duidelijk stroomschema op voor herkennen van een (potentieel) datalek bij de Tweede Kamer. En voeg duidelijke criteria en herkenbare voorbeelden toe.
- Onderzoek de mogelijkheden om team beveiligingsincidenten en Datalekteam te laten samenwerken en mogelijk te integreren. Dit zorgt voor tijdswinst en voorkomt langs elkaar heen werken en dubbel werk. Bovendien verkleint het de kans op overschrijding van de wettelijke termijn meldplicht bij de AP.
- Stel criteria en voorbeelden op van datalekken binnen de Tweede Kamer die bij AP en/of betrokkene moeten worden gemeld.
- Rapporteer regelmatig aan de sleutelfiguren welke datalekken zich hebben voorgedaan binnen de Tweede Kamer, zodat er een beter beeld is van het soort datalekken binnen de Tweede Kamer en wat de impact is op betrokkenen.

3.3 Samenstelling en rollen datalekteam

Het datalekteam bestaat momenteel uit zeven personen[3]. Dit aantal is in de loop van de tijd zo gegroeid zonder aanwijsbare reden voor het toevoegen van deze personen aan het datalekteam. Zo is onduidelijk waarom BVA, Security Officer, Security Architect en CISO deel uitmaken van het team dat in eerste instantie beoordeelt of er sprake is van een datalek.
Daarnaast wordt geconstateerd dat bij de leden van de huidige datalekteam verschillende urgentie is om te reageren op een melding. Ook blijken datalekmeldingen niet altijd (tijdig) afgesloten te worden.

Het team dat zich bezighoudt met beveiligingsincidenten werkt met een klein kernteam dat naar gelang het incident met verschillende personen kan worden uitgebreid. Geadviseerd wordt om het datalekteam in te krimpen en bij de eerste incidentmelding te starten met een klein kernteam bestaande uit FG, PO en aangevuld met een medewerker privacy-ondersteuning. Dit kernteam bepaalt of er sprake is van een datalek, naar welke oplosgroep het datalek moet worden opgeschaald en wie deel moet uitmaken van die oplosgroep. De privacymedewerker zorgt voor het in gang zetten van de noodzakelijke acties zoals het bijeenroepen van de oplosgroep en het verzamelen en documenteren van de noodzakelijke informatie en de communicatie. De behandeling en afhandeling van datalekken zal met deze aanpak veel efficiënter verlopen en het risico op overschrijding van wettelijke termijnen (zoals het binnen 72 uur melden van een datalek bij de AP) aanzienlijk doen verminderen. Ook wordt voorgesteld om beide kernteams (team Beveiligingsincidenten en Datalekteam) beter te laten samenwerken en wellicht te integreren bij elke incidentmelding, om in een zo vroeg mogelijk stadium samen te bepalen of er behalve een beveiligingsincident ook sprake is van een datalek.

Aanbevelingen

- Beperk het datalekteam tot een kern van drie personen, bestaande uit FG, PO en een medewerker privacy-ondersteuning

---

[3] 5.1.2.e (5.1.2.i), 5.1.2.e (5.1.2.i), 5.1.2.e (CISO), 5.1.2.e (5.1.2.i 5.1.2.i), 5.1.2.e (5.1.2.i 5.1.2.i), 5.1.2.e (5.1.2.i) en 5.1.2.e (plv. 5.1.2.i).

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 20 april 2022 13:10
Aan: 5.1.2.e
Onderwerp: RE: Rapportage evaluatie datalekken

Ha 5.1.2.e

Dank voor je feedback.
Dit nemen we mee bij de actiepunten, te weten in het overleg met de medewerkers van de SD.

Met vriendelijke groet,

5.1.2.e

5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
Kamer 5.1.2.i
E 5.1.2.e@tweedekamer.nl | | www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e@tweedekamer.nl>
Verzonden: dinsdag 19 april 2022 17:37
Aan: 5.1.2.e <5.1.2.e@tweedekamer.nl>
Onderwerp: RE: Rapportage evaluatie datalekken

Beste 5.1.2.e

Zojuist heb ik kans gehad om het mooie document door te lezen. Mijn feedback komt wat verlaat, maar vereist geen aanpassingen aan het document.
Misschien ten overvloede, want ik geloof dat het volgende zeker gedekt wordt door de tekst, maar roep graag in herinnering, dat we winst kunnen maken als we de standaardoplossing **"Intrekken verzonden email"** uitbreiden.
Daar zou bijv. een automatische stap in kunnen, waarbij we escaleren ter beoordeling van een potentieel datalek, zoals we dat ook in de oplossing potentieel datalek doen. We krijgen overigens maar beperkt het verzoek te helpen bij het intrekken van mails, maar alle kleine beetjes helpen.

Met vriendelijke groet,

5.1.2.e
Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

Van: 5.1.2.e <5.1.2.e@tweedekamer.nl>
Verzonden: woensdag 6 april 2022 14:59

Aan: 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2i 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2i <5.12e @tweedekamer.nl>; 5.1.2e 5.12 <5.12.e @tweedekamer.nl>; 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2i <5.1.2e @tweedekamer.nl>; 5.1.2i <5.1.2e @tweedekamer.nl>; 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2i <5.1.2e @tweedekamer.nl>; 5.1.2i 5.1.2e @tweedekamer.nl>; 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2e <5.1.2e @tweedekamer.nl>; 5.1.2e 5.1 <5.1.2e @tweedekamer.nl>; 5.1.2e <5.1.2e @tweedekamer.nl>
CC: 5.1.2e <5.1.2e @tweedekamer.nl>
Onderwerp: Rapportage evaluatie datalekken

Beste collega's,

In januari jl. zijn jullie geïnterviewd over de aanpak van datalekken binnen de Tweede Kamer.
Bijgaand stuur ik jullie de rapportage die een weergave is van ieders input in deze interviews. Voor elk van de vier thema's die zijn besproken heb ik aanbevelingen geformuleerd.

Aan ieder van jullie het verzoek om de rapportage kritisch door te lezen. Herken je de weergave en kun je de aanbevelingen ondersteunen?
Na jullie kritische blik wordt de rapportage aangeboden aan de CIO (5.1.2e), FG (5.1.2e) en CISO (5.1.2e 5.1.2e).

Ik hoor het graag uiterlijk maandag 11 april a.s.. Je kunt je feedback in de tekst weergeven d.m.v. een opmerking of tekstvoorstel.
Alvast bedankt voor de medewerking.

Met vriendelijke groet,

5.1.2e

5.1.2e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten Generaal

Postbus 20018, 2500 EA
T 5.1.2e | +5.1.2e
Kamer 5.1.2e
E 5.1.2e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 11 augustus 2022 18:23
Aan: 5.1.2.e
CC: TK-DA-SD-Coordinatie; 5.1.2.e
Onderwerp: Evaluatie/afstemming gezamelijke afhandeling potentiele datalekken Servicedesk Datalekteam I2208 0240

Beste 5.1.2.e beste collega's van het datalekteam,

In het kader van kwaliteitsbewaking van onze gezamenlijke procedure stel ik voor samen te kijken naar I2208 0240.
Het lijkt mij een goed idee het datalekteam te laten zien welke informatie wij uit welke systemen kunnen halen, zodat het datalekteam weet wat de waarde daarvan is.
Bijv:
1. Welke informatie heeft vodafone voor ons over het laatste verbruik?
2. Wat gebeurt er en ik welke volgorde als wij een toestel de opdracht versturen zichzelf te wissen?
3. Welke verschillende "opties" hebben wij tussen modellen en installaties van toestellen?

Een andere overweging die ik graag bespreek is of er tussen de verschillende handelingen een verschillende prioriteit is.
Wat er in het geval van drukte op de Servicedesk prioriteit heeft. Een potentieel Datalek is een arbeidsintensieve procedure en een belangrijke procedure.
Het is daarom belangrijk daar een helder beeld bij te hebben, als servicedesk en als organisatie.

Met vriendelijke groet,

5.1.2.e 5.1.2.e

5.1.2.i
Dienst Automatisering
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(5.1.2.i | + (5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Wat is een (potentieel) datalek?
Een potentieel datalek is een incident waarbij persoonsgegevens, waarvoor de Tweede Kamerorganisatie verantwoordelijk is, zijn gelekt naar personen of instanties die geen toegang mogen hebben tot deze persoonsgegevens. Ook het verloren gaan of wijzigen/beschadigen van deze persoonsgegevens valt onder datalekken.
Fractiemedewerkers en Tweede Kamerleden zijn zelf verantwoordelijk voor de persoonsgegevens die zij verwerken. Een potentieel datalek bij een fractie/Kamerlid is geen datalek voor de Tweede Kamerorganisatie. De Privacy Officer kan fracties desgewenst adviseren.

Voorbeelden van potentiele datalekken

1. Iemand meldt dat hij een datadrager kwijt is en/of is gestolen. Denk aan een telefoon, IPad, Laptop of USB-stick.

2. Iemand meldt een gevonden datadrager, zoals telefoon, IPad, laptop of USB-stick

3. Iemand meldt een verkeerde autorisatie, waardoor iemand mogelijk onbedoelde toegang heeft gekregen tot persoonsgegevens.

4. Iemand meldt een verkeerd geadresseerde e-mail te hebben verzonden (intern of extern).

5. Een leverancier of FAB meldt dat er een incident is met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk voor is.

6. Overige meldingen van een incident met persoonsgegevens, waarbij de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegeven:
   a. Gevonden papieren dossier met persoonsgegevens in vergaderzaal Tweede Kamer
   b. Papieren document met persoonsgegevens in openstaande prullenbak of op/naast printer
   c. Onbedoelde vermelding van persoonsgegevens door de Tweede Kamerorganisatie op internet bijvoorbeeld op www.tweedekamer.nl

---
******

Welke acties moet de SD uitvoeren bij een melding van een (potentieel) datalek

Per categorie datalekken staat hieronder het stappenplan met uit te voeren acties

1. **Iemand meldt dat hij een datadrager kwijt is en/of is gestolen. Denk aan een telefoon, Ipad, Laptop of USB-stick.**

   Acties:
   a. SD stelt de volgende vragen aan de melder:
      - Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of met identieke cijfers (bv. 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
      - Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
      - Is het toestel al online geweest na de ontvreemding/vermissing?
      Antwoorden op bovenstaande vragen in TOPdesk toevoegen aan het incident

b. Wordt de datadrager gebruikt om toegang te krijgen tot de Tweede Kamer werkomgeving, zoals e-mail, agenda, contactpersonen, en/of dataopslag voor de Tweede Kamer?
Zo ja, dan de datadrager voorzien zijn van MDM. Voer met toestemming van de eigenaar een partiële wipe uit (hierbij wordt alleen de Kamerinformatie, e-mail en Kamerapps gewist) of een volledige wipe (de hele telefoon wordt gewist, dus ook eventuele privédata).
Antwoord op bovenstaande vragen in TOPdesk toevoegen aan het incident

Let op: De SD kan op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

c. Is de melder iemand uit de ambtelijke organisatie?
Het incident wordt in behandeling genomen door het datalekteam van de Tweede Kamer. Stuur melder het Formulier melding datalek om in te vullen en terug te sturen.

d. Is de melder iemand van een fractie (medewerker, Kamerlid)?
Dan moet de fractie of het Kamerlid het (potentiële) datalek behandelen. Het incident hoeft niet te worden geregistreerd in TOPdesk. De melder kan desgewenst advies vragen aan de Privacy Officer van de Tweede Kamer.

2. Iemand meldt een gevonden datadrager, zoals telefoon, IPad, laptop of USB-stick

Acties:
Op Plein2 staat: Gevonden voorwerpen kunnen worden ingeleverd bij één van de beveiligingsloges in het pand. Vanuit hier wordt een centrale registratie bijgehouden.

--------→ Onderstaande vragen beantwoorden:
- Wat moet worden gedaan met een gevonden datadrager? Naar SD of naar Beveiligingsdienst?
- Is een gevonden datadrager een potentieel datalek voor de TK? Zo ja, moet dit incident worden opgenomen in TOPdesk als potentieel datalek en worden voorgelegd aan het datalekteam?

3. Iemand meldt een verkeerde autorisatie, waardoor iemand onbedoeld toegang heeft gekregen tot persoonsgegevens.

Acties:
- Het feit dat iemand onbedoeld toegang heeft gekregen tot persoonsgegevens door een verkeerde autorisatie wordt opgevat als potentieel datalek. Stuur melder het Formulier melding datalek om in te vullen en terug te sturen.
- Het Datalekteam zal vervolgens beoordelen of sprake is van een datalek.

4. Iemand meldt een verkeerd geadresseerde e-mail te hebben verzonden

Acties:
a. Help de melder allereerst met het intrekken van de e-mail.
Informeer melder over de beperkingen van het intrekken van een e-mail, zodat melder kan inschatten wat de risico's zijn.
b. Zijn er persoonsgegevens betrokken bij de verkeerd geadresseerde e-mail?
Zo ja, dan is er sprake van een potentieel datalek.
c. Is de verzender van de foutief geadresseerde e-mail werkzaam binnen de ambtelijke organisatie?
Zo ja, dan is er sprake van een potentieel datalek voor de Tweede Kamerorganisatie. Zet het incident in TOPdesk en stuur melder het Formulier melding datalek om in te vullen en terug te sturen. Het datalekteam zal beoordelen of sprake is van een datalek.

d. Is de verzender van de foutief geadresseerde e-mail werkzaam bij een fractie of is het een Kamerlid?
Zo ja, dan is het een potentieel datalek voor de fractie of voor het Kamerlid. Het incident hoeft niet te worden geregistreerd in TOPdesk. De melder kan desgewenst advies vragen aan de Privacy Officer van de Tweede Kamer.
e. Is de e-mail foutief verzonden naar iemand binnen de Tweede Kamerorganisatie of buiten de Tweede Kamerorganisatie? Het antwoord is nodig om de ernst van het incident te kunnen bepalen.
f. Registreer de antwoorden op bovenstaande vragen in TOPdesk. Het datalekteam zal beoordelen of het een datalek is.

5. **Een leverancier of FAB meldt dat er een incident is met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk voor is.**
Behandelen als potentieel datalek en onmiddellijk, dus zonder vertraging, doorzetten naar het datalekteam.
Stuur melder het Formulier melding datalek en voeg het ingevulde formulier toe aan TOPdesk. Het datalekteam zal beoordelen of sprake is van een datalek.

Let op: binnen 72 uur na de melding van het datalek moet het datalekteam beoordeelt hebben of het datalek aan de Autoriteit Persoonsgegevens moet worden gemeld.
--------→ SD heeft de volgende bereikbaarheid
Maandag t/m vrijdag 8:30 uur – 23:59 uur
Weekend en feestdagen 12:00 uur – 21:00 uur
Is dit voldoende bereikbaarheid voor de AVG? Buiten deze tijdstippen aansluiten bij piketdienst voor informatiebeveiligingsincidenten?

6. **Overige meldingen van een incident met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegeven:**
a. Gevonden papieren dossier met persoonsgegevens in vergaderzaal Tweede Kamer
b. Papieren document met persoonsgegevens in openstaande prullenbak of op/naast printer
c. Onbedoelde vermelding van persoonsgegevens door de Tweede Kamerorganisatie op internet bijvoorbeeld op www.tweedekamer.nl

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

---
******

Commented [5.1.2i]: Deze tekst staat in het huidige script. Weghalen?

Vervolgens moet de melder de volgende e-mail ontvangen van de SD:

Geachte ……,

Dank voor het melden van een incident waar persoonsgegevens bij zijn betrokken, een potentieel Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het datalek.

Commented [5.1.2.i]: Na melding dus ALTIJD een meldformulier datalekken sturen naar melder.

Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk,
De Dienst Automatisering draagt uw melding vervolgens ter verdere afhandeling over aan het Datalekteam. Dit team zal uw melding in behandeling nemen en u informeren over de voortgang en de afhandeling. Indien nadere informatie nodig is zal iemand van het team contact met u opnemen.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande leden van het datalekteam:

Mw. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.i
Mw. C 5.1.2.e 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

******

Het datalekteam krijgt vervolgens onderstaand bericht met de melding van het potentieel datalek en de antwoorden op de uitvraag die de SD heeft gedaan. De e-mail aan het Datalekteam bevat ook de link naar het incident in TOPdesk

Geacht Datalekteam

Melding met nummer: I2302 1326 is aan u overgedragen.

Het betreft : Melding datalek [door SD in te vullen: categorie datalek]

De SD stelt vast dat er bij het incident persoonsgegevens zijn betrokken en dat de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegevens. Er is derhalve sprake van een potentieel datalek.

De SD heeft de volgende acties uitgevoerd: Zie per categorie datalekken de acties hierboven. In de e-mail aan het datalekteam moeten de antwoorden op de uitgevoerde acties staan.

De SD draagt het potentieel datalek hiermee over aan het datalekteam ter beoordeling en behandeling.

Klik hier om naar het incident te gaan.

Vertrouwend u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

******

Tot slot moet er een e-mail naar melder worden gestuurd waarin de melder wordt geïnformeerd over de afhandeling van het datalek. Dit kan door verzending van een e-mail vergelijkbaar aan de afhandeling van een andere TOPdesk-melding, bv. I2302 1152

Geachte ……,

Betreft: uw melding van xx-xx-2023 met als onderwerp Potentieel datalek vanwege [invullen categorie datalek (bv verkeerd geadresseerde e-mail)] .

Hartelijk dank voor de melding van een potentieel datalek

- beknopte samenvatting wat er aan de hand was
- hoe is het incident opgelost
- welke maatregelen zijn genomen om herhaling te voorkomen

Heeft u nog vragen of opmerkingen? Neem dan contact op met de Servicedesk ICT. Dit kan telefonisch via nummer 5.1.2.i of door deze e-mail te beantwoorden.

Graag horen wij hoe u onze dienstverlening beoordeelt.
Door op één van onderstaande linkjes te klikken, wordt een nieuw e-mail window geopend.
U kunt de e-mail eventueel aanvullen met opmerkingen, de e-mail zal zowel naar 5.1.2.i als de DA-servicemanagers gestuurd worden.

 Tevreden	 Voldoende	 Ontevreden

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

- Laat het Datalekteam en het team Beveiligingsincidenten nauwer met elkaar samenwerken en onderzoek de mogelijkheden tot integratie van beide kernteams.

3.4 Analyse van de administratie van datalekken

De AVG verplicht organisaties om alle datalekken, ongeacht of deze moeten worden gemeld aan de AP en/of betrokkenen, te documenteren in een datalekregister. Het doel van het registreren is het leren van de datalekken die zich hebben voorgedaan, zodat deze in de toekomst zoveel mogelijk worden voorkomen. Een ander doel van het datalekregister is dat aan de Autoriteit Persoonsgegevens kan worden aangetoond dat datalekken daadwerkelijk worden gemonitord en opgevolgd.
Tot slot kan het datalekregister worden gebruikt door de FG van de Tweede Kamer om te rapporteren aan het MT, diensthoofden en andere sleutelfiguren binnen de Tweede Kamer over welke datalekken zich hebben voorgedaan. Uit deze jaarlijkse rapportage kunnen trends en ontwikkelingen worden gehaald en de rapportage kan worden vergeleken met de jaarrapportages die de AP maakt over datalekken. In de terugblik AVG 2019 en 2020 is voor het eerst aan het MT gerapporteerd over datalekken.

De administratie van de datalekken vindt binnen de Tweede Kamer plaats in TopDesk. Het bijhouden van het datalekregister is een arbeidsintensieve en tijdrovende klus.
Voorgesteld wordt om na te gaan wie de administratie van het datalekregister het beste bij kan houden. Daarnaast moet bekeken worden of de opzet van het register, zoals nu vormgegeven is in TopDesk, voldoet aan de verplichtingen van de AVG[4].

Tot slot wordt in zijn algemeenheid door de geïnterviewden opgemerkt dat er geen optimaal gebruik wordt gemaakt van de informatie uit het datalekregister. Gesuggereerd wordt om het register efficiënter in te zetten voor rapportage, analyse en informatiedeling met FG, AVG-contactpersonen, MT, diensthoofden en andere sleutelfiguren. Daarnaast is het aanbevelingswaardig om regelmatig met de security collega's van bureau CISO terug te kijken naar de datalekken die zich hebben voorgedaan en te bespreken wat er is gebeurd en welke maatregelen breed genomen zouden moeten worden. Datalekken komen immers altijd voort uit een security-incident.

Aanbevelingen

- Bepaal wie het datalekregister gaat bijhouden.
- Samen met de FG onderzoeken of het datalekregister van de Tweede Kamer voldoet aan de verplichtingen van de AVG.
- Onderzoeken hoe het datalekregister binnen de Tweede Kamer efficiënter kan worden ingezet voor analyse, rapportage en informatiedeling.

---

[4] De volgende informatie over een datalek moet worden gedocumenteerd:

- Een korte omschrijving van het datalek
- Datum waarop het datalek plaatsvond
- Wat er met de gegevens is gebeurd (zijn ze verloren gegaan, of door een onbevoegde ingezien, gekopieerd of gewijzigd?)
- Van welke groep(en) personen er gegevens gelekt zijn, en om hoeveel personen het gaat
- Om welke soorten gegevens het gaat
- De (mogelijke) gevolgen van de inbreuk (bijvoorbeeld een risico op identiteitsfraude of reputatieschade)
- De maatregelen die zijn genomen naar aanleiding van het lek. Welke actie is ondernomen om schade te voorkomen of zo veel mogelijk te beperken (bijvoorbeeld het op afstand wissen van gegevens, of het wijzigen van wachtwoorden. Maar ook: wat heeft u gedaan om te zorgen dat het niet nog een keer kan gebeuren?)

Bijlage 1 – Lijst van geïnterviewde personen

17 januari 2022 - 5.1.2.e 5.1.2.e en 5.1.2.e – Service Desk van de Dienst Automatisering

18 januari 2022 - 5.1.2.e – 5.1.2.i

18 januari 2022 - 5.1.2.e – 5.1.2.i 5.1.2.i

18 januari 2022 - 5.1.2.e – 5.1.2.i

18 januari 2022 - 5.1.2.e – 5.1.2.i

19 januari 2022 - 5.1.2.e en 5.1.2.e - Servicemanagers bij Dienst 5.1.2.e

19 januari 2022 - 5.1.2.e 5.1.2.i en 5.1.2.e (SD)

20 januari 2022 - 5.1.2.e - 5.1.2.i

20 januari 2022 - 5.1.2.e - functioneel 5.1.2.i 5.1.2.e

25 januari 2022 - 5.1.2.e – 5.1.2.e voor de 5.1.2.i

27 januari 2022 - 5.1.2.e – Beveiligingsambtenaar (BVA)

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 14 maart 2023 17:14
Aan: 5.1.2.e
CC: Functionaris gegevensbescherming
Onderwerp: voorstel nieuw script van de Servicedesk bij melding datalekken
Bijlagen: 0230301 SD en script datalekken.docx

Ha 5.1.2.e

Ik ben bezig met het actualiseren en verbeteren van het script van de SD bij melding datalekken.
In de bijlage tref je het voorstel aan. Vorige week heb ik overlegt met 5.1.2.e en hij heeft mij een aantal nuttige tips gegeven over het script dat gehanteerd wordt bij securitymeldingen bij de SD.

Wil jij meelezen met mijn voorstel en jouw feedback geven?
Graag met name kijken naar de tekst bij datalek categorie 2 en datalek categorie 5.
Hier stel ik vragen die beantwoord moeten worden. Ben benieuwd naar jouw antwoorden op deze vragen.

Na jouw feedback ga ik het script bespreken met 5.1.2.e van de ServiceDesk.

Met vriendelijke groet,

5.1.2.e

5.1.2.i
Tweede Kamer der Staten-Generaal

mijn werkdagen zijn maandag, dinsdag en woensdag

Postbus 20018, 2500 EA, Den Haag
5.1.2.i M 5.1.2.e
E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Docnr40

Wat is een (potentieel) datalek?
Een potentieel datalek is een incident waarbij persoonsgegevens, waarvoor de Tweede Kamerorganisatie verantwoordelijk is, zijn gelekt naar personen of instanties die geen toegang mogen hebben tot deze persoonsgegevens. Ook het verloren gaan of wijzigen/beschadigen van deze persoonsgegevens valt onder datalekken.
Fractiemedewerkers en Tweede Kamerleden zijn zelf verantwoordelijk voor de persoonsgegevens die zij verwerken. Een potentieel datalek bij een fractie/Kamerlid is geen datalek voor de Tweede Kamerorganisatie. De Privacy Officer kan fracties desgewenst adviseren.

Voorbeelden van potentiele datalekken

1. Iemand meldt dat hij een datadrager kwijt is en/of is gestolen. Denk aan een telefoon, IPad, Laptop of USB-stick.

2. Iemand meldt een gevonden datadrager, zoals telefoon, IPad, laptop of USB-stick

3. Iemand meldt een verkeerde autorisatie, waardoor iemand mogelijk onbedoelde toegang heeft gekregen tot persoonsgegevens.

4. Iemand meldt een verkeerd geadresseerde e-mail te hebben verzonden (intern of extern).

5. Een leverancier of FAB meldt dat er een incident is met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk voor is.

6. Overige meldingen van een incident met persoonsgegevens, waarbij de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegeven:
   a. Gevonden papieren dossier met persoonsgegevens in vergaderzaal Tweede Kamer
   b. Papieren document met persoonsgegevens in openstaande prullenbak of op/naast printer
   c. Onbedoelde vermelding van persoonsgegevens door de Tweede Kamerorganisatie op internet bijvoorbeeld op www.tweedekamer.nl

---
******

Welke acties moet de SD uitvoeren bij een melding van een (potentieel) datalek

Per categorie datalekken staat hieronder het stappenplan met uit te voeren acties

1. **Iemand meldt dat hij een datadrager kwijt is en/of is gestolen. Denk aan een telefoon, Ipad, Laptop of USB-stick.**

   Acties:
   a. SD stelt de volgende vragen aan de melder:
      - Is het toestel beveiligd met een serieel code (5.1.2.h+5.1.2.i of met identieke cijfers (bv. '5.1.2.h+5.1.2.i 5.1.2.h+5.1.2.i ?
      - Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
      - Is het toestel al online geweest na de ontvreemding/vermissing?
      Antwoorden op bovenstaande vragen in TOPdesk toevoegen aan het incident

b. Wordt de datadrager gebruikt om toegang te krijgen tot de Tweede Kamer werkomgeving, zoals e-mail, agenda, contactpersonen, en/of dataopslag voor de Tweede Kamer?
Zo ja, dan de datadrager voorzien zijn van MDM. Voer met toestemming van de eigenaar een partiële wipe uit (hierbij wordt alleen de Kamerinformatie, e-mail en Kamerapps gewist) of een volledige wipe (de hele telefoon wordt gewist, dus ook eventuele privédata).
Antwoord op bovenstaande vragen in TOPdesk toevoegen aan het incident

Let op: De SD kan op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

c. Is de melder iemand uit de ambtelijke organisatie?
Het incident wordt in behandeling genomen door het datalekteam van de Tweede Kamer. Stuur melder het Formulier melding datalek om in te vullen en terug te sturen.

d. Is de melder iemand van een fractie (medewerker, Kamerlid)?
Dan moet de fractie of het Kamerlid het (potentiële) datalek behandelen. Het incident hoeft niet te worden geregistreerd in TOPdesk. De melder kan desgewenst advies vragen aan de Privacy Officer van de Tweede Kamer.

2. Iemand meldt een gevonden datadrager, zoals telefoon, IPad, laptop of USB-stick

Acties:
Op Plein2 staat: Gevonden voorwerpen kunnen worden ingeleverd bij één van de beveiligingsloges in het pand. Vanuit hier wordt een centrale registratie bijgehouden.

--------→ Onderstaande vragen beantwoorden:
- Wat moet worden gedaan met een gevonden datadrager? Naar SD of naar Beveiligingsdienst?
- Is een gevonden datadrager een potentieel datalek voor de TK? Zo ja, moet dit incident worden opgenomen in TOPdesk als potentieel datalek en worden voorgelegd aan het datalekteam?

3. Iemand meldt een verkeerde autorisatie, waardoor iemand onbedoeld toegang heeft gekregen tot persoonsgegevens.

Acties:
- Het feit dat iemand onbedoeld toegang heeft gekregen tot persoonsgegevens door een verkeerde autorisatie wordt opgevat als potentieel datalek. Stuur melder het Formulier melding datalek om in te vullen en terug te sturen.
- Het Datalekteam zal vervolgens beoordelen of sprake is van een datalek.

4. Iemand meldt een verkeerd geadresseerde e-mail te hebben verzonden

Acties:
a. Help de melder allereerst met het intrekken van de e-mail.
Informeer melder over de beperkingen van het intrekken van een e-mail, zodat melder kan inschatten wat de risico's zijn.
b. Zijn er persoonsgegevens betrokken bij de verkeerd geadresseerde e-mail?
Zo ja, dan is er sprake van een potentieel datalek.
c. Is de verzender van de foutief geadresseerde e-mail werkzaam binnen de ambtelijke organisatie?
Zo ja, dan is er sprake van een potentieel datalek voor de Tweede Kamerorganisatie. Zet het incident in TOPdesk en stuur melder het Formulier melding datalek om in te vullen en terug te sturen. Het datalekteam zal beoordelen of sprake is van een datalek.

d. Is de verzender van de foutief geadresseerde e-mail werkzaam bij een fractie of is het een Kamerlid?
Zo ja, dan is het een potentieel datalek voor de fractie of voor het Kamerlid. Het incident hoeft niet te worden geregistreerd in TOPdesk. De melder kan desgewenst advies vragen aan de Privacy Officer van de Tweede Kamer.
e. Is de e-mail foutief verzonden naar iemand binnen de Tweede Kamerorganisatie of buiten de Tweede Kamerorganisatie? Het antwoord is nodig om de ernst van het incident te kunnen bepalen.
f. Registreer de antwoorden op bovenstaande vragen in TOPdesk. Het datalekteam zal beoordelen of het een datalek is.

5. **Een leverancier of FAB meldt dat er een incident is met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk voor is.**
Behandelen als potentieel datalek en onmiddellijk, dus zonder vertraging, doorzetten naar het datalekteam.
Stuur melder het Formulier melding datalek en voeg het ingevulde formulier toe aan TOPdesk. Het datalekteam zal beoordelen of sprake is van een datalek.

   Let op: binnen 72 uur na de melding van het datalek moet het datalekteam beoordeelt hebben of het datalek aan de Autoriteit Persoonsgegevens moet worden gemeld.
   --------→ SD heeft de volgende bereikbaarheid
   Maandag t/m vrijdag 8:30 uur – 23:59 uur
   Weekend en feestdagen 12:00 uur – 21:00 uur
   Is dit voldoende bereikbaarheid voor de AVG? Buiten deze tijdstippen aansluiten bij piketdienst voor informatiebeveiligingsincidenten?

6. **Overige meldingen van een incident met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegeven:**
   a. Gevonden papieren dossier met persoonsgegevens in vergaderzaal Tweede Kamer
   b. Papieren document met persoonsgegevens in openstaande prullenbak of op/naast printer
   c. Onbedoelde vermelding van persoonsgegevens door de Tweede Kamerorganisatie op internet bijvoorbeeld op www.tweedekamer.nl

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

---
******

Commented [6.12e]: Deze tekst staat in het huidige script. Weghalen?

Vervolgens moet de melder de volgende e-mail ontvangen van de SD:

Geachte ……,

Dank voor het melden van een incident waar persoonsgegevens bij zijn betrokken, een potentieel Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het datalek.

Commented [5.1.2.e]: Na melding dus ALTIJD een meldformulier datalekken sturen naar melder.

Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk,
De Dienst Automatisering draagt uw melding vervolgens ter verdere afhandeling over aan het Datalekteam. Dit team zal uw melding in behandeling nemen en u informeren over de voortgang en de afhandeling. Indien nadere informatie nodig is zal iemand van het team contact met u opnemen.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande leden van het datalekteam:

Mw. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

******

Het datalekteam krijgt vervolgens onderstaand bericht met de melding van het potentieel datalek en de antwoorden op de uitvraag die de SD heeft gedaan. De e-mail aan het Datalekteam bevat ook de link naar het incident in TOPdesk

Geacht Datalekteam

Melding met nummer: I2302 1326 is aan u overgedragen.

Het betreft : Melding datalek [door SD in te vullen: categorie datalek]

De SD stelt vast dat er bij het incident persoonsgegevens zijn betrokken en dat de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegevens. Er is derhalve sprake van een potentieel datalek.

De SD heeft de volgende acties uitgevoerd: Zie per categorie datalekken de acties hierboven. In de e-mail aan het datalekteam moeten de antwoorden op de uitgevoerde acties staan.

De SD draagt het potentieel datalek hiermee over aan het datalekteam ter beoordeling en behandeling.

Klik hier om naar het incident te gaan.

Vertrouwend u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

******

Tot slot moet er een e-mail naar melder worden gestuurd waarin de melder wordt geïnformeerd over de afhandeling van het datalek. Dit kan door verzending van een e-mail vergelijkbaar aan de afhandeling van een andere TOPdesk-melding, bv. I2302 1152

Geachte ……,

Betreft: uw melding van xx-xx-2023 met als onderwerp Potentieel datalek vanwege [invullen categorie datalek (bv verkeerd geadresseerde e-mail)] .

Hartelijk dank voor de melding van een potentieel datalek

- beknopte samenvatting wat er aan de hand was
- hoe is het incident opgelost
- welke maatregelen zijn genomen om herhaling te voorkomen

Heeft u nog vragen of opmerkingen? Neem dan contact op met de Servicedesk ICT. Dit kan telefonisch via nummer 5.1.2.i of door deze e-mail te beantwoorden.

Graag horen wij hoe u onze dienstverlening beoordeelt.
Door op één van onderstaande linkjes te klikken, wordt een nieuw e-mail window geopend.
U kunt de e-mail eventueel aanvullen met opmerkingen, de e-mail zal zowel naar 5.1.2.i als de DA-servicemanagers gestuurd worden.

		
Tevreden	Voldoende	Ontevreden

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

Docnr41

Wat is een (potentieel) datalek?
Een potentieel datalek is een incident waarbij persoonsgegevens, waarvoor de Tweede Kamerorganisatie verantwoordelijk is, zijn gelekt naar personen of instanties die geen toegang mogen hebben tot deze persoonsgegevens. Ook het verloren gaan of wijzigen/beschadigen van deze persoonsgegevens valt onder datalekken.
Fractiemedewerkers en Tweede Kamerleden zijn zelf verantwoordelijk voor de persoonsgegevens die zij verwerken. Een potentieel datalek bij een fractie/Kamerlid is geen datalek voor de Tweede Kamerorganisatie. De Privacy Officer kan fracties desgewenst adviseren.

Voorbeelden van potentiele datalekken

1. Iemand meldt dat hij een datadrager kwijt is en/of is gestolen. Denk aan een telefoon, IPad, Laptop of USB-stick.

2. Iemand meldt een gevonden datadrager, zoals telefoon, IPad, laptop of USB-stick

3. Iemand meldt een verkeerde autorisatie, waardoor iemand mogelijk onbedoelde toegang heeft gekregen tot persoonsgegevens.

4. Iemand meldt een verkeerd geadresseerde e-mail te hebben verzonden (intern of extern).

5. Een leverancier of FAB meldt dat er een incident is met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk voor is.

6. Overige meldingen van een incident met persoonsgegevens, waarbij de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegeven:
   a. Gevonden papieren dossier met persoonsgegevens in vergaderzaal Tweede Kamer
   b. Papieren document met persoonsgegevens in openstaande prullenbak of op/naast printer
   c. Onbedoelde vermelding van persoonsgegevens door de Tweede Kamerorganisatie op internet bijvoorbeeld op www.tweedekamer.nl

---
******

Welke acties moet de SD uitvoeren bij een melding van een (potentieel) datalek

Per categorie datalekken staat hieronder het stappenplan met uit te voeren acties

1. **Iemand meldt dat hij een datadrager kwijt is en/of is gestolen. Denk aan een telefoon, Ipad, Laptop of USB-stick.**

   Acties:
   a. SD stelt de volgende vragen aan de melder:
      - Is het toestel beveiligd met een serieel code (5.1.2.h+5.1.2.i of met identieke cijfers (bv. '5.1.2.h+5.1.2.i 5.1.2.h+5.1.2.i ?
      - Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
      - Is het toestel al online geweest na de ontvreemding/vermissing?
      Antwoorden op bovenstaande vragen in TOPdesk toevoegen aan het incident

b. Wordt de datadrager gebruikt om toegang te krijgen tot de Tweede Kamer werkomgeving, zoals e-mail, agenda, contactpersonen, en/of dataopslag voor de Tweede Kamer?
Zo ja, dan de datadrager voorzien zijn van MDM. Voer met toestemming van de eigenaar een partiële wipe uit (hierbij wordt alleen de Kamerinformatie, e-mail en Kamerapps gewist) of een volledige wipe (de hele telefoon wordt gewist, dus ook eventuele privédata).
Antwoord op bovenstaande vragen in TOPdesk toevoegen aan het incident

Let op: De SD kan op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

c. Is de melder iemand uit de ambtelijke organisatie?
Het incident wordt in behandeling genomen door het datalekteam van de Tweede Kamer. Stuur melder het Formulier melding datalek om in te vullen en terug te sturen.

d. Is de melder iemand van een fractie (medewerker, Kamerlid)?
Dan moet de fractie of het Kamerlid het (potentiële) datalek behandelen. Het incident hoeft niet te worden geregistreerd in TOPdesk. De melder kan desgewenst advies vragen aan de Privacy Officer van de Tweede Kamer.

2. Iemand meldt een gevonden datadrager, zoals telefoon, IPad, laptop of USB-stick

Acties:
Op Plein2 staat: Gevonden voorwerpen kunnen worden ingeleverd bij één van de beveiligingsloges in het pand. Vanuit hier wordt een centrale registratie bijgehouden.

--------→ Onderstaande vragen beantwoorden:
- Wat moet worden gedaan met een gevonden datadrager? Naar SD of naar Beveiligingsdienst?
- Is een gevonden datadrager een potentieel datalek voor de TK? Zo ja, moet dit incident worden opgenomen in TOPdesk als potentieel datalek en worden voorgelegd aan het datalekteam?

3. Iemand meldt een verkeerde autorisatie, waardoor iemand onbedoeld toegang heeft gekregen tot persoonsgegevens.

Acties:
- Het feit dat iemand onbedoeld toegang heeft gekregen tot persoonsgegevens door een verkeerde autorisatie wordt opgevat als potentieel datalek. Stuur melder het Formulier melding datalek om in te vullen en terug te sturen.
- Het Datalekteam zal vervolgens beoordelen of sprake is van een datalek.

4. Iemand meldt een verkeerd geadresseerde e-mail te hebben verzonden

Acties:
a. Help de melder allereerst met het intrekken van de e-mail.
Informeer melder over de beperkingen van het intrekken van een e-mail, zodat melder kan inschatten wat de risico's zijn.
b. Zijn er persoonsgegevens betrokken bij de verkeerd geadresseerde e-mail?
Zo ja, dan is er sprake van een potentieel datalek.
c. Is de verzender van de foutief geadresseerde e-mail werkzaam binnen de ambtelijke organisatie?
Zo ja, dan is er sprake van een potentieel datalek voor de Tweede Kamerorganisatie. Zet het incident in TOPdesk en stuur melder het Formulier melding datalek om in te vullen en terug te sturen. Het datalekteam zal beoordelen of sprake is van een datalek.

Commented [5.1.2.1]: Bij een USB-stick kunnen we vanzelfsprekend een stuk minder. Het is wel goed om te weten of er een wachtwoord op zit.

Commented [5.1.2.2]: Is daar een mailadres of telefoonnummer van/voor dat we kunnen doorgeven? Of moeten we naar de 3 a 4 personen uit de standaard mail verwijzen?

Commented [5.1.2.3]: Het lijkt me 5.2.1
5.2.1

Commented [5.1.2.4]: We zullen sowieso een incident maken, we loggen immers dat we iemand helpen, dan wel een vraag beantwoorden.

d. Is de verzender van de foutief geadresseerde e-mail werkzaam bij een fractie of is het een Kamerlid?
Zo ja, dan is het een potentieel datalek voor de fractie of voor het Kamerlid. Het incident hoeft niet te worden geregistreerd in TOPdesk. De melder kan desgewenst advies vragen aan de Privacy Officer van de Tweede Kamer.
e. Is de e-mail foutief verzonden naar iemand binnen de Tweede Kamerorganisatie of buiten de Tweede Kamerorganisatie? Het antwoord is nodig om de ernst van het incident te kunnen bepalen.
f. Registreer de antwoorden op bovenstaande vragen in TOPdesk. Het datalekteam zal beoordelen of het een datalek is.

5. **Een leverancier of FAB meldt dat er een incident is met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk voor is.**
Behandelen als potentieel datalek en onmiddellijk, dus zonder vertraging, doorzetten naar het datalekteam.
Stuur melder het Formulier melding datalek en voeg het ingevulde formulier toe aan TOPdesk. Het datalekteam zal beoordelen of sprake is van een datalek.

Let op: binnen 72 uur na de melding van het datalek moet het datalekteam beoordeelt hebben of het datalek aan de Autoriteit Persoonsgegevens moet worden gemeld.
--------→ SD heeft de volgende bereikbaarheid
Maandag t/m vrijdag 8:30 uur – 23:59 uur
Weekend en feestdagen 12:00 uur – 21:00 uur
Is dit voldoende bereikbaarheid voor de AVG? Buiten deze tijdstippen aansluiten bij piketdienst voor informatiebeveiligingsincidenten?

6. **Overige meldingen van een incident met persoonsgegevens waar de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegeven:**
a. Gevonden papieren dossier met persoonsgegevens in vergaderzaal Tweede Kamer
b. Papieren document met persoonsgegevens in openstaande prullenbak of op/naast printer
c. Onbedoelde vermelding van persoonsgegevens door de Tweede Kamerorganisatie op internet bijvoorbeeld op www.tweedekamer.nl

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

---
******

Commented [5.1.2.i(5]: Is daar een mailadres of telefoonnummer van/voor dat we kunnen doorgeven? Of moeten we naar de 3 a 4 personen uit de standaard mail verwijzen?

Commented [5.1.2.i]: Deze tekst staat in het huidige script. Weghalen?

Commented [5.1.2.i(7]: Deze tekst is in orde, er wordt een ander item aangemaakt in TOPdesk voor het verloren apparaat. Op deze manieren helpen we ervoor te zorgen, dat een apparaat dat wordt vervangen vanwege verlies of diefstal, ook door de datalekcheck gaat (vanuit die andere wijziging).

Commented [5.1.2.i(8]: Dit is dus alleen van toepassing bij de ambtenarij

Vervolgens moet de melder de volgende e-mail ontvangen van de SD:

Geachte ……,

Dank voor het melden van een incident waar persoonsgegevens bij zijn betrokken, een potentieel Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het datalek.

Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk,
De Dienst Automatisering draagt uw melding vervolgens ter verdere afhandeling over aan het Datalekteam. Dit team zal uw melding in behandeling nemen en u informeren over de voortgang en de afhandeling. Indien nadere informatie nodig is zal iemand van het team contact met u opnemen.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande leden van het datalekteam:

Mw. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

******

Het datalekteam krijgt vervolgens onderstaand bericht met de melding van het potentieel datalek en de antwoorden op de uitvraag die de SD heeft gedaan. De e-mail aan het Datalekteam bevat ook de link naar het incident in TOPdesk

Geacht Datalekteam

Melding met nummer: I2302 1326 is aan u overgedragen.

Het betreft : Melding datalek [door SD in te vullen: categorie datalek]

De SD stelt vast dat er bij het incident persoonsgegevens zijn betrokken en dat de Tweede Kamerorganisatie verantwoordelijk is voor deze persoonsgegevens. Er is derhalve sprake van een potentieel datalek.

De SD heeft de volgende acties uitgevoerd: Zie per categorie datalekken de acties hierboven. In de e-mail aan het datalekteam moeten de antwoorden op de uitgevoerde acties staan.

Commented 5.1.2.e **:** Kan of moet?

Commented [5.1.2.e **]:** Na melding dus ALTIJD een meldformulier datalekken sturen naar melder.

Commented 5.1.2.e **:** Bij het leveren van een nieuw toestel is het makkelijk het formulier ingevuld te ontvangen. Mochten er 'vertragingen' zijn, dan stel ik voor dat we dat escaleren naar het Datalekteam.

Commented [5.1.2.e **:** Dit is een goed punt ter bespreking met 5.1.2.e Het betreft hier extra werk voor de Service Desk. De beschrijving staat immers in het incident en deze dienst aan het datalek is een uitbreiding van scope en daarmee een (te bespreken) resourceclaim.

Ook kan dit een vertragende factor zijn.

N.B. Wanneer de melding complex is, valt deze niet onder de in het contract beschreven verantwoordelijkheden van de avond- en weekenddienst. We moeten dat dus goed controleren en afstemmen.

Commented 5.1.2.e **:** Ik neem aan dat we juist ook willen escaleren als we bepaalde antwoorden niet hebben kunnen verkrijgen, of er technische issues zouden zijn bij het versturen van een wis-opdracht (ter illustratie).

De SD draagt het potentieel datalek hiermee over aan het datalekteam ter beoordeling en behandeling.

Klik hier om naar het incident te gaan.

Vertrouwend u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

******

Tot slot moet er een e-mail naar melder worden gestuurd waarin de melder wordt geïnformeerd over de afhandeling van het datalek. Dit kan door verzending van een e-mail vergelijkbaar aan de afhandeling van een andere TOPdesk-melding, bv. I2302 1152

Geachte .....,

Betreft: uw melding van xx-xx-2023 met als onderwerp Potentieel datalek vanwege [invullen categorie datalek (bv verkeerd geadresseerde e-mail)] .

Commented 5.1.2.e : Uitbreiding, kijken of hier een technische oplossing voor is.

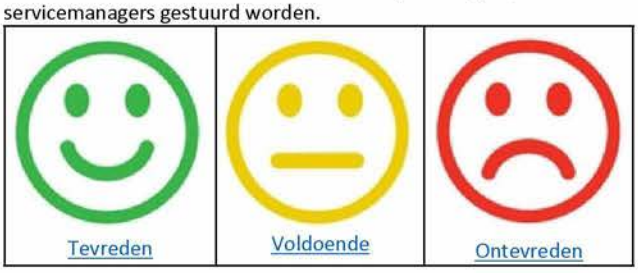
Hartelijk dank voor de melding van een potentieel datalek

- beknopte samenvatting wat er aan de hand was
- hoe is het incident opgelost
- welke maatregelen zijn genomen om herhaling te voorkomen

Commented [5.1.2.e : Deze input komt vanuit 5.2.1

Heeft u nog vragen of opmerkingen? Neem dan contact op met de Servicedesk ICT. Dit kan telefonisch via nummer 5.1.2.i of door deze e-mail te beantwoorden.

Graag horen wij hoe u onze dienstverlening beoordeelt.
Door op één van onderstaande linkjes te klikken, wordt een nieuw e-mail window geopend.
U kunt de e-mail eventueel aanvullen met opmerkingen, de e-mail zal zowel naar 5.1.2.i als de DA-servicemanagers gestuurd worden.



Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i@tweedekamer.nl

5.1.2.e

Onderwerp: script datalekken in TopDesk
Locatie: B67 zaaltje volgt

Begin: ma 24-4-2023 15:30
Einde: ma 24-4-2023 16:30
Tijd weergeven als: Voorlopig

Terugkeerpatroon: (geen)

Vergaderingsstatus: Nog niet gereageerd

Organisator: 5.1.2.e
Verplichte deelnemers: 5.1.2.e ; 5.1.2.e 5.1.2.e ; 5.1.2.e 5.1.2.i (5.1.2.e)

Ha 5.1.2.e 5.1.2.e en 5.1.2.e

Samen met de Servicedesk ben ik bezig het script voor datalekken in TopDesk te actualiseren.
Bijgaand de conceptversie.

Graag wil ik met 5.1.2.e en 5.1.2.e (ketenregie) en met 5.1.2.e (leveranciersmanager van de Servicedesk) afstemmen wat nodig hebben voor de implementatie.
Ik heb maandag 24 april een gaatje gevonden in ieders agenda.
Wil je mij laten weten of je aanwezig kunt zijn?
Bij voorkeur fysiek op B67.

Ik hoor graag van jullie.

5.1.2.e

Onderwerp: Aanbieding verslag Evaluatie aanpak datalekken binnen de Tweede Kamer
Locatie: Oudkamer D3.51

Begin: di 10-5-2022 11:00
Einde: di 10-5-2022 11:15
Tijd weergeven als: Voorlopig

Terugkeerpatroon: (geen)

Vergaderingsstatus: Nog niet gereageerd

Organisator: 5.1.2.e
Verplichte deelnemers: 5.1.2.e 5.1.2.e ; 5.1.2.e ; 5.1.2.e

Beste 5.1.2.e en 5.1.2.e

Het lukt toch niet om het rapport donderdag 14 april aan te bieden. Daarom hierbij een nieuw datumvoorstel. Volgens Outlook zou dit moeten lukken in jullie agenda's. Ik hoor het graag.

Groet,
5.1.2.e

AVG-beleid Tweede Kamerorganisatie periode 2018 - 2023

Inleiding

Deze notitie gaat over wat er binnen de Tweede Kamerorganisatie in de afgelopen vijf jaar bereikt is om te voldoen aan de AVG en waar nog uitdagingen liggen. De notitie is opgesteld door de Privacy Officer van de Tweede Kamer en dient om het MT te informeren over de stand van zaken.

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. De AVG gaat over informationele privacy en richt zich op het verwerken en verzamelen van persoonsgegevens. Persoonsgegevens betreft alle informatie die direct of indirect herleidbaar is naar een individueel persoon. Denk bijvoorbeeld aan NAW-gegevens, telefoonnummer, een foto, financiële gegeven en medische gegevens. Maar het houdt niet op bij zulke feitelijke gegevens: ook gegevens die een waardering over een persoon inhouden, bijvoorbeeld een verslag functioneringsgesprek, zijn persoonsgegevens. En de inhoud van een burgerbrief is te herleiden tot een persoon en dus ook een persoonsgegeven.

Tweede Kamer en de AVG

De Tweede Kamerorganisatie ondersteunt Tweede Kamerleden bij hun parlementaire taken en maakt het werk van de Tweede Kamer toegankelijk en inzichtelijk voor de samenleving. Kamerambtenaren zorgen onder meer voor verslaglegging, informatievoorziening, documentatie, archivering, beheer en beveiliging van het Kamergebouw, informatiebeveiliging, doelmatig en rechtmatig financieel beheer, personeelszaken en externe communicatie. Om dit werk te kunnen doen is het vaak noodzakelijk persoonsgegevens te verwerken van Kamerambtenaren, Kamerleden, fractiemedewerkers, burgers en bezoekers. Denk bijvoorbeeld aan persoonsgegevens die gebruikt worden voor de toegangspas, de uitvoering van het personeelsbeleid, restaurantrekeningen, nieuwsbrieven en uitgifte IT-middelen.
Daarnaast ondersteunt de ambtelijke organisatie de Tweede Kamerleden procedureel en inhoudelijk bij het constitutionele proces van medewetgeving en controle op het regeringsbeleid. Ook hier kunnen persoonsgegevens verwerkt worden, zoals de persoonsgegevens in burgerbrieven die naar de Tweede Kamer worden gestuurd. Op al deze processen van de Tweede Kamerorganisatie is de AVG van toepassing indien er persoonsgegevens betrokken zijn.

In het vastgestelde Privacybeleid van de Tweede Kamer staat:
“De Tweede Kamer wil (naast het voldoen aan alle wet- en regelgeving) zorgvuldig, veilig en rechtmatig omgaan met persoonsgegevens, waarbij de

belangen van betrokkenen zoveel mogelijk centraal staan. Uitgangspunt is dat steeds een weging plaatsvindt tussen de noodzaak voor het verwerken van persoonsgegevens en de gevolgen van deze verwerking voor de eigenaar van die gegevens, de betrokkene."

Ter waarborging van het privacybeleid heeft de Tweede Kamerorganisatie verschillende organisatorische, technische en fysieke maatregelen getroffen. Deze maatregelen bieden de kaders en handvatten voor medewerkers van de Tweede Kamerorganisatie om op de gewenste wijze te kunnen handelen wanneer het gaat om persoonsgegevens.

In deze notitie wordt nader op deze maatregelen ingegaan en geeft de Privacy Officer een oordeel over de stand van zaken.
Achtereenvolgens komen aan de orde:

1. Governance : Functionaris Gegevensbescherming (FG), contactpersonen AVG, eigenaarschap diensthoofden
2. AVG-register
3. Datalekken
4. DPIA
5. Rechten van betrokkenen
6. Privacy by design
7. Verwerkersovereenkomsten

Conclusies en aanbevelingen

Governance

Geadviseerd wordt om in 2023 extern onderzoek uitvoeren naar de stand van zaken AVG en de invulling van de verschillende rollen (FG, PO, AVG-contactpersoon), met speciale aandacht voor de mogelijkheid om de rol van FG extern te beleggen om zo de onafhankelijkheid en beschikbare tijd beter te kunnen waarborgen.
Daarnaast moet binnen elke dienst bekeken worden of de rol van AVG-contactpersoon bij de juiste persoon is belegd, namelijk bij iemand met voldoende overzicht over wat binnen de dienst wordt gedaan met persoonsgegevens.

AVG-register

In 2023 wordt verder gewerkt aan het actueel houden van het AVG-register en worden de mogelijkheden onderzocht om het register intern en/of extern te publiceren.

Datalekken
Er worden binnen de Tweede Kamerorganisatie jaarlijks weinig datalekken gemeld. Niet melden van datalekken is een overtreding van de AVG met als risico een boeteoplegging. Bijkomend risico is dat er niet wordt geleerd van fouten en rechten en vrijheden van betrokkenen mogelijk gevaar lopen.
De datalekprocedure moet bekend zijn binnen de hele organisatie en onderdeel van de dagelijkse werkzaamheden, zodat mogelijke fouten worden gecorrigeerd.

DPIA
Een DPIA is een beoordeling van de privacyrisico's van een verwerking van persoonsgegevens en benoemt de mogelijke maatregelen om die risico's te beperken. Een (beknopte) DPIA moet standaard worden meegenomen bij alle nieuwe processen waar persoonsgegevens bij zijn betrokken.

Rechten van betrokkenen
In 2023 en verder zal aandacht gegeven blijven worden aan de (borging van de) kennis over de rechten van betrokkenen en de procedures die hiervoor zijn ingericht.

Privacy by design / Privacy by default
Aanbevolen wordt om de verplichting in te stellen dat bij alle nieuwe diensten en projecten waar persoonsgegevens worden verwerkt standaard de PO te betrekken en waar nodig advies in te winnen bij de FG.

Verwerkersovereenkomst
2023 en verder zal het bepalen van de rol van verwerker en het maken van afspraken met een verwerker een belangrijk onderdeel zijn en blijven van de AVG-werkzaamheden. Er zal nader worden gewerkt aan de standaardisering van het bepalen van de rol van verwerker, als ook aan de uitbreiding van de kennis over de eigen rol van de diensten hierbij.

Nadere toelichting

1. Governance: hoe zijn de taken en verantwoordelijkheden voor de AVG belegd binnen de Tweede Kamerorganisatie?

De AVG raakt alle facetten van de Tweede Kamerorganisatie. Daarom moeten de taken en verantwoordelijkheden die voortvloeien uit de AVG binnen de hele Tweede Kamerorganisatie zijn belegd en ingebed. Dat betekent dat de hele Tweede Kamerorganisatie iets met de AVG moet doen en dus niet alleen de juridisch adviseur, de privacy officer en/of de Functionaris voor de Gegevensbescherming.

De verantwoordelijkheden voor de AVG zijn verdeeld via de bekende three lines of defence:
de 1ste lijn bestaat de de medewerkers die binnen de afdelingen of teams het eerste aanspreekpunt zijn over AVG. De 2e lijn bestaat uit de Privacy Officer

(PO) en de 3e lijn bestaat uit de Functionaris voor de Gegevensbescherming (FG).

Binnen de Tweede Kamerorganisatie zijn de taken en verantwoordelijkheden als volgt belegd:

Wie	**Rol**
Griffier van de Tweede Kamer	Heeft de rol van Verwerkingsverantwoordelijke voor alle verwerkingen van persoonsgegevens die binnen de Tweede Kamerorganisatie plaatsvinden
1e lijn	De ambtelijke diensten van de Tweede Kamer voeren het intern beheer uit voor de gegevensverwerking: • Het diensthoofd is namens de Griffier verantwoordelijk voor alle verwerkingen van persoonsgegevens die binnen de dienst plaatsvinden. • Elke dienst heeft minimaal één AVG-contactpersoon. De taken van de AVG-contactpersoon zijn: a. fungeren als 'adviesloket' bij vragen binnen de eigen dienst over de AVG; b. inventariseren, beoordelen, bijhouden en melden van verwerkingen persoonsgegevens; c. aanspreekpunt voor de FG bij incidenten (waaronder datalekken) en privacy verzoeken; d. zorgen dat de AVG blijvend onder de aandacht is van de medewerkers van de eigen dienst en draagt zo bij aan het privacy bewustzijn van de Tweede Kamer.
2e lijn	De Privacy Officer • Adviseert en ondersteunt de ambtelijke organisatie bij AVG-taken en vragen; • Adviseert bij afspraken met leveranciers; • Zorgt voor de uitvoering van een DPIA; • Begeleidt de AVG-contactpersonen van de diensten; • Adviseert bij verzoeken in het kader van de rechten van betrokkenen • Adviseert bij AVG-vragen en klachten • Stelt het AVG-beleid op • Zorgt voor kennisborging en bewustwording binnen de Tweede Kamerorganisatie

3e lijn	De Functionaris voor de Gegevensbescherming (FG) • houdt intern en onafhankelijk toezicht op de naleving van de AVG door de ambtelijke organisatie van de Tweede Kamer; • is contactpersoon voor de rechten van betrokkenen • adviseert op uitgevoerde DPIA's • is contactpersoon voor de Autoriteit Persoonsgegevens (AP)

Kamerfracties en Kamerleden hebben hun eigen verantwoordelijkheid voor de AVG

Kamerfracties zijn de Verwerkingsverantwoordelijke voor de persoonsgegevens die binnen de eigen fractie worden verwerkt, bijvoorbeeld ten behoeve van het eigen personeel en de eigen fractieorganisatie. Fracties moeten zelf zorgen dat al deze verwerkingen AVG-proof zijn en opgenomen worden in een eigen AVG-register. Kamerleden vallen hiërarchisch niet onder der fractieorganisatie en dus ook niet onder verwerkingsverantwoordelijkheid van de fractie. Elk Kamerlid is dan ook zelf als verwerkingsverantwoordelijke verantwoordelijk voor de verwerking van persoonsgegevens die bijvoorbeeld door burgers worden gestuurd in e-mails.

Aanbevelingen:

- De Tweede Kamer heeft een wettelijke verplichting om een FG aan te stellen. Deze functionaris moet voldoende tijd en middelen hebben om zijn taken onafhankelijk uit te kunnen voeren. De afgelopen jaren is gebleken dat de FG onvoldoende tijd heeft gehad om zijn rol goed uit te kunnen voeren. De vele juridische vraagstukken die tevens behandeld worden door de ambtenaar met de rol van FG verdringen de aandacht die de AVG nodig heeft. Bovendien bestaat het risico dat organisatiebelang de neutrale kijk verhinderd die voor de AVG nodig is.
- Laat in 2023 extern onderzoek uitvoeren naar de stand van zaken AVG binnen de Tweede Kamerorganisatie en de belegde rollen
- Management moet top-down met regelmaat aandacht vragen voor en informeren naar de naleving van de AVG binnen de ambtelijke organisatie. En diensthoofden laten rapporteren (bijvoorbeeld als onderdeel van de MARAP) over de stand van zaken binnen de diensten. FG moet hiervoor een checklist ontwikkelen
- Het is de taak van elk diensthoofd om regelmatig met de eigen AVG-contactpersoon te bespreken wat de stand van zaken is van de AVG. Dit helpt bij de borging van het AVG gedachtengoed en het initiëren van verbeteracties die voor de eigen dienst prioriteit hebben. De AVG-contactpersoon moet voldoende waardering en tijd krijgen om de werkzaamheden uit te voeren.
- De rol van AVG-contactpersoon moet nader worden bekeken. Is de rol binnen alle diensten goed belegd met voldoende overzicht over wat er binnen de dienst gebeurt op gebied van AVG?

2. AVG-verwerkingsregister

Alle verwerkingen van persoonsgegevens worden opgenomen in het digitale AVG-verwerkingsregister van de Tweede Kamerorganisatie. Dit is een dynamisch register dat door elke dienst zelf moet worden ingevuld en bijgehouden. Het diensthoofd is eigenaar van de verwerkingen binnen de eigen dienst en monitort jaarlijks samen met de AVG-contactpersoon en/of de Privacy Officer (PO)/Functionaris voor de Gegevensbescherming (FG) of de verwerkingen nog volledig en up-to-date zijn.

Stand van zaken AVG-verwerkingsregister Tweede Kamerorganisatie per 2 mei 2023:

In het AVG-register van de Tweede Kamerorganisatie staan 140 verwerkingen van persoonsgegevens. De meeste verwerkingen vinden plaats bij de stafdienst HR en de Beveiligingsdienst. Ook de Dienst Informatie en Archief verwerkt relatief veel persoonsgegevens.

Nog niet alle verwerkingen zijn vastgesteld in het AVG-register. De FG van de Tweede Kamer heeft tot taak de rechtmatigheid, volledigheid en duidelijkheid van de verwerkingen in het AVG-register vast te stellen, maar heeft hier in de praktijk geen tijd voor beschikbaar gehad.
De Privacy Officer van de Tweede Kamer heeft tot nu toe 29 van de 140 verwerkingen vastgesteld. Het vaststellen van verwerkingen in het AVG-register is geen doel op zich. Ook verwerkingen die nog in bewerking zijn kunnen bijdragen aan de doelstellingen van het AVG-register. De formele vaststelling dient echter op enig moment wel plaats te vinden, omdat daarmee aangetoond wordt hoe persoonsgegevens worden verwerkt.

3. Datalekken

De AVG kent geen concrete definitie van een 'datalek', maar spreekt in de plaats daarvan van een inbreuk in verband met persoonsgegevens.
De definitie van een inbreuk in verband met persoonsgegevens is:
"een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens".

Voor een datalek is het noodzakelijk dat er persoonsgegevens in het geding zijn. Als dat niet het geval is kan er nog wel sprake zijn van een beveiligingsincident dat moet worden verholpen. Dat betekent dat alle datalekken beveiligingsincidenten zijn, maar dat niet alle beveiligingsincidenten noodzakelijkerwijs datalekken zijn. Datalekken worden besproken in de artikelen 33 en 34 van de AVG.

Voorbeelden van datalekken binnen de Tweede Kamer zijn:
- verlies van een fysiek dossier of telefoon/iPad/usb-stick waardoor iemand mogelijke toegang heeft tot persoonsgegevens;
- wanneer bepaalde persoonsgegevens per ongeluk zijn vernietigd of onjuist blijken te zijn
- wanneer persoonsgegevens onbevoegd of onbedoeld zijn ingezien door personen, bijvoorbeeld door het onbeveiligd versturen van gevoelige persoonsgegevens versturen of door verkeerde machtiging van bestanden;
- wanneer gegevens door ransomware of systeemstoring niet meer toegankelijk zijn

Datalekken moeten verplicht worden geregistreerd in een datalekregister, ook de minder ernstige datalekken die niet gemeld hoeven te worden aan de AP.
De Tweede Kamer gebruikt TopDesk als datalekregister.

Op de website van de Autoriteit Persoonsgegevens staat een tweeledig doel van dit datalekregister:

- De organisatie leert van eerdere datalekken en neemt maatregelen om de kans op nieuwe datalekken te verminderen;
- Met het datalekregister kan aan de AP worden aangetoond dat de organisatie zich houdt aan de meldplicht datalekken.

De Tweede Kamerorganisatie heeft een datalekprocedure ingericht[1] en er is een op maat gemaakte e-learning datalekken beschikbaar.

Overzicht van aantallen en categorieën gemelde datalekken in de periode 2019-2023

Omschrijving incident	2019	%	2020	%	2021	%	2022	%	2023 t/m 1 mei 2023	%
Verloren/gestolen/gevonden gegevensdrager (telefoon, Ipad, laptop, usb-stick)	22	42%	16	41%	18	40%	32	58%	13	54%
P-documenten in verkeerd p-dossier	7	13%	4	10%	3	7%	2	4%		
Foutieve machtigingen	6	12%	1	3%	10	22%	11	20%		
e-mail met persoonsgegevens naar verkeerde ontvanger gestuurd	6	12%	1	3%	4	9%	5	9%	4	17%
Document met persoonsgegevens onbedoeld gepubliceerd op internet	1	2%	2	5%	3	7%				
printincidenten met persoonsgegevens	1	2%	1	3%	2	4%	1	2%	1	4%
Hack-incident met persoonsgegevens/telefoonoplichting (spoofing)	1	2%	4	10%			1	2%		
Documenten met persoonsgegevens onbeheerd gevonden			1	3%	1	2%	3	5%	2	8%
Datalek fractie/Kamerlid/andere organisatie, dus geen datalek Tweede Kamerorganisatie	7	13%	8	21%	4	9%			1	4%
Geen datalek want geen persoonsgegevens betrokken bij incident	1	2%	1	3%					3	13%
Totaal	**52**	100%	**39**	100%	**45**	100%	**55**	100%	**24**	100%

[1] Zie Plein2 voor de procedure datalekken, http://plein2/node/23736

Toelichting op de tabel

- Over 2018 zijn geen incidenten met persoonsgegevens in TopDesk bijgehouden.
- De categorie potentiële datalekken die het meest frequent wordt gemeld betreft het verlies van een gegevensdrager zoals een mobiele telefoon of iPad. Melder is zich vaak niet bewust dat dit een potentieel datalek kan zijn, maar meldt zich bij 5.1.2.i met het verzoek om een nieuwe gegevensdrager.
- Er worden binnen de Tweede Kamer jaarlijks weinig datalekken gemeld, in de afgelopen jaren tussen de 40 en 55 meldingen. Dit lage aantal meldingen lijkt niet realistisch. Onbekend is wat wel een realistisch aantal zou zijn.
- Het niet melden van datalekken is een risico omdat dit een overtreding is van de AVG met het risico op een boete. Een belangrijker risico is dat er bij niet melden van een datalek niet wordt geleerd van de fout, waardoor de rechten en vrijheden van personen mogelijk niet gewaarborgd zijn.
- Mogelijke redenen voor het niet-melden van een datalek:
    - Men lost het incident zelf op zonder melding bij 5.1.2.i
    - Men beoordeelt het incident niet als datalek
    - Men vindt het vervelend om een datalek te melden, omdat men een fout heeft gemaakt

In 2022 is de datalekprocedure geëvalueerd. Dit heeft geresulteerd in een aantal aanbevelingen en actiepunten die in 2023 verder worden geïmplementeerd. De belangrijkste zijn:

- Blijvende aandacht voor het borgen van de kennis en bewustwording over datalekken (zoals in de campagne Veilig werken met informatie), waardoor de meldingsbereidheid zal toenemen en de Tweede Kamerorganisatie leert van gemaakte fouten en verbeteringen kan aanbrengen aan processen en systemen.
- Actualisering van de datalekprocedure in samenwerking met de medewerkers van de servicedesk en de functioneel beheerder van het datalekregister
- Sleutelfiguren (relatiebeheerders, diensthoofden, MT, AVG-contactpersonen) regelmatig informeren over gemelde datalekken, zodat men een beter beeld heeft wanneer zich datalekken voordoen binnen de Tweede Kamerorganisatie

4. DPIA – brengt de privacyrisico's van een gegevensverwerking in beeld en benoemt de mogelijke maatregelen

Een Data Protection Impact Assessment (DPIA) is:

- Een systematische beschrijving van de gegevensverwerking
- Een beoordeling van de privacy risico's
- Benoemen van maatregelen om die risico's aan te pakken

- Specifiek: nagaan of de gegevensverwerking rechtmatig is

Een DPIA is niet:

- instrument om vast te stellen of een voorgenomen gegevensverwerking in lijn is met de privacyregelgeving (compliance)
- vaste vorm of vragenlijst

Een DPIA is verplicht wanneer er waarschijnlijk sprake is van een hoog risico van de verwerking van persoonsgegevens voor de betrokkenen. Vaak betreft het dan gevoelige of bijzonder persoonsgegevens. Maar ook wanneer er geen verplichting is kan het raadzaam zijn om een DPIA uit te voeren om zicht te krijgen op mogelijke privacy risico's.

Een DPIA wordt binnen de Tweede Kamer om verschillende redenen uitgevoerd:
- zorgvuldigheidsredenen (b.v. Parlementaire Enquêtecommissie Aardgaswinning Groningen, Parlementaire Enquêtecommissie Fraude en Dienstverlening)
- aard, hoeveelheid of complexiteit van de persoonsgegevens (b.v. IAM, Cameratoezicht)
- verplichting (Biometrisch systeem voor de toegangscontrole)

Aandachtspunten:

- Een DPIA uitvoeren is geen eenmalige exercitie, maar een continu proces. Het is de taak van de betreffende dienst om te monitoren of de gegevensverwerking verandert. Bijvoorbeeld wanneer een nieuwe technologie gebruikt wordt, of dat de persoonsgegevens voor een ander doel of op een andere locatie gebruikt gaan worden (zoals straks B67).
- Een DPIA moet periodiek worden uitgevoerd, ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld 1 keer per 3 jaar. In de DPIA-rapportage wordt afgesproken wanneer de DPIA herhaald moet worden.
- Monitoring door diensthoofd op de naleving van de besluiten van de DPIA.
- De FG van de Tweede Kamer adviseert de verwerkingsverantwoordelijke over een uitgevoerde DPIA (AVG, artikel 35, lid 2) en ziet toe op de uitvoering van een DPIA (AVG , artikel 39 lid 1 onder c). Dat advies moet samen met de beslissingen van de verwerkingsverantwoordelijke in de DPIA worden gedocumenteerd.

Overzicht van de uitgevoerde DPIA's in de periode 2016 – 2023

Datum	Dienst	Onderwerp	uitgevoerd door
2016			
20160901	Beveiligingsdienst	PIA Biometrische camera bewaking	INKX
2019			
20191102	Beveiligingsdienst	DPIA rapportage IAM fase 1	VKA
20191114	Beveiligingsdienst	DPIA rapportage Bezoekersregistratie	VKA
2021			
20210225	Enquêtecommissie	DPIA PEAG	VKA
20210226	DIA	DPIA Archiefbeheersysteem	DIA
20210419	Beveiligingsdienst	DPIA Biometrisch systeem Tweede Kamer	VKA
20211123	DA	DPIA rapportage MS Teams	VKA
2022			
20220315	Beveiligingsdienst	DPIA Cameratoezicht	VKA
20220315	Beveiligingsdienst	DPIA Toegangscontrolesysteem (TCS)	VKA
20220518	Stafdienst HR	DPIA Recruitment tool	VKA
20220815	Enquêtecommissie	DPIA PEFD	VKA
20221117	CIO Office	DPIA Woo loket	VKA
20221215	Bureau CISO	DPIA rapportage IAM fase 2	VKA

*VKA = Verdonk, Klooster en Associates. VKA is de begeleider van de workshop DPIA

5. AVG-rechten van betrokkenen

Mensen hebben AVG-rechten om controle te houden over hun persoonsgegevens. De Tweede Kamer moet zorgen dat de systemen, processen en de interne organisatie zijn ingericht op deze rechten en alle medewerkers op de hoogte zijn hoe dit proces is ingericht.

Sinds de inwerkingtreding van de AVG in 2018 heeft de Tweede Kamerorganisatie een aantal inzageverzoeken en verwijderingsverzoeken ontvangen. Elk verzoek betrof een unieke situatie, waar met maatwerk gehoor aan is gegeven. Een verzoek moet binnen 1 maand na indiening beantwoord, een paar keer was een langere termijn nodig omdat een proces nog onvoldoende ingericht bleek om tijdig aan een verzoek te kunnen voldoen. De betreffende dienst heeft daarbij het advies gekregen het proces aan te passen.

Ook heeft de Tweede Kamerorganisatie sinds 2018 een aantal klachten en informatieverzoeken ontvangen. In samenwerking met de betreffende diensten zijn deze klachten en informatieverzoeken behandeld. Waar van toepassing heeft dit geleid tot aanpassing van bestaande processen en/of de informatieverstrekking.

Overzicht aantal en soort verzoeken betrokkenen periode 2018 - 2023					
jaartal	aantal	soort	kenmerk	Afhandeling	bijzonderheden
2018	2	Verwijderingsverzoek	AVG2018VV101	Ingediend oktober 2018, afgehandeld 2 juni 2020	naturalisatiewet - procedure met KOOP ingericht
		Verwijderingsverzoek	AVG2018VV102	Ingediend oktober 2018, afgehandeld 2 juni 2020	naturalisatiewet - procedure met KOOP ingericht
2019	3	Inzageverzoek	AVG2019VI101	Ingediend 12 maart 2019, afgehandeld dec 2019	betrokkenheid advocaat. Dossier BVA
		Inzageverzoek	AVG2019VI102	Ingediend 25 juli 2019, afgehandeld 18 december 2020	betrokkenheid Landsadvocaat en Rechtbank Den Haag
		Inzageverzoek	AVG2019VI103	afgehandeld binnen termijn 4 weken	concept-procedure met griffie commissie opgesteld
2020	3	Verwijderingsverzoek	AVG2020VV101	afgehandeld 4 maanden na indiening verzoek	naturalisatiewet - aanvullende procedure met KOOP
		Verwijderingsverzoek	AVG2020VV102	afgehandeld 3 maanden na indiening verzoek	naturalisatiewet - aanvullende procedure met KOOP
		Verwijderingsverzoek	AVG2020VV103	afgehandeld binnen 1 week na indiening verzoek	publicatie op internet, brief onterecht niet
2021	3	Verwijderingsverzoek	AVG2021VV101	afgehandeld 2 december 2021, indiening verzoek 10 januari 2021. Betreft herhaalde verzoeken omdat hij steeds opnieuw weer vindbaar was.	naturalisatiewet - verzoek niet meer vindbaar te zijn via Google search
		Verwijderingsverzoek	AVG2021VV102	afgehandeld binnen 5 weken na indiening verzoek	Verzoek om verwijdering telefoonnummer uit Parlisdocumenten
		Informatieverzoek	AVG2021VI103	afgehandeld binnen 1 week na indiening verzoek	verzoek inwoner Californië over toepasselijkheid GDPR
		Informatieverzoek	AVG2021VI103*	afgehandeld binnen 1 week na indiening verzoek	verzoek inwoner Parijs over inzageprocedure website www.kabinetsformatie2017.nl
2022	7	Inzageverzoek	AVG2022VI101	afgehandeld binnen 1 maand na indiening verzoek	naturalisatiewet - verzoek niet meer vindbaar te zijn via Google search
		Inzageverzoek	AVG2022VI102	afgehandeld binnen 5 weken na indiening verzoek	Verzoek inzage door burger die in diverse Parlisdocumenten persoonsgegevens heeft staan.
		Informatieverzoek	AVG2022VINF101	afgehandeld binnen 1 maand na indiening verzoek	Verzoek om informatie over verwerking persoonsgegevens na bezoek aan Tweede Kamer
		Informatieverzoek	AVG2022VINF102	afgehandeld binnen 1 week na indiening verzoek	Onbedoeld online gepubliceerd document met gsm nummers
		Informatieverzoek	AVG2022VINF103	afgehandeld binnen 5 weken na indiening verzoek	Verzoek om informatie over verwerking biometrische gegevens bij bezoek aan Tweede Kamer
		Verwijderingsverzoek	AVG2022VV101	afhandeling niet bekend	naturalisatiewet - verzoek niet meer vindbaar te zijn via Google search
		Verwijderingsverzoek	AVG2022VV102	afgehandeld 16 september 2022, indiening verzoek 27 juni 2022. Betreft herhaalde verzoeken omdat verzoeker steeds opnieuw vindbaar bleef	naturalisatiewet - verzoek niet meer vindbaar te zijn via Google search
2023	2	Verwijderingsverzoek	AVG2023VV101	afgehandeld binnen 3 weken na indiening verzoek	door TK gepubliceerd vertrouwelijk document, is destijds door ministerie openbaar aangeboden. Door TK tijdelijk in concept gezet in afwachting van gelakt document
		Verwijderingsverzoek	AVG2023VV102	afgehandeld binnen 1 maand na indiening verzoek	verzoek verwijdering persoonsgegevens in document petitieaanbieding
		* per abuis 2x zelfde kenmerk gebruikt!			

Klachten over gebruik persoonsgegevens

In de periode 2018-2023 heeft de FG van de Tweede Kamer een aantal klachten ontvangen over gebruik persoonsgegevens door de Tweede Kamer.

1. Een burger beklaagde zich over het gebruik van zijn persoonsgegevens in een onderzoek van de vaste commissie voor Economische Zaken en Klimaat. Dit betreft het Onderzoek naar schadevergoeding NAM. De Tweede Kamer wil weten of betrokken burgers tevreden zijn over de afhandeling. De burger beklaagt zich dat de Tweede Kamer zonder zijn toestemming in bezit is gekomen van zijn persoonsgegevens.
2. Een oud-senator meldt dat zijn huisadres vindbaar is op internet. Hij verwijst met een link naar de vindplaats. Het betreft een Kamerstuk uit 2004, toen het gangbaar was om privéadressen van Tweede Kamerleden desgewenst te publiceren in een openbaar Kamerstuk.
3. Deelnemers aan verschillende rondetafelgesprekken stellen vragen over persoonsgegevens die op het internet worden gepubliceerd. Dit onderwerp is momenteel nog in bespreking.

6. Privacy by design en privacy by default (artikel 25 AVG)

Privacy by design houdt in dat bij het ontwerpen van producten en diensten zo vroeg mogelijk aandacht wordt besteed aan de bescherming van persoonsgegevens. Wanneer in processen en aanschaf van systemen geen rekening wordt gehouden met de AVG is het moeilijk om de AVG volledig toe te passen. Zoals de mogelijkheid om gegevens te verwijderen, inzage te verlenen in verwerking persoonsgegevens, passende organisatorische en technische beveiliging.
Voorbeeld van Privacy by design binnen de Tweede Kamerorganisatie: De Facilitaire dienst heeft bij de vervanging van de printers de bescherming van persoonsgegevens is meegenomen bij de aanschaf van de huidige multifunctionele printers (MFP's). Hierdoor worden datalekken en inbreuken op informatiebeveiliging beter voorkomen. Vertrouwelijke documenten worden beschermd door deze alleen aan de juiste gebruikers vrij te geven en de veiligheid van netwerkprinters is verbeterd door een accurate wijze van verificatie van de gebruikers.

Privacy by default houdt in dat de standaardinstellingen van een product of dienst rekening houden met de bescherming van persoonsgegevens, en er niet vooraf hokjes of velden zijn aangevinkt. Bijvoorbeeld 'Locatiegegevens bijhouden' moet standaard uitstaan op een telefoon, je moet hiervoor een actieve handeling uitvoeren. En op het formulier voor een bezoek aan de Tweede Kamer of toesturen van een nieuwsbrief worden uitsluitend de noodzakelijke persoonsgegevens gevraagd op in te vullen.

7. Verwerkersovereenkomsten

De ambtelijke organisatie van de Tweede Kamer heeft voor bijna alle verwerkingen van persoonsgegevens door ambtenaren worden uitgevoerd de rol van Verwerkingsverantwoordelijke. Dat is degene die doel en middelen van de verwerking bepaalt. Zonder de verwerkingsverantwoordelijke zou de verwerking niet plaatsvinden.

De ambtelijke organisatie maakt voor het verwerken van persoonsgegevens regelmatig gebruik van leveranciers zoals een IT-leveranciers die een softwaresysteem levert waar de Tweede Kamer persoonsgegevens in opslaat. In dat geval moet worden nagegaan of en welke onderlinge afspraken er moeten worden gemaakt over het beveiligingsniveau en onder welke voorwaarden de leverancier de persoonsgegevens al dan niet mag verwerken.

Dit wordt de verwerkersovereenkomst genoemd. Het afsluiten van een verwerkersovereenkomst moet in verhouding staan tot het doel namelijk dat er zorgvuldig wordt omgegaan met persoonsgegevens en geen doel op zicht zijn. De AVG eist slechts dat er schriftelijke afspraken gemaakt worden en dat kan ook door een geheimhoudingsverklaring op te nemen in de algemene inkoopvoorwaarden.

Binnen de ambtelijke organisatie van de Tweede Kamer bestaan nog steeds veel vragen over hoe de rol van verwerker moet worden bepaald en welke afspraken er vervolgens gemaakt moeten worden. In 2023 en verder zal blijvend aandacht besteed worden aan hoe diensten hier zelf hun rol en verantwoordelijkheid kunnen pakken.

Tweede Kamer
DER STATEN-GENERAAL

Oplegnotitie Prodecure datalekken

Stafdienst Personeel en Organisatie
5.1.2.e
Lange Houtstraat 1
2511 CV Den Haag
T 5.1.2.e
M 5.1.2.e
E 5.1.2.e @tweedekamer.nl

aan het MT
bijlagen 1. Procedure meldplicht datalekken Tweede Kamer
2. Communicatieplan

Aard van de bespreking
Ter informatie

Beknopte samenvatting
In de MT-vergadering van 7 maart 2016 is een conceptversie van de procedure meldplicht datalekken Tweede Kamer besproken. Tijdens deze vergadering is door het MT aangegeven dat de regeling voor de korte termijn volstaat, maar dat het nog wel toegesneden moet worden op de specifieke omstandigheden bij de Tweede Kamer en dat daarnaast specifieke aandacht moet zijn voor communicatieaspecten naar de Kamerbewoners en enkele specifieke doelgroepen zoals de ambtelijk secretarissen van de fracties. De werkgroep datalekken heeft een communicatieplan (bijlage 2) opgesteld dat hierin moet voorzien. Daarnaast heeft het MT aangegeven dat er een sluitende vervangingsregeling moet komen. De vervangingsregeling is als bijlage 4 aan de procedure meldplicht datalekken Tweede Kamer toegevoegd (bijlage 1).

Hoewel de Ondernemingsraad geen advies- of instemmingsrecht heeft, wordt het MT geadviseerd de procedure ter informatie door te geleiden aan de ondernemingsraad.

Beslispunten
Het MT wordt geadviseerd in te stemmen met:

1. het communicatieplan zoals bijgevoegd in bijlage 2;

2. het laten plaatsvinden van een evaluatie van de procedure 2 maanden na de inwerkingtreding hiervan; en

3. het ter informatie doorgeleiden van de procedure aan de Ondernemingsraad.

Eerder behandeld in MT
Op 7 maart 2016 is een conceptversie van de procedure behandeld.

Financiële consequenties
geen

Personele consequenties

Geen, behalve de inzet van de leden van de werkgroep datalekken:

- 5.1.2.e (stafdienst P&O)
- 5.1.2.e (Bureau IP)
- 5.1.2.e (Dienst Automatisering)
- 5.1.2.e (Beveiligingsdienst)
- 5.1.2.e (stafdienst Communicatie)
- 5.1.2.e (stafdienst FEZ)

Infrastructurele consequenties

geen

IT-consequenties

geen

Advies hP&O

Advies hFEZ

Advies hCOM

Doorgeleiding

Ondernemingsraad

- Informatie

Datalekken: wat zijn dat?
De Tweede Kamer zorgt voor goede beveiliging van persoonsgegevens, door het nemen van technische en organisatorische maatregelen. Toch kan het gebeuren dat persoonsgegevens bij iemand terecht komen die er geen toegang toe mag hebben. Of dat het digitale systeem van de Tweede Kamer wordt gehackt, waardoor we niet meer bij onze informatie kunnen.
Of dat er een laptop/tablet/smartphone wordt gestolen of verloren.
Ook het langer bewaren van persoonsgegevens dan afgesproken is een datalek, tenzij de betrokkene daar expliciet toestemming voor heeft gegeven.
In al die gevallen is er sprake van een datalek.

Wat moet je doen bij een datalek?
Alle datalekken die plaatsvinden binnen de Tweede Kamer moeten worden geregistreerd. En ernstige datalekken moeten door de Tweede Kamer worden gemeld aan de Autoriteit Persoonsgegevens.

Het is daarom noodzakelijk dat je een datalek meldt.
Vul het formulier Melding datalek in en stuur het formulier naar 5.1.2.i @tweedekamer.nl

Formulier Melding datalek

Of neemt contact op met de Servicedesk van de Tweede Kamer via toestelnummer 5.1.2.i of via mailadres 5.1.2.i @tweedekamer.nl
Je ontvangt dan via 5.1.2.i het formulier Melding datalek met het verzoek alle relevante informatie in te vullen en het formulier te retourneren.

Wat gebeurt er met de Melding datalek?

- Allereerst wordt het datalek gedicht
- Tegelijkertijd wordt zorgvuldig nagegaan welke persoonsgegevens gelekt zijn. En of mensen benadeeld zijn door het lek
- Er wordt gekeken wat de oorzaak is van het datalek en hoe een herhaling voorkomen kan worden
- Indien noodzakelijk wordt de Autoriteit Persoonsgegevens geïnformeerd over het datalek en de mensen van wie de gegevens gelekt zijn
- Tot slot wordt de melder geïnformeerd over de afhandeling van het datalek

Hoe voorkom je datalekken?
Datalekken kunnen het beste worden voorkomen door een combinatie van technische en organisatorische maatregelen. Hier moet de Tweede Kamerorganisatie voor zorgen, dat er voldoende maatregelen zijn zodat er zo min mogelijk datalekken voorkomen.

Maar je kunt zelf ook veel doen. De meeste datalekken worden namelijk veroorzaakt door menselijke fouten.

Voorbeelden van wat je kunt doen:

- Zorg voor kennis en bewustwording en doe de module Datalekken. Leer wat persoonsgegevens zijn, hoe je een datalek kunt herkennen en hoe je een datalek moet melden (hier toevoegen link naar de module)
- Wees voorzichtig met je smartphone, tablet en/of laptop met daarop zakelijke email en werkomgeving. Binnen de Tweede Kamer geldt het verplichte gebruik van MDM op je mobiele telefoon.
- Vergrendel je computer/tablet/telefoon en zorg dat je bureau leeg is als je afwezig bent en je kasten/bureaulade op slot.
- Lees de Gedragsregeling voor de digitale werkomgeving. Deze gedragsregeling is er zodat Kamerambtenaren op een verantwoorde en veilige wijze gebruik kunnen maken van de digitale werkomgeving en bewust omgaan met sociale media.
- Zorg voor een sterk wachtwoord. Sinds 25 februari 2019 gelden nieuwe eisen voor een wachtwoord, namelijk minimaal 14 karakters lang. Wachtwoorden van deze lengte zijn bijna onmogelijk te kraken door hackers.
- Bespreek binnen je dienst hoe zorgvuldig met persoonsgegevens wordt omgegaan en maak elkaar hiervan bewust.
- Zorg dat machtigingen en toegang tot systemen op orde zijn en regelmatig worden geactualiseerd, zodat alleen bevoegden toegang hebben tot de persoonsgegevens.
- Plaats e-mailadressen van mensen die elkaar niet kennen bij voorkeur in het bcc-veld in plaats van het cc-veld
- Bewaar papieren personeelsdossiers niet in een open archiefkast
- Check na het printen of je al je printjes hebt meegenomen. Check ook de glasplaat!

Ernstige datalekken binnen 72 melden bij de Autoriteit Persoonsgegevens (AP)
De Tweede Kamer kan te maken krijgen met een ernstig datalek. Hieronder wordt verstaan dat grote hoeveelheden persoonsgegevens onbedoeld terecht zijn gekomen bij onbevoegden en dat dit mogelijk ernstige risico's en schade voor betrokkenen kan opleveren.
In dat geval moet de Tweede Kamer het datalek binnen 72 melden aan de AP.
Het datalekteam adviseert het MT of een melding aan de AP noodzakelijk is.

Fracties en datalekken
Fracties zijn zelf verantwoordelijk voor de persoonsgegevens die zij zelf verwerken. Wanneer fracties te maken hebben met een datalek en niet weten wat er moet gebeuren kan advies worden gevraagd aan het datalekteam via toestel 5.1.2.i of een mail naar 5.1.2.i @tweedekamer.nl . Fracties zijn daarna zelf verantwoordelijk voor het melden van het lek aan de Autoriteit Persoonsgegevens en/of de persoon wiens gegevens gelekt zijn.

I2001 0015 Mobiel toestel verloren

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Mobiel toestel verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	3 januari 2020 16:04
Doorlooptijd	15 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	2 januari 2020 18:07
Afgemeld	Ja
Datum afgemeld	2 januari 2020 18:07
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 2 januari 2020 10:36

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 2 januari 2020 18:07

Mevrouw heeft haar toestel weer gevonden.
Langs de balie geweest.
Sim kaart uitgeleverd.
Toestel is ingesteld.
Was fractie toestel en niet van de kamer.

5.1.2.e **onzichtbaar voor aanmelder** — 2 januari 2020 15:27

Mevrouw heeft de iPhone weer gevonden.
Zij is langsgekomen om het toestel opnieuw in te regelen.
Het toestel moest verwijderd worden om MDM opnieuw te installeren.

Toestel iPhone
IMEI/MEID: 5.1.2.h + 5.1.2.i
Serial number: 5.1.2.h + 5.1.2.i

5.1.2.e **onzichtbaar voor aanmelder** 2 januari 2020 10:42
Meneer 5.1.2.e belde om te melden dat de telefoon van mevrouw 5.1.2.e verloren is geraakt
Hij vroeg om een full-wipe van het toestel (deze is verder in beheer van de fractie). De full wipe uitgevoerd.
Nummer overgezet naar een nieuwe simkaart op verzoek van meneer 5.1.2.e en hem gemaild.

5.1.2.e **onzichtbaar voor aanmelder** 2 januari 2020 10:36
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante

wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	2 januari 2020 10:34		Potentieel datalek
Gerealiseerde doorlooptijd	07:26	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	07:26		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	07:26		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	2 januari 2020 12:29
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	standaardprocedure is uitgevoerd, gsm is zelfde dag weer gevonden
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	betrokkene heeft zelf gemeld
Getroffen maatregelen	Standaardprocedure is uitgevoerd door SD
Beschrijving inbreuk	gsm verloren. Dezelfde dag melding dat gsm is gevonden

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2001 0702 Mobiele telefoon verloren

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst Financieel Economische Zaken
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Mobiele telefoon verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	23 januari 2020 15:12
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Data handling Team
Behandelaarsgroep	Data handling Team
Status	In behandeling
Gereed	Ja
Datum gereed	21 januari 2020 18:01
Afgemeld	Ja
Datum afgemeld	23 januari 2020 10:50
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 20 januari 2020 8:52

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

telefoon verloren afgelopen weekend. Mevrouw gaat nog aangifte doen van verlies.
Mevrouw zou graag een nieuwe telefoon ontvangen.

Actie

5.1.2.e — 21 januari 2020 18:01

Geen datalek dat gemeld dient te worden bij de AP. Ik meld de melding gereed.

5.1.2.e Mailimport 20 januari 2020 9:22

Datum verzonden: 20-jan-2020 9:13
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: RE: I2001 0702 Aanmelden datalek

Met vriendelijke groet,
5.1.2.e
onbekend
Stafdienst Financieel Economische Zaken
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: maandag 20 januari 2020 08:52
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2001 0702 Aanmelden datalek

Geachte mevrouw 5.1.2.e

Dank voor het melden van een Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
Dit team zal u informeren over de voortgang en de afhandeling.

Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i). Dit kan telefonisch of middels het beantwoorden van deze e-mail.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 20 januari 2020 8:57

@datalekteam zouden jullie het potentiele datalek willen beoordelen?

5.1.2.e **onzichtbaar voor aanmelder** 20 januari 2020 8:56

Mevrouw is haar mobiele telefoon (samsung) kwijtgeraakt afgelopen weekend. Zij zal nog aangifte gaan doen van verlies of diefstal. Ze vermoedt dat het toestel verloren is.

De MDM server geeft aan dat de laatste keer dat het toestel synchroniseerde 17-1 om 11:26 was. Ik heb een selective wipe opdracht gegeven.
Toestel is niet meer online geweest sinds de vermissing.
Ontgrendelcode van het toestel was de geboortedatum van mevrouw zelf.

5.1.2.e **onzichtbaar voor aanmelder** 20 januari 2020 8:52

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	20 januari 2020 8:42		Potentieel datalek
Gerealiseerde doorlooptijd	18:48	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	18:48		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	18:48		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	20 januari 2020 12:26
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	standaardprocedure is uitgevoerd
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene heeft zelf gemeld
Getroffen maatregelen	Standaardprocedure is uitgevoerd door SD
Beschrijving inbreuk	gsm verloren/gestolen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2001 0975 Verloren iPad

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	VVD
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Verloren iPad
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2114
Soort	Tablet
Voorraad	ServiceDesk

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	18 februari 2020 11:26
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	Wacht op klant
Gereed	Ja
Datum gereed	17 februari 2020 9:43
Afgemeld	Ja
Datum afgemeld	17 februari 2020 9:43
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 24 januari 2020 16:49

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e **onzichtbaar voor aanmelder** 17 februari 2020 9:43

Mevrouw neemt telefonisch contact op en geeft door dat de betreffende iPad gevonden is. Deze lag onder haar autostoel. Aangegeven dat er een Selective Wipe heeft plaats gevonden (waarschijnlijk) en dat ze hiervoor moet langs komen bij de balie om weer MDM op geïnstalleerd te hebben.
Ze komt in de loop van de week langs.

5.1.2.e **onzichtbaar voor aanmelder** 14 februari 2020 9:37
Mevrouw nogmaals uitgenodigd.

5.1.2.e **onzichtbaar voor aanmelder** 12 februari 2020 17:50

Mevrouw gemaild met het verzoek ons te bellen

5.1.2.e **onzichtbaar voor aanmelder** 5 februari 2020 10:21
ToDo:
Wenselijkheid van een wissel nagaan.
Mevrouw vragen of zij met behulp van iCloud het apparaat nog wil proberen te wipen.
Data nummer op een andere simkaart zetten.
Al twee keer gebeld maar helaas geen gehoor.

5.1.2.e 5 februari 2020 9:56
Het datalekteam stelt vast dat er geen acties nodig zijn vanuit het datalekteam en meldt het incident gereed.
Datalekteam verzoekt SD om contact op te nemen met mevrouw omdat ze nog niet is langs geweest bij de SD-balie, o.a. voor andere simkaart en de icloud wipe.

5.1.2.e **onzichtbaar voor aanmelder** 4 februari 2020 14:57
@Datalekteam: Aanmelder meldt op 24 januari dat ze haar iPad (TABL2114) verloren heeft. Er is door 5.1.2.i een Selective Wipe uitgezet, maar deze is nog niet doorgekomen. Het apparaat is de afgelopen 18 dagen niet online geweest. Mevrouw geeft aan dat haar ontgrendelcode niet makkelijk te raden is (dus niet 0000 of 1234).

I2001 0975.PNG

5.1.2.e **onzichtbaar voor aanmelder** 4 februari 2020 14:53
Aanmelder is maandag niet langs geweest. iPad heeft Selective Wipe nog niet uitgevoerd.

Aanmelder meldt dat ze geen makkelijk te raden unlock code heeft en komt morgen langs voor de iCloud wipe.

5.1.2.e **onzichtbaar voor aanmelder** 24 januari 2020 16:52
Mevrouw meldt dat zij haar TK iPad verloren is, TABL2114.
Selective Wipe request gestuurd, maar door het afsluiten van Citrix is het niet duidelijk of deze aankomt.
Selective wipe was requested at 24-1-20 16:53:00. This operation is carried out upon device connection.
Mevrouw komt maandag langs de balie, er wordt een poging gedaan een wipe uit te voeren via iCloud.

5.1.2.e **onzichtbaar voor aanmelder** 24 januari 2020 16:49
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	24 januari 2020 16:47		Potentieel datalek
Gerealiseerde doorlooptijd	144:56	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	84:45		
Aangepaste doorlooptijd	60:11		
Doorlooptijd 'Afgerond'	55:24		
Doorlooptijd 'Uitvoering'	04:47		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	24 januari 2020 12:23
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Standaardprocedure is uitgevoerd
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene heeft zelf gemeld
Getroffen maatregelen	Standaardprocedure is uitgevoerd door SD
Beschrijving inbreuk	I-pad verloren. 17 febr melding dat I-pad is gevonden

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2001 1254 Datalek melding P-direkt

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst HR
Locatie (Aanmelder)	5.1.1.e

Details

Korte omschrijving	Datalek melding P-direkt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	3 februari 2020 8:56
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	3 februari 2020 14:31
Afgemeld	Ja
Datum afgemeld	7 februari 2020 12:17
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 30 januari 2020 12:03

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — Mailimport 30 januari 2020 11:56

Datum verzonden: 30-jan-2020 11:36
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: melding datalekken

Bijgaand zend ik het ingevulde formulier datalek.

Mijn vervolg stappen zijn:
- Betrokkenen op de hoogte stellen
- P-Direkt verzoeken de betreffende documenten in de juiste dossiers onder te brengen

Met vriendelijke groet,

5.1.2.e
Adviseur HR - Stafdienst HR
Tweede Kamer der Staten-Generaal
Aanwezig: dinsdag tot en met vrijdag
(oneven weken: dinsdag tot en met donderdag)

Postbus 20018, 2500 EA Den Haag
T (+ 5.1.2.e | M 5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Vanaf 2 januari 2019 is de Tweede Kamer aangesloten op P-Direkt. Het shared service center voor de Rijksoverheid op het gebied van personeels– en salarisadministratie. U kunt als ambtenaar van de Tweede Kamer hier uw personeelszaken regelen, zoals verlof registreren, IKB aanvragen en uw personeelsdossier inzien. Ook kunt u vanaf deze datum op Rijksportaal veel wet- en regelgeving en andere handige informatie terugvinden, die u eerst aantrof in het personeelshandboek.
Op Plein2 (http://plein2/personeelszaken) vindt u informatie over de aansluiting bij P-Direkt, zoals de veelgestelde vragen en een wegwijzer voor het P-Direkt portaal.

Actie

5.1.2.e 3 februari 2020 14:31
5.1.2.e heeft gelijk. Zie onderstaande actie van HR. Het is geen meldingswaardig incident. Ik meld het hierbij af. Ik rapporteer wil richting HR het aantal zelfde soort incidenten en zal daarbij de vraag stellen of er gerichte actie komt om andere dossiers te controleren.

mail: 31 januari 2020 5.1.2.e : Bijgaand zend ik het ingevulde formulier datalek.

Mijn vervolg stappen zijn:
Betrokkenen op de hoogte stellen

P-Direkt verzoeken de betreffende documenten in de juiste dossiers onder te brengen

5.1.2.e **onzichtbaar voor aanmelder** 30 januari 2020 13:49
Volgens mij hoeft dit niet te worden gemeld aan de AP. Dit omdat de informatie terecht is gekomen bij een betrouwbare ontvanger, zoals dat heet. Ik zou het wel netjes vinden als de betrokkenen worden ingelicht, zij het dat dit niet is verplicht.

5.1.2.e **onzichtbaar voor aanmelder** 30 januari 2020 12:03
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit

om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	30 januari 2020 11:56		Potentieel datalek
Gerealiseerde doorlooptijd	21:35	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	21:35		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	21:35		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	30 januari 2020 11:24
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Geringe impact op betrokkene
Melding aan betrokkenen ja/nee	Ja
waarom wel/niet melden aan betrokkenen	Betrokkene is geinformeerd door HR-adviseur
Mogelijke consequenties	informatie van betrokkenen wordt mogelijk bekend bij collega's
Getroffen maatregelen	P-gegevens zijn in juiste dossiers geplaatst
Beschrijving inbreuk	P-gegevens in verkeerde P-dossier

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2002 0288 iPad (in werktas) zo juist gestolen

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e 5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e tweedekamer.nl
Afdeling	GroenLinks
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	iPad (in werktas) zo juist gestolen
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL1848
Soort	Tablet
Vestiging	Overig

Planning

Impact	VIP
Urgentie	3. Kan verder, beinvloed parlementair proces
Prioriteit	2 Hoog
SLA-streefdatum	11 februari 2020 11:54
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	17 februari 2020 17:28
Afgemeld	Ja
Datum afgemeld	20 februari 2020 10:30
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 7 februari 2020 14:12

iPad is gestolen.

5.1.2.e — 7 februari 2020 14:00

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 17 februari 2020 17:28

Noodzakelijke acties zijn uitgevoerd door SD.
Geen nadere vragen vanuit het Datalekteam. Dit incident wordt door het datalekteam gereed gemeld en wordt toegevoegd aan het register Datalekken.

5.1.2.e 7 februari 2020 14:12
Meneer was bij het Polititebureau bezig met de aangifte van diefstal, toen hij is gebeld voor overleg over type "wipe".

5.1.2.e 7 februari 2020 14:12
* IPad is gestolen.
* Full Wipe opdracht is gegeven vanuit MDM.
* Stand van zaken na uitzenden wipe-actie:
MDM status: Check-in pending
Last push initiation: 7-2-20 14:04:53
Last notification completion: 7-2-20 14:04:53
Last device reply time: 7-2-20 11:03:21

5.1.2.e **onzichtbaar voor aanmelder** 7 februari 2020 14:00

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is.

Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	7 februari 2020 13:35		Potentieel datalek
Gerealiseerde doorlooptijd	60:53	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	13:19		
Aangepaste doorlooptijd	47:34		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	47:34		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	7 februari 2020 11:16
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Standaardprocedure is uitgevoerd door SD
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene reeds op de hoogte, heeft zelf gemeld
Getroffen maatregelen	Standaardprocedure is uitgevoerd door SD
Beschrijving inbreuk	I-pad gestolen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2002 0393 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL1967
Soort	Tablet
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	19 februari 2020 10:45
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	13 februari 2020 16:59
Afgemeld	Ja
Datum afgemeld	14 februari 2020 10:33
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 10 februari 2020 14:46

IPad is gestolen.

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 13 februari 2020 16:59

Geconstateerd wordt dat alle noodzakelijke stappen zijn uitgevoerd door de servicedesk. Er zijn

geen nadere vragen bij het datalekteam. En ook geen acties voor het datalekteam om uit te zetten.
Datalekteam meldt dit incident gereed. Incident wordt in TopDesk toegevoegd aan het datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 10 februari 2020 14:53
W2002 170 Hardware - Verlies Tablet_lever

5.1.2.e **onzichtbaar voor aanmelder** 10 februari 2020 14:51
Tas met laptop is gestolen.
Full wipe opdracht doorgegeven aan get apparaat met toestemming van mevrouw.
Nummer gekoppeld aan een nieuw SIM kaart.

5.1.2.e **onzichtbaar voor aanmelder** 10 februari 2020 14:46
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de

klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	10 februari 2020 14:45		Potentieel datalek
Gerealiseerde doorlooptijd	30:44	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	26:30		
Aangepaste doorlooptijd	04:14		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	04:14		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	10 februari 2020 12:17
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Standaardprocedure uitgevoerd
Melding aan betrokkenen ja/nee	Nee
Getroffen maatregelen	Standaardprocedure is uitgevoerd door SD
Beschrijving inbreuk	Tas met laptop gestolen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2002 0633 Melding datalek (reeds afgehandeld)

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Griffie Plenair - Bureau Wetgeving
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Melding datalek (reeds afgehandeld)
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	17 februari 2020 17:20
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	14 februari 2020 11:08
Afgemeld	Ja
Datum afgemeld	17 februari 2020 13:27
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 14 februari 2020 10:52

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 14 februari 2020 10:51

Datum verzonden: 13-feb-2020 12:05
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Melding datalek (reeds afgehandeld)

Met vriendelijke groet,
5.1.2.e
5.1.2.e

5.1.2.e
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

-----Oorspronkelijk bericht-----
Van: NoReply@tweedekamer.nl <NoReply@tweedekamer.nl>
Verzonden: donderdag 13 februari 2020 12:04
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Scan vanaf een 5.1.2.h+5.1.2.i MFP

Er is een scan gemaakt vanaf een 5.1.2.h+5.1.2.i MFP. U vindt de scan als bijlage bij deze e-mail.

Actie

5.1.2.e 14 februari 2020 11:08
Het datalek is reeds gedicht en gemeld bij de Autoriteit Persoonsgegevens (kenmerk: 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i). De Griffier is ook in kennis gesteld van het Datalek. VWS heeft bij het doorsturen van een brief van een burger aan de Tweede Kamer persoonsgegevens gelekt. Dit soort brieven wordt door de Tweede Kamer op de website geplaatst en zijn dus op internet terug te vinden. De door VWS weggelakte naam werd weer herkenbaar toen de brief door de Kamer werd verwerkt (de plaatsing op de website). VWS heeft het lek bij de Kamer gemeld bij de Kamer en de AP. De Kamer heeft de brief of-line gehaald en uit cache bij Google. VWS heeft contact opgenomen met de betrokkenen. De Kamer hoeft niet meer te doen.

Half maart bespreken de Privacy officer en de FG van de Kamer met die van VWS. De voorgeschreven procedure ('echt' weglakken) zal daarbij nog eens onder de aandacht gebracht worden etc.

Ik meld de melding gereed.

5.1.2.e **onzichtbaar voor aanmelder** 14 februari 2020 10:53
@Datalek:
Melding aangemaakt zodat jullie hem administratief af kunnen handelen.

5.1.2.e **onzichtbaar voor aanmelder** 14 februari 2020 10:52
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk

te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	14 februari 2020 10:50		Potentieel datalek
Gerealiseerde doorlooptijd	00:18	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:18		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:18		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	11 februari 2020 10:18
Melding aan AP ja/nee	Ja
Waarom wel/niet melden aan AP	kenmerk: 5.1.2.h + 5.1.2.i gezondheidsinfo kind, naam moeder, leeftijd zoon
Melding aan betrokkenen ja/nee	Nee
Mogelijke consequenties	onbevoegden kunnen kennisnemen gezondheidsgegevens
Getroffen maatregelen	ministerie VWS wijst medewerkers opnieuw op interne procedure
Beschrijving inbreuk	Op internet een niet-geanonimiseerde brief gepubliceerd

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2003 0191 Verdachte link

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	VVD
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Verdachte link
Soort incident	Datalek
Categorie	Security Expert Team
Subcategorie	Security Expert Team

Planning

Impact	Organisatie
Urgentie	4. Kan verder met alternatief
Prioriteit	2 Hoog
Streefdatum	4 maart 2020 11:30
Doorlooptijd	3 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	4 maart 2020 5.1.2.e
Afgemeld	Ja
Datum afgemeld	6 maart 2020 15:50
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — Mailimport 3 maart 2020 18:01

Datum verzonden: 3-mrt-2020 17:16
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Verdachte link

Beste collega's,

Een van onze collega's zocht op Google naar een Tweede Kamer mailadres en stuitte toen op de volgende link:

5.1.2.h + 5.1.2.i

Vormt dit nog een veiligheidsrisico (datalek) voor de Kamer?

Groet,
5.1.2.e

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 4 maart 2020 10:55

deze is al eerder afgemeld.

5.1.2.e **onzichtbaar voor aanmelder** — 3 maart 2020 18:03

Warm overgedragen aan 5.1.2.e

Informatie

Aanmelddatum	3 maart 2020 18:01	Standaardoplossing	Er is geen standaardoplossing gekoppeld
Gerealiseerde doorlooptijd	02:25		
Doorlooptijd 'On hold'	00:00	Geëscaleerd	Ja
Aangepaste doorlooptijd	02:25	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	02:25		

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2004 0208 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Verslag en Redactie
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7425
Soort	Mobiel telefoontoestel
Vestiging	Domeinen Roerende Zaken

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	9 april 2020 16:00
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	6 april 2020 15:11
Afgemeld	Ja
Datum afgemeld	6 april 2020 15:22
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 4 april 2020 16:54

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).

a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek

b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek

c) In andere gevallen het incident behandelen als Datalek.

2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 6 april 2020 15:12

SD heeft de noodzakelijke stappen uitgevoerd, full wipe is aangezet. Datalekteam heeft geen nadere vragen en meld het incident gereed.
Incident wordt toegevoegd aan datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 6 april 2020 10:36
Het zou MT7425 betreffen.

5.1.2.e 4 april 2020 18:06
gebruiker heeft aangegeven dat hij zijn telefoon op een bankje buiten kwijt is geraakt. Ligt er niet meer en wordt niet opgenomen als hij belt. Het lukt hem niet om op accounts.google.nl in te loggen om hieruit de locatie te vinden.

5.1.2.e 4 april 2020 16:57
ik heb de full whipe aangezet, gaat om een samsung en dus niet het iphone model. was maar 1 android device op zijn naam in MDM.
Meneer is bereikbaar op 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 4 april 2020 16:54

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante

wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	4 april 2020 16:44		Potentieel datalek
Gerealiseerde doorlooptijd	06:41	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	06:41		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	06:41		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	4 april 2020 15:11
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Nee, standaardprocedure is uitgevoerd door SD
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene heeft vermissing zelf gemeld
Getroffen maatregelen	Standaardprocedure is uitgevoerd door SD
Beschrijving inbreuk	GSM vermist

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2004 0326 Melding datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Facilitaire Dienst
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Melding datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	13 april 2020 13:01
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	7 april 2020 15:12
Afgemeld	Ja
Datum afgemeld	7 april 2020 15:58
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 7 april 2020 15:05

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — Mailimport 7 april 2020 15:01

Datum verzonden: 7-apr-2020 14:43
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: melding datalek

Bijlage n.a.v. overleg met 5.1.2.e

Met vriendelijke groet,

5.1.2.e
5.1.2.e 5.1.2.e
Facilitaire Dienst
Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e 7 april 2020 15:13

Vandaag telefonisch besproken met 5.1.2.e Incident is ter sprake gekomen in MT van 3 februari 2020, maar daarna was er nog geen actie ondernomen richting register datalekken.
Formulier is nu ingevuld ingestuurd.
Oorzaak van het incident is menselijke fout, bestaande procedure is niet gevolgd. FD heeft betrokken collega's gewezen op bestaande procedure inzake afvoer in papiercontainers.
Datalekteam heeft geen verdere vragen en meld dit incident gereed. 5.1.2.e zal 5.1.2.e bedanken voor inzenden formulier. Incident wordt toegevoegd aan datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 7 april 2020 15:06

Melding doorgezet naar het Datalekteam.

5.1.2.e **onzichtbaar voor aanmelder** 7 april 2020 15:05

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	7 april 2020 15:01		Potentieel datalek
Gerealiseerde doorlooptijd	00:11	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:11		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:11		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	1 februari 2020 15:13
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Er is te weinig informatie over datalek om te melden bij AP
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Geen idee wie mogelijke betrokkenen zijn
Mogelijke consequenties	Geen idee, omdat teveel onduidelijk is
Getroffen maatregelen	Bestaande beleid is nogmaal onder de aandacht gebracht
Beschrijving inbreuk	Papiercontainer was overvol en niet goed afgesloten. Weggewaaide docs

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2004 0606 Verlies tablet, potentieel datalek

Tweede Kamer

5.1.2.e Tweede Kamer)

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.1.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Verlies tablet, potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	17 april 2020 12:02
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	12 mei 2020 13:40
Afgemeld	Ja
Datum afgemeld	12 mei 2020 14:58
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 16 april 2020 17:34

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 12 mei 2020 13:40

SD heeft de noodzakelijke stappen, voor zover mogelijk, uitgevoerd. Onduidelijk waarom de tablet niet in de MDM server stond. Melder heeft 20 april nieuwe iPad ontvangen mét MDM. Datalekteam heeft geen nadere vragen en meld het incident gereed. Incident wordt toegevoegd aan datalekregister.

5.1.2.e **onzichtbaar voor** 16 april 2020 17:35

aanmelder
@Datalekteam, mevrouw is haar tablet 4 a 5 maanden geleden verloren. Betreft tabl2026.
In die tijd heeft mevrouw thuis gezocht naar de tablet omdat zij dacht hem thuis verloren te zijn.
De tablet is echter niet meer te vinden, wij kunnen ook geen locatie achterhalen. Een partial wipe of full wipe is niet uit te voeren omdat de tablet niet in de MDM server staat.

5.1.2.e **onzichtbaar voor aanmelder** 16 april 2020 17:34

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder

geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	16 april 2020 17:32		Potentieel datalek
Gerealiseerde doorlooptijd	167:08	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	167:08		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	167:08		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	16 april 2020 13:40
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene is melder
Mogelijke consequenties	Ongeautoriseerde toegang tot i-pad
Getroffen maatregelen	Er is een nieuwe i-pad uitgegeven mét MDM
Beschrijving inbreuk	I-pad verloren gemeld. Geen (partitiele) wipe mogelijk.

Overige Opmerkingen

5.1.2.e 12 mei 2020 13:43

Onduidelijk waarom i-pad niet verbonden is met MDM-server. Nieuwe uitgegeven i-pad wél verbonden met MDM

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2005 0552 Iphone kwijt

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e tweedekamer.nl
Afdeling	PVV
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Iphone kwijt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	19 mei 2020 15:00
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

5.1.2.e	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	25 mei 2020 11:02
Afgemeld	Ja
Datum afgemeld	26 mei 2020 10:02
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 17 mei 2020 16:57

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 17 mei 2020 16:53

Datum verzonden: 17-mei-2020 16:38
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Iphone kwijt

Helaas heb ik mijn iphone laten liggen in de trein.
Kunt u hem blokkeren svp?

5.1.2.e

Sent from my iPad

Actie

5.1.2.e 25 mei 2020 11:02
SD heeft de noodzakelijke stappen uitgevoerd, selective wipe is aangezet. Datalekteam heeft geen nadere vragen en meld het incident gereed.
Incident wordt toegevoegd aan datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 20 mei 2020 9:47
@Datalekteam: Zie onderstaande extra informatie van aanmelder.

5.1.2.e Mailimport 20 mei 2020 9:44
Datum verzonden: 19-mei-2020 13:53
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: I2005 0552 nadere gegevens omtrent verlies telefoon

L.S.,

n.a.v. telefoongesprek heden met dhr. 5.1.2.e over het verlies van mijn door de Kamer verstrekte mobiele telefoon,
beantwoord ik hierbij zijn vraag om nadere gegevens:

1. Waar/wanneer is de telefoon verloren en wat heb ik daarna gedaan ?

Ik heb de telefoon helaas laten liggen in een trein van Arriva. Omdat het oplaadpunt onder de stoel zit, ben ik hem bij het opstaan vergeten.
Betreft de trein van Arriva op zondag 17 mei 2020, welke van station Beek-Elsloo reed naar station Roermond (tijd: 15.52 – 16.26u)
Daar ben ik overgestapt in een NS trein richting Eindhoven. Toen ik mij realiseerde dat ik de telefoon had laten liggen, heb ik met mijn iPad om 16.39u
een mailtje over de vermissing gestuurd naar 5.1.2.i
Omdat ik geen respons kreeg en niet kon bellen, heb ik per mail een kennis verzocht om 5.1.2.i telefonisch in kennis te stellen van de vermissing en te vragen
om de telefoon te blokkeren.
Deze kennis (mevr. 5.1.2.e) bevestigde mij rond 17.00u per mail dat ze telefonisch de melding/verzoek om de telefoon te blokkeren bij 5.1.2.i had gedaan.

2. Dhr 5.1.2.e wil graag een bewijs van aangifte van de vermissing bij de politie.

Dit blijkt niet mogelijk. De politie behandelt geen verloren voorwerpen maar verwijst naar de gemeente (https://www.politie.nl/aangifte-of-melding-doen/melden-van-verloren-goed.html).
Het blijkt dat de gemeente Roermond (waar ik de telefoon in de trein achterliet) ook geen melding van verlies accepteert. Hetzelfde geldt voor Arriva.
Wat de gemeente en Arriva wel doen, is gevonden voorwerpen die bij hen worden gebracht door een vinder op een website (www.iLost.nl) plaatsen.
Als je iets bent verloren kun je daarop kijken en als je daar een identiek voorwerp ziet, kun je dat melden.
Vervolgens treedt dan een procedure in werking waarmee je moet aantonen dat het daadwerkelijk jouw voorwerp is.
Ik heb de vermissing daar gemeld en tevens gekeken in het register van gevonden voorwerpen op die website.
Helaas komt de iphone er niet in voor.

Met vriendelijke groet,
5.1.2.e (Publiek)
Kamerlid

Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 19 mei 2020 13:18
Apparaat is voor het laatst 4 dagen geleden aangeweest.

5.1.2.e **onzichtbaar voor aanmelder** 19 mei 2020 13:11
Het toestel is beveiligd met willekeurige cijfers (geen rijtje of dezelfde cijfers.)
Het toestel is niet beveiligd met een makkelijk te raden code.

Aanmelder gaat aangifte doen bij de politie van verlies/diefstal.

Aanmelder stuurt nog de gegevens op omtrent de tijd van verlies en door hem reeds ondernomen acties.

Wipe is aangevraagd (zie screenshot).Heel

5.1.2.e **onzichtbaar voor aanmelder** 19 mei 2020 12:58
Aanmelder belt terug. Hij heeft al op de site van Arriva gekeken en geeft aan zijn telefoon nog niet tegen te zijn gekomen op de Lost and Found pagina's.

5.1.2.e 18 mei 2020 10:17
Ik mis informatie over de uitvraag naar het wachtwoord. Is de IPhone na het verlaten van de trein online geweest en was de wipe daarmee/daardoor succesvol?

5.1.2.e **onzichtbaar voor aanmelder** 18 mei 2020 8:22
Mijns inziens geen datalek. Er heeft een wipe plaatsgevonden.

5.1.2.e 17 mei 2020 19:00
Dank voor uw bericht. Ik ben met verlof.
Maandag 25 mei 2020 ben ik weer aanwezig en zal ik uw mail beantwoorden.

mvg,
5.1.2.e

5.1.2.e 17 mei 2020 18:39
Op de MDM-server aangemeld. Op gebruiker gezocht en in het overzicht is één iPhone te zien. er is gekozen voor de Selective Wipe. Melding wordt verder doorgezet naar Datalekteam

5.1.2.e 17 mei 2020 18:30
Proxy bypass ingesteld voor MDM server voor de medewerker van de ServiceDesk. Pagina opent nu goed.

5.1.2.e 17 mei 2020 18:18
De juiste link is 5.1.2.h + 5.1.2.i

5.1.2.e **onzichtbaar voor aanmelder** 17 mei 2020 18:02

Ook even 5.1.2.i 5.1.2.e gebeld en hij heeft geadviseerd deze melding bij datalek team te zetten.

5.1.2.e **onzichtbaar voor aanmelder** 17 mei 2020 17:51

MDM link werkt niet in de beheer omgeving van Tweede Kamer. Hiervoor contact opgezocht met Piketdienst 1 en gesproken met 5.1.2.e Hij geeft hiervoor Servicedesk(Piket) Workspace te bellen.
Hij gaat zelf ook naar deze melding kijken.

5.1.2.e **onzichtbaar voor aanmelder** 17 mei 2020 16:57

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail

en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	17 mei 2020 16:53		Potentieel datalek
Gerealiseerde doorlooptijd	50:02	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	50:02		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	50:02		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	17 mei 2020 10:58
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Nee, standaardprocedure is uitgevoerd
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene heeft de vermissing zelf gemeld
Getroffen maatregelen	Selective wipe is aangezet
Beschrijving inbreuk	GSM in trein laten liggen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2005 0553 Hardware - Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e tweedekamer.nl
Afdeling	PVV
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Hardware - Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	19 mei 2020 15:00
Doorlooptijd	16 uur
On hold	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Afgemeld	Ja
Datum afgemeld	18 mei 2020 10:43
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 17 mei 2020 17:05

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 18 mei 2020 10:43

Duplicaat van I2005 0552
Geen SO van in deze categorie.
Melding gesloten.

5.1.2.e **onzichtbaar voor aanmelder** — 17 mei 2020 17:18

Ik kom de MDM website niet op. Hierdoor gebeld naar piket.
Piket heeft niet opgenomen

5.1.2.e **onzichtbaar voor aanmelder** — 17 mei 2020 17:08

Tel van verloren telefoon

5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 17 mei 2020 17:08

Aanmelder: 5.1.2.e

Tel: 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 17 mei 2020 17:05

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde

cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	17 mei 2020 17:04	Potentieel datalek
Gerealiseerde doorlooptijd	02:13	
Doorlooptijd 'On hold'	00:00	
Aangepaste doorlooptijd	02:13	
Doorlooptijd 'Afgerond'	00:00	
Doorlooptijd 'Uitvoering'	02:13	

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Behandelaar	Servicedesk
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2005 1010 Hardware - Telefonie - Phising

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e 5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Hardware - Telefonie - Phising
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	2 juni 2020 15:00
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	26 augustus 2020 11:54
Afgemeld	Ja
Datum afgemeld	26 augustus 2020 11:54
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 2 juni 2020 11:01

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — 31 mei 2020 15:03

De gebruiker geeft aan dat zij slachtoffer is van WhatsApp fraude.

5.1.2.e 5.1.2.e

Actie

5.1.2.e — 26 augustus 2020 11:54

In overleg met 5.1.2.e en het Security team gesloten.

5.1.2.e **onzichtbaar voor aanmelder** 2 juni 2020 9:14
@ST: Zie onderstaande voor info van TOPDesk kaart aangaande het telefoonnummer.

5.1.2.e 1 juni 2020 18:03
Zijn drie extra meldingen van zelfde soort berichten binnen gekomen.
I2006 0003, I2006 0004 en I2006 0005

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 19:03
Het wordt niet dinsdag, maar zoveel mogelijk vandaag opgepakt.

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 17:30
5.1.2.e weer gebeld. Dit wordt dinsdag verder opgepakt.
We kunnen niet zien of dit nummer eventueel actief is.

Er is geen datalek en er is geen telefoon kwijt.

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 17:03
5.1.2.e heeft gebeld en gevraagd of dit nummer eventueel actief is.

Ik bel hem dalijk terug met een antwoord

Tel: 5.1.2.e

5.1.2.e Mailimport 31 mei 2020 15:40
Datum verzonden: 31-mei-2020 15:06
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Schermfoto 2020-05-31 om 15.05.31 I2005 1010

Hallo 5.1.2.e

Bijgaand het nummer van 5.1.2.e 5.1.2.e oud tweede kamerlid vd PvdA.

Hrt grt 5.1.2.e 5.1.2.e

5.1.2.e 5.1.2.e Mailimport 31 mei 2020 15:40
Datum verzonden: 31-mei-2020 14:58
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: 5.1.2.e 5.1.2.e @tweedekamer.nl>
Onderwerp: Fwd: Vals bericht I2005 1010

Begin doorgestuurd bericht:

Van: 5.1.2.e <5.1.2.e@5.1.2.e>
Datum: 31 mei 2020 om 14:14:24 CEST
Aan: "5.1.2.e 5.1.2.e @tweedekamer.nl>
Onderwerp: Vals bericht

Dag 5.1.2.e

Hopelijk gaat t allemaal goed met je.

Vandaag ontving ik een app bericht vanaf jouw 06-183 nummer met een verzoek om 500 euro. Dat bericht komt natuurlijk niet van jou. Goed om dit wel te weten en te melden bij de beveiligingsbeambte van de Kamer.

Met vriendelijke groet,

5.1.2.e 5.1.2.e
Tel 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 15:19
Mailtje verstuurd naar 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 15:14
De derde security officer nam op. Hij vraagt om een samenvatting van het incident per mail

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 15:10
Bij de tweede gaat die geen eens over

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 15:09
Ik heb hiervoor de eerste Security Officer gebeld om aan te geven dat dit probleem speelt, hij nam niet op

5.1.2.e **onzichtbaar voor aanmelder** 31 mei 2020 15:05
De aanmelder geeft aan dat ze zelf ook een andere nummer van een oud tweede kamer lid heeft ontvangen (5.1.2.e 5.1.2.e).
Precies hetzelfde bericht

5.1.2.e 31 mei 2020 15:03
Tel van 5.1.2.e 5.1.2.e

Het nummer dat meneer 5.1.2.e ziet is: 5.1.2.e
Dit is het oude nummer.

Het bericht:
Kan jij misschien 500 euro overmaken ....

Informatie

Aanmelddatum	31 mei 2020 14:52		Potentieel datalek
Gerealiseerde doorlooptijd	592:24	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	592:24		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	592:24		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	31 mei 2020 14:38
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Telefoonspoofing

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2006 0002 Telefoon kwijt

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	PvdA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Telefoon kwijt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7522
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	3 juni 2020 17:17
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	4 juni 2020 14:28
Afgemeld	Ja
Datum afgemeld	5 juni 2020 9:30
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 1 juni 2020 15:14

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteam

5.1.2.e Mailimport 1 juni 2020 15:08

Datum verzonden: 1-jun-2020 11:24
Naar: 5.1.2.i < 5.1.2.i @tweedekamer.nl>
Onderwerp: Telefoon kwijt

Beste,

Gister ben ik mijn telefoon kwijtgeraakt. Ik heb een van mijn tassen bij mijn voordeur vergeten en toen ik erachter kwam was deze helaas al weg. De telefoon stond uit en ik kan de locatie dus niet

achterhalen met de Find my IPhone app. Hierbij de vraag welke stappen ik moet nemen gezien dit een telefoon van de Kamer betreft? Vast dank voor jullie hulp.

Met vriendelijke groet,

5.1.2.e
Politiek adviseur PvdA-Tweede Kamerfractie
M 5.1.2.e

Actie

5.1.2.e 4 juni 2020 14:28
SD heeft de noodzakelijke stappen uitgevoerd, selectieve wip is uitgevoerd via Xen Mobile console. Datalekteam heeft geen nadere vragen en meld het incident gereed. Het incident wordt toegevoegd aan het datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 4 juni 2020 9:44
Mevr. 5.1.2.e belde voor een update over de situatie. Onderstaande genomen acties met haar doorgenomen. Mevr. 5.1.2.e was hiermee gerustgesteld.

5.1.2.e **onzichtbaar voor aanmelder** 3 juni 2020 15:42
Naar aanleiding van onderstaande bericht van aanmelder, een update van de situatie verstuurd.

5.1.2.e Mailimport 3 juni 2020 15:38
Datum verzonden: 3-jun-2020 15:03
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2006 0002 - Aanmelding Datalekteam

Beste,

Ik begrijp na mijn mail van vanmorgen niet precies wat ik met deze mail en bijlage moet?

Kunt u mij laten weten welke stappen ik moet nemen om een nieuwe telefoon te krijgen?

Vast dank

Met vriendelijke groet,

5.1.2.e
Politiek adviseur PvdA-Tweede Kamerfractie
M 5.1.2.e

> Op 3 jun. 2020 om 12:25 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte mevrouw 5.1.2.e
>
>
> Melding met nummer: I2006 0002 is aangemaakt.
>
> Het betreft :Telefoon kwijt
>
> De Dienst Automatisering draagt uw melding ter verdere afhandeling over aan het Datalekteam .
>
> Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.
>
> Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande personen:
>
> Dhr. 5.1.2.e tst. 5.1.2.e
> Mw. 5.1.2.e tst. 5.1.2.e
> Dhr. 5.1.2.e tst. 5.1.2.e
> Dhr. 5.1.2.e tst 5.1.2.e
>
> Met vriendelijke groet,
>

> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl
> <Formulier melding datalek - Tweede Kamer v3.docx>

5.1.2.e **onzichtbaar voor aanmelder** 3 juni 2020 10:54

Selective Wipe is uitgevoerd via Xen Mobile console

5.1.2.e Mailimport 3 juni 2020 10:42

Datum verzonden: 3-jun-2020 10:18
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2006 0002 Telefoon kwijt

Beste,

Hierbij de nadere informatie over de verloren telefoon. Nog een vraag: betekent het volledig wipen van de telefoon dat er geen enkele informatie meer is om vanuit de cloud te downloaden naar een nieuwe telefoon? Als dat het geval is graag alleen de wipe die Kamerinformatie laat verdwijnen. Mocht ik met een complete wipe wel nog een nieuwe telefoon kunnen installeren met al mijn contacten etc vanuit de cloud, dan mag er een volledige wipe gebeuren.

- IPhone 7
- Ja het is een telefoon verstrekt door de Kamer
- Ja het is een serieel code
- Nee het is een betrekkelijk lastige code
- Mocht het nodig zijn kunt u mij bereiken op het nummer van mijn partner: 5.1.2.e

Dat leidt mij tot een laatste vraag: gezien de thuiswerksituatie en het feit dat ik niet over een andere telefoon beschik is het momenteel erg puzzelen hoe ik mijn werk goed kan doen. Kunt u mij een indicatie geven van hoe lang het duurt voordat ik een nieuwe telefoon zou kunnen ontvangen? Moet ik daar met mijn HR functionaris of iemand anders nog wat voor doen? En tot slot, is het mogelijk mijn oude nummer te behouden gezien mijn contacten dat nummer hebben en overstappen lastig is?

Vast dank!

Met vriendelijke groet,

5.1.2.e
Politiek adviseur PvdA-Tweede Kamerfractie
M 5.1.2.e

> Op 1 jun. 2020 om 16:07 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte mevrouw 5.1.2.e
>
> Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.
>
> Wij zullen de mobile telefoon vanaf afstand "wipen". Dit betekend dat als iemand hem online laat komen, dat alle kamergegevens verwijderd worden.
> We kunnen ook een volledige wipe instellen. Dan zal ook alle eventuele privé data van de telefoon verwijderd worden. Dit moet echter wel ook in overleg met u gebeuren.
> Graag horen we dan ook als u graag heeft als we de full wipe uitvoeren.
>
> Voor u hebben we de volgende vragen:
> -Wat is het merk en model van de telefoon?
> -Is het een door ons uitgegeven telefoon?
> -Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i' of '5.1.2.h + 5.1.2.i')?
> -Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar, postcode) of is het een lastigere code? (Graag niet de code zelf noemen bij het antwoorden)

> -Op welk telefoonnummer bent u op het moment bereikbaar voor eventueel verder contact?
>
> Verder raden we u aan aangifte bij de politie te doen van deze verdwijning.
>
> U kunt de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail. Wanneer wij binnen 3 werkdagen
> niets van u vernemen, dan gaan wij ervan uit dat het incident niet meer actueel is en sluiten wij deze.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 1 juni 2020 17:01

Er staat geen gekoppelde telefoon in topdesk.
Ik kan niet bij
5.1.2.h + 5.1.2.i
De handleiding voor mRemote is niet terug te vinden, is niet bijgevoegd in het SO en niet kunnen vinden op SharePoint.
Aangegeven in overdracht dat de telefoon nog gewiped moet worden.

5.1.2.e geprobeerd te bellen, maar ze nam niet op. Waarschijnlijk is 5.1.2.e het nummer van de missende telefoon.
Mail gestuurd met de belangrijke vragen en stappen. Plus het vragen om een telefoonnummer waar ze wel op bereikbaar is.

5.1.2.e 1 juni 2020 16:04

Wij zullen de mobile telefoon vanaf afstand "wipen". Dit betekend dat als iemand hem online laat komen, dat alle kamergegevens verwijderd worden.
We kunnen ook een volledige wipe instellen. Dan zal ook alle eventuele privé data van de telefoon verwijderd worden. Dit moet echter wel ook in overleg met u gebeuren.

Voor u hebben we de volgende vragen:
-Wat is het merk en model van de telefoon?
-Is het een door ons uitgegeven telefoon?
-Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
-Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar, postcode) of is het een lastigere code? (Graag niet de code zelf noemen bij het antwoorden)
-Op welk telefoonnummer bent u op het moment bereikbaar voor eventueel verder contact?

Verder raden we u aan aangifte bij de politie te doen van deze verdwijning.

5.1.2.e **onzichtbaar voor aanmelder** 1 juni 2020 15:14

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	1 juni 2020 15:08		Potentieel datalek
Gerealiseerde doorlooptijd	27:50	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	05:09		
Aangepaste doorlooptijd	22:41		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	22:41		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	1 juni 2020 14:37
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	GSM verloren

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2006 0003 Phishing via oud telefoonnummer

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	VVD
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Phishing via oud telefoonnummer
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	4 juni 2020 8:36
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	26 augustus 2020 11:54
Afgemeld	Ja
Datum afgemeld	26 augustus 2020 11:54
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 2 juni 2020 11:46

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 1 juni 2020 17:07

Datum verzonden: 1-jun-2020 9:31
Naar: 5.1.2.i < 5.1.2.i @tweedekamer.nl>
Onderwerp: 5.1.2.e 5.1.2.e

Ook ik ontving een verzoek van 5.1.2.e 5.1.2.e voor 500,-
Verstuurd vanaf mijn iPhone

Actie

5.1.2.e 26 augustus 2020 11:54
In overleg met 5.1.2.e en het Security team gesloten.

5.1.2.e **onzichtbaar voor aanmelder** 5 juni 2020 9:32
@ST: Zie onderstaande melding. Ik weet niet of dit nu door jullie al is behandeld of niet.

5.1.2.e 4 juni 2020 15:03
Dit betreft een incident voor het securityteam en niet voor het datalekteam. Gaat over telefoonspoofing via Whatsapp-berichten.
Incident wordt door het datalekteam gereedgemeld

5.1.2.e **onzichtbaar voor aanmelder** 2 juni 2020 8:31
@ST: Zie onderstaande melding.

5.1.2.e 1 juni 2020 17:54
Verwant aan I2005 1010

Informatie

Aanmelddatum	1 juni 2020 17:07		Potentieel datalek
Gerealiseerde doorlooptijd	583:47	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	583:47		
Doorlooptijd 'Afgerond'	03:59		
Doorlooptijd 'Uitvoering'	579:48		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	1 juni 2020 14:36
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Telefoonspoofing

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2006 0004 Melding fakebericht

5.1.2.e 5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	SGP
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Melding fakebericht
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	3 juni 2020 14:07
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	26 augustus 2020 11:54
Afgemeld	Ja
Datum afgemeld	26 augustus 2020 11:54
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — Mailimport 1 juni 2020 17:07

Datum verzonden: 1-jun-2020 12:15
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Melding fakebericht

Beste mensen,

Via de ambtelijk secretaris kreeg ik het bericht over telefoonspoofing. Ook ik heb gisteren via whatsapp het bericht gehad uit naam van 5.1.2.e 5.1.2.e Het was in mijn waarneming evident fake, daarom heb ik het onmiddellijk verwijderd.

Met harteljjke groet,
5.1.2.e 5.1.2.e

Verstuurd vanaf mijn iPhone

Actie

5.1.2.e — 26 augustus 2020 11:54
In overleg met 5.1.2.e en het Security team gesloten.

5.1.2.e **onzichtbaar voor aanmelder** — 2 juni 2020 8:32
@ST: Zie onderstaande melding.

5.1.2.e — 1 juni 2020 17:55
Verwant aan I2005 1010

Informatie

Aanmelddatum	1 juni 2020 17:07	Standaardoplossing	Er is geen standaardoplossing gekoppeld
Gerealiseerde doorlooptijd	583:47		
Doorlooptijd 'On hold'	00:00	Geëscaleerd	Ja
Aangepaste doorlooptijd	583:47	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	583:47		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	1 juni 2020 14:35
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Telefoonspoofing

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2006 0005 Telefoonspoofing

5.1.2.e Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	PvdA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Telefoonspoofing
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	3 juni 2020 14:07
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	26 augustus 2020 11:54
Afgemeld	Ja
Datum afgemeld	26 augustus 2020 11:54
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — Mailimport 1 juni 2020 17:07

Datum verzonden: 31-mei-2020 21:10
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Telefoonspoofing 5.1.2.e 5.1.2.e

Ik heb ook telefoonspoofing bericht van 5.1.2.e 5.1.2.e gehad. En meteen haar nummer geblokkeerd. Hartelijke groet 5.1.2.e
Verstuurd vanaf mijn iPhone

Actie

5.1.2.e — 26 augustus 2020 11:54

In overleg met 5.1.2.e en het Security team gesloten.

5.1.2.e **onzichtbaar voor aanmelder** — 2 juni 2020 9:41

5.1.2.e **onzichtbaar voor aanmelder** — 2 juni 2020 8:32

@ST: Zie onderstaande melding.

5.1.2.e — 1 juni 2020 17:55

Verwant aan I2005 1010

Informatie

Aanmelddatum	1 juni 2020 17:07	Standaardoplossing	Er is geen standaardoplossing gekoppeld
Gerealiseerde doorlooptijd	583:47		
Doorlooptijd 'On hold'	00:00	Geëscaleerd	Ja
Aangepaste doorlooptijd	583:47	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	583:47		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	1 juni 2020 14:35
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Telefoonspoofing

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2006 0771 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2h + 5.1.2i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	PvdA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	18 juni 2020 16:48
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	18 juni 2020 19:56
Afgemeld	Ja
Datum afgemeld	19 juni 2020 9:36
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 16 juni 2020 19:16

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 18 juni 2020 19:56

De heer 5.1.2.e is vandaag bij de balie langsgekomen en zijn nieuw toestel in ontvangst genomen.
melding wordt bij deze afgesloten.

5.1.2.e **onzichtbaar voor aanmelder** — 18 juni 2020 9:39

TODO:
- Contact opnemen met aanmelder en afspraak maken met aanmelder voor het ophalen van zijn nieuwe telefoon (volgens W2006 199 ligt die al klaar op de plank).

5.1.2.e Mailimport 18 juni 2020 9:36
Datum verzonden: 17-jun-2020 14:13
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2006 0771 Potentieel datalek

Beste collega's,

Zouden jullie een indicatie kunnen geven van wanneer ik mogelijk weer de beschikking heb over een telefoon?

Alvast bedankt!

Vriendelijke groet,

5.1.2.e 5.1.2.e
Lid Tweede Kamer Partij van de Arbeid
Woordvoerder Zorg/Defensie

> Op 16 jun. 2020 om 19:40 heeft 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.
>
> Wij zullen de mobile telefoon vanaf afstand "wipen". Dit betekend dat als iemand hem online laat komen, dat alle kamergegevens verwijderd worden.
> We kunnen ook een volledige wipe instellen. Dan zal ook alle eventuele privé data van de telefoon verwijderd worden. Dit moet echter wel ook in overleg met u gebeuren.
> Graag horen we dan ook als u graag heeft als we de full wipe uitvoeren.
>
> Voor u hebben we de volgende vragen:
> -Wat is het merk en model van de telefoon?
> -Is het een door ons uitgegeven telefoon?
> -Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ' of ' 5.1.2.h + 5.1.2.i ')?
> -Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar, postcode) of is het een lastigere code? (Graag niet de code zelf noemen bij het antwoorden)
> -Op welk telefoonnummer bent u op het moment bereikbaar voor eventueel verder contact?
>
> Verder raden we u aan aangifte bij de politie te doen van deze verdwijning.
>
> U kunt de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail. Wanneer wij binnen 3 werkdagen
> niets van u vernemen, dan gaan wij ervan uit dat het incident niet meer actueel is en sluiten wij deze.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 17 juni 2020 17:22
SD heeft de noodzakelijke stappen uitgevoerd, full wipe is aangezet. Datalekteam heeft geen nadere vragen en meld het incident gereed.

Incident wordt toegevoegd aan datalekregister.

5.1.2.e Mailimport 17 juni 2020 10:32
Datum verzonden: 17-jun-2020 10:30
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: RE: I2006 0771 - Aanmelding Datalekteam

Dag collega's,

Hierbij het door mij ingevulde formulier.

Met vriendelijke groet,

5.1.2.e

Postbus 20018, 2500 EA
5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: dinsdag 16 juni 2020 19:26
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2006 0771 - Aanmelding Datalekteam

5.1.2.e

Melding met nummer: I2006 0771 is aangemaakt.

Het betreft :Potentieel datalek

De Dienst Automatisering draagt uw melding ter verdere afhandeling over aan het Datalekteam .

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande personen:

Dhr. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst 5.1.2.e

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 21:17
Het lijkt om MT7488 Gevonden door het serienummer uit de screenshot te zoeken onder "Objecten"
Toestel is nooit 06 gekoppeld lijkt.

IMEI: 5.1.2.h + 5.1.2.i
Serienummer: 5.1.2.h + 5.1.2.i

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 19:54

Full wipe requested op basis van onderstaand email

5.1.2.e Mailimport 16 juni 2020 19:53
Datum verzonden: 16-jun-2020 19:50
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2006 0771 Potentieel datalek

Dag.

Even puntsgewijs.

Iphone 7
Uitgegeven door jullie (juni 2018)
Code met identieke cijfers
Code makkelijk te raden
Alternatief telefoonnummer volgt (voor die tijd: via de email).

Jullie mogen een full wipe uitvoeren

Vriendelijke groet,

5.1.2.e 5.1.2.e
Lid Tweede Kamer Partij van de Arbeid
Woordvoerder Zorg/Defensie

> Op 16 jun. 2020 om 19:40 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.
>
> Wij zullen de mobile telefoon vanaf afstand "wipen". Dit betekend dat als iemand hem online laat komen, dat alle kamergegevens verwijderd worden.
> We kunnen ook een volledige wipe instellen. Dan zal ook alle eventuele privé data van de telefoon verwijderd worden. Dit moet echter wel ook in overleg met u gebeuren.
> Graag horen we dan ook als u graag heeft als we de full wipe uitvoeren.
>
> Voor u hebben we de volgende vragen:
> -Wat is het merk en model van de telefoon?
> -Is het een door ons uitgegeven telefoon?
> -Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i' of '5.1.2.h + 5.1.2.i')?
> -Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar, postcode) of is het een lastigere code? (Graag niet de code zelf noemen bij het antwoorden)
> -Op welk telefoonnummer bent u op het moment bereikbaar voor eventueel verder contact?
>
> Verder raden we u aan aangifte bij de politie te doen van deze verdwijning.
>
> U kunt de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail. Wanneer wij binnen 3 werkdagen
> niets van u vernemen, dan gaan wij ervan uit dat het incident niet meer actueel is en sluiten wij deze.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 19:39

Gebeld op kamer vast nummer => niet kunnen bereiken
Onderstaand in een mail gestuurd:

Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.

Wij zullen de mobile telefoon vanaf afstand "wipen". Dit betekend dat als iemand hem online laat komen, dat alle kamergegevens verwijderd worden.

We kunnen ook een volledige wipe instellen. Dan zal ook alle eventuele privé data van de telefoon verwijderd worden. Dit moet echter wel ook in overleg met u gebeuren.
Graag horen we dan ook als u graag heeft als we de full wipe uitvoeren.

Voor u hebben we de volgende vragen:
-Wat is het merk en model van de telefoon?
-Is het een door ons uitgegeven telefoon?
-Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
-Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar, postcode) of is het een lastigere code? (Graag niet de code zelf noemen bij het antwoorden)
-Op welk telefoonnummer bent u op het moment bereikbaar voor eventueel verder contact?

Verder raden we u aan aangifte bij de politie te doen van deze verdwijning.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 19:34

Bewust nog niet nummer op ander simkaart overgezet ivm uitgezette selective wipe opdracht

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 19:32

Selective requested

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 19:25

Betrfet 5.1.2.e => ik zie geen telefoon gekoppeld aan dit nummer
Imei in Xen mobile kunnen vinden 5.1.2.h + 5.1.2.i
Selective wipe uitgevoerd

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2020 19:16

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden

gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	16 juni 2020 19:11		Potentieel datalek
Gerealiseerde doorlooptijd	19:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	19:00		
Doorlooptijd 'Afgerond'	01:48		
Doorlooptijd 'Uitvoering'	17:12		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	15 juni 2020 17:19
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Nee, standaardprocedure is uitgevoerd door SD
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Betrokkene heeft vermissing zelf gemeld
Getroffen maatregelen	Standaardprocedure full wipe is uitgevoerd door SD
Beschrijving inbreuk	GSM verloren

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2007 0450 Telefoon verloren

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2h + 5.1.2i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Telefoon verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7585
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	14 juli 2020 16:58
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	17 juli 2020 9:02
Afgemeld	Ja
Datum afgemeld	17 juli 2020 9:02
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 13 juli 2020 9:56

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — 12 juli 2020 22:28

De gebruiker meldt dat het mobiele apparaat niet naar behoren functioneert.

5.1.2.e — Mailimport 12 juli 2020 22:21

Datum verzonden: 11-jul-2020 19:00
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Telefoon

Beste helpdesk,

Helaas is mijn telefoon in de Waddenzee gevallen toen ik een enthousiast filmpje wilde maken. Graag bespreek ik maandag wat de mogelijkheden zijn om een nieuwe telefoon op te sturen. Ik hoop dat dit mogelijk is?

Hartelijke groet,

5.1.2.e
D66

Verstuurd vanaf mijn iPad

Actie

5.1.2.e **onzichtbaar voor aanmelder** 17 juli 2020 9:02
Daar de beveiliging al heeft aangegeven met deze melding klaar te zijn, de simkaart reeds is opgestuurd en er een wijziging loopt voor vervanging van de verloren mobiel, wordt dit incident afgemeld.

5.1.2.e Mailimport 16 juli 2020 16:53
Datum verzonden: 16-jul-2020 16:20
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0450 Telefoon verloren

Heel veel dank voor de goede service!

Verstuurd vanaf mijn iPad

> Op 16 jul. 2020 om 15:17 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Hierbij willen wij u informeren over de status van uw incident beschreven in het onderwerp van deze e-mail.
>
> Uw rijkspas is geblokkeerd. Vanaf 24 augustus ligt de nieuwe Rijkspas klaar. De Servicebalie is nu gesloten. Zij zijn vanaf 24 augustus weer open van maandag t/ m donderdag van 09.00 uur – 13.00 uur Vrijdag gesloten. Wilt u een paspoort of ID-kaart meenemen (GEEN RIJBEWIJS) bij het afhalen van zijn nieuwe Rijkspas?
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 16 juli 2020 16:19
Simkaart is gestuurd op 16-07-2020
track en trace: 3SRRDT4821854

5.1.2.e **onzichtbaar voor aanmelder** 16 juli 2020 15:17
Onderstaande doorgegeven aan aanmelder.

mailimport, m Mailimport 16 juli 2020 15:15
Afzender: 5.1.2.i @tweedekamer.nl
Datum verzonden: 16-jul-2020 13:32
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2007 0450 Telefoon verloren

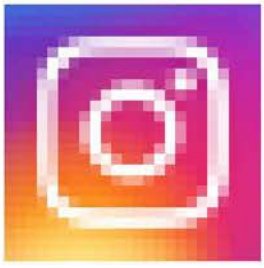
De pas van dhr. 5.1.2.e is geblokkeerd. Vanaf 24 augustus ligt de nieuwe Rijkspas klaar.

De Servicebalie is nu gesloten. Zij zijn vanaf 24 augustus weer open van maandag t/ m donderdag van 09.00 uur – 13.00 uur
Vrijdag gesloten.
Dhr. 5.1.2.e moet wel een paspoort of ID-kaart meenemen (GEEN RIJBEWIJS) bij het afhalen van zijn nieuwe Rijkspas.

gr. 5.1.2.e

Met vriendelijke groet,

5.1.2.e
Managementassistent
Beveiligingsdienst
Tweede Kamer der Staten-Generaal
Lange Houtstraat 1 kamer 5.1.2.e **2511 CV Den Haag**
T +(5.1.2.e **| F +(**5.1.2.e **| M +(**5.1.2.e
E 5.1.2.e **@tweedekamer.nl | I www.tweedekamer.nl**



Wacht niet op het perfecte moment, maar pak het moment en maak het perfect

Van: 3060
Verzonden: donderdag 16 juli 2020 11:10
Aan: 5.1.2.i
CC: 5.1.2.e
Onderwerp: I2007 0450 Telefoon verloren

Geachte heer/mevrouw,

De heer 5.1.2.e (5.1.2h + 5.1.2i) is zijn rijkspas verloren in de Waddenzee. Graag verzoeken we u om zijn pas te blokkeren.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
5.1.2.i

5.1.2.e Mailimport 16 juli 2020 13:57
Datum verzonden: 16-jul-2020 13:52
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0450 Telefoon verloren

Heel veel dank daarvoor!

Het adres waar de SIM-kaart naar kan worden opgestuurd is:

5.1.2.e

Hartelijke groet,

5.1.2.e

Verstuurd vanaf mijn iPad

> Op 16 jul. 2020 om 11:12 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Hierbij willen wij u informeren over de status van uw incident beschreven in het onderwerp van deze e-mail.
>
> Helaas kunnen we niet een telefoon aan u opsturen in Harlingen. Wel is er besloten, na overleg, dat een simkaart opgestuurd kan worden. Zou u ons het adres kunnen toesturen naar waar wij deze simkaart kunnen sturen? U kunt dan op een later tijdstip uw telefoon ophalen bij de servicedesk balie.
>
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 16 juli 2020 11:10
Mail aanmelder beantwoord dat we niet een telefoon kunnen opsturen, maar wel een simkaart.

5.1.2.e **onzichtbaar voor aanmelder** 16 juli 2020 11:06
Met dhr. 5.1.2.e van de beveiligingsdienst was toevallig aan de balie. Het probleem met betrekking tot de pas aan hem voorgelegd. Hij gaf aan dat er een mail gestuurd kon worden aan het beveiligingssecretariaat met in de cc 5.1.2.e met het verzoek om de pas van aanmelder te blokkeren. Dit gedaan vanuit dit incident.

5.1.2.e Mailimport 16 juli 2020 10:55
Datum verzonden: 16-jul-2020 10:31
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0450 Telefoon verloren

Goedemorgen!

Hartelijk dank voor uw bericht. Betekent dit dat de telefoon naar Harlingen wordt gestuurd? Vriendelijke groet,
5.1.2.e

Verstuurd vanaf mijn iPad

Op 15 jul. 2020 om 13:25 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:

Geachte heer 5.1.2.e

Uw incident beschreven in het onderwerp is in behandeling genomen onder incidentnummer: I2007 0450.

Wilt u weten wat de voortgang is van deze melding? Kijkt u dan op Plein2 > Aanvragen & hulp > ICT-service online.

Voor vragen is de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 16 juli 2020 10:41
Ik meld de melding gereed. Geen (ernstig) datalek (hoewel verlies van informatie op zich ook een datalek kan zijn) . Verder eens met heeft feit dat er geen telefoon opgestuurd gaat worden. Minder bereikbaarheid kan snel opgelost worden om in Den Haag een afspraak te maken.

Ik zie wel dat de toegangspas ook verloren is gegaan bij het maken van het filmpje. Los van de vraag over hoe dit dan kan, lijkt me een melding bij de beveiligingsdienst van belang. Die dingen kunnen drijven en gevonden worden. Pakken jullie die op?

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 11:39
Nagevraagd bij dhr. 5.1.2.e met betrekking tot het opsturen van een telefoon. We kunnen geen telefoon opsturen. Wel een simkaart. Aanmelder zou hiermee beperkte mogelijkheden hebben voor communicatie binnen de Tweede Kamer.

5.1.2.e Mailimport 13 juli 2020 11:23
Datum verzonden: 13-jul-2020 11:16
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0450 Telefoon

Heel veel dank voor de service, bijgaand de antwoorden op de gestelde vragen,
Met vriendelijke groet,
5.1.2.e

NB Het zou heel fijn zijn als de telefoon kan worden verzonden aan:
4.1.1

Verstuurd vanaf mijn iPad

> Op 13 jul. 2020 om 10:28 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.
>
> - We wilden graag een wipe uitvoeren op uw toestel. Dit kan in de vorm van een partial wipe (waarbij enkel de gegevens van de Tweede Kamer worden verwijdert) of een full wipe (waarbij alle gegevens worden verwijdert). Wij wilden graag weten welke van deze twee vormen voor u de voorkeur heeft.

Liefst een partial wipe, nog liever helemaal geen wipe.

> - Heeft u hier melding van gemaakt bij de politie? Dit kan o.a via https://www.verlorenofgevonden.nl/. Zo niet, dan raden we u aan dit alsnog te doen en een kopie van het proces verbaal aan ons toe te sturen.

Ja, net verstuurd
>
> - Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i' of '5.1.2.h + 5.1.2.i')?
>

Nee

> - Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
>
Nee

> - Zou u voor ons zo nauwkeurig mogelijk de omstandigheden (tijd/locatie) waaronder u de telefoon verloren heeft?
>

Telefoon is overboord gevallen in het vaarwater tussen Terschelling en Vlieland

> U kunt de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e

Mailimport 13 juli 2020 11:23

Datum verzonden: 13-jul-2020 11:13
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: I2007 0450 Fwd: Bevestiging registratie verloren voorwerp V0093-2020000176

Bijlage bij I 2007 0450

Verstuurd vanaf mijn iPad

Begin doorgestuurd bericht:

Van: Gemeente Terschelling Verloren of Gevonden <noreply@verlorenofgevonden.nl>
Datum: 13 juli 2020 om 11:12:59 CEST
Aan: "5.1.2.e " <5.1.2.e @tweedekamer.nl>
Onderwerp: Bevestiging registratie verloren voorwerp V0093-2020000176
Antwoord aan: gemeente@terschelling.nl

PerfectView

Registratie verloren voorwerp V0093-2020000176

[https://resources.perfectview.nl/logos/640x100_Verlorenofgevonden_Logo.png]

Geachte heer 5.1.2.e
Bij deze ontvangt u een bevestiging van de registratie van uw **verloren** voorwerp bij de Gemeente Terschelling met registratienummer **V0093-2020000176**.
Het betreft de registratie met de volgende omschrijving.

Het verloren voorwerp
Beschrijving iPhone
Categorie apparatuur - mobiele telefoon
Kleur zwart
Merk Apple Iphone
Opschrift Geen
Waarde groter dan 450 Euro

De locatie
Plaats Terschelling
Locatie Stortemelk
Verloren op 11-07-2020

Uw gegevens

De 5.1.2.e

U heeft aangegeven dat
- u deze gegevens naar waarheid heeft ingevuld.
- u akkoord gaat met de privacy statement van de gemeente.

Klik hier als u het voorwerp heeft teruggevonden en wilt afmelden bij de gemeente.

De melding van het verloren voorwerp wordt na 3 maanden (waarde voorwerp minder dan € 450) of na 1 jaar (waarde voorwerp groter dan €450) gearchiveerd en daarmee niet meer bewaakt door de gemeente.

Meer informatie over uw rechten en plichten ten aanzien van verloren en gevonden voorwerpen kunt u nalezen op de FAQ pagina.

Heeft u vragen neem dan contact op met de Gemeente Terschelling.

Adres Burg. van Heusdenweg 10A Telefoon
8881 EB E-mail gemeente@terschelling.nl
Terschelling Website

5.1.2h + 5.1.2i

5.1.2.e

Mailimport 13 juli 2020 10:47

Datum verzonden: 13-jul-2020 10:30
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0450 Telefoon

Goedemorgen!

Ik bel u zo even. De telefoon lig op de bodem van de zee, dus ik ben niet bang voor een datalek. Mijn OV-kaart en toegangspas voor de kamer zaten er ook in, dus ik hoop dat we een oplossing kunnen vinden. Ik bel u zo even met de telefoon van mijn vriendin. Kan dat op nummer 5.1.2.i ?
Vriendelijke groet,
5.1.2.e

Verstuurd vanaf mijn iPad

> Op 13 jul. 2020 om 10:28 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.
>
> - We wilden graag een wipe uitvoeren op uw toestel. Dit kan in de vorm van een partial wipe (waarbij enkel de gegevens van de Tweede Kamer worden verwijdert) of een full wipe (waarbij alle gegevens worden verwijdert). Wij wilden graag weten welke van deze twee vormen voor u de voorkeur heeft.
>
> - Heeft u hier melding van gemaakt bij de politie? Dit kan o.a via https://www.verlorenofgevonden.nl/. Zo niet, dan raden we u aan dit alsnog te doen en een kopie van het proces verbaal aan ons toe te sturen.
>
> - Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i ' of '5.1.2.h + 5.1.2.i ')?
>
> - Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
>
> - Zou u voor ons zo nauwkeurig mogelijk de omstandigheden (tijd/locatie) waaronder u de telefoon verloren heeft?
>
> U kunt de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 10:46
Aanmelder belde terug. Hij zal de vragen die hem zijn toegestuurd beantwoorden. Aanmelder wilde graag weten of wij ook over zijn Ov-kaart gaan. Aangegeven dat hij dit met de AS'er van zijn fractie dient te bespreken. Aanmelder wilde weten of wij de nieuwe telefoon naar Harlingen konden opsturen. Aangegeven dit intern te zullen bespreken en contact met aanmelder hierover zullen opnemen. Aanmelder is te bereiken per mail of door te bellen naar 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 10:28
Mail gestuurd met extra vragen.

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 9:57
Gaat door in W2007 120.

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 9:56
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 8:23
TODO:
- Bespreken met coordinatie.
- Wijziging voor vervanging starten.

5.1.2.e **onzichtbaar voor aanmelder** 13 juli 2020 8:21

Dit verzoek is ingediend als incident, terwijl het eigenlijk als wijziging had moeten worden ingeschoten. Dit incident dient gesloten te worden en verder afgehandeld te worden via het relevante wijzigingssjabloon.
Koppel de betreffende wijziging aan dit incident via "opgelost door wijziging". Beoordeel zelf of de gebruiker over het sluiten van dit incident moet worden gemaild; indien je de gebruiker mailt, vermeld dan het wijzigingsnummer waarin het verzoek verder wordt afgehandeld en vraag om verder dit nummer te gebruiken in het mailverkeer betreffende dit verzoek.

5.1.2.e **onzichtbaar voor aanmelder** 12 juli 2020 22:31

Dagdienst:
Zouden jullie kunnen nagaan of het om een werktoestel gaat of om een privé toestel.

Heb voor nu MT7585 gekoppeld aan deze ticket, indien het om zijn werktoestel gaat.

5.1.2.e **onzichtbaar voor aanmelder** 12 juli 2020 22:28

Let op! Indien het een privé-apparaat betreft, gebruik dan de standaardoplossing "Ondersteuning privé mobiele apparatuur"

- Koppel het betreffende MT-/TABL-nummer aan het incident
- Inventariseer of dit een hardwarematig/softwarematig/instellingen probleem is
- Indien dit probleem niet verholpen kan worden, dient een wijziging voor vervanging geopend te worden. Koppel in dat geval de nieuwe wijziging aan dit incident.

Informatie

Aanmelddatum	12 juli 2020 22:21		Potentieel datalek
Gerealiseerde doorlooptijd	38:32	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	01:36		
Aangepaste doorlooptijd	36:56		
Doorlooptijd 'Afgerond'	00:22		
Doorlooptijd 'Uitvoering'	36:34		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	11 juli 2020 14:34
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	GSM verloren

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2007 0635 Verloren/gestolen mobiel apparaat teruggevonden

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2h + 5.1.2i
Geslacht	Vrouw
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Verloren/gestolen mobiel apparaat teruggevonden
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	21 juli 2020 15:00
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	Autoimport mail
Gereed	Ja
Datum gereed	21 juli 2020 12:09
Afgemeld	Ja
Datum afgemeld	21 juli 2020 12:09
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 19 juli 2020 15:30

Mevrouw 5.1.2.e heeft gebeld en geeft aan dat zij een oproep heeft gekregen van het nummer van 5.1.2.e 5.1.2.e Zij hebben aangegeven dat de mobiele toestel is afgegeven bij de receptie balie van hotel New York te Rotterdam. Mevrouw 5.1.2.e heeft ook uit voorzorg gelijk mevrouw 5.1.2.e gemaild.

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop). TK apparaat
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Ja
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Ja
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteam

Actie

5.1.2.e 21 juli 2020 12:24

Goede acties allemaal! Voor de duidelijkheid: (potentieel) datalek is AVG/privacy officer/FG. Laten we ons aan het meldingsprotocol houden, overleg blijven zoeken of desnoods het protocol aanpassen.

5.1.2.e Mailimport 21 juli 2020 12:07
Datum verzonden: 21-jul-2020 12:00
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>, 5.1.2.e 5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e "
<5.1.2.e @tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e "
<5.1.2.e @tweedekamer.nl>, "5.1.2.e " <5.1.2.e @tweedekamer.nl>
CC: "5.1.2.i " <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2007 0635 - TOPdesk melding

Goedemorgen allen,

De toelichting van mijn kant is opgenomen in Top desk, de melding/ het incident is hiermee afgehandeld.

Hartelijke groet,

5.1.2.e MSc
Beveiligingsambtenaar|Risicomanager
Staf DBI
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T (+5.1.2.e | M (+5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 3060
Verzonden: dinsdag 21 juli 2020 11:38
Aan: 5.1.2.e 5.1.2.e ; 5.1.2.e ; 5.1.2.e ; 5.1.2.e 5.1.2.e5.1.2.e ; 5.1.2.e
Onderwerp: I2007 0635 - TOPdesk melding

Geacht Datalekteam

Melding met nummer: I2007 0635 is aan u overgedragen.

Het betreft : Melding datalek
Verloren/gestolen mobiel apparaat teruggevonden

20-07-2020 08:39 5.1.2.e
@Datalekteam: Zijn er nog acties die hier genomen dienen te worden, of kan het incident afgemeld worden?

19-07-2020 16:14 5.1.2.e
Datum verzonden: 19-jul-2020 15:37
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0635 Aanmelden datalek

De telefoon is weer in bezit van eigenaar!

Verstuurd vanaf mijn iPhone

> Op 19 jul. 2020 om 15:31 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte mevrouw 5.1.2.e
>
> Dank voor het melden van een Datalek.
>
> Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
> Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
> Dit team zal u informeren over de voortgang en de afhandeling.
>
> Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Dit kan telefonisch of middels het beantwoorden van deze e-mail.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl
> <Formulier melding datalek - Tweede Kamer v3.docx>

19-07-2020 15:55 5.1.2.e
Mevrouw 5.1.2.e gebeld en aangegeven dat een email is verzonden naar haar en dat er ook mogelijk telefonisch met haar contact wordt opgezocht.

19-07-2020 15:52 5.1.2.e
5.1.2.e heeft terug gebeld en geeft aan dat BVA hier e.e.a. gaat uitvragen bij mevrouw 5.1.2.e Aan de hand daarvan wordt de impact bepaald. Ook aangegeven dat 5.1.2.e 5.1.2.e weer bereikbaar is.

19-07-2020 15:47 5.1.2.e
Opnieuw contact opgezocht met Security officer, voice in gesproken. Bellen over een kwartier opnieuw

19-07-2020 15:44 5.1.2.e
5.1.2.e 5.1.2.e heeft zelf ook contact opgezocht om 15:27 uur en geeft aan dat zij bij Hotel New York aan het wachten was op een vriendin en bij de aankomst van de vriendin heeft zij haar toestel op open op stoel gelaten. Hierna heeft ze haar tas gepakt en vergeten haar toestel mee te nemen. En dit is het moment waar zij haar toestel is kwijtgeraakt. Een mevrouw heeft deze gezien en heeft direct de eerste contact van haar oproepen geschiedenis gebeld(mevrouw 5.1.2.e). En heeft het bij de balie van hotel New York achtergelaten.

Verder geeft mevrouw 5.1.2.e aan dat hier niet echt sprake een datalek.

19-07-2020 15:39 5.1.2.e
Contact genomen met Security Offiver 1e 5.1.2.e 5.1.2.e met de vraag of zij kunnen adviseren of er sprake kan zijn van potentiele datalek, aangezien de toestel ontgrendeld was en TK data makkelijk bereikbaar. Hij heeft gevraagd om naar MDM server te kijken of er het toestel daar inactive is.

Details van MDM

MDM details.PNG

19-07-2020 15:33 5.1.2.e
Opnieuw contact genomen met mevrouw 5.1.2.e en gevraagd vanuit welk nummer zij terug was gebeld met de informatie van de verloren mobiele toestel en gevraagd of het nummer dan ook eindigt met 2309. Zij heeft dit bevestigd. Dit houdt in dat de mobiele toestel in deze tijd onbeheerd open was.

19-07-2020 15:30 5.1.2.e

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2h + 5.1.2i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2h + 5.1.2i 5.1.2h + 5.1.2i
o Bij iPhones/iPads houd je dit format aan 5.1.2h + 5.1.2i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2h + 5.1.2i of een met identieke cijfers (bv. ' 5.1.2h + 5.1.2i 5.1.2h + 5.1.2i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Doorloop onderstaande stappen:
- Heeft de gebruiker al een nieuw apparaat? In dit geval dient het oude apparaat te worden geretourneerd aan de Servicebalie.

- Indien de gebruiker nog geen nieuw mobiel apparaat heeft gekregen, ga na of het apparaat reeds gewist is. Indien dit zo is, dient de gebruiker ondersteund te worden bij het opnieuw in stellen van het apparaat.
- Koppel het MT-/TABL-nummer aan dit incident en pas de hardware/telefoniekaart aan

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 21 juli 2020 11:57

Afgelopen zondagmiddag heb ik hierover zowel per mail als telefonisch contact gehad met mevr. 5.1.2.e De beschrijving hieronder (15.44 uur) spoort met de (telefonische) toelichting van mevr. 5.1.2.e Gelet op de korte tijdsspanne van het onbeheerd achter laten van de mobiele telefoon, de adequate actie van de vinder van het toestel (mevr. 5.1.2.e beschikt over de contactgegevens van de vinder) , de verificatie op de handelingen die de vinder heeft verricht namelijk alleen contact zoeken met mevr. 5.1.2.e heb ik mevr. 5.1.2.e meegedeeld dat wij afzin van nader onderzoek in het kader van een potentieel datalek. Mevr. 5.1.2.e heb ik aandacht gevraagd voor de vergrendeling van de telefoon met het verzoek deze wat krapper in te regelen.
De conclusie is dat verder onderzoek niet plaatsvindt en dat deze melding is afgehandeld.
Hgr.
5.1.2.e
BVA

5.1.2.e **onzichtbaar voor aanmelder** 20 juli 2020 8:39

@Datalekteam: Zijn er nog acties die hier genomen dienen te worden, of kan het incident afgemeld worden?

5.1.2.e Mailimport 19 juli 2020 16:14

Datum verzonden: 19-jul-2020 15:37
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2007 0635 Aanmelden datalek

De telefoon is weer in bezit van eigenaar!

Verstuurd vanaf mijn iPhone

> Op 19 jul. 2020 om 15:31 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte mevrouw 5.1.2.e
>
> Dank voor het melden van een Datalek.
>
> Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
> Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
> Dit team zal u informeren over de voortgang en de afhandeling.
>
> Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i). Dit kan telefonisch of middels het beantwoorden van deze e-mail.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>

> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl
> <Formulier melding datalek - Tweede Kamer v3.docx>

5.1.2.e 19 juli 2020 15:55

Mevrouw 5.1.2.e gebeld en aangegeven dat een email is verzonden naar haar en dat er ook mogelijk telefonisch met haar contact wordt opgezocht.

5.1.2.e **onzichtbaar voor aanmelder** 19 juli 2020 15:52

5.1.2.e heeft terug gebeld en geeft aan dat BVA hier e.e.a. gaat uitvragen bij mevrouw 5.1.2.e Aan de hand daarvan wordt de impact bepaald. Ook aangegeven dat 5.1.2.e 5.1.2.e weer bereikbaar is.

5.1.2.e 19 juli 2020 15:47

Opnieuw contact opgezocht met Security officer, voice in gesproken. Bellen over een kwartier opnieuw

5.1.2.e 19 juli 2020 15:44

5.1.2.e 5.1.2.e heeft zelf ook contact opgezocht om 15:27 uur en geeft aan dat zij bij Hotel New York aan het wachten was op een vriendin en bij de aankomst van de vriendin heeft zij haar toestel op open op stoel gelaten. Hierna heeft ze haar tas gepakt en vergeten haar toestel mee te nemen. En dit is het moment waar zij haar toestel is kwijtgeraakt. Een mevrouw heeft deze gezien en heeft direct de eerste contact van haar oproepen geschiedenis gebeld(mevrouw 5.1.2.e). En heeft het bij de balie van hotel New York achtergelaten.

Verder geeft mevrouw 5.1.2.e aan dat hier niet echt sprake een datalek.

5.1.2.e **onzichtbaar voor aanmelder** 19 juli 2020 15:39

Contact genomen met Security Offiver 1e 5.1.2.e 5.1.2.e met de vraag of zij kunnen adviseren of er sprake kan zijn van potentiele datalek, aangezien de toestel ontgrendeld was en TK data makkelijk bereikbaar. Hij heeft gevraagd om naar MDM server te kijken of er het toestel daar inactive is.

Details van MDM

MDM details.PNG

5.1.2.e **onzichtbaar voor aanmelder** 19 juli 2020 15:33

Opnieuw contact genomen met mevrouw 5.1.2.e en gevraagd vanuit welk nummer zij terug was gebeld met de informatie van de verloren mobiele toestel en gevraagd of het nummer dan ook eindigt met 2309. Zij heeft dit bevestigd. Dit houdt in dat de mobiele toestel in deze tijd onbeheerd open was.

5.1.2.e **onzichtbaar voor aanmelder** 19 juli 2020 15:30

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.

Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2h + 5.1.2i
5.1.2h + 5.1.2i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2h + 5.1.2i
5.1.2h + 5.1.2i
o Bij iPhones/iPads houd je dit format aan 5.1.2h + 5.1.2i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2h + 5.1.2i of een met identieke cijfers (bv. '5.1.2h + 5.1.2i 5.1.2h + 5.1.2i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Doorloop onderstaande stappen:
- Heeft de gebruiker al een nieuw apparaat? In dit geval dient het oude apparaat te worden geretourneerd aan de Servicebalie.
- Indien de gebruiker nog geen nieuw mobiel apparaat heeft gekregen, ga na of het apparaat reeds gewist is. Indien dit zo is, dient de gebruiker ondersteund te worden bij het opnieuw in stellen van het apparaat.
- Koppel het MT-/TABL-nummer aan dit incident en pas de hardware/telefoniekaart aan

Informatie

Aanmelddatum	19 juli 2020 14:44		Potentieel datalek
Gerealiseerde doorlooptijd	13:09	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	13:09		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	13:09		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	19 juli 2020 16:34
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Getroffen maatregelen	Vanwege kamerlid opgeschaald naar BVA.
Beschrijving inbreuk	Gsm korte tijd onbeheerd laten liggen in horeca gelegenheid

Overige Opmerkingen

5.1.2.e 17 augustus 2020 16:38

BVA heeft het incident behandeld, waarschijnlijk omdat het een kamerlid betrof. BVA heeft incident gereed gemeld toen de gsm na korte tijd weer terug was bij Kamerlid.
Kamerlid heeft zelf aangegeven dat er geen sprake was van een datalek!
FG heeft aangegeven dat in vervolg de afgesproken procedure moet worden gevolgd.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2007 0679 2- vragen foutieve brief in mijn P-direkt

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Analyse en Onderzoek
Locatie (Aanmelder)	5.1.2.i

Details

omschrijving	2- vragen foutieve brief in mijn P-direkt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	24 juli 2020 17:45
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	16 november 2020 11:47
Afgemeld	Ja
Datum afgemeld	16 november 2020 12:26
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 21 juli 2020 10:17

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mailimport, m Mailimport 21 juli 2020 10:15

Afzender: 5.1.2.i tweedekamer.nl
Datum verzonden: 21-jul-2020 10:13
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e " <5.1.2.e @tweedekamer.nl>, 5.1.2.e " <5.1.2.e @tweedekamer.nl>

Onderwerp: FW: 2- vragen foutieve brief in mijn P-direkt

Hallo Collega's,

Graag zou ik een datalek willen melden.

Met vriendelijke groet,
5.1.2.e

Medewerker Personeelsbeheer
Stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T (+ 5.1.2.e
E 5.1.2.i tweedekamer.nl
I www.tweedekamer.nl

Van: 5.1.2.e van - 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 21 juli 2020 09:45
Aan: StafdienstHR <5.1.2.i tweedekamer.nl>
Onderwerp: FW: 2- vragen foutieve brief in mijn P-direkt

Dag Collega HR,

In mijn dossier van P-direkt zit een foutieve brief.
- Zie bijlage, die is voor mevrouw 5.1.2.e
- Ik was op zoek naar mijn verslag van het laatste voortgangsgesprek.
- Weet jij waar ik dat kan vinden?

Met vriendelijke groet,
5.1.2.e
managementassistent
Dienst Analyse en Onderzoek
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e 5.1.2.e tweedekamer.nl>
Verzonden: dinsdag 21 juli 2020 09:41
Aan: 5.1.2.e 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: 2- vragen foutieve brief in mijn P-direkt

Ha 5.1.2.e
Graag even opnemen met StafdienstHR.

Groet, 5.1.2.e

Van: 5.1.2.e van - 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 21 juli 2020 09:40
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: 2- vragen foutieve brief in mijn P-direkt

Dag 5.1.2.e

In mijn dossier van P-direkt zit een foutieve brief.
- Zie bijlage, die is voor mevrouw 5.1.2.e
- Ik was op zoek naar mijn verslag van het laatste voortgangsgesprek.
- Weet jij waar ik dat kan vinden?

Met vriendelijke groet,
5.1.2.e
managementassistent
Dienst Analyse en Onderzoek
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA

T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e 16 november 2020 12:19
Betrokkenen zijn door stafdienst HR geïnformeerd over het incident. Oorzaak menselijke fout. Datalekteam meldt incident gereed. Wordt toegevoegd aan datalekregister.

5.1.2.e 16 november 2020 11:47
Betrokkenen zijn door stafdienst HR geïnformeerd over het incident. Oorzaak menselijke fout. Datalekteam meldt incident gereed. Wordt toegevoegd aan datalekregister.

5.1.2.e 8 september 2020 14:46
HR moet gewezen worden op procedure en mevrouw 5.1.2.e moet alsnog geïnformeerd worden over fout (en dat die inmiddels is hersteld.

5.1.2.e 22 juli 2020 15:27
Zodra de collega van wie de gegevens verkeerd waren gearchiveerd en de collega die dit heeft aangekaart tekst en uitleg hebben gekregen, kan pas de melding gereed gemeld worden. Hieronder de correspondentie met p-direkt. In de klantgesprekken met P-Direkt zal dit verder opgepakt worden. Het betreft geen meldingswaardig datalek,

Geachte heer 5.1.2.e

Op 22 juli 2020 heb ik vanuit team klachten van P-Direkt vernomen dat u nog een aantal vragen heeft over een datalek van de tweede kamer. Ik ben de coördinator datalekken bij P-Direkt en ik beantwoord graag uw vragen. Het zou niet mogen voorkomen dat het document van een andere medewerker in een verkeerd personeelsdossier wordt geplaatst. Om te voorkomen dat dit gebeurd hanteert P-Direkt het vier ogen principe. Deze maatregel zou afdoende moeten zijn om dit soort datalekken te voorkomen. Na onderzoek is gebleken dat het datalek is ontstaan door een menselijke fout. De teamleider neemt dit op met de betreffende medewerker.

Heeft u vragen over deze reactie?
Neemt u dan gerust contact op.

Met vriendelijke groet,
5.1.2.e
Medewerker Security en Kwaliteit
.....
P-Direkt
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schenkkade 100 | 2595 AS | Den Haag | 4e verdieping
Postbus 20011 | 2500 EA | Den Haag
.....
M 5.1.2.e
E 5.1.2.e @p-direkt.minbzk.nl

** Niet verwijderen **
{SrvReqNo:[1003065471]}
** Niet verwijderen **

Oorspronkelijke tekst
Van:
StafdienstHR <5.1.2.i tweedekamer.nl>

Aan:
'5.1.2.i @p-direkt.nl' <5.1.2.i @p-direkt.nl>

CC:

Verzonden:

22.07.20 09:43:04

Onderwerp:
RE: 1003065471 Verkeerde stuk in dossier van medewerker

Geachte mevrouw 5.1.2.e

Hartelijk dank voor uw terugkoppeling. Graag wil ik nog wel vragen wat voor (technische) maatregelen jullie hierin gaan ondernemen om herhaling te voorkomen. Daarnaast zou ik een terugkoppeling van de bespreking met de securtiy officer van P-direkt willen hebben. Aangezien dit vragen zijn die wij nodig hebben in het kader van datalek.

Mocht u vragen hebben dan kunt u met mij contact opnemen.

Hopend u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
5.1.2.e

Medewerker Personeelsbeheer
Stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T (+ 5.1.2.e
E 5.1.2.i tweedekamer.nl< 5.1.2.i @tweedekamer.nl>
I www.tweedekamer.nl<http://www.tweedekamer.nl/>

Van: 5.1.2.i @p-direkt.nl < 5.1.2.i @p-direkt.nl>
Verzonden: woensdag 22 juli 2020 08:30
Aan: 5.1.2.e < 5.1.2.e @tweedekamer.nl>
Onderwerp: 1003065471 Verkeerde stuk in dossier van medewerker

Geachte heer 5.1.2.e

Op 21 juli 2020 heeft u een klacht ingediend bij P-Direkt. U geeft aan dat een brief van een medewerker in een verkeerde personeelsdossier is toegevoegd. U vraagt hoe dit kan en vraagt om dit te corrigeren. In deze e-mail geef ik u antwoord.

De brief is uit het personeelsdossier van mevrouw 5.1.2.e verwijderd

Hierbij bied ik u namens P-Direkt mijn welgemeende excuses aan voor deze situatie. Met het oog op de privacy zou het niet mogen voorkomen dat het document van een andere medewerker in een verkeerd dossier is geplaatst. De oorzaak is dat er een cijfer van het personeelsnummer verkeerd is overgenomen. Ik heb het document direct laten overzetten. Bedankt voor uw melding. Wij nemen deze uiterst serieus. Uw klacht/melding heb ik met de security officer van P-Direkt besproken en gaat er intern mee aan de slag.

Heeft u vragen over deze reactie?
Neemt u dan gerust contact op. Dit kunt u doen door deze e-mail te beantwoorden. Wilt u dat wij u bellen? Geef dit dan aan in uw e-mail en vermeld hierbij uw telefoonnummer. Wij bellen u dan zo snel mogelijk terug.

Met vriendelijke groet,

5.1.2.e

Medewerker contactcenter
Team Klachten
.....
P-Direkt
Schenkkade 100 I 2595 AS I Den Haag
Postbus 20011 I 2500 EA I Den Haag
.....
T 5.1.2.e

5.1.2.i @p-direkt.nl< 5.1.2.e @p-direkt.nl>
http://www.p-direkt.nl<http://www.p-direkt.nl/>

** Niet verwijderen **
{SrvReqNo:[1003065471]}
** Niet verwijderen **

** Niet verwijderen **
{SrvReqNo:[1003065471]}
** Niet verwijderen **

Oorspronkelijke tekst
Van:

5.1.2.e

Aan:

5.1.2.i @MCP.P-DIREKT.MINBZK.NL< 5.1.2.i @MCP.P-DIREKT.MINBZK.NL>

CC:

Verzonden:

21.07.20 11:07:17

Onderwerp:

Verkeerde stuk in dossier van medewerker

Er is een brief van mevrouw 5.1.2.e in een personeelsdossier gekomen van mevrouw 5.1.2.e 5.1.2.e Hoe is dat mogelijk als het vanuit een opdracht wordt ingestuurd van de medewerker.
Graag dit corrigeren.
Er is hiervan een melding gemaakt wegen datalek.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

5.1.2.e 21 juli 2020 14:10
Dit betreft een datalek en ik zal HR het volgende berichten:

Dank voor het bericht via 5.1.2.i (potentieel datalek). HR wordt verzocht het volgende te doen en de FG daarover binnen twee weken na heden een terugkoppeling te geven:

1. nagaan hoe het datalek heeft kunnen plaatsvinden en wie verantwoordelijk is voor het foutief invoegen van de bestanden;
2. contact op te nemen met degenen die de bestanden foutief in de dossiers heeft gevoegd om concrete afspraken te maken om herhaling te voorkomen;
3. de betrokkenen (de melder en degene over wie de informatie gaat te berichten en in kennis te stellen van de fout, het herstellen daarvan en de afspraken die zijn gemaakt om herhaling te voorkomen.

Pas na terugkoppeling vanuit HR wordt de melding al dan niet gereed gemeld.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 10:18
@DatalekTeam: Aanmelder meldt brieven die niet aan haar gericht zijn te hebben ontvangen in haar P-Direkt portaal.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 10:17
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij

het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	21 juli 2020 10:15		Potentieel datalek
Gerealiseerde doorlooptijd	799:32	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	799:32		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	799:32		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	21 juli 2020 11:49
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Geen meldingswaardig datalek
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Ja, betrokkene is per email geinformeerd
Mogelijke consequenties	Ambtenaar heeft kennisgenomen van niet voor haar bedoelde personeelsinformatie
Getroffen maatregelen	P-direkt heeft brief in juiste p-dossier opgenomen
Beschrijving inbreuk	Brief ambtenaar in foutief personeelsdossier

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2007 0712 Datalek

5.1.2.e Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	VVD
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7682
Soort	Mobiel telefoontoestel
Vestiging	Domeinen Roerende Zaken

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	22 juli 2020 10:09
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	21 juli 2020 16:30
Afgemeld	Ja
Datum afgemeld	21 juli 2020 16:30
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 21 juli 2020 15:51

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 16:30

Aanmelder belde. Hij heeft zijn telefoon teruggevonden. Incident is bij deze afgemeld.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 16:02

Wijziging aangemaakt in W2007 209.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 16:01
@DatalekTeam: Is er verder nog informatie die jullie wensen te weten?

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 16:01
Aanmelder gemaild met de informatie om zijn telefoon te vinden.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 15:58
Aanmelder meldt dat hij zijn telefoon kwijt geraakt op het terras in Frankrijk. Aanmelder meldt dat hij +/- 10 minuten geleden (15:31) erachter kwam dat zijn mobiel weg was.
Het toestel is beveiligd met een niet makkelijk te raden.
Aanmelder gaat melding bij de politie
Aanmelder is te bereiken via 5.1.2.e

Aanmelder wil graag een partial wipe laten uitvoeren, hij wenst graag de optie te behouden om zijn telefoon te vinden. Selective Wipe ingesteld door in de MDM server het mobiel te selecteren -> Secure -> Selective Wipe.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2020 15:51
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer

online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	21 juli 2020 15:39		Potentieel datalek
Gerealiseerde doorlooptijd	00:51	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:51		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:51		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	21 juli 2020 11:52
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	GSM kwijt, echter na half uur weer gevonden

Overige Opmerkingen

5.1.2.e 15 september 2020 12:00

GSM kwijt op terras in Frankrijk. Echter is na half uur weer teruggevonden

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2008 0158 Printopdracht van iemand anders tussen mijn printopdrachten

5.1.2.e 5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer .nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	5.1.2.h + 5.1.2.i
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	12 augustus 2020 14:37
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	12 augustus 2020 12:38
Afgemeld	Ja
Datum afgemeld	12 augustus 2020 12:38
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 11 augustus 2020 10:33

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e 5.1.2.e — Mailimport 10 augustus 2020 17:30

Datum verzonden: 10-aug-2020 17:05
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e " <5.1.2.e @tweedekamer.nl>
Onderwerp: Printopdracht van iemand anders tussen mijn printopdrachten

L.S.,

Vandaag ben ik voor het eerst weer aan het werk na 3 weken vakantie. Ik heb zojuist mijn eerste

printopdracht gegeven. Bij het inloggen op de printer (met mijn eigen gebruikersnaam en wachtwoord) stond ook een andere printopdracht, afkomstig van een andere gebruiker. Dit bleek een planning te zijn van personeelsgesprekken, afkomstig van gebruiker 5.1.2.h + 5.1.2.i Uit de bereikbaarheidsgids maak ik op dat dit 5.1.2.e 5.1.2.e is van DAO, ik zet haar ook even in de cc zodat zij op de hoogte is (en wellicht een idee heeft hoe dit is gekomen). Het leek mij goed dit even bij jullie te melden. In dit geval is het geen ernstig probleem en geen gevoelig document, maar blijkbaar is het dus mogelijk dat printopdrachten bij een andere gebruiker terechtkomen. Aangezien mensen hier met regelmaat documenten afdrukken waarvan we onder geen beding willen dat die bijvoorbeeld door iemand van een andere fractie gelezen kunnen worden, lijkt me dit wel problematisch. Willen jullie uitzoeken hoe dit mogelijk is en hoe dit kan worden voorkomen?

Vriendelijke groet,
5.1.2.e

--
5.1.2.e
Politiek Secretaris Tweede Kamerfractie D66

Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e **onzichtbaar voor aanmelder** 12 augustus 2020 12:38
In overleg met coordinatie incident afgemeld.

5.1.2.e Mailimport 12 augustus 2020 12:37
Datum verzonden: 5.1.2.e 10:21
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: I2008 0158 OPGELOST: 5.1.2.h + 5.1.2.i pasnummer 000000000

Ter info…

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(31)5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.i 5.1.2.i @tweedekamer.nl>
Verzonden: woensdag 12 augustus 2020 08:45
Aan: 5.1.2.e @tweedekamer.nl>
Onderwerp: FW: 5.1.2.h + 5.1.2.i pasnummer 000000000

Goedemorgen heren,

De problemen zouden opgelost moeten zijn.
Als gebruikers in kwestie nu langs de beveiligingsdienst gaan , zouden ze na de eerstvolgende synchronisatie weer moeten kunnen printen.
Met vriendelijke groet,
5.1.2.e
Procesmanager
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(31) 6- 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Werkdagen: maandag, dinsdag, woensdag en donderdag

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 12 augustus 2020 08:17

Aan: TK-DA-Hosting <5.1.2.i @tweedekamer.nl>; TK-DA-Operations <5.1.2.i
5.1.2.i @tweedekamer.nl>; Belder, N. <5.1.2.e @tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: 5.1.2.h + 5.1.2.i pasnummer 000000000

Allen,

Hierbij een status update:
5.1.2.e heeft het zetten van het pasnummer '0000000000' voor inactieve en tijdelijke passen weer aangepast zodat deze net zoals voorheen weer leeg is.
Van de betreffende gebruikers is in AD nu in idd het pasnummer (extensionattribute1) weer leeg.
Rond 08:00 uur vanochtend was 5.1.2.h + 5.1.2.i volledig bijgewerkt:

- Delegates verwijderd
- Betreffende gebruikers gelocked (zoals verwacht: gebruiker heeft geen pasnummer)

Met vriendelijke groet,
5.1.2.e
Systeembeheerder
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | M +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

[https://www.tweedekamer.nl/sites/default/files/atoms/images/facebook.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/twitter.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/linkedin.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/instagram_0.png]

5.1.2.e **onzichtbaar voor aanmelder** 12 augustus 2020 8:38
TODO:
- Uitzoeken of het incident afgemeld mag worden na overleg met coordinatie.

5.1.2.e 12 augustus 2020 8:19
5.1.2.e heeft het zetten van het pasnummer '0000000000' voor inactieve en tijdelijke passen weer aangepast zodat deze net zoals voorheen weer leeg is.
Van de betreffende gebruikers is in AD nu in idd het pasnummer (extensionattribute1) weer leeg.
Rond 08:00 uur vanochtend was 5.1.2.h + 5.1.2.i volledig bijgewerkt:
- Delegates verwijderd
- Betreffende gebruikers gelocked (zoals verwacht: gebruiker heeft geen pasnummer)

5.1.2.e 11 augustus 2020 13:37
5.1.2.h + 5.1.2.i heeft aangegeven dat er geen mogelijkheden zijn zonder de software aan te passen:

5.1.2.e

Wij hebben vandaag overleg gehad over gemelde issue en hierbij een opsomming over het geen geconstateerd.

---- Een eis van het IWR project was dat overheidsmedewerkers over de domeinen heen konden printen. Nu zijn er medewerkers die een account bij IWR member 1 hebben en ook een account bij IWR member 2. Echter is het rijks pasnummer een unieke code en zo kunnen medewerkers via 5.1.2.h + 5.1.2.i als rijks pasnummer identiek is.
Deze eis is dus verwerkt in 5.1.2.h + 5.1.2.i (Als unieke pasnummer identiek is worden de gebruikers elkaars delegates).
---- Bij de tweede kamer is ook handmatig aanmelden toegestaan.
--- De code '0000000000'" is geen een uniek rijks pasnummer.

Dus ons advies is inderdaad; Met de huidige versie van 5.1.2.h + 5.1.2.i is de enige oplossing om de '0000000000'" weer te veranderen in <leeg> in extensionattribute1 in AD.

Stel dat we dit gedrag willen aanpassen , zal een nieuw statement of work gemaakt moeten worden van 5.1.2.h + 5.1.2.i en zal 5.1.2.h + 5.1.2.i moeten worden aangepast.
In de huidige versie zit geen optie om het gedrag op pasnummer '0000000000'" aan te passen.

Met vriendelijke groeten,

Ad Goes

5.1.2.e **onzichtbaar voor aanmelder** 11 augustus 2020 12:51
zie ook I2008 0180

5.1.2.e 11 augustus 2020 12:37
Contact gehad met 5.1.2.e (BEV), vanavond gaat 5.1.2.e er voorzorgen dat het pasnummer net zoals voorheen weer leeg is i.p.v. '0000000000'.
5.1.2.h + 5.1.2.i kijkt in de tussentijd wat de mogelijkheden zijn om het automatisch zetten van delegates aan te passen.

5.1.2.e Mailimport 11 augustus 2020 11:10
Datum verzonden: 10-aug-2020 21:17
Naar: 5.1.2.e <5.1.2.e @tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>, Beheer IAM <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @xerox.com>, "'5.1.2.e (External)'" <5.1.2.e @xerox.com>, "5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.i 5.1.2.i @tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e 5.1.2.e" <5.1.2.e @tweedekamer.nl>, 5.1.2.i <5.1.2.i 5.1.2.i @tweedekamer.nl>, 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: I2008 0158 Passnummer i.c.m. Follow Me

Heren,

Vandaag hebben we een incident binnen gekregen dat een gebruiker (5.1.2.e - Politiek Secretaris Tweede Kamerfractie D66) een printopdracht van een andere gebruiker (5.1.2.e DAO) tussen zijn Follow Me opdrachten had.
Uit onderzoek blijkt dat beide users als pasnummer '0000000000' (extensionattribute1 in AD) hebben.
Er zijn in totaal nu 179 users met als pasnummer '0000000000' (zie bijlage). Vermoeden is dat IAM dit als pasnummer instelt als de pas geblokkeerd wordt omdat een gebruiker een bepaalde periode zijn kamerpas niet heeft gebruikt. Voorheen (CDP) werd het pasnummer dan leeg gemaakt.

@BeheerIAM: Klopt het bovenstaande? Zo ja, is het mogelijk om de pasnummers bij blokkade weer leeg te maken i.p.v. te vullen met '0000000000'?

Uit verder onderzoek blijkt dat 5.1.2.h + 5.1.2.i IDM de gebruikers met pasnummer '0000000000' in 5.1.2.h + 5.1.2.i als elkaars delegate heeft ingesteld:

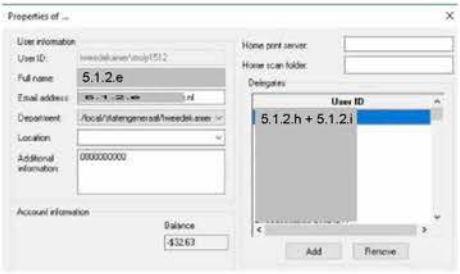


image003.jpg.jpeg

Dit kan verklaren waarom de gebruiker een opdracht van iemand anders tussen zijn Follow Me opdrachten heeft gekregen.

@5.1.2.h + 5.1.2.i Hoe komt het bovenstaande? En hoe kunnen we dit voorkomen?

Uit voorzorg ga ik nu de 179 gebruikers in 5.1.2.h + 5.1.2.i op Account Locked zetten. (een voor eenL).

Met vriendelijke groet,
5.1.2.e
Systeembeheerder
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | M +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

[https://www.tweedekamer.nl/sites/default/files/atoms/images/facebook.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/twitter.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/linkedin.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/instagram_0.png]

5.1.2.e **onzichtbaar voor aanmelder** 11 augustus 2020 8:57
Met mevr. 5.1.2.e gebeld en de huidige stand van zaken doorgegeven. Mevr. 5.1.2.e gaf aan dat ze hier rekening mee zou houden wanneer ze weer in de Tweede Kamer is en dus dan mogelijk niet kan printen via de MFP's.

5.1.2.e Mailimport 11 augustus 2020 8:54
Datum verzonden: 11-aug-2020 8:47
Naar: "5.1.2.e <5.1.2.e @tweedekamer.nl>, 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: I2008 0158 Printopdracht van iemand anders tussen mijn printopdrachten

Beste 5.1.2.e en DA,

Dank voor het melden! Dit is inderdaad een document dat ik vorige week heb geprint. Ik was vergeten de printer te wijzigen in mijn huisprinter en de Follow me-instelling was nog actief. Niets aan de hand leek me, want dat zou gekoppeld moeten zijn aan mijn pas of gebruikersnaam & inloggegevens. Ik vind dit heel vreemd en heb er geen verklaring voor, dus de vraag aan DA blijft staan. Gelukkig bevat dit document geen vertrouwelijke gegevens. Ik ga nu wel heel goed opletten op mijn instellingen!

Met vriendelijke groet,

5.1.2.e

Teamleider informatiespecialisten
Dienst Analyse en Onderzoek
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | M +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 10 augustus 2020 17:06
Aan: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Printopdracht van iemand anders tussen mijn printopdrachten

L.S.,

Vandaag ben ik voor het eerst weer aan het werk na 3 weken vakantie. Ik heb zojuist mijn eerste printopdracht gegeven. Bij het inloggen op de printer (met mijn eigen gebruikersnaam en wachtwoord) stond ook een andere printopdracht, afkomstig van een andere gebruiker. Dit bleek een planning te zijn van personeelsgesprekken, afkomstig van gebruiker 5.1.2.h + 5.1.2.i. Uit de bereikbaarheidsgids maak ik op dat 5.1.2.e is van DAO, ik zet haar ook even in de cc zodat zij op de hoogte is (en wellicht een idee heeft hoe dit is gekomen). Het leek mij goed dit even bij jullie te melden. In dit geval is het geen ernstig probleem en geen gevoelig document, maar blijkbaar is het dus mogelijk dat printopdrachten bij een andere gebruiker terechtkomen. Aangezien

mensen hier met regelmaat documenten afdrukken waarvan we onder geen beding willen dat die bijvoorbeeld door iemand van een andere fractie gelezen kunnen worden, lijkt me dit wel problematisch. Willen jullie uitzoeken hoe dit mogelijk is en hoe dit kan worden voorkomen?

Vriendelijke groet,
5.1.2.e

--
5.1.2.e
Politiek Secretaris Tweede Kamerfractie D66

Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e Mailimport 11 augustus 2020 8:40
Datum verzonden: 10-aug-2020 21:17
5.1.2.e <5.1.2.e @tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>, 5.1.2.i <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @xerox.com>, "'5.1.2.e (External)'" <5.1.2.e @xerox.com>, "5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.i @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, 5.1.2.i 5.1.2.i @tweedekamer.nl>, 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: I2008 0158 Passnummer i.c.m. Follow Me

Heren,

Vandaag hebben we een incident binnen gekregen dat een gebruiker (5.1.2.e - Politiek Secretaris Tweede Kamerfractie D66) een printopdracht van een andere gebruiker (5.1.2.e DAO) tussen zijn Follow Me opdrachten had.
Uit onderzoek blijkt dat beide users als pasnummer '0000000000' (extensionattribute1 in AD) hebben.
Er zijn in totaal nu 179 users met als pasnummer '0000000000' (zie bijlage). Vermoeden is dat IAM dit als pasnummer instelt als de pas geblokkeerd wordt omdat een gebruiker een bepaalde periode zijn kamerpas niet heeft gebruikt. Voorheen (CDP) werd het pasnummer dan leeg gemaakt.

@BeheerIAM: Klopt het bovenstaande? Zo ja, is het mogelijk om de pasnummers bij blokkade weer leeg te maken i.p.v. te vullen met '0000000000'?

Uit verder onderzoek blijkt dat 5.1.2.h+5.1.2.i IDM de gebruikers met pasnummer '0000000000' in 5.1.2.h + 5.1.2.i als elkaars delegate heeft ingesteld:

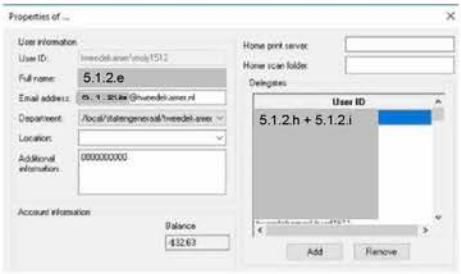


image003.jpg.jpeg

Dit kan verklaren waarom de gebruiker een opdracht van iemand anders tussen zijn Follow Me opdrachten heeft gekregen.

@5.1.2.h+5.1.2.i Hoe komt het bovenstaande? En hoe kunnen we dit voorkomen?

Uit voorzorg ga ik nu de 179 gebruikers in 5.1.2.h + 5.1.2.i op Account Locked zetten. (een voor eenL).

Met vriendelijke groet,
5.1.2.e

Systeembeheerder
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e | M +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

[https://www.tweedekamer.nl/sites/default/files/atoms/images/facebook.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/twitter.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/linkedin.png]

[https://www.tweedekamer.nl/sites/default/files/atoms/images/instagram_0.png]

5.1.2.e 11 augustus 2020 7:02
De accounts die gisteravond in 5.1.2.h + 5.1.2.i op locked gezet zijn staan nog steeds locked .

5.1.2.e 10 augustus 2020 21:47
Uit onderzoek blijkt dat beide users als pasnummer '0000000000' (extensionattribute1 in AD) hebben.
Er zijn in totaal nu 179 users met als pasnummer '0000000000'. Het vermoeden is dat IAM dit als pasnummer instelt als de pas geblokkeerd wordt omdat een gebruiker een bepaalde periode zijn kamerpas niet heeft gebruikt. Voorheen (CDP) werd het pasnummer dan leeg gemaakt.

BeheerIAM via de mail gevraagd: Klopt het bovenstaande? Zo ja, is het mogelijk om de pasnummers bij blokkade weer leeg te maken i.p.v. te vullen met '0000000000'?

Uit verder onderzoek blijkt dat 5.1.2.h + 5.1.2.i IDM de gebruikers met pasnummer '0000000000' in 5.1.2.h + 5.1.2.i als elkaars delegate heeft ingesteld.
Dit kan verklaren waarom de gebruiker een opdracht van iemand anders tussen zijn Follow Me opdrachten heeft gekregen.

5.1.2.h + 5.1.2.i via de mail gevraagd: Hoe komt het bovenstaande? En hoe kunnen we dit voorkomen?
Uit voorzorg heb ik nu de 179 gebruikers in 5.1.2.h + 5.1.2.i op Account Locked zetten. Morgenochtend controleren of 5.1.2.h + 5.1.2.i deze accounts niet weer unlocked heeft.

5.1.2.e **onzichtbaar voor aanmelder** 10 augustus 2020 17:49
@ WSM: We hebben contact opgenomen met 5.1.2.e en hem op de hoogte gebracht.

Informatie

Aanmelddatum	10 augustus 2020 17:30		Potentieel datalek
Gerealiseerde doorlooptijd	14:08	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	14:08		
Doorlooptijd 'Afgerond'	00:07		
Doorlooptijd 'Uitvoering'	14:01		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	10 augustus 2020 14:33
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Prints van andere eigenaar ontvangen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2008 0450 Datalek: Lid Krol toegang tot CDA maillijst

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Datalek: Lid Krol toegang tot CDA maillijst
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Groep
Urgentie	1. Kan niet verder, beinvloed parlementair proces
Prioriteit	1 Urgent
SLA-streefdatum	19 augustus 2020 14:39
Doorlooptijd	1 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	16 november 2020 11:27
Afgemeld	Ja
Datum afgemeld	16 november 2020 12:54
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 19 augustus 2020 13:46

Ik word net gebeld door CDA dat de fractie Krol is toegevoegd aan hun maillijsten en dat alle mail nu van de CDA bij Krol ligt.

Actie

5.1.2.e — 16 november 2020 11:27

Gelet op het verstrijken van de tijd is geen nadere actie nodig. Onderzoek heeft geen oorzaak of aanleiding gevonden. Nu nog communiceren is niet oppertuun. Incident gereed gemeld

5.1.2.e **onzichtbaar voor aanmelder** — 4 september 2020 15:15

Het MT is al over dit incident geïnformeerd en ook over de afhandeling ervan.

5.1.2.e — 4 september 2020 13:50

Na overleg met 5.1.2.e

* een distributielijst met namen/e-mailadres abusievelijk toevoegen aan een verkeerde fractie (in dit geval die van de CDA aan fractie Krol betreft een datalek. Het onjuist adresseren (naamwisseling) van een e-mail is strikt genomen ook een datalek. Een hele distributielijst dus ook. Ik zie het niet als een meldingswaardig datalek. Wel als een informatiebeveiligingsincident.
* ik heb begrepen dat het lek inmiddels gedicht is en dat niet langer sprake is van een lopend informatiebeveiligingsincident.
* met 5.1.2.e afgesproken:

1. 5.1.2.e en ik pakken het lek op;
2. ik stel een conceptbrief aan 5.1.2.e met bevestiging van de melding en de huidige bevindingen etc. Dit concept leg ik an 5.1.2.e en 5.1.2.e voor
3. 5.1.2.e pakt het al in gang gezette onderzoek verder op
4. 5.1.2.e en/of 5.1.2.e informeren het MT.

5.1.2.e **onzichtbaar voor aanmelder** 19 augustus 2020 15:25

Gesprek gehad met 5.1.2.e IAM heeft pas 19-08-2020 de groep Krol aangemaakt. Zie screenshots van de login IAM.

5.1.2.e **onzichtbaar voor aanmelder** 19 augustus 2020 14:28

Datalek formulier toegevoegd

5.1.2.e **onzichtbaar voor aanmelder** 19 augustus 2020 14:22

Lijstje foutieve mails met datum/tijd en geadresseerden toegevoegd

5.1.2.e **onzichtbaar voor aanmelder** 19 augustus 2020 13:47
Graag toevoegen Datalekformulier en doorzetten naar Datalekteam.

Informatie

Aanmelddatum	19 augustus 2020 13:39	Standaardoplossing	Er is geen standaardoplossing gekoppeld
Gerealiseerde doorlooptijd	596:18		
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	596:18		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	596:18		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	1 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	19 augustus 2020 14:27
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Onbevoegde machtiging maillijst

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2008 0769 WhatsApp account gehackt van Kamerlid

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	2504
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	WhatsApp account gehackt van Kamerlid
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	31 augustus 2020 12:30
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	31 augustus 2020 10:58
Afgemeld	Ja
Datum afgemeld	31 augustus 2020 10:58
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 30 augustus 2020 18:16

De heer 5.1.2.e heeft gebeld en geeft aan dat 5.1.2.e WhatsApp is gehackt. Hij heeft de melding gekregen dat hij 500 eur moeten betalen.

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 31 augustus 2020 10:58

Gaat verder in I2008 0770

5.1.2.e — 30 augustus 2020 18:16

Gevraagd of 5.1.2.e in staat is 5.1.2.i te bellen? De heer 5.1.2.e vraagt 5.1.2.e ons te bellen

Informatie

Aanmelddatum	30 augustus 2020 18:10
Gerealiseerde doorlooptijd	02:28
Doorlooptijd 'On hold'	00:00
Aangepaste doorlooptijd	02:28
Doorlooptijd 'Afgerond'	00:00
Doorlooptijd 'Uitvoering'	02:28
Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens	Wel gebruikt en gehaald

Standaardoplossing	Er is geen standaardoplossing gekoppeld
Geëscaleerd	Ja
Behandelaar (de-)escaleren	Servicedesk

dienstcontract?	
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	30 augustus 2020 14:26
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Mogelijke hack WhatsApp account Kamerlid

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2008 0770 Potentieel datalek WhatsApp

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek WhatsApp
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	1. Kan niet verder, beinvloed parlementair proces
Prioriteit	1 Urgent
SLA-streefdatum	31 augustus 2020 9:30
Doorlooptijd	1 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	16 december 2020 8:43
Afgemeld	Ja
Datum afgemeld	16 december 2020 12:08
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 30 augustus 2020 19:43

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

De heer 5.1.2.e heeft gebeld en geeft aan via zijn WhatsApp berichten zijn verzonden naar heel veel contacten van zijn telefoon. Hij heeft een bericht gekregen om zijn 06-nummer te verifiëren. Daarop heeft hij geklikt en hierna is heeft hij heel veel oproepen en berichten gekregen. Het gaat om volgende nummer: 5.1.2.e Het nummer waarop 5.1.2.e 5.1.2.e bereikbaar 5.1.2.e

Verder heeft hij ook WhatsApp actief op zijn iPads.

Zijn moeder 5.1.2.e (5.1.2.h + 5.1.2.i heeft gereageerd op deze bericht en heeft geld overgemaakt. Ook contact opgezocht met vrouw van de heer 5.1.2.e ****, om te vragen wat voor bericht precies is verzonden naar haar 06-nummer 5.1.2.e)? Het bericht luidt:

" Kan jij misschien 500 eur missen tot vanavond 21:00 uur? Er is een spoed geval en ik kan niet bij mijn spaargeld komen. Ik stuur het je vanavond terug."

Gevraagd of 2FA actief was? Hij geeft aan dit niet te weten.
Gevraagd of all zijn vrienden een bericht hebben ontvangen: hij zegt ik weet niet of alle vrienden een bericht hebben ontvangen maar ik werd wel ineens wel vaak gebeld.
Is WhatsApp QR-code doorgegeven aan iemand anders?: Hij geeft aan dat zijn iPads bij zijn vrouw is en dat daar wel de whatsApp op actief is.

iPhone: 5.1.2.h + 5.1.2.i

5.1.2.e dient 5.1.2.e aangifte te doen bij de Politie.

Actie

5.1.2.e 16 december 2020 12:08
Afgemeld

5.1.2.e **onzichtbaar voor aanmelder** 16 december 2020 8:43

dit incident is afgehandeld

5.1.2.e **onzichtbaar voor aanmelder** 31 augustus 2020 11:10
Met de heer 5.1.2.e gebeld hij heeft aangegeven dat wij als servicedesk MDM opnieuw mogen installeren.

Daarnaast **MOETEN** wij de app **lookout** ook installeren en meneer wijzen op het feit dat er een Multifactorauthenticatie moet aanzetten.

5.1.2.e **onzichtbaar voor aanmelder** 31 augustus 2020 10:51
Meneer belde op met de vraag of hij mdm opnieuw op zijn mobiel en tablet kon krijgen.
Aangegeven dat dit op locatie moet en niet via de telefoon.
meneer zou vanmiddag in de Kamer zijn.

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2020 20:13

Ik heb Dhr. 5.1.2.e ingelicht over de huidige stand van zaken. Ook heb ik met hem, voor de zekerheid, dubbel gecheckt of er inderdaad geen mogelijkheid is om verder te gaan met het activeren van WhatsApp, maar hij krijgt geen codes binnen en de "bel mij" functie werkt niettemin.

Mocht het nodig zijn is hij buiten kantooruren bereikbaar op het volgende nummer:
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2020 20:00

5.1.2.e gebeld. Hij gaat schakelen met de BVA of hier iets mee kan worden met WhatsApp op landelijk niveau.

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2020 19:57

Volgende acties verricht:

- AD account wachtwoord gewijzigd en dit gecommuniceerd met 5.1.2.e
- Alle iPads en iPhone in MDM gekozen voor **full wiped** optie
- Contact opgezocht met 5.1.2.e alle bovenstaande informatie wat 5.1.2.e heeft gevraagd aan de heer van Helvert gevraagd en informatie verzameld.
- De heer 5.1.2.e dient opnieuw zijn iPhone in te stellen en WhatsApp te activeren. Vervolgens moet hij alle bestaande sessies van WhatsApp afmelden. Dit geprobeerd te realiseren bij de heer 5.1.2.e maar hij geeft aan dat hij voor activeren van zijn iPhone een verificatie code van iCloud nodig heeft. 5.1.2.e geeft aan dat hij via een pc ook op iCloud kan aanmelden om de code te

ontvangen. Dit moet z.s.m. worden uitgevoerd. En verder is het belangrijk dat de heer 5.1.2.e 2FA aanzet. Hierin moet DA hem begeleiden. Mijn collega 5.1.2.e is op de hoogte gesteld van alle details van deze melding en neemt verder actie. Mijn dienst zit er al sinds 19:30 uur al op.

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2020 19:56

19:38 - ben aan het bellen met 5.1.2.e we beginnen het proces
19:45 - iOS opgestart
19:48 - WhatsApp geïnstalleerd
19:51 - volgens WhatsApp (enigszins geparafraseerd): "U heeft te vaak geprobeerd te raden, controleer bij uw provider, wacht tot er een nieuwe code naar u is gestuurd, u kunt het na 10 uur en 29 minuten opnieuw proberen"
19:55 - Ik ga weer met 5.1.2.e bellen.
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2020 19:43

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	30 augustus 2020 18:12		Potentieel datalek
Gerealiseerde doorlooptijd	731:43	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	731:43		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	731:43		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	1 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	30 augustus 2020 14:25
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Dit is geen datalek. Kamerlid heeft problemen met installeren WhatsApp

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2008 0793 Potentieel datalek WhatsApp

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek WhatsApp
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	1. Kan niet verder, beinvloed parlementair proces
Prioriteit	1 Urgent
SLA-streefdatum	31 augustus 2020 11:54
Doorlooptijd	1 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	8 september 2020 14:49
Afgemeld	Ja
Datum afgemeld	9 september 2020 8:54
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 31 augustus 2020 10:54

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK e**xchange ge**gevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen

Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN *ALLE GEVALLEN => behandelen als potentieel Datalek*
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

De heer 5.1.2.e heeft gebeld en geeft aan via zijn WhatsApp berichten zijn verzonden naar heel veel contacten van zijn telefoon. Hij heeft een bericht gekregen om zijn 06-nummer te verifiëren. Daarop heeft hij geklikt en hierna is heeft hij heel veel oproepen en berichten gekregen. Het gaat om volgende nummer: 5.1.2.e Het nummer waarop 5.1.2.e 5.1.2.e bereikbaar 5.1.2.h + 5.1.2.i

Verder heeft hij ook WhatsApp actief op zijn iPads.

Zijn moeder 5.1.2.e 5.1.2.h + 5.1.2.i gereageerd op deze bericht en heeft geld overgemaakt. Ook contact opgezocht met vrouw van de heer 5.1.2.e ****, om te vragen wat voor bericht precies is verzonden naar haar 06-nummer 5.1.2.e)? Het bericht luidt:

" Kan jij misschien 500 eur missen tot vanavond 21:00 uur? Er is een spoed geval en ik kan niet bij mijn spaargeld komen. Ik stuur het je vanavond terug."

Gevraagd of 2FA actief was? Hij geeft aan dit niet te weten.
Gevraagd of all zijn vrienden een bericht hebben ontvangen: hij zegt ik weet niet of alle vrienden een bericht hebben ontvangen maar ik werd wel ineens wel vaak gebeld.
Is WhatsApp QR-code doorgegeven aan iemand anders?: Hij geeft aan dat zijn iPads bij zijn vrouw is en dat daar wel de whatsApp op actief is.

iPhone: 5.1.2.h + 5.1.2.i

5.1.2.e dient 5.1.2.e aangifte te doen bij de Politie.

Actie

5.1.2.e 8 september 2020 14:49
Dit voorval betreft geen datalek. FG meldt het voorval gereed.

5.1.2.e **onzichtbaar voor aanmelder** 31 augustus 2020 11:10
Met de heer 5.1.2.e gebeld hij heeft aangegeven dat wij als servicedesk MDM opnieuw mogen installeren.

Daarnaast **MOETEN** wij de app **lookout** ook installeren en meneer wijzen op het feit dat er een Multifactorauthenticatie moet aanzetten.

5.1.2.e **onzichtbaar voor aanmelder** 31 augustus 2020 10:56
Voor informatie zie I2008 0770.

5.1.2.e **onzichtbaar voor aanmelder** 31 augustus 2020 10:54
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via

MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Meneer belde op met de vraag of hij mdm opnieuw op zijn mobiel en tablet kon krijgen.
Aangegeven dat dit op locatie moet en niet via de telefoon.
meneer zou vanmiddag in de Kamer zijn.

Ik heb Dhr. 5.1.2.e ingelicht over de huidige stand van zaken. Ook heb ik met hem, voor de zekerheid, dubbel gecheckt of er inderdaad geen mogelijkheid is om verder te gaan met het activeren van WhatsApp, maar hij krijgt geen codes binnen en de "bel mij" functie werkt niettemin.

Mocht het nodig zijn is hij buiten kantooruren bereikbaar op het volgende nummer:
5.1.2.e

5.1.2.e gebeld. Hij gaat schakelen met de BVA of hier iets mee kan worden met WhatsApp op landelijk niveau.

Volgende acties verricht:

- AD account wachtwoord gewijzigd en dit gecommuniceerd met 5.1.2.e 5.1.2.e
- Alle iPads en iPhone in MDM gekozen voor full wiped optie
- Contact opgezocht met 5.1.2.e alle bovenstaande informatie wat 5.1.2.e heeft gevraagd aan de heer 5.1.2.e 5.1.2.e gevraagd en informatie verzameld.
- De heer 5.1.2.e dient opnieuw zijn iPhone in te stellen en WhatsApp te activeren. Vervolgens moet hij alle bestaande sessies van WhatsApp afmelden. Dit geprobeerd te realiseren bij de heer 5.1.2.e maar hij geeft aan dat hij voor activeren van zijn iPhone een verificatie code van iCloud nodig heeft. 5.1.2.e geeft aan dat hij via een pc ook op iCloud kan aanmelden om de code te ontvangen. Dit moet z.s.m. worden uitgevoerd. En verder is het belangrijk dat de heer 5.1.2.e 2FA aanzet. Hierin moet DA hem begeleiden. Mijn collega 5.1.2.e 5.1.2.e is op de hoogte gesteld van alle details van deze melding en neemt verder actie. Mijn dienst zit er al sinds 19:30 uur al op.

19:38 - ben aan het bellen met 5.1.2.e we beginnen het proces
19:45 - iOS opgestart
19:48 - WhatsApp geïnstalleerd
19:51 - volgens WhatsApp (enigszins geparafraseerd): "U heeft te vaak geprobeerd te raden, controleer bij uw provider, wacht tot er een nieuwe code naar u is gestuurd, u kunt het na 10 uur en 29 minuten opnieuw proberen"
19:55 - Ik ga weer met 5.1.2.e bellen.
5.1.2.e

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	31 augustus 2020 10:54		Potentieel datalek
Gerealiseerde doorlooptijd	60:55	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	60:55		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	60:55		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	1 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2009 0084 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	SP
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	1. Kan niet verder, beinvloed parlementair proces
Prioriteit	1 Urgent
SLA-streefdatum	1 september 2020 16:59
Doorlooptijd	1 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	16 november 2020 11:30
Afgemeld	Ja
Datum afgemeld	16 november 2020 12:47
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 1 september 2020 16:01

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Mevrouw belt: haar whatsapp-account lijkt gehackt te zijn. Bekenden krijgen berichtjes van haar, waarin "zij" hen vraagt 500 euro over te maken. Ze wordt ook steeds gebeld. Wat nu?

Actie

5.1.2.e 16 november 2020 11:30

Het betreft een security incident. Bovendien betrof het de eigen verantwoordelijkheid van de

betrokkenen. Ergo: altijd tweefactorauthenticatie altijd aan!. Gereedmelding

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2020 16:02
Mevrouw is aan het werk in de Tweede Kamer. We vragen haar naar de servicedesk te komen.

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2020 16:01
Mevrouw belt: haar whatsapp-account lijkt gehackt te zijn. Bekenden krijgen berichtjes van haar, waarin "zij" hen vraagt 500 euro over te
maken. Ze wordt ook steeds gebeld. Wat nu?

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2020 16:01
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:

-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	1 september 2020 15:59		Potentieel datalek
Gerealiseerde doorlooptijd	508:31	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	508:31		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	508:31		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	1 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	1 september 2020 14:23
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	WhatsApp account Kamerlid lijkt gehackt

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2009 0261 Potentieel datalek - mobiel toestel verloren

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Beveiligingsdienst
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek - mobiel toestel verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7853
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	7 september 2020 15:00
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	16 november 2020 11:35
Afgemeld	Ja
Datum afgemeld	16 november 2020 13:03
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 3 september 2020 18:47

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 16 november 2020 11:35

Standaardprocedure (full wipe) is uitgevoerd door servicedesk. Datalekteam heeft geen verdere vragen en meld het incident gereed. Incident wordt toegvoegd aan datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 4 september 2020 15:31
@Datalekteam: Zijn er nog meer acties die jullie uitgevoerd wensen te hebben?

5.1.2.e **onzichtbaar voor aanmelder** 3 september 2020 19:00

Meneer meldt dat hij zijn telefoon is kwijtgeraakt in de trein. De pincode van het apparaat is niet makkelijk te raden. Full wipe is op het toestel uitgezet. Wijziging voor het leveren van een vervangend toestel is gestart in W2009 093.

5.1.2.e **onzichtbaar voor aanmelder** 3 september 2020 18:47

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:

-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	3 september 2020 18:31		Potentieel datalek
Gerealiseerde doorlooptijd	487:35	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	487:35		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	487:35		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	3 september 2020 14:21
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	GSM verloren

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2009 0368 Datalek melding

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Griffie Plenair - Bureau Wetgeving
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Datalek melding
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	9 september 2020 12:22
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	30 september 2020 8:06
Afgemeld	Ja
Datum afgemeld	30 september 2020 16:06
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 7 september 2020 15:26

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mailimport, m — Mailimport 7 september 2020 15:22

Afzender: fg@tweedekamer.nl
Datum verzonden: 7-sep-2020 13:18
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek

Collega's,

Deze melding heb ik per e-mail ontvangen. Is het mogelijk dat jullie hiervan een Topdeskmelding maken zodat de melding via het datalekteam wordt opgepakt?

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
T +(31) 5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 4 september 2020 14:56
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek

Hallo 5.1.2.e

Bijgaand het ingevulde formulier melding datalek.

Fijn weekend alvast!

Met vriendelijke groet,
5.1.2.e
5.1.2.e
5.1.2.e
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
5.1.2.e
5.1.2.e

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: donderdag 3 september 2020 16:18
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Fwd: datalek

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Datum: 3 september 2020 om 16:07:22 CEST
Aan: "5.1.2.e" <5.1.2.e @tweedekamer.nl>
Kopie: Functionaris gegevensbescherming <fg@tweedekamer.nl>, 5.1.2.e
<5.1.2.e @tweedekamer.nl>
Onderwerp: datalek

Beste 5.1.2.e

Via een mail van 5.1.2.e en 5.1.2.e (zie hieronder) vernam ik het incident. Door de drukte op het werk ben je vast nog niet toegekomen aan het doen van de melding van het datalek. Weet dat ik daar begrip voor heb. Zodra dat kan, ontvangen wij graag de melding. Dan kunnen we nagaan of en zo ja welke stappen verder genomen moeten worden.

Dank en groet,

5.1.2.e

We hebben de werkwijze griffies commissie bij inzagerecht bekeken, heldere beschrijving! We hebben nog een paar kleine suggesties en vragen die je als het goed is terug kunt zien in het bestand. Wanneer schikt het jullie om hierover verder te praten?

V.w.b. het onderwerp brieven derden, zouden wij nog een terugkoppeling geven van het overleg met de 3 hGC's. Bijgevoegd de meest recente versie van de notitie die met hen besproken is. Kort gezegd kunnen zij zich vinden in de notitie. We hebben de vraagpunten die daarin worden opgenomen besproken en geconcludeerd dat er geen noodzaak is om adresgegevens op te vragen als er een emailadres bekend is. De huidige werkwijze moet dus worden aangepast. Hiermee gaan we aan de slag, door een handleiding te maken voor de nieuwe werkwijze. Die zullen we t.z.t. naar jullie sturen.

Daarnaast werd ik (5.1.2.e) afgelopen zaterdag gebeld door een burger waarvan morgen een burgerinitiatief plenair wordt behandeld. Op de website van de TK was haar e-mail gepubliceerd als bijlage van een Kamerbrief. In deze e-mail stond haar telefoonnummer. Dit is dus een datalek. Ik heb hier zaterdag contact over gehad met 5.1.2.e 5.1.2.e Zij zou een melding datalek doen. Is dit inmiddels ook bij jullie terechtgekomen?

We horen van jullie.

5.1.2.e
5.1.2.e en 5.1.2.e

Actie

5.1.2.e 30 september 2020 8:07

Op basis van onderstaand bericht van de GC meld ik dit incident als gereed.

Hallo 5.1.2.e

Zie onderstaande mail van de griffier van de commissie J&V inzake het datalek. Zij hebben vandaag een mail aan betrokkene gestuurd. Ik hoop dat dit afdoende is.

Voor wat betreft jouw vraag of het proces zo kan worden ingericht dat herhaling voorkomen kan worden kan ik het volgende zeggen. Wij proberen altijd een check te maken in de ontvangen stukken of er onbedoeld privacygevoelige gegevens in voorkomen, maar in de honderden stukken die wij per week ontvangen komt het helaas wel eens voor dat er iets tussendoor glipt. Het blijft mensenwerk..

Met vriendelijke groet,
5.1.2.e
5.1.2.e
5.1.2.e

Van: 5.1.2.e <
Onderwerp: RE: datalek

Beste 5.1.2.e

Aan betrokkene is per mail medegedeeld dat haar e-mailadres en daarmee ook haar telefoonnummer is verwijderd van de Website van de TK, die als bijlage was gepubliceerd bij een Kamerbrief. Wij hebben hier ook onze excuses voor aangeboden.
De mailwisseling van een maand geleden is echter niet bewaard gebleven.
Dit is alles wat ik daarover kan zeggen, hoop dat het afdoende is.
Met vriendelijke groet,
5.1.2.e (5.1.2.e)
adjunct griffier
GC Bestuur en Onderwijs
Tweede Kamer der Staten-Generaal

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 29 september 2020 13:05
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek

Super. Dank jullie wel!

Met vriendelijke groet,
5.1.2.e
5.1.2.e
5.1.2.e

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 29 september 2020 12:24
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: datalek

Ha 5.1.2.e

De betreffende mail is nog niet aan betrokkene verstuurd. We gaan dit vandaag doen en zullen je een afschrift sturen, zodat 5.1.2.e vervolgens geïnformeerd kan worden.

Met vriendelijke groet,
5.1.2.e
adjunct griffier
GC Bestuur en Onderwijs
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 28 september 2020 16:05
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: Fwd: datalek

Hoi 5.1.2.e en 5.1.2.e

Zie de onderstaande mail 5.1.2.e Ik heb jullie op 9 en 15 september al een mail hier over gestuurd. Ik begreep van 5.1.2.e dat 5.1.2.e dit na haar vakantie zou oppakken. Kunnen jullie mij een afschrift sturen van de mail aan betrokkene zodat ik 5.1.2.e kan informeren? Dank!
Met vriendelijke groet,
5.1.2.e
5.1.2.e

Begin doorgestuurd bericht:
Van: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Datum: 28 september 2020 om 15:48:35 CEST
Aan: "5.1.2.e" <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: datalek

Beste 5.1.2.e

Deze mail is vast aan je aandacht ontsnapt. Graag een korte update.

5.1.2.e

Met vriendelijke groet,
5.1.2.e

5.1.2.e 8 september 2020 10:14
Uit onderstaande mailwisseling volgt dat het 'lek' de dag na melding is gedicht. Ik vind het geen meldingswaardig incident. IK zal de Griffie dit melden met het verzoek contact op te nemen de betrokkenen/melder --voor zover dat nog niet gedaan is -- en hen vragen conform staand beleid een kort briefje of mailtje te sturen met een samenvatting van het incident, hoe dit opgelost is en met excuses voor het ongemak dat dit heeft opgeleverd etc. Daarnaast zal ik continue aandacht vragen om herhaling te voorkomen. Ik meld het incident gereed zodra ik een kopie van het bericht aan

betrokkene/melder heb heb ontvangen.

5.1.2.e

Hallo 5.1.2.e

Dat klopt. Vorige week zaterdag is het stuk al uit Parlis verwijderd en daarmee van de website van de Kamer. Maandag jl. is het stuk ook van overheid.nl verwijderd!

Met vriendelijke groet,
5.1.2.e
5.1.2.e

Op 4 sep. 2020 om 15:27 heeft 5.1.2.e <5.1.2.e @tweedekamer.nl> het volgende geschreven:

Top, dank je wel.

Begrijp ik goed dat het telefoonnummer inmiddels niet meer zichtbaar is online?

Jij ook heel fijn weekend toegewenst,

5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 7 september 2020 15:30
@Datalekteam: Op verzoek van de Functionaris gegevensbescherming, incident op jullie naam gezet.

5.1.2.e **onzichtbaar voor aanmelder** 7 september 2020 15:26
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer

is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	7 september 2020 15:22		Potentieel datalek
Gerealiseerde doorlooptijd	154:38	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	154:38		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	154:38		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	7 september 2020 14:21
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Persoonsgegevens per abuis gepubliceerd op internet

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2010 0529 Potentieel datalek: Telefoon verloren

Tweede Kamer

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	PvdA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek: Telefoon verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7481
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	15 oktober 2020 17:20
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	16 november 2020 11:39
Afgemeld	Ja
Datum afgemeld	16 november 2020 13:05
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 14 oktober 2020 10:52

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 16 november 2020 11:39

Standaardprocedure (full wipe) is uitgevoerd door servicedesk. Datalekteam heeft geen verdere vragen en meld het incident gereed. Incident wordt toegvoegd aan datalekregister.

5.1.2.e 14 oktober 2020 19:47
Is er navraag gedaan naar de beveiliging van het toestel? Zie hieronder

5.1.2.e **onzichtbaar voor aanmelder** 14 oktober 2020 10:53
Mevrouw is haar mobiele toestel verloren.
Formulier is gestuurd naar mevrouw.
Full wipe opdracht gegeven naar het toestel met toestemming van mevrouw.
Mobiele nummer naar nieuwe SIM kaart gezet.

5.1.2.e **onzichtbaar voor aanmelder** 14 oktober 2020 10:52
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde

cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	14 oktober 2020 10:50		Potentieel datalek
Gerealiseerde doorlooptijd	219:19	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	219:19		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	219:19		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	14 oktober 2020 14:18
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	GSM verloren

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2010 1071 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e / 5.1.2.e
E-mail	5.1.2.e @tweedekamer .nl
Afdeling	Dienst Analyse en Onderzoek
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7601
Soort	Mobiel telefoontoestel
Vestiging	Domeinen Roerende Zaken

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	3 november 2020 15:00
Doorlooptijd	16 uur
On hold	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Afgemeld	Ja
Datum afgemeld	31 oktober 2020 13:02
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 31 oktober 2020 12:23

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 31 oktober 2020 13:03

Teruggebeld naar mevrouw 5.1.2.e
Telefoon was dankzij stappen in I2010 1073 te volgen terug gevonden.

5.1.2.e **onzichtbaar voor aanmelder** — 31 oktober 2020 12:58

Vandaag tussen 10:30 en 11:00 mobiel kwijt geraakt.

Nog niet terug kunnen vinden.
Ik zou MDM controleren en 5.1.2.e zou in de tussentijd de locatie van de telefoon opzoeken volgens stappen in I2010 1073.

5.1.2.e 31 oktober 2020 12:53
Mobiele telefoon kwijt.
Android, IMEI: 358491091473511

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
Geen serieel code of identieke cijfers
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker) nee
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken) In MDM last connection: 10/30/20 3:52:56 am

5.1.2.e **onzichtbaar voor aanmelder** 31 oktober 2020 12:23
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer

online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?) Verschillende cijfers.
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	31 oktober 2020 12:16	Potentieel datalek
Gerealiseerde doorlooptijd	00:00	
Doorlooptijd 'On hold'	00:00	
Aangepaste doorlooptijd	00:00	
Doorlooptijd 'Afgerond'	00:00	
Doorlooptijd 'Uitvoering'	00:00	
Contractnummer	Datalekken	
Dienst	Datalekken	
Korte omschrijving	Datalekken	
Dienstenniveau	Storingsafhandeling	
SLA-doorlooptijd	16 uur	
Behandelaar	Servicedesk	
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald	
Servicewindow	Service window	

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2011 0452 Whatsapp gehackt

5.1.2.e Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Whatsapp gehackt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	12 november 2020 14:46
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	12 november 2020 11:04
Afgemeld	Ja
Datum afgemeld	12 november 2020 11:40
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 12 november 2020 8:57

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Aanmelder meldt dat zijn whatsapp gehackt is.

Actie

Slootweg, Evert 5.1.2.e Mailimport 12 november 2020 11:39
Datum verzonden: 12-nov-2020 9:03
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>

Onderwerp: RE: I2011 0452 Aanmelden datalek

hierbij

Met vriendelijke groet,
5.1.2.e 5.1.2.e
Lid Tweede Kamer CDA

Postbus 20018
2500 EA Den Haag

T +(5.1.2.e | E e.slootweg@tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: donderdag 12 november 2020 08:57
Aan: Slootweg, E. <e.slootweg@tweedekamer.nl>
Onderwerp: I2011 0452 Aanmelden datalek

Geachte heer Slootweg,

Dank voor het melden van een Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
Dit team zal u informeren over de voortgang en de afhandeling.

Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i). Dit kan telefonisch of middels het beantwoorden van deze e-mail.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 12 november 2020 11:02
Gebruiker is langs geweest aan de servicebalie. Ik heb whatsapp kunnen herstellen door opnieuw in te loggen en de 2-factor-authentication in te schakelen.

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 10:40
Aanmelder is langs de balie gekomen. Whatsapp opnieuw ingesteld. Aanmelder heeft zijn account terug. Zodra hij langs de balie komt, dient aanmelder nog zijn 2-factor authentication te activeren.

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 9:14
Aanmelder verteld dat hij een paar dagen geleden een link heeft doorgestuurd naar iemand die hij niet kende.

Met dhr. 5.1.2.e van Beveiliging gebeld. Hij geeft aan dat zij direct contact hebben met Facebook en binnen een uur een account kunnen blokkeren. Alternatief kan de gebruiker na 10 uur zelf zijn account terugvragen via Whatsapp.

Aanmelder aangeraden om langs de balie te komen voor een herinstallatie van Whatsapp en het activeren van 2-factor authentication.

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 8:57
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:

Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	12 november 2020 8:56		Potentieel datalek
Gerealiseerde doorlooptijd	02:08	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	01:48		
Aangepaste doorlooptijd	00:20		
Doorlooptijd 'Afgerond'	00:02		
Doorlooptijd 'Uitvoering'	00:18		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	10 november 2020 14:15
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Mogelijke hack WhatsApp Kamerlid

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2011 0462 Potentieel datalek: Whatsapp gehackt

Tweede Kamer

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek: Whatsapp gehackt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	7 december 2020 8:38
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	28 december 2020 15:31
Afgemeld	Ja
Datum afgemeld	28 december 2020 17:07
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 12 november 2020 11:06

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteam

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 28 december 2020 15:31

Dit incident is afgehandeld.

5.1.2.e **onzichtbaar voor aanmelder** — 8 december 2020 14:53

@ST: Zie formulier aanmelder. Hebben jullie verder nog vragen?

5.1.2.e

Mailimport 8 december 2020 14:43

Datum verzonden: 8-dec-2020 14:42
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: " 5.1.2.e 5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2011 0462 - Aanmelding Datalekteam

Beste lezer,

Van het gesprek zojuist begrijp ik dat u het toch prettig vindt bijgevoegd formulier alsnog te ontvangen ook al heb ik maar weinig informatie.
Tevens twee foto's toegevoegd

Hartelijke groet, 5.1.2.e
Drs. 5.1.2.e
Lid Tweede Kamer der Staten-Generaal (CDA)
Portefeuilles :medische zorg, GGZ, gehandicaptenbeleid, post, telecom, vitale sectoren
5.1.2.e @tweedekamer.nl I https://www.cda.nl 5.1.2.e
CDA-Fractie, Postbus 20018, 2500 EA Den Haag, T 5.1.2.i

5.1.2.e

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: donderdag 12 november 2020 11:36
Aan: 5.1.2.e 5.1.2.e @tweedekamer.nl>
Onderwerp: I2011 0462 - Aanmelding Datalekteam

Geachte mevrouw 5.1.2.e

Melding met nummer: I2011 0462 is aangemaakt.

Het betreft :Potentieel datalek: Whatsapp gehackt

De Dienst Automatisering draagt uw melding ter verdere afhandeling over aan het Datalekteam .

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande personen:

Dhr. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst 5.1.2.e

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
5.1.2.i

5.1.2.e 16 november 2020 11:42
Dit is geen incident voor het datalekteam. Datalekteam meldt het incident gereed.

5.1.2.e **onzichtbaar voor aanmelder** 13 november 2020 9:10
@ST: Zie informatie van aanmelder hieronder. Willen jullie nog meer weten?

5.1.2.e Mailimport 13 november 2020 8:19
Datum verzonden: 5.1.2.e 20:34
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e" 5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2011 0462 Potentieel datalek: Whatsapp gehackt

Beste lezer,

Twee-factor authenticatie stond aan
Hack waarschijnlijk dinsdagavond jl om 1935u.
Ik heb de link niet aangeklikt maar een kopie van de app gemaakt en deze gezonden aan 5.1.2.e
Hieronder foto's daarvan ter illustratie

Hartelijke groet, 5.1.2.e
Drs. 5.1.2.e
Lid Tweede Kamer der Staten-Generaal (CDA)
Portefeuilles :medische zorg, GGZ, gehandicaptenbeleid, post, telecom, vitale sectoren
5.1.2.e @tweedekamer.nl | https://www.cda.nl 5.1.2.e
CDA-Fractie, Postbus 20018, 2500 EA Den Haag, T 5.1.2.i

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: donderdag 12 november 2020 11:15
Aan: 5.1.2.e 5.1.2.e @tweedekamer.nl>
Onderwerp: I2011 0462 Potentieel datalek: Whatsapp gehackt

Geachte mevrouw 5.1.2.e

Om uw incident beschreven in het onderwerp verder te kunnen behandelen is er extra informatie nodig.

Het Security team heeft de volgende informatie nodig voor onderzoek naar de WhatsApp Hack:
- Zou u ons kunnen melden sinds wanneer deze hack speelt?
- Had u Twee-factor authenticatie aanstaan op WhatsApp?

Mocht u geen Twee-factor authenticatie aan hebben staan op Whatsapp vragen we u om dit aan te zetten.
Mocht u nog vragen hebben dan verzoeken we u om contact op te nemen met de Servicebalie.

U kunt de servicedesk telefonisch bereiken op (070 318) 5.1.2.i Wilt u reageren op dit incident via e-mail, beantwoord dan deze e-mail. Wanneer wij binnen 3 werkdagen
niets van u vernemen, dan gaan wij ervan uit dat het incident niet meer actueel is en sluiten wij deze.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(31)70-318 5.1.2.i | 5.1.2.i @tweedekamer.nl

Datum verzonden: 12-nov-2020 12:02
Naar: 5.1.2.i <5.1.2.i @tweedekamer.nl>, " 5.1.2.e " <5.1.2.e @tweedekamer.nl>, " 5.1.2.e '
<5.1.2.e @tweedekamer.nl>, " 5.1.2.e <5.1.2.e @tweedekamer.nl>, " 5.1.2.e
<5.1.2.e @tweedekamer.nl>, " 5.1.2.e " <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2011 0462 - TOPdesk melding

Op dit moment is niet duidelijk of dit een incident is voor het security team of het datalekteam.
Gaat het om een hack? Het datalekteam verzoekt om eerst door het security team te laten uitzoeken wat er aan de hand is.

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T 5.1.2.e | + 5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: donderdag 12 november 2020 11:36
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e
5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: 5.1.2.e

Geacht Datalekteam

Melding met nummer: I2011 0462 is aan u overgedragen.

Het betreft : Melding datalek
Potentieel datalek: Whatsapp gehackt

12-11-2020 11:36 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!

o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

12-11-2020 11:10 5.1.2.e
5.1.2.e geprobeerd te bellen en haar persoonlijk medewerker geprobeerd te bellen, maar beide nemen niet op.
5.1.2.e kan haar ook niet bereiken op het moment en geeft aan dat ze vooral in bespreking zal zijn.
Mail verstuurd om de vragen van Security Team uit te vragen.

Persoonlijk medewerker: 5.1.2.e 5.1.2.e)

12-11-2020 11:06 5.1.2.e
Kamerlid 5.1.2.e
- Uitvragen wanneer de hack is ontstaan
- 2FA: controleren of ze dit gedaan hebben.

12-11-2020 11:06 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten

waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 11:36

Mevrouw 5.1.2.e geprobeerd te bellen en haar persoonlijk medewerker geprobeerd te bellen, maar beide nemen niet op.
5.1.2.e kan haar ook niet bereiken op het moment en geeft aan dat ze vooral in bespreking zal zijn.
Mail verstuurd om de vragen van Security Team uit te vragen.

Persoonlijk medewerker: 5.1.2.e 5.1.2.e)

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 11:10

.

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 11:06

Kamerlid Joba 5.1.2.e
- Uitvragen wanneer de hack is ontstaan
- 2FA: controleren of ze dit gedaan hebben.

5.1.2.e **onzichtbaar voor aanmelder** 12 november 2020 11:06

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i) of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.

* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	12 november 2020 10:57		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	308:34	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	308:34		
Doorlooptijd 'Afgerond'	155:11		
Doorlooptijd 'Uitvoering'	153:23		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	12 november 2020 14:13
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Beschrijving inbreuk	Mogelijke WhatsApp hack Kamerlid

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2012 0881 Datalek in dossier medewerker

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst HR
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Datalek in dossier medewerker
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	4 januari 2021 10:42
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 29 december 2020 12:48

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 29 december 2020 12:42

Date sent: Dec 29, 2020 10:06 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: datalek in dossier medewerker

Beste heer/dame

Zie bijgaand formulier

Met vriendelijke groet,

5.1.2.e
Adviseur HR
Stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e of 06-| E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
T +(5.1.2.e
Werkzaam op ma-di-dond-vrij

Actie

5.1.2.e 29 december 2020 17:02

Ik heb aan 5.1.2.e nadere informatie gevraagd over de oorzaak van het datalek, de oplossing en gezegd dat betrokkenen geïnformeerd dienen te worden door stafdienst HR.
Wanneer ik deze informatie retour ontvang van 5.1.2.e zal ik deze toevoegen aan het datalekregister.

5.1.2.e Mailimport 29 december 2020 14:03

Date sent: Dec 29, 2020 12:54 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e " <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e 5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e " <5.1.2.e @tweedekamer.nl>
Subject: Re: I2012 0881 - TOPdesk melding

Beste Servicedesk, Datalek meldingen zijn voor het Datalek team en niet voor het security team. Kunnen jullie deze melding aan het datalek team toewijzen? Alvast dank.

Groet,
5.1.2.e

Verstuurd vanaf een mobiel apparaat, dus kort en zakelijk.

Op 29 dec. 2020 om 12:51 5.1.2.i @tweedekamer.nl het volgende geschreven:

Geacht Security Team

Melding met nummer: I2012 0881 is aan u overgedragen.

Het betreft : Melding datalek
datalek in dossier medewerker

29-12-2020 12:51 5.1.2.e
@ST: Dit betreft de P Direkt dossier van medewerker 5.1.2.e 5.1.2.e (5.1.2.h + 5.12.i) van afdeling HR.

Zouden jullie dit kunnen oppakken?

29-12-2020 12:48 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
https:// 5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 29 december 2020 12:51
@ST: Dit betreft de P Direkt dossier van medewerker 5.1.2.e 5.1.2.e (GROY0307) van afdeling HR.

Zouden jullie dit kunnen oppakken?

5.1.2.e **onzichtbaar voor aanmelder** 29 december 2020 12:48
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle

potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	29 december 2020 12:42		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	00:00	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	29 december 2020 14:07
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Mogelijke consequenties	Inzage informatie
Getroffen maatregelen	Onbekend
Beschrijving inbreuk	P-gegevens in verkeerd P-dossier

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2102 0692 Potentieel datalek

5.1.2.e Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e tweedekamer.nl
Afdeling	VVD
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	16 februari 2021 12:30
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	16 februari 2021 14:04
Afgemeld	Ja
Datum afgemeld	17 februari 2021 8:57
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 15 februari 2021 19:17

Wachtwoord reset melding in I2102 0691
Security melding in I2102 0692

Situatie: Meneer zijn account stopte opeens met werken
Error: Gebruikersnaam of wachtwoord onjuist
Welke account: Mail account
Sinds: Net
Heeft het hiervoor gewerkt: Ja, de hele dag werkte het gewoon
Mogelijkheid tot verlopen: Nee, laatst nog een reset uitgevoerd
Reden melding: Meneer heeft het vermoeden dat dit een hacking attempt is geweest in verband met zijn positie

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek

6) Zet de melding op het datalekteam

Gebruiker meldt dat de PC aangeeft dat: 'De opgegeven gebruikersnaam of wachtwoord is niet correct'.
Heeft hij eerder nog wel kunnen inloggen: Ja, eerder vandaag

Actie

5.1.2.e **onzichtbaar voor aanmelder** 17 februari 2021 9:04
Met dhr. 5.1.2.e gebeld. Hij geeft aan dat dit incident afgemeld mag worden.

5.1.2.e **onzichtbaar voor aanmelder** 16 februari 2021 9:59
@ST: Aanmelder is geholpen in I2102 0691. Kunnen jullie dit onderzoeken?

5.1.2.e **onzichtbaar voor aanmelder** 15 februari 2021 20:22

20:21 gebeld door security officer 5.1.2.e zij zien wat raar met de inlog en zullen er verder naar kijken, maar er is nu geen actie nodig
@dagdienst, zouden jullie kunnen kijken naar deze melding na de wachtwoord reset van de balie in I2102 0691. Ik kan geen passende behandelaar vinden om naar de security kant van dit incident te kijken.

5.1.2.e **onzichtbaar voor aanmelder** 15 februari 2021 19:45

-Het account van meneer was niet gelocked
-Meneer kon zich niet verfieren
-Wachtwoord voor de veiligheid veranderd naar iets onbekends
-Wachtwoord reset zal uitgevoerd worden in I2102 0691

@dagdienst, zouden jullie kunnen kijken naar deze melding na de wachtwoord reset van de balie in I2102 0691. Ik kan geen passende behandelaar vinden om naar de security kant van dit incident te kijken.

5.1.2.e **onzichtbaar voor aanmelder** 15 februari 2021 19:26

19:26 Gebeld met Security officer 5.1.2.e hij geeft aan dat DA piket eerst naar meneer zijn account zal moeten kijken voordat zij iets hieraan kunnen doen.

5.1.2.e **onzichtbaar voor aanmelder** 15 februari 2021 19:20

Meneer kan bereikt worden op 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 15 februari 2021 19:19

Onderstaande SO niet relevant omdat het hier gaat om een account wat laatst nog gereset is wat opeens niet meer is gaan werken en niet om een verloren apparaat

5.1.2.e **onzichtbaar voor aanmelder** 15 februari 2021 19:17

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:// 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ; 5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	15 februari 2021 19:15		Potentieel datalek
Gerealiseerde doorlooptijd	05:34	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	05:34		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	05:34		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	15 februari 2021 19:15
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	WW en gebruikersnaam zijn gereset
Beschrijving inbreuk	Geen datalek, account ineens gelocked

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2102 0895 Tijdelijke toegang tot gedeelde postbus

Tweede Kamer

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Automatisering

Details

Korte omschrijving	Tijdelijke toegang tot gedeelde postbus
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	25 februari 2021 11:24
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	15 november 2021 16:04
Afgemeld	Ja
Datum afgemeld	15 november 2021 16:13
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 19 februari 2021 12:49

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 15 november 2021 16:05

Per vandaag gereed gemeld. Per abuis is door de FG het juiste vinkje niet aangevinkt, zie bericht 20 juli hieronder.

5.1.2.e **onzichtbaar voor aanmelder** 20 juli 2021 12:47

@Datalekteam: Meestal verschijnt de mailbox vanzelf in het account van aanmelder na een paar minuten. Afhankelijk van de gegeven rechten (volledige toegang, verzenden als, verzenden

namens) kan men de mails in de mailbox inzien (enkel bij de eerste). Als jullie laten weten wanneer jullie dit gezien hebben, sluit ik hem hierna af.

5.1.2.e 20 juli 2021 12:12
Dank voor de melding. Gelet de inmiddels verstreken tijd zal ik het datalek gereed melden. Ook qua (informatie-)beveiliging is dit een incident geweest. Het heeft gevoelige informatie kunnen betreffen.

vraag: betekent dat iemand gemachtigd is voor een postbus ook direct mails kan inzien?

5.1.2.e **onzichtbaar voor aanmelder** 20 juli 2021 11:06
Nooit geëscaleerd en dus niet zichtbaar geweest voor Datalek team.

5.1.2.e **onzichtbaar voor aanmelder** 19 februari 2021 13:04
@Datalekteam: Graag advies over eventueel verder te ondernemen stappen.

5.1.2.e **onzichtbaar voor aanmelder** 19 februari 2021 12:55
In W2101 318 heb ik per ongeluk mevr. 5.1.2.e (5.1.2.h + 5.1.2.i) toegevoegd aan de de mailbox "Informatie Beveiliging". Dit is mij destijds niet opgevallen. Dit had namelijk mevr. 5.1.2.e (5.1.2.h + 5.1.2.i) moeten zijn. Gebruikers worden toegevoegd op basis van gebruikersaccounts.

Vandaag werd ik toevallig geconfronteerd door een collega van mevr. 5.1.2.e (Dhr. 5.1.2.e -> I2102 0890) met de melding dat mevr. 5.1.2.e nog altijd geen toegang heeft tot deze mailbox. Bij nader onderzoeken kwam mijn eerder gemaakte fout naar boven. Ik heb hierop contact gehad met coördinatie van de ServiceDesk, en direct mevr. 5.1.2.e (5.1.2.h + 5.1.2.i) de rechten tot deze mailbox ontnomen en deze rechten voor mevr. 5.1.2.e (5.1.2.h + 5.1.2.i) gerealiseerd.

Effectief heeft mevr. 5.1.2.e van 25 januari 2021 tot en met 19 februari 2021 toegang gehad tot de postbus Informatie Beveiliging.

5.1.2.e **onzichtbaar voor aanmelder** 19 februari 2021 12:49
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:/ 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
  -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	19 februari 2021 12:49		Potentieel datalek
Gerealiseerde doorlooptijd	1817:45	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	1817:45		
Doorlooptijd 'Afgerond'	00:35		
Doorlooptijd 'Uitvoering'	1817:10		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	19 februari 2021 12:49
Melding aan AP ja/nee	Ja
Waarom wel/niet melden aan AP	Nee, want beoordeeld als gering risico. Foutief gemachtigde heeft geen misbruik gemaakt.
Melding aan betrokkenen ja/nee	Ja
waarom wel/niet melden aan betrokkenen	Nee, want beoordeeld als gering risico. Foutief gemachtigde heeft geen misbruik gemaakt
Mogelijke consequenties	Lichamelijke, materiële of immateriële schade mogelijk voor betrokkene
Getroffen maatregelen	Foutieve autorisatie gecorrigeerd

Beschrijving inbreuk	Verkeerde persoon met zelfde achternaam gemachtigd voor postbus

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2104 0425 Privé nummer gelekt naar buiten

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Privé nummer gelekt naar buiten
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	9 april 2021 16:53
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	9 april 2021 16:05
Afgemeld	Ja
Datum afgemeld	9 april 2021 16:17
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 9 april 2021 12:55

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

De heer 5.1.2.e belt namens aanmelder. Hij geeft aan dat het TK-nummer van aanmelder bekend is geworden buiten de Tweede Kamer om. Aanmelder wordt nu lastig gevallen door burgers die hem te pas en te onpas bellen.

Actie

5.1.2.e 9 april 2021 16:05

Uit de zeer beperkte informatie die het datalekteam heeft ontvangen maak ik op dat het Tweede

Kamer telefoonnummer van de heer 5.1.2.e bekend is geworden buiten de Tweede Kamer, waardoor hij te pas en te onpas wordt gebeld. Aan het datalekteam wordt gevraagd om te onderzoeken hoe dit kan gebeuren.
Voor het datalekteam is het nog onduidelijk om welk telefoonnummer het gaat: is dit het vaste telefoonnummer of mobiele telefoonnummer van de heer 5.1.2.e
Op Plein2 in de bereikbaarheidsgids staat het doorkiesnummer van de heer 5.1.2.e vermeld. Deze bereikbaarheidsgids is uitsluitend intern raadpleegbaar.
Op de website van de Tweede Kamer worden door de Tweede Kamerorganisatie geen telefoonnummers van Kamerleden vermeld, uitsluitend emailadressen.
Voor ons is onbekend welke contactgegevens de heer 5.1.2.e mogelijk zelf deelt, bijvoorbeeld in zijn emailhandtekening.

Er is een quickscan uitgevoerd op de vindbaarheid van het zakelijke mobiele telefoonnummer van de heer 5.1.2.e Met als resultaat dat op de social media geen telefoonnummers van de heer 5.1.2.e zijn gevonden. Wel is het mobiele telelefoonnummer van de heer 5.1.2.e vindbaar op webpagina's zoals de pagina Persbericht,CDA parlementariër Pieter Omzigt spreekt over Aramese Christenen in Turkije en Irak.doc (aramean-dem.org) en op de website Kandidaten Tweede Kamerverkiezingen 2021 naar woonprovincie: deelselectie - Parlement.com.
Deze laatste website heeft geen enkele relatie met de Tweede Kamer maar is van het PDC.
Het is ons niet bekend wie deze telefoonnummers beschikbaar heeft gesteld aan deze webpagina's.

Op basis van bovenstaande is het datalekteam van mening dat de Tweede Kamer geen oorzaak kan aangegeven dat waarom de heer 5.1.2.e te pas en te onpas gebeld wordt op zijn zakelijke tweede kamertelefoonnummer.
Verder is het datalekteam van mening dat er geen oorzaak is vanwege een lek vanuit een Tweede Kamer systeem. Daarmee wordt deze melding niet beschouwd als een datalek en ook niet als zodanig geregistreerd.

Wanneer de CDA-fractie of de heer 5.1.2.e aanvullende suggesties heeft om te onderzoeken horen wij dat graag.
Voor nu meldt het datalekteam deze melding als gereed.

5.1.2.e **onzichtbaar voor aanmelder** 9 april 2021 13:28
@Datalekteam: Het telefoonnummer van aanmelder is gelekt naar buiten toe en hij wordt nu lastig gevallen door mensen die hem op zijn TK-nummer bellen. Op verzoek van dhr. 5.1.2.e (en de AS'er van het CDA, de heer de 5.1.2.e) graag onderzoeken hoe dit heeft kunnen gebeuren.

5.1.2.e Mailimport 9 april 2021 13:27
Date sent: Apr 9, 2021 1:02 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e ' <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e M." <5.1.2.e @tweedekamer.nl>, 5.1.2.e " <5.1.2.e @tweedekamer.nl>, "5.1.2.e "
<r. 5.1.2.e @tweedekamer.nl>
Subject: Re: I2104 0425 - TOPdesk melding

Beste Servicedesk, dit is een datalek en moet naar het datalek team toe. Groet, 5.1.2.e

Op 9 apr. 2021 om 12:58 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:

Geacht Security Team

Melding met nummer: I2104 0425 is aan u overgedragen.

Het betreft : Melding datalek
Privé nummer gelekt naar buiten

09-04-2021 12:58 5.1.2.e
@ST: Het telefoonnummer van aanmelder is gelekt naar buiten toe en hij wordt nu lastig gevallen door mensen die hem op zijn TK-nummer bellen. Op verzoek van dhr. 5.1.2.e (en de AS'er van het CDA, de heer 5.1.2.e) graag onderzoeken hoe dit heeft kunnen gebeuren.

09-04-2021 12:55 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.

Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
https://5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 9 april 2021 13:08
Beste 5.1.2.e dit is een datalek. Ik zet em door naar het datalek team. Groet, 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 9 april 2021 12:58
@ST: Het telefoonnummer van aanmelder is gelekt naar buiten toe en hij wordt nu lastig gevallen door mensen die hem op zijn TK-nummer bellen. Op verzoek van dhr. 5.1.2.e (en de AS'er van het CDA, de heer 5.1.2.e) graag onderzoeken hoe dit heeft kunnen gebeuren.

5.1.2.e **onzichtbaar voor aanmelder** 9 april 2021 12:55
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https://5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante

wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	9 april 2021 12:53		Potentieel datalek
Gerealiseerde doorlooptijd	03:12	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	03:12		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	03:12		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	9 april 2021 12:53
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Een quickscan uitgevoerd op de vindbaarheid van het zakelijke mobiele telefoonnummer
Beschrijving inbreuk	Geen datalek TK. Betrokkene heeft telefoonnummer zelf gepubliceerd op internet

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2104 1420 Verkeerde persoon toegevoegd aan mailbox

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Automatisering

Details

Korte omschrijving	Verkeerde persoon toegevoegd aan mailbox
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	6 mei 2021 14:15
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 30 april 2021 16:16

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 20 juli 2021 12:15

Zonder meer details heeft deze melding niet zoveel waarde. Graag meer informatie toevoegen over de betrokkenen. Verder ben ik benieuwd of er een protocol is voor het toekennen van rechten en/of daarin een controlemechanisme is opgenomen.

5.1.2.e **onzichtbaar voor aanmelder** 20 juli 2021 11:07

Niet geëscaleerd en dus niet zichtbaar geweest voor Datalekteam. Bij deze aangepast.

5.1.2.e **onzichtbaar voor aanmelder** 30 april 2021 16:20

@Datalekteam: Zie hieronder voor de info.

5.1.2.e **onzichtbaar voor aanmelder** 30 april 2021 16:19
Tijdens het uitvoeren van mijn reguliere werkzaamheden heb ik tijdelijk iemand toegang verleend tot een postbus waar zij geen toegang tot hoorde te hebben. Daar de uitkomst van de toevoeging raar op mij overkwam ben ik hier binnen een minuut of 5 achtergekomen en heb ik de foutieve persoon verwijdert en de juiste toegevoegd (en dit bevestigd in de Exchange Server).

5.1.2.e **onzichtbaar voor aanmelder** 30 april 2021 16:16
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:/ 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)

* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	30 april 2021 16:15		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	30 april 2021 16:16
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Persoon verwijderd
Beschrijving inbreuk	Persoon toegang verleend tot een postbus waar zij geen toegang tot hoorde te hebben

Overige Opmerkingen

5.1.2.e 17 september 2021 11:15

17 sept 2021: Ik kan dit incident niet meer openen en daardoor datalekregister niet invullen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2105 1088 Per ongeluk verkeerde persoon rechten toegekend tot mailbox

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Automatisering

Details

Korte omschrijving	Per ongeluk verkeerde persoon rechten toegekend tot mailbox
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	3 juni 2021 11:42
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	9 juni 2021 12:38
Afgemeld	Ja
Datum afgemeld	10 juni 2021 8:52
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 31 mei 2021 9:24

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — 28 mei 2021 14:33

In W2105 441, per ongeluk de aanvrager mevrouw 5.1.2.e de rechten gegeven i.p.v. mevrouw 5.1.2.e

Actie

5.1.2.e — 9 juni 2021 12:38

Goed gehandeld. Het advies het proces zo in te richten dat niet niet meer voorkomt of het huidige proces hierop te controleren (om dit in de toekomst te voorkomen). Ik meld de melding hierbij af en

registreer de melding in het datalakregister..

5.1.2.e **onzichtbaar voor aanmelder** 28 mei 2021 14:35
@Datalek: Ik heb de fout binnen 5 minuten gecorrigeerd, maar wil bij deze toch even melden.

5.1.2.e **onzichtbaar voor aanmelder** 28 mei 2021 14:33
De gebruiker doet een aanvraag voor een rechtenaanpassing, geen sjabloon aanwezig.
Beoordeel of de gebruiker hiertoe gemachtigd is en of dit standaarddienstverlening is. Indien dit niet zo is, dient de aanvraag via de klantvertegenwoordiger bij Service Management te worden neergelegd.

Informatie

Aanmelddatum	28 mei 2021 13:42		Potentieel datalek
Gerealiseerde doorlooptijd	74:56	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	74:56		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	74:56		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	28 mei 2021 13:42
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Binnen 5 minuten gecorrigeerd
Beschrijving inbreuk	Per ongeluk verkeerde persoon rechten toegekend tot mailbox

Overige Opmerkingen

5.1.2.e 17 september 2021 11:17
17 sept. 2021: incident is reeds afgemeld. Ik kan niet bij de gegevens en datalekregister niet invullen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2106 0055 Datalek: Verkeerd document personeelsdossier

5.1.2.e

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CIO Office

Details

omschrijving	Datalek: Verkeerd document personeelsdossier
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	7 juni 2021 16:00
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 2 juni 2021 8:40

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mailimport, m — Mailimport 2 juni 2021 8:30

Sender: 5.1.2.i tweedekamer.nl
Date sent: 5.1.2.e 8:05 5.1.2.e
To: "5.1.2.e" <5.1.2.e @tweedekamer.nl>
CC: 5.1.2.i <5.1.2.i @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>
Subject: RE: Verkeerd document personeelsdossier

Beste 5.1.2.e

Dat is vervelende van het document dat bij jou in het dossier is gekomen. Het is inderdaad een

datalek.
Zou je bijgaande link willen lezen en het formulier dat hierbij hoort verder in willen vullen? Datalekken | Plein2
Groeten,
5.1.2.e
medewerker personeelsbeheer
Stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.i tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 1 juni 2021 17:23
Aan: StafdienstHR <5.1.2.i tweedekamer.nl>
Onderwerp: Verkeerd document personeelsdossier

Goedemiddag,

In mijn personeelsdossier vond ik tot mijn verbazing een document dat niet van mij is, maar van een andere collega binnen de Tweede Kamer. Omdat het ook om 'persoonlijke' gegevens gaat is dit misschien zelfs wel een datalek. Ik zou dit document verwijderd willen zien uit mijn dossier. Kunnen jullie dit regelen? Moet dit ook nog ergens worden gemeld als datalek?

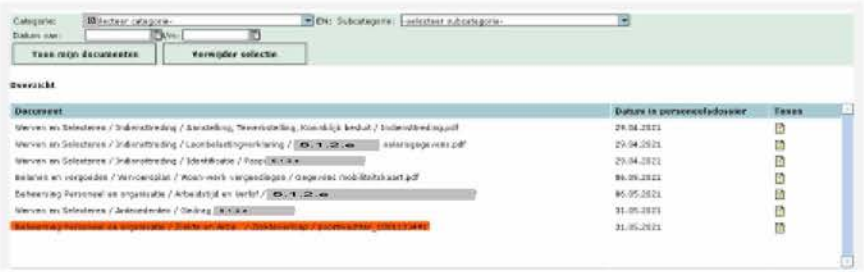


image001.png

Met vriendelijke groet,
5.1.2.e
5.1.2.e
CIO Office
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
M 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e **onzichtbaar voor aanmelder** 20 juli 2021 11:08
Niet geëscaleerd en dus niet zichtbaar geweest voor Datalekteam. Bij deze aangepast.

5.1.2.e Mailimport 2 juni 2021 10:20
Date sent: Jun 2, 2021 9:30 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: I2106 0055 Melding Datalek

Goedemorgen,

Hierbij wil ik melding maken van een datalek in mijn personeelsdossier. Ik hoor graag of het ingevulde formulier voldoende is.

Met vriendelijke groet,
5.1.2.e
Projectleider
CIO Office

Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
M 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 2 juni 2021 8:41
@Datalekteam: Wij hebben nog geen contact gehad met aanmelder over deze situatie. Zijn er vragen die jullie hierover hebben?

5.1.2.e **onzichtbaar voor aanmelder** 2 juni 2021 8:40
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:/ 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)

* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het 5.1.2.i team

Informatie

Aanmelddatum	2 juni 2021 8:30		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	2 juni 2021 8:30
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Mogelijke consequenties	Schending Privacy
Getroffen maatregelen	Onbekend
Beschrijving inbreuk	Verkeerd document personeelsdossier

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2106 0343 Mogelijke beveiligingsincidenten

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Bureau CISO

Details

Korte omschrijving	Mogelijke beveiligingsincidenten
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	14 juni 2021 8:47
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 10 juni 2021 10:40

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 8 juni 2021 10:47

Date sent: Jun 8, 2021 10:28 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: Beheer IAM <5.1.2.i @tweedekamer.nl>
Subject: Mogelijke beveiligingsincidenten

Goedemorgen 5.1.2.i

Het blijkt dat het dienstverband van dhr 5.1.2.e (5.1.2.h + 5.1.2.i) sinds 30-4 beëindigd is. Dit is helaas pas gisteren vanuit HR via het P-Direkt systeem in IAM binnengekomen. Hierdoor zijn het account, de mailbox en de toegang tot de Tweede Kamer gedurende de periode van beëindiging

dienstverband tot vandaag actief gebleven. Vanuit Beheer IAM is het niet mogelijk om na te gaan of er daadwerkelijk gebruik gemaakt is van de mogelijkheden, maar conform het proces melden we deze situatie aan jullie.

Een soortgelijke situatie is bij 5.1.2.e aan de hand. Zijn dienstverband was beëindigd op 2-6 en is ook pas sinds vanmorgen bekend geworden binnen IAM.

Wij hebben de betreffende identiteiten in IAM de oorspronkelijke einddatum gegeven waardoor de uitstroom direct is gestart.

Wanneer er meer informatie nodig is, horen wij dit graag.

Met vriendelijke groet,
5.1.2.e
Functioneel beheerder IAM
Bureau CISO
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
M (+5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
(woensdags afwezig)

Actie

5.1.2.e **onzichtbaar voor aanmelder** 8 juni 2021 11:34
@Datalekteam: Kunnen jullie hier naar kijken?

Informatie

Aanmelddatum	8 juni 2021 10:47		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	8 juni 2021 10:47
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Inloggen in TK account
Getroffen maatregelen	In IAM de oorspronkelijke einddatum gegeven waardoor de uitstroom direct is gestart.
Beschrijving inbreuk	2 personen toegang tot TK account na uitdiensttreding

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2106 0575 Datalek document in verkeerd personeelsdossier

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
E-mail	5.1.2.e @p-direkt.minbzk.nl

Details

Korte omschrijving	Datalek document in verkeerd personeelsdossier
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	17 juni 2021 13:50
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 11 juni 2021 15:51

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mailimport, m Mailimport 11 juni 2021 15:50

Sender: 5.1.2.e @p-direkt.minbzk.nl
Date sent: Jun 11, 2021 3:30 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Datalek Tweede Kamer

Hallo,

Zojuist kwam mij een datalek onder ogen waarbij gegevens van een medewerker van de Tweede Kamer gelekt zijn, vandaar dat ik u informeer.

1) Op welke datum is het datalek geconstateerd?
9 juni 2021

2) Op welke datum is het datalek ontstaan?
31 mei 2021
3) Wat is er gebeurd?
Er is een document in een verkeerd personeelsdossier geplaatst.
4) Welke gegevens betreft het?
Het betreft een kopie ontvangstbevestiging Wia-aanvraag. Hierop staan naw-gegevens en BSN
5) Welke partijen zijn betrokken?
Medewerker A Tweede Kamer – In zijn personeelsdossier zat het verkeerd geplaatste document.
Medewerker B Tweede Kamer – Van hem zijn persoonsgegevens gelekt.
Medewerker C, personeelsbeheer Tweede Kamer – Heeft het datalek geconstateerd en gemeld.
6) Wat is het gevolg?
Medewerker A heeft kennis kunnen nemen van de gegevens van medewerker B.
7) Wat is de opvolging?
Het document is naar het juiste personeelsdossier verplaatst. Betrokkene (medewerker B) is door P-Direkt geïnformeerd over het datalek.
8) Wat is de oorzaak?
Het datalek is veroorzaakt door een foutieve verwerking van P-Direkt. Huidige maatregelen zouden afdoende moeten zijn.
Mocht u nog aanvullende informatie nodig hebben dan is dat uiteraard geen enkel probleem.

Met vriendelijke groet,
5.1.2.e

5.1.2.e (zij/haar)
Medewerker Security en Kwaliteit
.....
P-Direkt
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Schenkkade 100 | 2595 AS | Den Haag | Kamer 4.07
Postbus 20011 | 2500 EA | Den Haag
.....
M 5.1.2.e
E 5.1.2.e @p-direkt.minbzk.nl
Webex ruimte https://rijksvideo.webex.com/meet/verena.poel

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Actie

5.1.2.e 15 juni 2021 10:03

Op 15 juni 2021 heeft de FG de melder (P-Direkt/Poel) het volgende bericht verstuurd:

Goedemorgen mevrouw 5.1.2.e

Naar aanleiding van het door u op 11 juni 2021 gemelde datalek bericht en verzoek ik u als volgt.

U meldt het volgende:

Op welke datum is het datalek geconstateerd?
9 juni 2021
Op welke datum is het datalek ontstaan?
31 mei 2021
Wat is er gebeurd?
Er is een document in een verkeerd personeelsdossier geplaatst.
Welke gegevens betreft het?
Het betreft een kopie ontvangstbevestiging Wia-aanvraag. Hierop staan naw-gegevens en BSN
Welke partijen zijn betrokken?

Medewerker A Tweede Kamer – In zijn personeelsdossier zat het verkeerd geplaatste document.
Medewerker B Tweede Kamer – Van hem zijn persoonsgegevens gelekt.
Medewerker C, personeelsbeheer Tweede Kamer – Heeft het datalek geconstateerd en gemeld.
Wat is het gevolg?
Medewerker A heeft kennis kunnen nemen van de gegevens van medewerker B.
Wat is de opvolging?
Het document is naar het juiste personeelsdossier verplaatst. Betrokkene (medewerker B) is door P-Direkt geïnformeerd over het datalek.
Wat is de oorzaak?
Het datalek is veroorzaakt door een foutieve verwerking van P-Direkt. Huidige maatregelen zouden afdoende moeten zijn.

Het betreft het lekken van bijzondere persoonsgegevens en u meldt dat de huidige maatregelen afdoende zouden moeten zijn. Blijkbaar is dit niet het geval en mijn vraag is derhalve waaruit die huidige maatregelen bestaan en waarom deze in dit geval niet voldoende zijn geweest. Ik verzoek u daarbij in te gaan op het bijzondere karakter van de gelekte gegevens en hoe dit soort lekken in de toekomst voorkomen worden. Ook betreft dit overigens niet de eerste keer dat gegevens in het personeelsdossier van iemand anders terecht komen. Ik verzoek u mij het bericht aan betrokken B te doen toekomen.

5.1.2.e **onzichtbaar voor aanmelder** 11 juni 2021 15:52
@Datalekteam: Zie melding aanmelder. Laat weten of jullie nog vragen hebben.

5.1.2.e **onzichtbaar voor aanmelder** 11 juni 2021 15:51
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv.

' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	11 juni 2021 15:50		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	11 juni 2021 15:50
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Inzage privé gegevens
Getroffen maatregelen	Document naar het juiste personeelsdossier verplaatst. Betrokkene geïnformeerd
Beschrijving inbreuk	Document in een verkeerd personeelsdossier geplaatst

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2106 0850 Onbekende USB stick gevonden

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Automatisering

Details

Korte omschrijving	Onbekende USB stick gevonden
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	19 juli 2021 13:35
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	Wacht op leverancier
Gereed	Ja
Datum gereed	14 juli 2021 14:33
Afgemeld	Ja
Datum afgemeld	15 juli 2021 16:12
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 16 juni 2021 12:55

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — 15 juni 2021 21:31

Ingebeld door 5.1.2.e techniek belde over een gevonden USB stick.

Sandisk USB stick.

Heeft verder niks met de USB stick gedaan.

Verder geen bijzonderheden qua uitelijk of markeringen

Actie

5.1.2.e **onzichtbaar voor aanmelder** 14 juli 2021 14:33
Ik heb de USB-stick opgehaald en de Chromebook wordt gereset en daarna opnieuw uitgeleverd. De USB-stick wordt op 20 oktober vernietigd wanneer niemand zich komt melden voor een verloren USB-stick.

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 11:12
Gisteren de USB-stick en Chromebook overhandigd aan 5.1.2.e in een sealbag. 5.1.2.e gaat de devices niet gebruiken, tot we meer weten over de inhoud op de USB-stick.

5.1.2.e **onzichtbaar voor aanmelder** 1 juli 2021 11:50

Overleg gehad met 5.1.2.e van SET.
SET was even in beraad geweest en hebben verzocht om de USB-stick & de Chromebook te komen ophalen voor (verder) onderzoek

Meegegeven aan 5.1.2.e De gevonden USB-stick & CB0094

-> Alle wachtwoorden die gebruikt zijn op de Chromebook zijn inmiddels aangepast.

5.1.2.e 16 juni 2021 17:07
USB-stick bekeken. Deze bevat geen data, maar is een *bootable* schijf met een Linux-distributie.
Toch nog overleggen (met Datalek/Security-team) wat er verder met het USB-stickje gedaan gaat worden.
Intussen ligt deze in de kluis voor hoe verder mee om te gaan.

5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2021 9:05
@Coordinatie: Moeten we dit nog doorzetten naar het datalekteam?

5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2021 9:05
USB is langs de balie gebracht en ligt nu op het bureau van dhr. 5.1.2.e

5.1.2.e 15 juni 2021 21:42
Aanmelder gewijzigd naar degene aan wie het overgedragen wordt.

5.1.2.e 15 juni 2021 21:32
Aaanmelder belt weer terug

Gevraagd of de USB stick bij de servicedesk achter gelaten kan worden en of hij morgen in de gelegenheid is.

Is morgen en de rest van de week niet aanwezig. Gaat het aan een collega overdragen.

Stopt de USB in een Envelope collega Taghavi zal de USB tzt langs komen brengen

5.1.2.e **onzichtbaar voor aanmelder** 15 juni 2021 21:31
Terwijl ik aan et inloggen was op de TK Citrix werd de call eruit gegooid

Geen passende SO gevonden

Informatie

Aanmelddatum	15 juni 2021 21:23		Potentieel datalek
Gerealiseerde doorlooptijd	196:03	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Coördinatieteamservicedesk
Doorlooptijd 'On hold'	188:10		
Aangepaste doorlooptijd	07:53		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	07:53		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	15 juni 2021 21:23
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Potentieel datalek
Getroffen maatregelen	De USB-stick isop 20 oktober vernietigd
Beschrijving inbreuk	Onbekende USB stick gevonden

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2106 0927 Telefoon in de water gevallen

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Telefoon in de water gevallen
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7873
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	22 juni 2021 17:53
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	21 juli 2021 13:12
Afgemeld	Ja
Datum afgemeld	22 juli 2021 8:27
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 21 juni 2021 11:08

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — 16 juni 2021 17:35

Telefoon in de water gevallen en valt niet meer terug te halen.

Actie

5.1.2.e — 21 juli 2021 13:12

FG/21 juli 2021: Gelet op het te water raken, hoeft de reactie op de vragen van de PO niet

afgewacht te worden. Ik meld de melding gereed.

5.1.2.e Mailimport 21 juni 2021 14:06
Date sent: Jun 21, 2021 1:48 PM
To: "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e' <5.1.2.e @tweedekamer.nl>, 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2106 0927 - TOPdesk melding

Ha 5.1.2.e

Goed punt.
Eén van mijn speerpunten voor 2021 is de procedure Datalekken.
Deze procedure moet worden geëvalueerd. Ook moet de e-learning Datalekken opnieuw onder de aandacht worden gebracht en moet het meldformulier datalekken worden geëvalueerd. Momenteel worden binnen de Tweede Kamer weinig tot geen datalekken gemeld, en de weinige datalekken die wel gemeld worden bestaan uit verloren/gestolen devices.

Wat betreft deze melding I2106009027: Ik zal het datalek registreren in ons datalekregister.
Hiervoor heb ik eerst nog informatie nodig van 5.1.2.i

- is het advies om te wipen opgevolgd en gelukt? Is nagegaan of het toestel nog online is geweest nadat het in het water is verdwenen?
- Is het van belang/mogelijk om te achterhalen op welke locatie het toestel in het water is gevallen?

Ik zal deze vragen ook in TOP-desk opnemen.

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Stafmedewerker Informatiebeveiliging
Bureau CISO
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T 5.1.2.e | +5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 21 juni 2021 13:17
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2106 0927 - TOPdesk melding

Ik denk dat er nu data uit de telefoon in het water is gelekt…
Serieus, wat moet je nu met zo'n melding?

Met vriendelijke groet,
5.1.2.e
5.1.2.i Architect
Bureau CISO
Tweede Kamer der Staten-Generaal
5.1.2.e
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: maandag 21 juni 2021 11:08
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2106 0927 - TOPdesk melding

Geacht Datalekteam

Melding met nummer: I2106 0927 is aan u overgedragen.

Het betreft : Melding datalek
Telefoon in de water gevallen

17-06-2021 11:24 5.1.2.e
Wij stellen de volgende acties voor:

- Probeer het device remote te wipen en te zorgen dat het device gewiped wordt zodra er een connectie wordt geconstateerd.
- Probeer de gebruiker nog om de locatie te vragen van het Device.
- Schakel Team Datalek in, meld het datalek bij hen.

16-06-2021 17:38 5.1.2.e
@Security
Meneer is zijn toestel in de water laten vallen en is niet meer terug te halen volgens meneer.
Heeft niet laten weten waar in de water.

Hebben jullie misschien nog eventueel toevoegingen?

Dank,
5.1.2.e

16-06-2021 17:36 5.1.2.e
Wordt verder opgepakt in W2106 451 Telefonie - Verlies mobiel toestel

16-06-2021 17:35 5.1.2.e
Dit verzoek is ingediend als incident, terwijl het eigenlijk als wijziging had moeten worden ingeschoten. Dit incident dient gesloten te worden en verder afgehandeld te worden via het relevante wijzigingssjabloon.
Koppel de betreffende wijziging aan dit incident via "opgelost door wijziging". Beoordeel zelf of de gebruiker over het sluiten van dit incident moet worden gemaild; indien je de gebruiker mailt, vermeld dan het wijzigingsnummer waarin het verzoek verder wordt afgehandeld en vraag om verder dit nummer te gebruiken in het mailverkeer betreffende dit verzoek.

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 21 juni 2021 13:49
Deze melding zal aan het datalekregister worden toegevoegd.

Hiervoor is nog nadere informatie nodig:
- is het advies om te wipen opgevolgd en gelukt? Is nagegaan of het toestel nog online is geweest nadat het in het water is verdwenen?
- Is het van belang/mogelijk om te achterhalen op welke locatie het toestel in het water is gevallen?

Verzoek aan de servicedesk om deze informatie op te vragen.

5.1.2.e **onzichtbaar voor aanmelder** 17 juni 2021 11:24
Wij stellen de volgende acties voor:

- Probeer het device remote te wipen en te zorgen dat het device gewiped wordt zodra er een connectie wordt geconstateerd.
- Probeer de gebruiker nog om de locatie te vragen van het Device.

- Schakel Team Datalek in, meld het datalek bij hen.

5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2021 17:38

@Security
Meneer is zijn toestel in de water laten vallen en is niet meer terug te halen volgens meneer.
Heeft niet laten weten waar in de water.

Hebben jullie misschien nog eventueel toevoegingen?

Dank,
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2021 17:36

Wordt verder opgepakt in W2106 451 Telefonie - Verlies mobiel toestel

5.1.2.e **onzichtbaar voor aanmelder** 16 juni 2021 17:35

Dit verzoek is ingediend als incident, terwijl het eigenlijk als wijziging had moeten worden ingeschoten. Dit incident dient gesloten te worden en verder afgehandeld te worden via het relevante wijzigingssjabloon.
Koppel de betreffende wijziging aan dit incident via "opgelost door wijziging". Beoordeel zelf of de gebruiker over het sluiten van dit incident moet worden gemaild; indien je de gebruiker mailt, vermeld dan het wijzigingsnummer waarin het verzoek verder wordt afgehandeld en vraag om verder dit nummer te gebruiken in het mailverkeer betreffende dit verzoek.

Informatie

Aanmelddatum	16 juni 2021 17:29		Potentieel datalek
Gerealiseerde doorlooptijd	233:13	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	233:13		
Doorlooptijd 'Afgerond'	02:24		
Doorlooptijd 'Uitvoering'	230:49		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	16 juni 2021 17:29
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Onbekend
Beschrijving inbreuk	Telefoon in het water gevallen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2107 0075 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Informatie en Archief
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	7 juli 2021 17:24
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	2 juli 2021 10:28
Afgemeld	Ja
Datum afgemeld	2 juli 2021 10:28
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 2 juli 2021 9:55

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 26 augustus 2021 12:36

Ik lees deze melding als volgt: gsm leek aanvankelijk onbevoegd meegenomen. Kort daarna bleek collega de gsm te hebben meegenomen, waarna de Servicedesk de incidentmelding heeft gesloten.
Geen acties meer nodig vanuit het datalekteam.

5.1.2.e **onzichtbaar voor aanmelder** — 2 juli 2021 10:28

Afgemeld want het betreft

mevrouw 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:15
Met 5.1.2.e het volgende afgesproken.
Full Wipe uitvoeren.
Mocht degene bereid zijn om het toestel terug te geven, het af laten geven bij de beveiligingsbalie aan de tweede kamer.
Als niet niemand opneemt of persoon niet bereid zijn om toestel terug te geven gebruiker vragen om aangifte te doen en de documenten daarvan koppelen aan de wijziging (met AVG redacted).

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 9:59
@Security Team
MT7633 schijnt door iemand meegenomen te zijn in een kroeg.
Mevrouw heeft de nummer gebeld en de persoon aan de andere kant van de lijn heeft verzocht om vandaag terug te bellen.
Zou jullie kunnen adviseren wat de beste stappen zijn om te nemen in dit geval.

Groetjes,
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 9:55
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	2 juli 2021 9:54		Potentieel datalek
Gerealiseerde doorlooptijd	00:34	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:34		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:34		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	2 juli 2021 9:54
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Servicedesk de incidentmelding heeft gesloten. Geen acties meer nodig vanuit het datalekteam.
Beschrijving inbreuk	Telefoon door collega meegenomen

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2107 0076 Potentieel datalek: telefoon verloren

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst Financieel Economische Zaken
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek: telefoon verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7860
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	5 juli 2021 16:33
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	21 juli 2021 13:09
Afgemeld	Ja
Datum afgemeld	22 juli 2021 8:27
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 2 juli 2021 10:06

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 21 juli 2021 13:09

FG/21 juli 2021 ik meld de melding gereed.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** — 2 juli 2021 16:10

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 15:49
In overleg met gebruiker en 5.1.2.e full whipe uitgevoerd en nummer aan nieuwe simkaart gekoppeld

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 13:40
1. aanvulling De pincode is niet serieel (complex bestaande uit verschillende getallen
2. ww-reset op account van mevr. uitgevoerd.
- we wachten op terugkoppeling of de telefoon weer in bezit is bij mevr.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 13:27
De gebruiker is bij de balie langsgeweest en heeft even geen contact met de collega die poogt de telefoon terug te krijgen bij de persoon die heeft opgenomen.
Het nummer geeft wanneer het gebeld wordt nu de voicemail. De telefoon kan uit staan, de batterij leeg zijn of de sim-kaart verwijderd. Wij wachten op contact met de andere collega

5.1.2.e 2 juli 2021 12:27
5.1.2.e

OM 9.59 uur is data gebruikt; kan ik daaruit concluderen dat degene die het toestel nu in zijn of haar bezit heeft, toegang heeft tot de informatie op het toestel en de applicaties? Is een full whipe dan niet aan te raden?

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:35
update: aangezien er een poging gaat worden gedaan de telefoon terug te krijgen, heeft 5.1.2.e de full whipe gecanceld

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:14
1. Gebruiker meldt dat het apparaat is verloren of gesloten
2. Het apparaat voor full whipe aangemeld in MDM
3. Zodra de whipe in MDM voltrokken is gaan we 5.1.2.e aan een nieuwe simkaart koppelen /// 5.1.2.e heeft gebeld met Datalekteam en gebruiker, ze gaan het toestel proberen terug te krijgen, nog niet wissen
4. Last access op het toestel is 6.19 uur geweest vandaag 2/juli/2021 //
We bellen Vodafone om te checken of er actief data wordt verbruikt op het nummer, zo stellen we vast of de simkaart eventueel uit het toestel is gehaald:
vandaag 10.03 hebben wij de whipe uitgevoerd, vodafone meldt dat om 9.59 uur een hele kleine hoeveelheid data is gebruikt.
De laatste oproep is gisteren (1-juli) om 17.15 uur gedaan

5. gebruiker is het apparaat waarschijnlijk sinds gisteravond (1/juli/2021 kwijt)

Gebruiker gaat vervangend apparaat nodig hebben om in te kunnen loggen vanuit huis met SMS-token
Uitvraag over ontgrendelingscode volgt nog

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:06
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
https: 5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	2 juli 2021 10:03		Potentieel datalek
Gerealiseerde doorlooptijd	126:36	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	126:36		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	126:36		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald

Datalekken

Datalekken

Datum constatering	2 juli 2021 10:03
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Full whipe
Beschrijving inbreuk	Verlies mobiel toestel

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2107 0077 Toegang tot verkeerde mailbox

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Automatisering

Details

Korte omschrijving	Toegang tot verkeerde mailbox
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	7 juli 2021 17:47
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 2 juli 2021 10:18

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 26 augustus 2021 12:39

Ik voeg deze melding toe aan het datalekregister.
Ook al is de onbevoegde machtiging van zeer korte duur geweest, formeel is het wel een datalek.
Afmelding van het incident voortaan laten doen door Privacy Officer die lid is van het datalekteam.

5.1.2.e **onzichtbaar voor aanmelder** — 20 juli 2021 11:08

Niet geëscaleerd en dus niet zichtbaar geweest voor Datalekteam. Bij deze aangepast.

5.1.2.e **onzichtbaar voor aanmelder** — 2 juli 2021 10:23

Dit naar aanleiding van het verzoek in W2107 023.

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:20
@Datalekteam: Zie hieronder. Mijn excuses!

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:19
Tijdens mijn werkzaamheden heb ik perongeluk dhr. 5.1.2.e voor +/- 30 seconden toegang gegeven tot een mailbox (persvoorlichting-Klein) waar hij geen toegang tot diende te hebben. Na het ontdekken van deze fout is het proces teruggedraaid en zijn zijn rechten op deze mailbox ontnomen.

5.1.2.e **onzichtbaar voor aanmelder** 2 juli 2021 10:18
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.

* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	2 juli 2021 10:17		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	2 juli 2021 10:17
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Toegang tot mailbox van iemand anders
Getroffen maatregelen	Rechten op deze mailbox ontnomen
Beschrijving inbreuk	Toegang tot verkeerde mailbox

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2107 0618 Melding datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
E-mail	5.1.2.e 5.1.2.e @tweedekamer.nl
Afdeling	GC Bestuur en Onderwijs
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Melding datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Organisatie
Urgentie	4. Kan verder met alternatief
Prioriteit	2 Hoog
SLA-streefdatum	21 juli 2021 15:11
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	21 juli 2021 12:59
Afgemeld	Ja
Datum afgemeld	21 juli 2021 13:15
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 21 juli 2021 11:19

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mailimport, m Mailimport 21 juli 2021 11:11

Sender: 5.1.2.i @tweedekamer.nl
Date sent: Jul 21, 2021 10:42 AM
To: " 5.1.2.e < 5.1.2.e @tweedekamer.nl>, " 5.1.2.e " < 5.1.2.e @tweedekamer.nl>
CC: " 5.1.2.e " < 5.1.2.e @tweedekamer.nl>, Commissie Verzoekschriften < 5.1.2.i @tweedekamer.nl>, " 5.1.2.e < 5.1.2.e @tweedekamer.nl>, 5.1.2.i < 5.1.2.i @tweedekamer.nl>
Subject: Melding datalek

Beste 5.1.2.e / 5.1.2.e

Vanochtend kreeg ik 5.1.2.e de onderstaande e-mail inzake de mededeling dat de reactie van de Minister voor Medische Zorg op het verzoekschrift van de heer 5.1.2.e als Kamerstuk was ingenomen door de Griffie Plenair. Het bleek dat ambtenaren van het ministerie van VWS deze inlichtingen naar de Griffie Plenair hadden gestuurd en niet naar de commissie voor de Verzoekschriften en de Burgerinitiatieven. In deze brief worden dus de naam en de adresgegevens volledig genoemd in de brief.

Na ontvangst van deze e-mail heb ik gelijk contact opgenomen met 5.1.2.e 5.1.2.e (van de Griffie Plenair) om hem te melden dat dit een datalek was en dat hij dit Kamerstuknummer moest verwijderen. Hij heeft de brief inmiddels ook uit Parlis gehaald.

Inmiddels heb ik ook een e-mail gestuurd naar de contactpersonen van het ministerie om te melden dat alle correspondentie m.b.t. lopende verzoekschriften via de Commissie gaat (en niet via de Griffie Plenair).

Omdat 5.1.2.e nu met vakantie is, stuur ik nu deze e-mail naar jullie toe zodat jullie ook op de hoogte zijn van deze kortstondig fout. Ik zet DA (5.1.2.i) nu ook in de cc zodat wij ook op de hoogte zijn van dit datalek.

Mocht ik nog iets moeten doen, dan hoor ik het graag van jullie.

Met vriendelijke groet,
5.1.2.e
Medewerker verzoekschriften en burgerinitiatieven (GC B&O)
Commissie voor de Verzoekschriften en Burgerinitiatieven van de Tweede Kamer der Staten-Generaal
Commissie voor de Verzoekschriften van de Eerste Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(31)5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: Commissie Verzoekschriften <5.1.2.i @tweedekamer.nl>
Verzonden: woensdag 21 juli 2021 09:26
Aan: Commissie VWS <cie.vws@tweedekamer.nl>; Commissie Verzoekschriften <5.1.2.i @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: RE: GP-VWS - Reactie op verzoek commissie inzake verzoekschrift van de heer 5.1.2.e over de subsidieregeling bonus zorgprofessionals COVID-19

Beste 5.1.2.e

Dank je wel voor jouw reactie. Wij (cie. Verzoekschriften) pakt dit verder over!

Met vriendelijke groet,
5.1.2.e
Medewerker verzoekschriften en burgerinitiatieven (GC B&O)
Commissie voor de Verzoekschriften en Burgerinitiatieven van de Tweede Kamer der Staten-Generaal
Commissie voor de Verzoekschriften van de Eerste Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(31)5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: Commissie VWS <cie.vws@tweedekamer.nl>
Verzonden: woensdag 21 juli 2021 09:25
Aan: Commissie Verzoekschriften <5.1.2.i @tweedekamer.nl>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: FW: GP-VWS - Reactie op verzoek commissie inzake verzoekschrift van de heer 5.1.2.e over de subsidieregeling bonus zorgprofessionals COVID-19

Goedemorgen collega's,

Onderstaande brief is door de griffie plenair geregistreerd voor de cie. VWS. Dit moet zijn Verzoekschriften.

29282-443
Reactie op verzoek commissie inzake verzoekschrift van de heer 5.1.2.e over de subsidieregeling bonus zorgprofessionals COVID-19
Brief regering
VWS
Procedurevergadering

Met vriendelijke groet,
5.1.2.e
Commissie assistent VWS
GC Sociaal en Financieel
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.e
M 5.1.2.e
E 5.1.2.e @tweedekamer.nl

Van: Parlis <Parlis@tweedekamer.nl>
Verzonden: woensdag 21 juli 2021 08:45
Onderwerp: GP-VWS - Reactie op verzoek commissie inzake verzoekschrift van de heer 5.1.2.e over de subsidieregeling bonus zorgprofessionals COVID-19

Bijgevoegd een of meer documenten die u ter kennisneming worden toegezonden:
· Reactie op verzoek commissie inzake verzoekschrift van de heer 5.1.2.e over de subsidieregeling bonus zorgprofessionals COVID-19
o Document openen
o Documentgegevens openen (incl. eventuele bijlagen)
o Document ontvangen op uw mobile device (3310 KB)
o Document openen in Outlook Web Access
o Documentgegevens openen in Outlook Web Access (incl. eventuele bijlagen)
De behandeling van dit document (of documenten) kunt u via de zaak 2021Z13915 volgen.
Een overzicht van meer documenten die vandaag of eerder bij de Griffie plenair zijn ontvangen, vindt u in Parlis: nieuwe documenten
Dit bericht is verzonden door Parlis. Het bericht is geautomatiseerd vervaardigd, u kunt het daarom niet beantwoorden.

Indien u vragen of opmerkingen heeft naar aanleiding van dit bericht, verzoeken wij u contact op te nemen met de afdeling Griffie plenair of de betreffende commissie.

De distributielijsten van Parlis worden met de grootst mogelijke zorg samengesteld. Indien u desondanks van mening bent dat u ten onrechte op deze lijsten terecht bent gekomen, of indien u deze mail in het vervolg niet meer wenst te ontvangen, verzoeken wij u dit door te geven aan de afdeling Griffie plenair of de betreffende commissie.

Actie

5.1.2.e 21 juli 2021 12:59
op 21 juli 2021 heb ik onderstaand bericht gemaild aan de melder. Ik sluit de melding hiermee af.

Beste 5.1.2.e

Dank voor de melding van het datalek (zie onderwerpsbalk). Ik stel vast dat alle noodzakelijke stappen zijn gezet, het datalek kortstondig heeft geduurd en dat eventuele toegang tot de informatie via Parlis onder het bereik van dezelfde verwerkingsverantwoordelijke valt. Geen verdere actie nodig.

5.1.2.e **onzichtbaar voor aanmelder** 21 juli 2021 11:20

@Datalek

Zie bovenstaande mail van aanmelder

5.1.2.e **onzichtbaar voor** 21 juli 2021 11:19

aanmelder
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	21 juli 2021 11:11		Potentieel datalek
Gerealiseerde doorlooptijd	01:48	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	01:48		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	01:48		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	21 juli 2021 11:11
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Alle noodzakelijke stappen zijn gezet
Beschrijving inbreuk	Brief verstuurd naar verkeerd adres met naam en adresgegevens

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0116 Melding datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst HR
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Melding datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	11 augustus 2021 14:01
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 5 augustus 2021 16:04

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — Mailimport 5 augustus 2021 16:01

Date sent: Aug 5, 2021 3:57 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Melding datalek

Ha collega's,

Hierbij wil ik graag een datalekmelding maken die vandaag ontdekt is bij Stafdienst HR. Er wordt ook een melding gemaakt bij P-direkt om de fout te herstellen. Tevens worden desbetreffende personen geïnformeerd door Stafdienst HR.

Met vriendelijke groet,
5.1.2.e
Medewerker stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
M +(5.1.2.e
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Aanwezig op maandag, dinsdag en donderdag

Alle informatie over de Tweede Kamer is te vinden op www.tweedekamer.nl. U kunt de Tweede Kamer ook volgen op Facebook en Twitter.
Kijk alle vergaderingen live of on demand met de app Debat Direct. Download gratis voor Apple, Android of Windows10.

Actie

5.1.2.e 26 augustus 2021 14:10
Vandaag email gestuurd naar de collega's van stafdienst HR met verzoek om nadere informatie.
Beste collega's van HR,

Het datalekteam heeft op 5 augustus jl. onderstaande melding ontvangen van 5.1.2.e over een datalek.

Wij hebben meer informatie nodig om de melding te behandelen en de benodigde stappen uit te zetten. Wie kan mij hier vandaag meer informatie over geven?
Ik voeg het formulier datalekken bij, dat bij een melding van een datalek ingevuld naar 5.1.2.i moet worden gestuurd.
Tevens de link naar de datalekpagina op Plein2 waar meer informatie is te vinden over de datalekprocedure van de Tweede Kamer en een e-learning Datalekken is te vinden.

Datalekken | Plein2

5.1.2.e Mailimport 5 augustus 2021 17:38
Date sent: Aug 5, 2021 5:12 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2108 0116 - TOPdesk melding

Dan houdt het op. Tijdens mijn vakantie kan en wil ik wel meelezen maar ga, wil en kan niet inloggen. Collega 5.1.2.e is ook afwezig. Het is aan u/jullie.

Op 5 aug. 2021 16:27 schreef 5.1.2.i <5.1.2.i @tweedekamer.nl>:

Geachte heer 5.1.2.e

Helaas kunnen wij niet de casus naar u toe sturen (in overleg met coördinatie).

U moet toch alsnog inloggen op TOPdesk of het eventueel via een collega ophalen van het datalekteam.

Wij hopen u hiermee voldoende geïnformeerd te hebben.
Met vriendelijke groet,
ServiceDesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.i @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: donderdag 5 augustus 2021 16:14
Aan: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: I2108 0116 - TOPdesk melding

Goedemiddag,

Kan vanuit hier niet inloggen. Graag ontvang ik de casus per mail. Is dat mogelijk?

Op 5 aug. 2021 16:05 schreef 5.1.2.i <5.1.2.i @tweedekamer.nl>:

Geacht Datalekteam

Melding met nummer: I2108 0116 is aan u overgedragen.

Het betreft : Melding datalek
Melding datalek

05-08-2021 16:05 5.1.2.e
@Datalekteam: Kunnen jullie iets met deze melding?

05-08-2021 16:04 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 5 augustus 2021 16:31
Heer 5.1.2.e teruggemaild, dat in overleg met coördinatie we de casus niet per mail kunnen opsturen.

5.1.2.e Mailimport 5 augustus 2021 16:28
Date sent: Aug 5, 2021 4:13 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Re: I2108 0116 - TOPdesk melding

Goedemiddag,

Kan vanuit hier niet inloggen. Graag ontvang ik de casus per mail. Is dat mogelijk?

Op 5 aug. 2021 16:05 schreef 5.1.2.i <5.1.2.i @tweedekamer.nl>:

Geacht Datalekteam

Melding met nummer: I2108 0116 is aan u overgedragen.

Het betreft : Melding datalek
Melding datalek

05-08-2021 16:05 5.1.2.e
@Datalekteam: Kunnen jullie iets met deze melding?

05-08-2021 16:04 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de

gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
https://5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 5 augustus 2021 16:05
@Datalekteam: Kunnen jullie iets met deze melding?

5.1.2.e **onzichtbaar voor aanmelder** 5 augustus 2021 16:04

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	5 augustus 2021 16:01		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	5 augustus 2021 16:04
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Persoonlijke informatie voor een andere medewerker in te zien.
Getroffen maatregelen	Melding Pdirect en betrokkenen geïnformeerd.
Beschrijving inbreuk	P-dossier documenten zijn bij een werknemer met dezelfde achternaam foutief geplaatst in P-direkt.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0139 Potentieel datalek: telefoon verloren

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	VVD
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek: telefoon verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7739
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	9 augustus 2021 13:14
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 9 augustus 2021 9:21

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 9 augustus 2021 9:14

Date sent: Aug 8, 2021 10:48 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Telefoon kwijt

Dag,

Graag maak ik zsm een afspraak omdat mijn iphone helaas kwijt is en niet is teruggevonden (waarvoor mijn welgemeende excuses).

Ik ben het beste bereikbaar via deze mail.

Groeten,

5.1.2.e

5.1.2.i

Actie

5.1.2.e 26 augustus 2021 14:12
Dit incident wordt toegevoegd aan het datalekregister

5.1.2.e 10 augustus 2021 16:11
Ingevulde Datalek Formulier gekoppeld aan de incident.

account, dummy Mailimport 10 augustus 2021 16:08
Date sent: Aug 10, 2021 3:46 PM
To: "5.1.2.e <5.1.2.e @tweedekamer.nl>
Subject: I2108 0139 Datalek formulier ingevuld

Er is een scan gemaakt vanaf een 5.1.2.h+5.1.2.i MFP. U vindt de scan als bijlage bij deze e-mail.

5.1.2.e **onzichtbaar voor aanmelder** 9 augustus 2021 9:27
W2108 064 verlies hierin gerapporteerd.

5.1.2.e **onzichtbaar voor aanmelder** 9 augustus 2021 9:24
@datalekteam, kunnen jullie dit verder oppakken?

5.1.2.e **onzichtbaar voor aanmelder** 9 augustus 2021 9:21
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:/5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!

o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	9 augustus 2021 9:14		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	9 augustus 2021 9:21
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend.
Getroffen maatregelen	Onbekend.
Beschrijving inbreuk	Verlies mobiele telefoon.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0313 Potentieel datalek

5.1.2.e Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e Salima
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7897
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	17 augustus 2021 15:30
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 17 augustus 2021 11:36

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 26 augustus 2021 14:13

Incident wordt toegevoegd aan het datalekregister

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** — 17 augustus 2021 12:45

@ Datalekteam,

Onderstaande handelingen die verzocht werden, zijn uitgevoerd door de Service Desk

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:42
WW-reset gedaan en nieuw ww vanuit Outlook opgestuurd I2108 0317 Wachtwoordreset

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:37

i2108 0313 (1).PNG

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:33

i2108 0313.PNG

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:31
Geachte mevrouw 5.1.2.e

Hierbij willen wij u informeren over de status van uw incident beschreven in het onderwerp van deze e-mail.

Op last van het Security Team gaan wij nu over tot het wissen van alle werkgegevens van uw telefoon (de partiele whipe). Tevens ontvangt u na de whipe per mail een nieuw wachtwoord voor uw tweede-kamer-account.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:27
5.1.2.e heeft zojuist gebeld, op last van het Security team doen we een partial whipe en een ww reset.
Het ww kan na de whipe worden verstuurd aan het TK adres dat mevr. op haar ipad kan ontvangen.

5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:23
Na overleg met 5.1.2.e doen we een partial whipe en een ww reset.

5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:19
ik zet em door naar het datalek team.

5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 12:18
Beste 5.1.2.e
Ik stel voor een full whipe en een reset van het ww. ik bel jullie even.

Groet,
5.1.2.e

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 11:52
@ Security,

Wij hebben zojuist deze melding binnengekregen van een verloren telefoon.
Wij hebben bij mevr. per mail nagevraagd of een partial of full whipe van haar telefoon haar

voorkeur heeft, bij uitblijven van antwoord voeren we de partial whipe uit

automatisch, akkoord Mailimport 17 augustus 2021 11:49
Date sent: Aug 17, 2021 11:48 AM
To: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Subject: RE: Telefoon kwijt I2108 0313 Potentieel datalek

Geachte mevr. 5.1.2.e

Dank voor de melding, we hebben deze in goede orde ontvangen en zijn blij deze nu via uw kamermail te ontvangen. We zullen uw werkprofiel nu van uw telefoon moeten verwijderen.
Daarbij hebben we twee opties of enkel het verwijderen van het werkprofiel of uw hele telefoon met alle persoonlijke gegevens erbij.
Kunt u aangeven welke optie uw voorkeur heeft? We kunnen deze handeling slechts één maal uitvoeren dus het zal niet mogelijk zijn uw persoonlijke gegevens als nog te verwijderen nadat we hebben gekozen voor enkel het verwijderen van het werkprofiel.

Kunnen we u op een ander nummer bereiken?

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

-----Oorspronkelijk bericht-----
Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 17 augustus 2021 11:39
Aan: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Onderwerp: Re: Telefoon kwijt

Geachte helpdesk even via mijn tweede kamer mailadres!

Sent from my iPad

> On Aug 17, 2021, at 11:28, 472 5.1.2.e wrote:
>
>
> Beste ICT helpdesk,
> Ik ben mijn telefoon kwijt kunnen jullie die blokkeren?
> Mvg
> 5.1.2.e
> Sent from my iPad

5.1.2.e **Salima** Mailimport 17 augustus 2021 11:49
Date sent: Aug 17, 2021 11:39 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Re: Telefoon kwijt I2108 0313

Geachte helpdesk even via mijn tweede kamer mailadres!

Sent from my iPad

> On Aug 17, 2021, at 11:28, 472 5.1.2.e 5.1.2.e wrote:
>
>
> Beste ICT helpdesk,
> Ik ben mijn telefoon kwijt kunnen jullie die blokkeren?
> Mvg
> 5.1.2.e
> Sent from my iPad

mailimport, m Mailimport 17 augustus 2021 11:39

Sender: 5.1.2.e
Date sent: Aug 17, 2021 11:28 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Telefoon kwijt 5.1.2.e

Beste ICT helpdesk,
Ik ben mijn telefoon kwijt kunnen jullie die blokkeren?
Mvg
5.1.2.e
Sent from my iPad

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 11:37
In overleg met 5.1.2.e prioriteit ingeschaald op 2. Kan niet verder
W2108 143 Telefonie - Verlies mobiel toestel

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 11:36
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	17 augustus 2021 11:30		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	17 augustus 2021 11:36
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Datalek.
Getroffen maatregelen	Partial whipe en een ww reset.
Beschrijving inbreuk	Verlies mobiel toestel.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0333 Ongevraagd "Hulp op Afstand"-verzoek

5.1.2.e Tweede Kamer)

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Partij voor de Dieren
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Ongevraagd "Hulp op Afstand"-verzoek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	23 augustus 2021 16:00
Doorlooptijd	36 uur
On hold	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Afgemeld	Ja
Datum afgemeld	18 augustus 2021 14:59
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 17 augustus 2021 18:46

mevrouw krijgt een melding dat 5.1.1.e contact probeert te maken via Hulp op Afstand met haar werkcomputer. Zij heeft echter niet gevraagd om hulp op afstand.

Tel nr: 5.1.2.e

Actie

5.1.2.e **onzichtbaar voor aanmelder** 18 augustus 2021 14:59

Met dhr. 5.1.2.e gebeld. Hij probeerde een gebruiker van DVR te assisteren echter deze gaf tot 2x toe het verkeerde VDI nummer door. Aanmelder gebeld en uitgelegd. Aanmelder gaat hiermee akkoord.

5.1.2.e **onzichtbaar voor aanmelder** 18 augustus 2021 8:24

TODO:
- Contact opnemen met 5.1.2.e en uitvragen waar het mis ging.

5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 21:49

@dagdienst: Weet niet zeker of dit daadwerkelijk een groot probleem is, lijkt ook niet meer voorgekomen te zijn sinds het belletje (nog geen reactie van mevrouw). Weten jullie wat hier verder gedaan moet worden?

5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 21:45

Zelf even wat uitgezocht:

Mevrouw heeft geen verloren telefoon in haar verleden.

5.1.2.e is iemand die bij ons werkt, Functioneel Beheerder. Kan zijn dat de verkeerde PC aan hem doorgegeven is.

5.1.2.e **onzichtbaar voor aanmelder** 17 augustus 2021 18:47

Telefonisch afgesproken dat ze eerst het formulier/informatie/ screenshot wanneer het weer

gebeurd naar ons opstuurt.

Informatie

Aanmelddatum	17 augustus 2021 18:38	Geen standaardoplossing aanwezig "Security"
Gerealiseerde doorlooptijd	06:29	
Doorlooptijd 'On hold'	00:00	
Aangepaste doorlooptijd	06:29	
Doorlooptijd 'Afgerond'	00:00	
Doorlooptijd 'Uitvoering'	06:29	

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Behandelaar	Servicedesk
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0358 Gebruiker toegang verleend tot verkeerde mailbox

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Automatisering

Details

Korte omschrijving	Gebruiker toegang verleend tot verkeerde mailbox
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Organisatie
Urgentie	4. Kan verder met alternatief
Prioriteit	2 Hoog
SLA-streefdatum	19 augustus 2021 10:24
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 18 augustus 2021 15:55

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 26 augustus 2021 14:18

Foutieve machtiging op mailbox in de periode 2 juli 2021 en 18 augustus 2021. Dit is een datalek en zal worden toegevoegd aan het datalekregister.
Incident in vervolg niet zelf gereedmelden/afmelden, dit is een taak van het datalekteam in concreto de Privacy Officer die lid is van het datalekteam.

5.1.2.e **onzichtbaar voor aanmelder** 18 augustus 2021 16:04

@Datalekteam: Op 2 juli 2021 in W2107 023 heb ik toegang verleend aan dhr. 5.1.2.e op de

mailbox van het persloket tijdens het uitvoeren van mijn routine werkzaamheden. Ik heb hierbij over het hoofd gezien dat de aanvraag was voor dhr. 5.1.2.e en niet dhr. 5.1.2.e Op 17 augustus ben ik benadert door de eigenaar van deze mailbox dat dhr. 5.1.2.e nog altijd geen toegang had tot deze postbus. Bij het nazoeken is mij niet opgevallen dat het om dhr. 5.1.2.e ging en niet dhr. 5.1.2.e
Op 18 augustus heb ik verzocht aan dhr. 5.1.2.e om contact met ons op te zoeken om de problemen die hij ervaarde uit te zoeken. Hierbij kwam aan het licht dat de verkeerde heer 5.1.2.e toegang had gekregen tot de betreffende mailbox. Dit heb ik direct na ontdekking gecorrigeerd en de rechten voor dhr. 5.1.2.e afgenomen en die van dhr. 5.1.2.e toegevoegd.

In het kort komt het erop neer dat dhr. 5.1.2.e onbedoeld anderhalve maand toegang heeft gehad tot een mailbox die niet voor hem bedoeld was.

5.1.2.e **onzichtbaar voor aanmelder** 18 augustus 2021 15:55

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.

* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	18 augustus 2021 15:54		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	18 augustus 2021 15:55
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Inzage in mail van iemand anders. Datalek
Getroffen maatregelen	Machtiging ingetrokken.
Beschrijving inbreuk	Foutieve machtiging op mailbox.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0393 Datalek iPad

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Internationaal en Ruimtelijk
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Datalek iPad
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2083
Soort	Tablet
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	24 augustus 2021 15:00
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	26 augustus 2021 14:19
Afgemeld	Ja
Datum afgemeld	26 augustus 2021 14:38
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 20 augustus 2021 19:40

5.1.2.e belde een gaf aan dat tijdens haar vakantie in haar auto was ingebroken waardoor haar spullen inclusief haar iPad is gestolen.

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2021 15:27

Wordt verder opgepakt in W2108 344

5.1.2.e **onzichtbaar voor aanmelder** 26 augustus 2021 14:38

5.1.2.e gebeld en aangegeven dat mevrouw in aanmerking komt voor een nieuwe ipad. Ze heeft in het verleden geen schade of verloren iPad gehad. Ik heb aangegeven dat mevrouw zelf de aanvraag kan doen en indien er in de toekomst met de ipad schade of verlies gemaakt wordt de kosten voor mevrouw zelf zijn.

5.1.2.e Mailimport 26 augustus 2021 14:27

Date sent: Aug 26, 2021 12:51 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2108 0393 Aanmelden datalek

Beste collega's,
Naar aanleiding van onderstaand en vooral het feit dat mijn iPad is gestolen, vroeg ik mij af of ik een nieuwe iPad kan aanvragen, of niet.
Ik hoor het graag.
Dank alvast,
5.1.2.e

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: vrijdag 20 augustus 2021 19:40
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2108 0393 Aanmelden datalek

Geachte mevrouw 5.1.2.e

Dank voor het melden van een Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
Dit team zal u informeren over de voortgang en de afhandeling.

Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i). Dit kan telefonisch of middels het beantwoorden van deze e-mail.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 26 augustus 2021 14:19

Incident gereed gemeld. Alle noodzakelijke stappen, zoals full wipe, zijn uitgevoerd.
Incident wordt toegevoegd aan datalekregister

5.1.2.e Mailimport 24 augustus 2021 16:08

Date sent: Aug 24, 2021 11:00 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2108 0393 Aanmelden datalek

Zie bijgaand.
Met vriendelijke groet,
5.1.2.e

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: vrijdag 20 augustus 2021 19:40
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2108 0393 Aanmelden datalek

Geachte mevrouw 5.1.2.e

Dank voor het melden van een Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
Dit team zal u informeren over de voortgang en de afhandeling.

Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i). Dit kan telefonisch of middels het beantwoorden van deze e-mail.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 24 augustus 2021 10:01

5.1.2.e
20 augustus 2021 22:04
@Datalekteam, kunnen jullie dit verder oppakken?

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 24 augustus 2021 10:01
full whipe bevel verstuurd, maar apparaat is al 9 dagen inactief

I2108 0393.PNG

5.1.2.e **onzichtbaar voor aanmelder** 20 augustus 2021 23:52

5.1.2.e
Dag collega's, hierbij het vervelende bericht dat mijn iPad is gestolen. Vandaag rond 16.00.
Datalek dus.
Groet,
5.1.2.e
Griffier commissie IenW

Dag, aanvullend: Zoek mij iPad staat aan, maar ik heb mijn Apple ID account net verwijderd via mijn telefoon omdat mijn visa nummer erin staat.
Ik weet niet of dat goed is, maar ik zit in Italië nu bij de carabinieri.
Groet
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 20 augustus 2021 22:04
@Datalekteam, kunnen jullie dit verder oppakken?

5.1.2.e **onzichtbaar voor aanmelder** 20 augustus 2021 19:50
5.1.2.e gaat akkoord met de full wipe. Zij had alleen één iPad (van melding I2108 0093), object ID daarvan genomen. Haar mobiel kan op elk moment opraken.

5.1.2.e **onzichtbaar voor aanmelder** 20 augustus 2021 19:40

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	20 augustus 2021 19:36		Potentieel datalek
Gerealiseerde doorlooptijd	34:19	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	34:19		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	34:19		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	20 augustus 2021 19:36
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Potentieel datalek
Getroffen maatregelen	Full whipe
Beschrijving inbreuk	Gestolen IPad

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0447 Datalek Parlis

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Griffie Plenair - Bureau Wetgeving
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Datalek Parlis
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	27 augustus 2021 16:00
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	17 september 2021 10:52
Afgemeld	Ja
Datum afgemeld	17 september 2021 10:58
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 23 augustus 2021 21:05

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 23 augustus 2021 21:02

Date sent: Aug 23, 2021 6:12 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>
Subject: Datatalek "5.1.2.e"

Beste Servicedesk,

Bij deze wil ik graag een melding doen over een datalek:

· Op 20 augustus 2021 is in Parlis een antwoord geregistreerd (2021D30810) met een bijlage (2021D30811) door de Griffie plenair. Dit is een antwoord van de minister-president op schriftelijke vragen gesteld door het Kamerlid Ouwehand (zie 2021D30379).
· De volledige naam van een burger (5.1.2.e) werd vermeld in beide documenten (antwoord en bijlage). In de bijlage werd het privé adres van 5.1.2.e ook vermeld. NB: de bijlage in kwestie is een afschrift van een brief die Mark Rutte aan 5.1.2.e heeft verzonden.
· Beide documenten (antwoord en bijlage), inclusief de volledige naam en het adres van de burger, waren helaas ook zichtbaar op TK.nl sinds 20 augustus door de koppeling die Parlis en de website TK.nl met elkaar delen.
· Vandaag, 23 augustus, is de naam "5.1.2.e ' in beide documenten geanonimiseerd door de Griffie plenair (vervangen door initialen). En haar privé adres is ook van de bijlage verwijderd. Door deze correctie uitgevoerd in het systeem Parlis toont de website TK.nl deze privé gegevens ook niet meer.
Ik hoop u hiermee voldoende te hebben geïnformeerd.
Met vriendelijke groet,

5.1.2.e
Functioneel beheerder Parlis
Griffie plenair/Bureau Wetgeving
5.1.2.e

Actie

5.1.2.e 27 september 2021 17:20
Brief naar betrokkene is uiteindelijk 21 september door FG aan de familie gestuurd. Daarmee zijn alle noodzakelijke stappen uitgevoerd.

5.1.2.e 17 september 2021 10:53
Brief naar betrokkene is opgesteld en wordt verstuurd door 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2021 8:42
@Datalekteam: Hebben jullie verder nog acties van ons nodig, of kan dit incident afgemeld worden?

5.1.2.e 26 augustus 2021 14:24
Datalek is op 24 augustus gemeld aan de AP.
FG van de Tweede Kamer stelt een brief op aan betrokkene met excuses voor deze menselijke fout.
Datalek is 23 augustus door griffier Plenair gedicht.
Partij voor de Dieren is geadviseerd de redactie van de betreffende schriftelijke vragen zoals vindbaar op de website van de PvdD, in overeenstemming te brengen met de redactie van deze schriftelijke vragen zoals vindbaar in Parlis en Officiële bekendmakingen.
De Privacy Officer heeft navraag gedaan bij ministerie van Algemene Zaken.

Wanneer brief aan betrokkene is verstuurd zal dit incident gereed gemeld worden en worden toegevoegd aan het register datalekken.

De Privacy Officer zorgt dat dit incident onder de aandacht wordt gebracht van betrokkenen ambtenaren en AVG-contactpersonen waarbij zorgvuldige omgang met persoonsgegevens in parlementaire documenten wordt benadrukt met aandacht voor noodzakelijkheid en proportionaliteit van die persoonsgegevens.

5.1.2.e Mailimport 25 augustus 2021 10:06
Date sent: Aug 24, 2021 3:53 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e " <5.1.2.e @tweedekamer.nl>
Subject: I2108 0447 (Datalek Parlis)

Beste Servicedeskmedewerkers,

Graag het onderstaande feitenrelaas van collega 5.1.2.e (zie gele markering) toevoegen aan

incident **I2108 0447** (Datalek Parlis).

Alvast bedankt!

Gr. 5.1.2.e

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: maandag 23 augustus 2021 18:01
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: datalek

Afgelopen vrijdag hebben wij het volgende document ontvangen: Documentgegevens openen (incl. eventuele bijlagen) . Bij deze brief zat een afschrift van het antwoord van de mp aan de jongedame in kwestie als bijlage. In deze brief waren de contactgegevens niet verwijderd.
Op maandagochtend ben ik gebeld door de moeder van de jongedame in kwestie. Hierna heb ik de volgende stappen ondernomen:
Ik heb de vragen gedepubliceerd en daarna deze en de antwoorden geanonimiseerd. Veder is de bijlage uitgedraaid, geanonimiseerd, gescand en vervolgens over de oude versie gezet. Vervolgens heb ik 5.1.2.e gebeld en hem het verteld over wat er gebeurt is en de acties die ik heb ondernomen. Aan het einde van de middag heb ik contact met 5.1.2.e hierover gehad.
Met vriendelijke groet,
5.1.2.e
inhoudelijk medewerker
Griffie Plenair - Bureau Wetgeving
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e 24 augustus 2021 11:02
5.1.2.e en 5.1.2.e gaan dit uitzoeken.
Wordt vervolgd.

5.1.2.e **onzichtbaar voor aanmelder** 23 augustus 2021 21:05
@Datalekteam: zouden jullie hiernaar willen kijken?

5.1.2.e **onzichtbaar voor aanmelder** 23 augustus 2021 21:05
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
https 5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	23 augustus 2021 21:02		Potentieel datalek
Gerealiseerde doorlooptijd	173:22	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	173:22		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	173:22		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	23 augustus 2021 10:47
Melding aan AP ja/nee	Ja
Waarom wel/niet melden aan AP	Ja, vanwege ernst vh incident en vanwege minderjarigheid
Melding aan betrokkenen ja/nee	Ja
waarom wel/niet melden aan betrokkenen	23 augustus belde moeder betrokkene, 21 september reactie FG gestuurd naar de familie.
Mogelijke consequenties	Negatieve effecten voor betrokkene, waaronder bedreigingen
Getroffen maatregelen	Document offline gehaald en procedure opnieuw onder aandacht gebracht
Beschrijving inbreuk	Document onbedoeld gepubliceerd op internet ipv Parlis

Overige Opmerkingen

5.1.2.e 17 september 2021 10:51

17 sept. heeft FG zijn reactie gestuurd naar griffie plenair met verzoek toe te sturen aan moeder betrokkene.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2108 0633 Onderzoeken of mail doorgestuurd is naar derden

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Beveiligingsdienst

Details

Korte omschrijving	Onderzoeken of mail doorgestuurd is naar derden
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	2 september 2021 9:55
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Security Team
Behandelaarsgroep	Security Team
Status	In behandeling
Gereed	Ja
Datum gereed	30 augustus 2021 15:09
Afgemeld	Ja
Datum afgemeld	31 augustus 2021 8:15
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 30 augustus 2021 9:54

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

5.1.2.e Mailimport 27 augustus 2021 11:55

Date sent: Aug 27, 2021 9:23 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: "5.1.2.e " <5.1.2.e @tweedekamer.nl>
Subject: Inleveren devices 5.1.2.e

Goedemorgen,

Naar aanleiding van het advies dat mij gegeven is door uw collega stuur ik deze mail.

Gisteren is een collega 5.1.2.e mij is gevraagd haar spullen in te leveren.
Haar Chromebook is momenteel tijdelijk in gebruik door 5.1.2.e 5.1.2.e dit op verzoek 5.1.2.e de 5.1.2.e haar telefoon heb ik op kantoor liggen, haar account is al disabled.

Mijn vraag is nu; wat is nodig en wat wordt er van mij verwacht te doen om dit goed af te handelen?

Daarnaast heb ik een vervelend onderbuikgevoel; ik heb haar 5.1.2.e een aantal stukken doorgestuurd (naar haar zakelijke mail) die vertrouwelijk zijn. Is er een mogelijkheid te weten of zij deze stukken heeft doorgestuurd naar derden, miss haar privé mail? Kan dit kwaad? Het gaat o.a. om het O&F rapport, de contourennota en het integraal crisisplan.

Ik hoor graag van jullie.

Met vriendelijke groet,
5.1.2.e
managementassistent
Beveiligingsdienst

Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e 30 augustus 2021 15:09
Ik heb deze ticket afgesloten, vanwege het vorige bericht:

5.1.2.e
onzichtbaar voor aanmelder
30 augustus 2021 14:54
In overleg met Hoofd Beveiligingsdienst besloten om 5.1.2.h + 5.1.2.i
deze stukken van haar zakelijke mailaccounts naar andere accounts.

5.1.2.e **onzichtbaar voor aanmelder** 30 augustus 2021 14:54
In overleg met Hoofd Beveiligingsdienst besloten om 5.1.2.h + 5.1.2.i
deze stukken van haar zakelijke mailaccounts naar andere accounts.

5.1.2.e 30 augustus 2021 11:23
in overleg met diensthoofd op Security Team geplaatst

5.1.2.e **onzichtbaar voor aanmelder** 27 augustus 2021 12:23
@DH: Kunnen jullie inzien of er toevallig mail verkeer is geweest vanuit de mail adres
van 5.1.2.e @tweedekamer.nl naar derden?
- Het betreft voornamelijk de vertrouwelijke stukken die zijn aangegeven door mevrouw 5.1.2.e

Informatie

Aanmelddatum	27 augustus 2021 11:55		Potentieel datalek
Gerealiseerde doorlooptijd	12:44	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	12:44		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	12:44		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	27 augustus 2021 11:55
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Potentieel datalek
Getroffen maatregelen	In overleg met Hoofd Beveiligingsdienst besloten om 5.1.2.h + 5.1.2.i

Beschrijving inbreuk	Doorsturen vanvertrouwelijke stukke

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 0023 Telefoon kwijt geraakt

5.1.2.e (Tweede Kamer)

Tweede Kamer DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst Communicatie
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Telefoon kwijt geraakt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	6 september 2021 17:57
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	14 oktober 2021 9:40
Afgemeld	Ja
Datum afgemeld	14 oktober 2021 9:40
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 1 september 2021 10:31

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 15 september 2021 10:16

Mevrouw heeft contact met mij opgenomen (15 september 2021) . Haar telefoon (en toegangspas!) heeft zij na twee weken teruggevonden in de auto. De zaak zal worden afgesloten.

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2021 11:26
Aanmelder meldt haar telefoon gevonden te hebben.

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2021 10:38
@DLT: Hebben jullie nog vragen voor ons/aanmelder?

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2021 10:32
Aanmelder meldt gisteren haar privé telefoon kwijt te zijn geraakt. Hier stonden wel gegevens op van de Tweede Kamer (e-mail e.d.) Met aanmelder afgesproken een partial wipe uit te voeren.

Aanmelder geeft aan dat ze haar telefoon heeft beveiligd met een vingerafdruk voor ontgrendelen en een 6 cijferige pincode voor toegang tot de Secure Hub.

Aanmelder gaat kijken op de vermoedelijke locatie waar ze haar telefoon verloren heeft om te kijken of ze hem daar hebben gevonden.

5.1.2.e **onzichtbaar voor aanmelder** 1 september 2021 10:31
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	1 september 2021 10:27		Potentieel datalek
Gerealiseerde doorlooptijd	293:43	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	293:43		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	293:43		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 0107 Printjes verdwenen

5.1.2.e (Tweede Kamer)

Tweede Kamer

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst Communicatie
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Printjes verdwenen
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MFP062
Soort	Multifunctionele printer
Vestiging	Tweede Kamer B67
Locatie	C.32 Gang

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	8 september 2021 9:36
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 2 september 2021 11:37

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

MFP062

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 3 september 2021 10:09

Hierbij het antwoord van Hosting:

Ik zie dat mevrouw 2x printjes heeft opgehaald om 10:32 en om 11:45

na deze tijdstippen is de eerste gebruiker:
om 10:37 heeft gebruiker doen1302 printjes gemaakt

en de tweede keer:
om11:48 heeft gebruiker puia2708 printjes gemaakt

Echter rond 11:02 zie ik geen printjes die ze heeft gemaakt.

5.1.2.e 2 september 2021 12:57
Ik ben benieuwd hoe het mogelijk is dat printjes zoekraken op de Multifunctioneel. Immers, alleen een rechthebbende kan met eigen toegangscodes of activeren Kamerpas, de printopdracht laten uitvoeren op de Multifunctioneel.

Ik stel voor dat het datalekteam de bevindingen van het onderzoek dat het hosting-team momenteel uitvoert afwacht
@Servicedesk: willen jullie de bevindingen van het Hostingteam toevoegen aan deze melding?

5.1.2.e **onzichtbaar voor aanmelder** 2 september 2021 11:40
Er is een potentieel datalek doordat mevrouw 5.1.2.e haar printjes mist van MFP062 rondom 11:02 uur.
Mevrouw wilt graag weten wie en waar haar printjes zijn gebleven.
Er is een melding gemaakt voor het opvragen wie er na haar op MFP062 heeft ingecheckt (I2109 0103 Inchecken van printer opvragen)
@Datalekteam, kunnen jullie dit verder oppakken?

5.1.2.e **onzichtbaar voor aanmelder** 2 september 2021 11:37
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	2 september 2021 11:36		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	2 september 2021 11:37
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Mogelijke consequenties	Datalek
Getroffen maatregelen	Nagegaan wie er heeft geprint om MFP062.
Beschrijving inbreuk	Printjes verdwenen.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 0432 Potentieel datalek: iPad verloren

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek: iPad verloren
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2043
Soort	Tablet
Vestiging	Domeinen Roerende Zaken

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	14 september 2021 10:47
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	9 september 2021 10:22
Afgemeld	Ja
Datum afgemeld	9 september 2021 10:22
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 8 september 2021 12:48

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e **onzichtbaar voor aanmelder** — 9 september 2021 10:22

Aanmelder heeft zijn iPad thuis gevonden.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 8 september 2021 13:11
@ datalekteam
Onderstaand hebben wij een potentieel datalek in behandeling genomen

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 8 september 2021 13:08
Aanmelder had de iPad naar alle waarschijnlijkheid in een verzegelde groene bak gestopt ter verhuizing.
Gebruiker heeft een melding gemaakt dat die bak kwijt was, gebruiker had als enige van de fractie niet zijn persoonlijke groene bak.
Na aanmaken van de melding (aangemeld bij facility), stond de groene bak open voor de kamer van de aanmelder (aanmelder heeft geen terugkoppeling gehad over de melding).
In de open bak zat niet meer de iPad.

In overleg met de gebruiker gaan we een selectieve whipe uitvoeren.
Zoals blijkt uit de screenshot was de iPad imei 35 303609 736869 7 reeds 81 dagen inactief, dat betekent dat de kamermail reeds 50 dagen niet meer toegankelijk is geweest
Selective wipe was requested at 9/8/21 1:04:51 pm. This operation is carried out upon device connection.

Is de ipad serieel vergrendeld?
NEE, geen 5.1.2.h + 5.1.2.i 555 of 5.1.2.h + 5.1.2.i combinatie van cijfers (niet voordehand liggend)
ook geen geboortejaar etc.
toestel is in de tussentijd niet online geweest

Aanmelder nog eens een tripplecheck gaat doen of u de iPad op een andere plaats kunt vinden, daarna contact met ons zal opnemen om vervolgacties samen af te stemmen

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 8 september 2021 12:48
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:/ 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	8 september 2021 12:47		Potentieel datalek
Gerealiseerde doorlooptijd	07:05	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	07:05		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	07:05		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 0616 Datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Griffie Plenair - Bureau Wetgeving
Locatie (Aanmelder)	5.1.2.e

Details

omschrijving	Datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	17 september 2021 11:35
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	5.1.2.e
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	17 september 2021 11:58
Afgemeld	Ja
Datum afgemeld	17 september 2021 14:07
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 13 september 2021 13:35

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 13 september 2021 13:35

Date sent: Sep 13, 2021 1:33 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Datalek

Beste medewerkers van de Servicedesk,

Bij deze weg meld ik een mogelijk geval van datalek.

· Een commissiemedewerker heeft een document (2021D32995) afkomstig van de heer 5.1.2.e per ongeluk verkeerd geregistreerd in Parlis. Het document in kwestie werd niet geregistreerd op de juiste manier, hierdoor werd het desbetreffende document niet gefilterd en dus wel getoond op de website van de Tweede Kamer en op de website van derde partijen (zoals 1848.nl die informatie kopieert via tk.nl).
· Het document 2021D32995 was vandaag ,13-09-2021, om 12.03 uur geregistreerd in Parlis en om 12.51 uur verwijderd.
· Het document in kwestie bevat o.a. een naam en een telefoonnummer. Het document is eigenlijk een brief vaan een burger gericht aan de Kamer (zulke brieven zijn niet openbaar natuurlijk).

Ik stuur via een aparte e-mailbericht de brief ik kwestie naar de privacy officer (5.1.2.e), en de e-mailcorrespondentie die al heeft plaatsgevonden tussen de commissie en de burger.

Alvast bedankt voor jullie inzet,

Met vriendelijke groet,

5.1.2.e
Functioneel beheerder Parlis
Griffie plenair/Bureau Wetgeving
5.1.2.e

Actie

5.1.2.e 17 september 2021 11:58
Het datalek is op 17 september gemeld bij de AP. De betrokkene wordt geïnformeerd door Griffie Plenair. Zie bijlagen in het register.

mailimport, m Mailimport 13 september 2021 15:30
Sender: cie.buza@tweedekamer.nl
Date sent: Sep 13, 2021 2:55 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: I2109 0616 toevoeging mail aan dossier datalek

Zal ik de mails die ik van de betrokken burger ontvang aan jullie doorsturen??
Hieronder een nieuwe mail van de afzender die ik zojuist ontvangen heb.
Met vriendelijke groet,
5.1.2.e
Commissie assistent
commissie Buitenlandse Zaken, contactgroep Frankrijk
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(31)5.1.2.e E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.i @bbl-ggz.nl>
Verzonden: maandag 13 september 2021 14:52
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.i @minaz.nl; 5.1.2.i @minbuza.nl; 5.1.2.e @minaz.nl; Commissie BUZA <cie.buza@tweedekamer.nl>
Onderwerp: Mail aan de persoonlijke assistenten van mijnheer Rutte en mevrouw Kaag

L.s.,

Ik begrijp dat u het beide erg druk heeft. Dan gaan er wel eens zaken verkeerd. Aangezien wij graag een veilige manier van communicatie proberen te bewerkstelligen wil ik u vragen hoe het zomaar kan dat e-mail adressen en namen van 5.1.2.e; via de commissie BuZA.

5.1.2.h + 5.1.2.i

Buiten reikwijdte
Buiten reikwijdte

deze data ging namelijk over hen.

Wij verwachten uw volledige medewerking om de zaken zo goed als het kan te herstellen.

5.1.2.h + 5.1.2.i

Met vriendelijke groet,

5.1.2.e en 5.1.2.h + 5.1.2.i

5.1.2.e 13 september 2021 15:00

Beste Service Desk,
Griffie Plenair en griffie commissie BuZa hebben het datalek gedicht is, door de betreffende email van de internetpagina van de Tweede Kamer te verwijderen. De betrokkene is per email door de commissie assistent geïnformeerd.
Functioneel Beheerder heeft op Google gecontroleerd of de email nog vindbaar was en heeft geconstateerd dat deze niet in de zoekresultaten was te vinden.

Inmiddels heeft betrokkene de Tweede Kamer verzocht om eerder toegezonden correspondentie te verwijderen. De betreffende commissie stuurt dit verwijderingsverzoek door naar fg@tweedekamer.nl

Privacy Officer zal met FG overleggen of dit datalek, gezien de ernst van de inhoud van de e-mail, moet worden gemeld aan de Autoriteit Persoonsgegevens.

5.1.2.e Mailimport 13 september 2021 14:42

Date sent: Sep 13, 2021 2:30 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: I2109 0616 datalek

Collega's

Er is vandaag een datalek geweest via Parlis.
De afzender van een brief heeft me gewezen op de openbaarheid van 2 bijlagen van zijn brief.
Ik stuur jullie in de bijlage van deze mail de reacties van de afzender die ik nadien ontvangen heb, om voor jullie het dossier compleet te houden.
Met vriendelijke groet,
5.1.2.e
Commissie assistent
commissie Buitenlandse Zaken, contactgroep Frankrijk
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 13 september 2021 13:52

@Datalekteam: Deze is rechtstreeks voor jullie. Hebben jullie hier nog vragen over?

5.1.2.e **onzichtbaar voor aanmelder** 13 september 2021 13:35

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:// 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	13 september 2021 13:35		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	36:23	Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	36:23		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	36:23		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 0719 Mogelijk ongeoorloofde toegang

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Bureau CISO
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Mogelijk ongeoorloofde toegang
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Organisatie
Urgentie	4. Kan verder met alternatief
Prioriteit	2 Hoog
SLA-streefdatum	15 september 2021 10:51
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 14 september 2021 16:25

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Kreeg vanaf vandaag de melding dat 5.1.2.e stond niet meer in het xml bestand van P-direkt. Navraag leerde dat mevr, 5.1.2.e sinds 26 augustus 2021 uit dienst is, maar dit is nooit doorgevoerd in IAM. Mevr, 5.1.2.e heeft vanaf vandaag geen toegang meer.

Actie

5.1.2.e **onzichtbaar voor aanmelder** 16 september 2021 8:47

@Datalekteam: Zie antwoord aanmelder hieronder.

Date sent: 5.1.2.e 8:28 PM
To: "5.1.2.e" <5.1.2.e @tweedekamer.nl>, 5.1.2.i <5.1.2.i @tweedekamer.nl>, "5.1.2.e"
<5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>, "5.1.2.e
<5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e"
<5.1.2.e @tweedekamer.nl>, "5.1.2.e" <5.1.2.e @tweedekamer.nl>
Subject: RE: I2109 0719 - TOPdesk melding

Geachte 5.1.2.e

Wij ontvingen daarover volgend bericht:
(tevens opgenomen in de bijlage en in I2109 0719)

5.1.2.e
14 september 2021 16:34
Date sent: Sep 14, 2021 4:32 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2109 0719 - Aanmelding Datalekteam

Beste 5.1.2.i

Bij deze de mail met de oorzaak van deze vertraagde uit dienst-actie. P-Direkt heeft het verzoek om de medewerkster uit dienst te zetten niet op tijd op kunnen pakken. Uiteindelijk is dit pas gister (op 13-9) uitgevoerd.

Met vriendelijke groet,
5.1.2.e
Functioneel beheerder IAM
Bureau CISO
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
M (+5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
(woensdags afwezig)

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
5.1.2.i

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 14 september 2021 17:04
Aan: 5.1.2.i <5.1.2.i @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e
<5.1.2.e @tweedekamer.nl>
Onderwerp: RE: I2109 0719 - TOPdesk melding

Goedemiddag,

Dit is bovenal een beveiligingsissue, toch? Ik ben benieuwd waarom de uitdiensttreding niet tijdig is doorgevoerd in IAM. Kan dat nagegaan worden?

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: dinsdag 14 september 2021 16:27
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.

nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2109 0719 - TOPdesk melding

5.1.2.e

Melding met nummer: I2109 0719 is aan u overgedragen.

Het betreft : Melding datalek
Mogelijk ongeoorloofde toegang

14-09-2021 16:26 5.1.2.e
@Datalekteam: Dhr. 5.1.2.e kreeg vandaag de melding dat 5.1.2.e niet meer in het xml bestand van P-direkt stond. Navraag leerde dat mevr, 5.1.2.e sinds 26 augustus 2021 uit dienst is, maar dit is nooit doorgevoerd in IAM. Mevr, 5.1.2.e heeft vanaf vandaag geen toegang meer. Mevr. 5.1.2.e heeft tot vandaag toegang gehad tot de Tweede Kamer omgeving. Het is onbekend of ze hier ook gebruik van heeft gemaakt.

14-09-2021 16:25 5.1.2.e
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e Mailimport 14 september 2021 20:22
Date sent: Sep 14, 2021 5:03 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>, "5.1.2.e " <5.1.2.e @tweedekamer.nl>, "5.1.2.e 5.1.2.e' <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e <5.1.2.e @tweedekamer.nl>, "5.1.2.e " <5.1.2.e @tweedekamer.nl>, "5.1.2.e " <5.1.2.e @tweedekamer.nl>
Subject: RE: I2109 0719 - TOPdesk melding

Goedemiddag,

Dit is bovenal een beveiligingsissue, toch? Ik ben benieuwd waarom de uitdiensttreding niet tijdig is doorgevoerd in IAM. Kan dat nagegaan worden?

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: dinsdag 14 september 2021 16:27
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2109 0719 - TOPdesk melding

Geacht Datalekteam

Melding met nummer: I2109 0719 is aan u overgedragen.

Het betreft : Melding datalek
Mogelijk ongeoorloofde toegang

14-09-2021 16:26 5.1.2.e

@Datalekteam: Dhr. 5.1.2.e kreeg vandaag de melding dat 5.1.2.e niet meer in het xml bestand van P-direkt stond. Navraag leerde dat mevr, 5.1.2.e sinds 26 augustus 2021 uit dienst is, maar dit is nooit doorgevoerd in IAM. Mevr, 5.1.2.e heeft vanaf vandaag geen toegang meer. Mevr. 5.1.2.e heeft tot vandaag toegang gehad tot de Tweede Kamer omgeving. Het is onbekend of ze hier ook gebruik van heeft gemaakt.

14-09-2021 16:25 5.1.2.e

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i #manage

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)

* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Klik hier om naar het incident te gaan.

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i).

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e Mailimport 14 september 2021 16:34
Date sent: Sep 14, 2021 4:32 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2109 0719 - Aanmelding Datalekteam

Beste 5.1.2.i

Bij deze de mail met de oorzaak van deze vertraagde uit dienst-actie. P-Direkt heeft het verzoek om de medewerkster uit dienst te zetten niet op tijd op kunnen pakken. Uiteindelijk is dit pas gister (op 13-9) uitgevoerd.

Met vriendelijke groet,
5.1.2.e
Functioneel beheerder IAM
Bureau CISO
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
M (+5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
(woensdags afwezig)

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: dinsdag 14 september 2021 16:27
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2109 0719 - Aanmelding Datalekteam

Geachte heer 5.1.2.e

Melding met nummer: I2109 0719 is aangemaakt.

Het betreft :Mogelijk ongeoorloofde toegang

De Dienst Automatisering draagt uw melding ter verdere afhandeling over aan het Datalekteam .

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande personen:

Dhr. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst 5.1.2.e

Met vriendelijke groet,

Servicedesk

Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 14 september 2021 16:26

@Datalekteam: Dhr. 5.1.2.e kreeg vandaag de melding dat 5.1.2.e niet meer in het xml bestand van P-direkt stond. Navraag leerde dat mevr, 5.1.2.e sinds 26 augustus 2021 uit dienst is, maar dit is nooit doorgevoerd in IAM. Mevr, 5.1.2.e heeft vanaf vandaag geen toegang meer. Mevr. 5.1.2.e heeft tot vandaag toegang gehad tot de Tweede Kamer omgeving. Het is onbekend of ze hier ook gebruik van heeft gemaakt.

5.1.2.e **onzichtbaar voor aanmelder** 14 september 2021 16:25

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de

klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	14 september 2021 16:21		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	00:00	Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	14 september 2021 16:25
Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee
Mogelijke consequenties	Ongeoorloofde toegang account omgeving
Getroffen maatregelen	Pdirect heeft mw op "uit dienst" ingevoerd.
Beschrijving inbreuk	Na uitdiensttreding toegang nog toegang tot de Tweede kamer omgeving.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 1211 Naam burger in officiële stukken

Tweede Kamer
DER STATEN-GENERAAL

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Bestuur en Onderwijs
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Naam burger in officiële stukken
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	29 september 2021 13:41
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	27 september 2021 15:17
Afgemeld	Ja
Datum afgemeld	27 september 2021 15:27
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 23 september 2021 15:46

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Aanmelder meldt dat ergens in het voorjaar een brief ontvangen met een vraag. Ze hebben deze vraag doorgezet naar de betreffende minister. In de titel van deze vraag is de voorletter en achternaam van de brief te zien. Dit is gebeurt in Parlis. Aanmelder gaat dit samen met de Functioneel Beheerder van Parlis aanpassen. Het betreft documentnummer 2021D27774. De naam is zichtbaar geweest van 7 juli tot 23 september.

Actie

5.1.2.e 27 september 2021 15:17

De adjunct-griffier die datalek heeft gemeld heeft het datalek gedicht op onderstaande wijze:
"Ik heb zelf de naam verwijderd uit parlis en met 5.1.2.e (vervanger 5.1.2.e) gecheckt of het zo goed was. Hij zei van wel.
De naam is dus niet gelakt, maar de titel van het document aangepast. Zie Aan bewindspersoon - rappel reactie | Tweede Kamer der Staten-Generaal

Waar nu 'rappel reactie' staat, stonden dus eerste de persoonsgegevens.

Daarmee is het datalek gedicht en wordt dit incident gereed gemeld. Het datalek wordt toegevoegd aan het datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 23 september 2021 15:46

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	23 september 2021 15:41		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	18:36	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	18:36		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	18:36		
Contractnummer	Datalekken		
Dienst	Datalekken		
Korte omschrijving	Datalekken		
Dienstenniveau	Storingsafhandeling		
SLA-doorlooptijd	36 uur		
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald		
Servicewindow	Service window		

Datalekken

Datalekken

Datum constatering	23 september 2021 15:14
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Nee
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Nee
Mogelijke consequenties	Niet bevoegden hebben kennis kunnen nemen van de klacht over Ziekenhuis
Getroffen maatregelen	Naam burger is uit de onderwerp regel gehaald
Beschrijving inbreuk	Tussen 7 juli en 23 september heeft een rappel over klacht van een burger onbedoeld online gestaan

Overige Opmerkingen

5.1.2.e 27 september 2021 15:17

Op 7 juli heeft de betreffende commissie bij de bewindspersoon gerappelleerd dat een klacht van een burger nog niet beantwoord is. Hierbij is in de onderwerp regel de naam van de burger onbedoeld vermeld. Toen dit op 23 september is ontdekt door de adjunct-griffier heeft deze de naam weggehaald in de onderwerp regel.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 1283 Telefoon kwijt geraakt

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Telefoon kwijt geraakt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7681
Soort	Mobiel telefoontoestel
Vestiging	Domeinen Roerende Zaken

Planning

Impact	Persoon
Urgentie	2. Kan niet verder
Prioriteit	3 Normaal
SLA-streefdatum	28 september 2021 17:05
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	27 september 2021 11:41
Afgemeld	Ja
Datum afgemeld	27 september 2021 12:22
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 27 september 2021 10:47

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 27 september 2021 11:40

Beste SD,
Fijn dat de telefoon weer is gevonden. Zojuist in contact met 5.1.2.e5.1.2.e gehoord dat er selective wipe was uitgevoerd door SD bij de melding vanmorgen.

De noodzakelijke stappen zijn hiermee gezet. Deze melding zal door mij worden toegevoegd aan het datalekregister, omdat de telefoon tussen vrijdag 24/9 18:00 en 27 september 11:30 uur kwijt was. Het incident wordt door het datalekteam gereed gemeld.

5.1.2.e **onzichtbaar voor aanmelder** 27 september 2021 11:31
Mevrouw belt dat ze de MT7681 heeft gevonden.

5.1.2.e **onzichtbaar voor aanmelder** 27 september 2021 10:58
@DLT: Hebben jullie nog vragen voor ons/aanmelder?

5.1.2.e **onzichtbaar voor aanmelder** 27 september 2021 10:48
Mevrouw geeft aan dat ze haar kamer telefoon MT7681 kwijt is geraakt. Het laatste moment dat mevrouw kan herinneren dat ze haar telefoon heeft gebruikt/gezien was vrijdag 24 september rond 18:00 uur.

5.1.2.e **onzichtbaar voor aanmelder** 27 september 2021 10:47
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	27 september 2021 10:35		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	01:06	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	01:06		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	01:06		
Contractnummer	Datalekken		
Dienst	Datalekken		
Korte omschrijving	Datalekken		
Dienstenniveau	Storingsafhandeling		
SLA-doorlooptijd	16 uur		
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald		
Servicewindow	Service window		

Datalekken

Datalekken

Datum constatering	27 september 2021 11:38
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Geen melding aan AP, telefoon is teruggevonden. Bij melding selective wipe uitgevoerd
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Geen melding aan betrokkenen, telefoon is teruggevonden. Bij melding selective wipe uitgevoerd
Mogelijke consequenties	minimaal
Getroffen maatregelen	Bij melding selective wipe uitgevoerd
Beschrijving inbreuk	Telefoon enkele dagen kwijt. Inmiddels telefoon weer teruggevonden

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 1413 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.e
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GroenLinks
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL1922
Soort	Tablet
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	4 oktober 2021 16:00
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	29 september 2021 11:35
Afgemeld	Ja
Datum afgemeld	30 september 2021 11:29
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 28 september 2021 22:45

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als 5.1.2.i incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Gebruiker is de Ipad verloren, 24 september te leiden.

Kan dit terugzien in de Iphone. Kan nu geen contact meer maken met het apparaat.

Telefoonnummer: 5.1.2.e

Actie

5.1.2.e Mailimport 30 september 2021 8:15

Date sent: Sep 29, 2021 4:32 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2109 1413 Aanmelden datalek

Bij dezen het formulier.

Groet,

5.1.2.e
5.1.2.e

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: dinsdag 28 september 2021 22:45
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Onderwerp: I2109 1413 Aanmelden datalek

Geachte mevrouw 5.1.2.e

Dank voor het melden van een Datalek.

Bij deze e-mail is een formulier gevoegd waarop alle informatie ingevuld kan worden die betrekking heeft op het Datalek.
Wij verzoeken u vriendelijk het formulier in te vullen en te retourneren naar de ServiceDesk, waarna het in behandeling kan worden genomen door het Datalekteam.
Dit team zal u informeren over de voortgang en de afhandeling.

Indien u nog vragen of opmerkingen heeft, kunt u contact opnemen met de Servicedesk (5.1.2.i). Dit kan telefonisch of middels het beantwoorden van deze e-mail.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 29 september 2021 10:28

Excuses, ik heb de melding verkeerd gelezen.
5.1.2.e heeft zojuist telefonisch toegelicht dat het om een vermissing ipad gaat.
SD heeft full wipe uitgevoerd. Hier zijn de noodzakelijke acties uitgevoerd. Ik zal de melding gereedmelden en toevoegen aan het datalekregister.

5.1.2.e **onzichtbaar voor aanmelder** 29 september 2021 10:20

@Datalekteam: Antwoorden op de onderstaande vragen
1. Aanmelder heeft de iPad verloren, wachtwoorden hebben hier niks mee te maken.
2. Zie punt 1.
3. Standaard procedure bij een verloren apparaat vereist een selective wipe. Full wipe kan na overleg met aanmelder. Aanmelder heeft gekozen voor full wipe.

5.1.2.e 29 september 2021 8:50

@SD - De context van dit potentieel datalek is onduidelijk. Graag antwoord op onderstaande vragen:
1. Klopt het dat gebruiker geen toegang had tot Ipad en dat de SD niet kon helpen het ww te resetten, omdat SD geen toegang kreeg tot Ipad?
2. Heeft SD inmiddels wel toegang gekregen tot de Ipad en het probleem voor gebruiker verholpen?
3. Wat is de reden van de wipe?

Graag jullie antwoorden

5.1.2.e **onzichtbaar voor aanmelder** 29 september 2021 1:44
@Datalekteam: Deze melding is per de SO naar jullie doorgezet

5.1.2.e **onzichtbaar voor aanmelder** 29 september 2021 1:40
Succesvol ingelogd op MDM-server:
Last connection 9/24/21 5:14:55 pm
Wipe was requested at 9/29/21 1:35:57 am

5.1.2.e **onzichtbaar voor aanmelder** 28 september 2021 23:11
Ik kan persoonlijk niet in het .loc account ivbm een verlopen wachtwoord. Aanwezige collega kan het ook niet oppakken, stuit op een zwart scherm in de beheerserver.

Op dit moment even wachten op de nachtdienst of we dit verder op kunnen pakken.

Verder nog de escalatieprocedure nageslagen op securitymeldingen. Verwijst terug naar de SO. Onduidelijk of een escalatie op dit moment nodig is uit het document.

Eerst kijken of de stappen in de SO verder opgepakt kunnen worden.

5.1.2.e **onzichtbaar voor aanmelder** 28 september 2021 23:09
- Gaat om een Ipad die de gebruiker vanuit Da heeft gekregen (2 jaar geleden)
- Zou deze vorige week inleveren was niet gelukt.
- Ipad is niet online geweest volgens de Iphone van de gebruiker
- Zou graag een full wipe willen.

- Hoeft geen extra wijziging voor aangemaakt worden heeft al een lopende wijziging voor een vervangende Ipad lopen

5.1.2.e **onzichtbaar voor aanmelder** 28 september 2021 22:45
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	28 september 2021 22:38		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	03:05	Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	03:05		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	03:05		
Contractnummer	Datalekken		
Dienst	Datalekken		
Korte omschrijving	Datalekken		
Dienstenniveau	Storingsafhandeling		
SLA-doorlooptijd	36 uur		
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald		
Servicewindow	Service window		

Datalekken

Datalekken

Datum constatering	24 september 2021 11:33
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Niet gemeld. SD heeft de noodzakelijke stappen, zoals full wipe uitgevoer
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Niet gemeld aan mogelijke betrokkene. SD heeft de noodzakelijke stappen gezet
Mogelijke consequenties	Onbevoegde toegang tot Tweede Kamer werkplek
Getroffen maatregelen	Na melding is direct full wipe uitgevoerd op Ipad
Beschrijving inbreuk	Ipad is verloren.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2109 1480 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
E-mail	5.1.2.e tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2342
Soort	Tablet
Vestiging	Overig

Planning

Impact	VIP
Urgentie	2. Kan niet verder
Prioriteit	2 Hoog
SLA-streefdatum	30 september 2021 12:30
Doorlooptijd	4 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	13 oktober 2021 15:22
Afgemeld	Ja
Datum afgemeld	14 oktober 2021 11:33
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 29 september 2021 20:43

Mevr. belt voor meneer 5.1.2.e

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 13 oktober 2021 15:22

Incident wordt hierbij gereed gemeld omdat IPad weer is gevonden.

5.1.2.e **onzichtbaar voor aanmelder** — 30 september 2021 10:14

Dhr. 5.1.2.e belt en meldt dat de heer 5.1.2.e zijn iPad weer heeft gevonden.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 29 september 2021 20:45

@ Datalekteam

Aanmelder belt, Kamerlid meneer de 5.1.2.e Romke is niet beschikbaar (formatieoverleg),
- Heeft waarschijnlijk zijn iPad in de plenaire zaal laten liggen, maar wil voor de zekerheid de iPad laten blokkeren.
Het nummer waarmee mevr. belt 5.1.2.e is inderdaad het nummer 5.1.2.e
Beleidsmedewerker D66

Aanmelder geeft na voorlichting voorkeur voor selective wipe (is voldoende zegt mevr.)
betreft TABL2342
Serienummer 5.1.2.h + 5.1.2.i
MAC-adres 5.1.2.h + 5.1.2.i

Apparaat is voor het laatst online geweest:
Last access 9/27/21 10:21:50 am
inactivity days 2 days

De Wipe uitgevoerd, Device is nu unmanaged vanaf:
Selective Wipe of Device Selective wipe was done at 9/29/21 8:52:08 pm.

TO DO:
De uitvraag betreffende vergrendeling moet worden gedaan met de heer 5.1.2.e
Dat zal de servicedesk volgaarne doen, ik zet toch de melding nu al door naar Datalekteam opdat jullie voor zo ver zijn ingelicht.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 29 september 2021 20:43

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer

is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	29 september 2021 20:40		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	92:22	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	92:22		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	92:22		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	4 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 0123 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Partij voor de Dieren

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT8536
Soort	Mobiel telefoontoestel
Vestiging	Domeinen Roerende Zaken

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	8 oktober 2021 16:00
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Servicedesk
Behandelaarsgroep	Servicedesk
Status	In behandeling
Gereed	Ja
Datum gereed	5 oktober 2021 9:32
Afgemeld	Ja
Datum afgemeld	5 oktober 2021 9:32
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 4 oktober 2021 21:36

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 13 oktober 2021 15:21

Omdat telefoon is teruggevonden geen nadere vragen van datalekteam.

5.1.2.e **onzichtbaar voor aanmelder** — 5 oktober 2021 9:29

Toestel is gevonden.
Was misplaatst.

5.1.2.e **onzichtbaar voor aanmelder** 5 oktober 2021 8:55
@Datalekteam: Laat weten of jullie nog verdere vragen hebben.

5.1.2.e **onzichtbaar voor aanmelder** 4 oktober 2021 21:50
- Apple 5.1.2.e
- Geen makkelijk te raden code
- Had andere apparaten niet gekoppeld, moet ngo gecheckt worden
- Full wipe

- Heeft een vervangend apparaat nodig.
- Waarschijnlijk tijdens de tramreis verloren of ontvreemd. Heeft het toestel nu niet meer in bezit.

5.1.2.e **onzichtbaar voor aanmelder** 4 oktober 2021 21:36
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	4 oktober 2021 21:35		Potentieel datalek
Gerealiseerde doorlooptijd	01:02	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	01:02		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	01:02		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 0482 Melding datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Sociaal en Financieel
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Melding datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	18 oktober 2021 17:30
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	13 oktober 2021 15:20
Afgemeld	Ja
Datum afgemeld	13 oktober 2021 16:13
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 12 oktober 2021 13:25

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 12 oktober 2021 12:16

Date sent: Oct 12, 2021 11:20 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Formulier melding datalek

Geachte collega's,

Mogelijk is er sprake van een datalek bij de cie VWS. Kunnen jullie mij het meldformulier doen

toekomen?

Met vriendelijke groet,
5.1.2.e
plaatsvervangend griffier
GC Sociaal en Financieel
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e 13 oktober 2021 15:20
Verder informatie over deze datalekmelding is te vinden onder nummer I21200482.

Deze melding wordt daarom gereed gemeld.

5.1.2.e **onzichtbaar voor aanmelder** 12 oktober 2021 13:26
Formulier is doorgestuurd.
Gebruiker heeft niet aangegeven wat voor datalek het is.
Wachten op reactie,

5.1.2.e **onzichtbaar voor aanmelder** 12 oktober 2021 13:25
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https://5.1.2.h + 5.1.2.i;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i?

- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	12 oktober 2021 12:16		Potentieel datalek
Gerealiseerde doorlooptijd	12:34	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	07:14		
Aangepaste doorlooptijd	05:20		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	05:20		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Melding aan AP ja/nee	Nee
Melding aan betrokkenen ja/nee	Nee

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 0582 Mogelijk datalek VWS

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Sociaal en Financieel
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Mogelijk datalek VWS
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	19 oktober 2021 12:36
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	13 oktober 2021 15:18
Afgemeld	Ja
Datum afgemeld	14 oktober 2021 11:40
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 13 oktober 2021 14:37

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — Mailimport 13 oktober 2021 14:36

Date sent: Oct 13, 2021 9:39 AM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Ingevuld formulier datalek VWS

Geachte collega's,

Hierbij een ingevuld meldingsformulier (mogelijk) datalek.

Met vriendelijke groet,
5.1.2.e
plaatsvervangend griffier
GC Sociaal en Financieel
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e@tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e 13 oktober 2021 15:18
Ik heb telefonisch reeds contact gehad over dit datalek met de griffier en adjunct-griffier van VWS. Tevens contact gehad met 5.1.2.e
Het betreft hier een datalek mbt medische gegevens namelijk de mentale gesteldheid van betrokkene. Dit zijn bijzondere persoonsgegevens waarvan de AVG aangeeft dat bijzondere persoonsgegevens niet verwerkt mogen worden tenzij ....
Bovendien zijn deze persoonsgegevens onbedoeld gepubliceerd, terwijl betrokkene expliciet had gevraagd de gegevens alleen met de Kamerleden te delen.
Wat daarnaast meespeelt is dat betrokkene als burger een brief heeft gestuurd naar de commissie VWS die voor een rondetafelgesprek gebruikt wordt als position paper. Griffie Plenair zal met de AVG-contactpersonen van de griffies commissies bespreken hoe de Tweede Kamer in rondetafelgesprekken om wil gaan met toegestuurde burgerbrieven. Tot nu toe werden position papers van organisaties betrokken en geen burgerbrieven met uitgebreide onderliggende persoonlijke problematiek, zoals gezondheidssituatie.

De griffier van commissie VWS heeft telefonisch contact gehad met betrokkene en hem geïnformeerd dat de informatie onbedoeld toch is gepubliceerd gedurende een korte periode en hiervoor zijn excuses aangeboden.

Het datalekteam onderneemt geen verdere acties. Wel is afgesproken dat de privacy officer geïnformeerd wordt over de afspraken die griffie plenair met griffie commissie maakt over het wel/niet betrekken van burgerbrieven bij rondetafelgesprekken, en waar nodig de privacy officer wordt betrokken.

Dit datalek wordt toegevoegd aan het datalekregister en hierbij tevens gereed gemeld.

5.1.2.e **onzichtbaar voor aanmelder** 13 oktober 2021 14:38
@Datalekteam:
Bijgevoegd formulier is ons toegestuurd. Graag jullie aandacht voor de mogelijke datalek.

5.1.2.e **onzichtbaar voor aanmelder** 13 oktober 2021 14:37
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.

- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	13 oktober 2021 14:36		Potentieel datalek
Gerealiseerde doorlooptijd	00:42	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:42		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:42		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	13 oktober 2021 14:36
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Datalek
Getroffen maatregelen	Contact gehad met betrokkene en geïnformeerd dat de informatie onbedoeld is gepubliceerd
Beschrijving inbreuk	Document met persoonsgegevens is openbaar te vinden geweest op de website van TK,

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 0956 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Internationaal en Ruimtelijk
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	29 oktober 2021 12:33
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	26 oktober 2021 15:06
Afgemeld	Ja
Datum afgemeld	26 oktober 2021 15:39
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 25 oktober 2021 15:04

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e — Mailimport 25 oktober 2021 14:33

Date sent: Oct 25, 2021 2:33 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: potentieel datalek

Beste 5.1.2.i

Na telefonisch contact met jullie het verkeerd verzonden bericht (zie bijlage) ingetrokken. Dit is in een aantal gevallen gelukt, maar niet bij iedereen. Graag jullie verdere advies.

Met vriendelijke groet,

5.1.2.e

Senningen overleg - werkgroep SENN/Foot - Aanbevelingen Benelux parlement

Actie

5.1.2.e 26 oktober 2021 15:06
Zojuist telefonisch contact gehad met 5.1.2.e
Afgesproken dat het datalek wordt toegevoegd aan het datalekregister, maar dat er verder geen melding bij AP of betrokkenen hoeft te worden gedaan.

Incident kan wordt hierbij gereedgemeld.

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 15:05
@Datalekteam: Zijn er nog verdere acties die aanmelder/SD dient te ondernemen in dit geval?

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 15:05
Gelinked aan I2110 0954. Mail is naar een verkeerde mailbox gestuurd. Aanmelder heeft de mail deels succesvol kunnen intrekken (en heeft een mail gestuurd met het verzoek aan de mensen die de mail al hadden geopend).

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 15:04
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	25 oktober 2021 14:33		Potentieel datalek
Gerealiseerde doorlooptijd	10:03	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	10:03		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	10:03		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	25 oktober 2021 14:33
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Potentieel datalek
Getroffen maatregelen	Aanmelder heeft mail deels kunnen intrekken
Beschrijving inbreuk	Mail naar een verkeerde mailbox gestuurd.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 0970 Potentieel datalek

5.1.2.e 5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Facilitaire Dienst
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT8440
Soort	Mobiel telefoontoestel
Voorraad	ServiceDesk

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	29 oktober 2021 15:23
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 25 oktober 2021 17:25

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 10 november 2021 14:17

Telefoon is teruggevonden.
Is er door SD onderzocht of er tussen moment van verlies en terugontvangen van de telefoon (onbevoegde) toegang is geweest?
Graag jullie reactie.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 11:43
In overleg met 5.1.2.e kamermail teruggezet en de melding weer op datalek team gezet

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 11:30
De telefoon is teruggevonden

5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 11:15
graag behandelen als datalek.

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:22
5.1.2.e gebeld en mevrouw gevraagd of toestel vergrendeld was , ze geeft aan dat het toestel op dat moment nog niet was vergrendeld en op die manier kon ze appen met collega's.
Daarna is het toestel wel in de vergrendeling geraakt, dus mevrouw kon daarna niet meer in de telefoon.
mevrouw gaf aan dat er verder geen ontgrendel pincode of wachtwoord was gevonden.

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:18
I2110 0972

Belde nog naar de bereikbaarheidsdienst om de reactie op de melding warm over te dragen.

Wilt graag nog antwoorden op de vragen die hieronder zijn gesteld.

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:10
Password reset uitgevoerd op 5.1.2.h + 5.1.2.i

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:01
Beste servicedesk,
Hier hebben wij wel een aantal vragen over. Betreft het een TK toestel? Zsm password reset uitvoeren. Wij willen exact weten hoe het mogelijk is dat een onbekend persoon toegang heeft gekregen tot het toetstel? Er is toegang verkregen dus per definitie datalek. Wij willen ook weten welke TK informatie er op het toestel stond.

Groet,
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:56
Zie W2110 599 - Telefonie - Verlies mobiel toestel wijziging

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:36
@Security, kunnen jullie dit verder behandelen?

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:31
Dit is gemeld door 5.1.2.e

Genoemde MT (MT8440) is verloren door de Aanmelder en gevonden door een onbekend persoon.
De onbekende persoon heeft via de Whatsapp laten weten dat het mobiele toestel is gevonden, en dat het toestel morgen om 8:30 opgehaald kan worden bij de Fietsenstalling van Den Haag Centraal Station. Er is contact geweest met de persoon die het toestel gevonden heeft. Een andere FD collega (5.1.2.e) heeft gebeld met het telefoonnummer die de onbekende persoon heeft achtergelaten in de Whatsapp.

Mogelijk kan deze onbekende persoon wel in het toestel omdat de toegangscode mogelijk is opgeschreven.

In overleg met C-RoI is er een Selective Wipe uitgevoerd op dit mobiele apparaat. Dhr. 5.1.2.e meldt dat het apparaat zowel Zakelijk als Privé gebruikt wordt door de Aanmelder en hierdoor is een Full Wipe niet wenselijk.

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:25
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:

Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:// 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

MT8440

Informatie

Aanmelddatum	25 oktober 2021 17:23		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	25 oktober 2021 17:25
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend persoon heeft toegang gekregen tot het toestel.
Getroffen maatregelen	Selective Wipe uitgevoerd
Beschrijving inbreuk	Verlies telefoon.

Overige Opmerkingen

5.1.2.e 21 juli 2022 12:17

Genoemde MT (MT8440) is verloren door de Aanmelder en gevonden door een onbekend persoon.
De onbekende persoon heeft via de Whatsapp laten weten dat het mobiele toestel is gevonden, en dat het toestel morgen om 8:30 opgehaald kan worden bij de Fietsenstalling van Den Haag Centraal Station. Er is contact geweest met de persoon die het toestel gevonden heeft. Een andere FD collega (5.1.2.e) heeft gebeld met het telefoonnummer die de onbekende persoon heeft achtergelaten in de Whatsapp.

Mogelijk kan deze onbekende persoon wel in het toestel omdat de toegangscode mogelijk is opgeschreven.

In overleg met C-RoI is er een Selective Wipe uitgevoerd op dit mobiele apparaat. Dhr. 5.1.2.e meldt dat het apparaat zowel Zakelijk als Privé gebruikt wordt door de Aanmelder en hierdoor is een Full Wipe niet wenselijk.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 0971 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Sociaal en Financieel
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7713
Soort	Mobiel telefoontoestel
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	29 oktober 2021 15:46
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	10 november 2021 14:14
Afgemeld	Ja
Datum afgemeld	10 november 2021 15:32
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 25 oktober 2021 17:47

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
   a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
   b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
   c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 10 november 2021 14:14

SD heeft de noodzakelijke stappen uitgevoerd, full wipe en wachtwoordreset.
Geen verdere acties noodzakelijk. Datalekteam meldt het incident gereed.

5.1.2.e Mailimport 29 oktober 2021 14:33

Date sent: Oct 29, 2021 1:44 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: Re: I2110 0971 Potentieel datalek

Dag collega's,

Foto's, waaronder enkele waar collega's opstaan. Verder whatsappgeschiedenis, sms'jes en documenten. Van die laatste misschien een paar stafnotitie, verder alleen openbaar toegankelijke documenten.

Groet,

5.1.2.e

Verstuurd vanaf mijn iPad

> Op 29 okt. 2021 om 11:24 5.1.2.i <5.1.2.i @tweedekamer.nl> het volgende geschreven:
>
> Geachte heer 5.1.2.e
>
> Hierbij willen wij u informeren over de status van uw incident beschreven in het onderwerp van deze e-mail.
>
> Graag vernemen wij welke informatie er op het verloren toestel stonden.
>
> Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.
>
> Met vriendelijke groet,
>
> Servicedesk
> Dienst Automatisering
> Tweede Kamer der Staten-Generaal
> Postbus 20018, 2500 EA Den Haag
> T +(31)70-318 5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 29 oktober 2021 11:25

@Datalekteam: Ik snap niet waarom dit niet direct bij jullie is geplaatst, maar bij deze. Als jullie nog vragen hebben, horen we dit graag.

5.1.2.e **onzichtbaar voor aanmelder** 29 oktober 2021 11:24

Mail gestuurd met verzoek ST.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 18:11

Voor het sluiten van deze wijziging moet het oude toestel van 5.1.2.h + 5.1.2.i uit MDM worden verwijderd (dit wordt niet gedaan vanuit de wissel wijziging)

5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 11:16

Weten jullie al wat voor gegevens er op het toestel stonden?

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 9:30

WW-reset wordt nu uitgevoerd aan de balie I2110 0993
Wachtwoordreset

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 9:19

Nummer gekoppeld aan nieuwe simkaart in:
5.1.1.e Potentieel datalek
oude SIM: 5.1.2.h + 5.1.2.i
nieuw SIM: 5.1.2.h + 5.1.2.i

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:26

Geachte heer 5.1.2.e

We hebben het verlies van uw telefoon aangemeld bij de security team en tevens een full wipe uitgevoerd op uw toestel. Op verzoek van de security team hebben wij uw tweedekamer account

wachtwoord gereset, hiervoor kunt contact opnemen met 5.1.2.i voor het aanpassen van uw wachtwoord.

Tevens wilt de security team weten wat voor gegevens er op uw toestel stonden?

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:06
Full Wipe geinitieerd op MT7713 (SN: R58M96B0NCF)

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 18:04
Wachtwoord is gereset en full wipe uitgevoerd

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:58
Beste servicedesk,
Graag een full wipe uitvoeren. Verder een password reset uitvoeren. Wij willen wel graag weten welke info er op het toestel stond. Ticket kan na deze acties worden doorgezet naar het datalek team.

Groet,
5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:55
W2110 598
Telefonie - Verlies mobiel toestel aangemaakt

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:54
Selective Wipe uitgevoerd op aanvraag van dhr. 5.1.2.e

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:49
Meneer geeft aan de telefoon de trein te hebben laten liggen. Meneer krijgt direct voicemail zodra hij het nummer belt.

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:48
@Security, kunnen jullie dit verder behandelen?

5.1.2.e **onzichtbaar voor aanmelder** 25 oktober 2021 17:47
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.

- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	25 oktober 2021 17:46		Potentieel datalek
Gerealiseerde doorlooptijd	110:28	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	110:28		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	110:28		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	25 oktober 2021 17:46
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Potentieel datalek
Getroffen maatregelen	Full wipe en wachtwoordreset
Beschrijving inbreuk	Telefoon verloren in trein

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 1035 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2111
Soort	Tablet
Vestiging	Domeinen Roerende Zaken

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	28 oktober 2021 12:27
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	27 oktober 2021 11:49
Afgemeld	Ja
Datum afgemeld	27 oktober 2021 12:10
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 26 oktober 2021 15:29

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 27 oktober 2021 11:49

Vergrendelde Ipad is onbeheerd achtergelaten in vergaderzaal en gevonden door medewerker FD. SD heeft Password reset uitgevoerd.
Eigenaar komt de Ipad ophalen bij de SD.
Vanuit datalekteam geen actie nodig. Datalekteam meld het incident gereed.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 17:04
mevr. had met 5.1.2.e gebeld, ik heb de telefoon overgenomen en mevr. over de status voorgelicht. Mevr. komt ipad straks tussen de bedrijven door ophalen

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 15:37
Nagevraagd bij 5.1.2.e of mevr. in vergadering is, ik stuur nu een mail aan gebruiker

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 15:29
Gebruiker proberen te bellen GGG

In telefonisch overleg met Ian en 5.1.2.e voeren we direct een Password reset uit
Wis is vooralsnog niet nodig

Collega van FD lever een gevonden iPad uit de 5.1.2.e zaal in.
Deze is niet ontgrendeld en blijkt van gekoppelde gebruiker te zijn

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 26 oktober 2021 15:29
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:// 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	26 oktober 2021 15:27		Potentieel datalek
Gerealiseerde doorlooptijd	05:52	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Datalekteam
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	05:52		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	05:52		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	26 oktober 2021 15:27
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Potentieel datalek
Getroffen maatregelen	SD heeft Password reset uitgevoerd
Beschrijving inbreuk	Ipad gevonden in vergaderzaal TK

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2110 1207 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
E-mail	5.1.2.e tweedekamer.nl
Afdeling	PVV
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	2 november 2021 14:13
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 29 oktober 2021 17:15

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 24 november 2021 17:53

De SD heeft géén middelen om gewonnen toegang tot het apparaat na te gaan. De SD kan wel controleren of er data verkeer is geweest na het verlies.
Verder is de "Selective wipe" uitgevoerd door de SD'er van dienst, en niet de aanmelder.

5.1.2.e 10 november 2021 14:11

Betrokkene heeft inmiddels nieuwe Iphone gekregen. Op het verloren toestel is direct na de melding van verlies door betrokkene een selective wipe uitgevoerd.

Vraag van het datalekteam aan de SD: is er na de melding van verlies van de telefoon onderzocht of er onbevoegde toegang is geweest tot de informatie op de telefoon? Graag jullie antwoord.

5.1.2.e **onzichtbaar voor aanmelder** 1 november 2021 16:25
Wijziging W2111 031 Telefonie - Verlies mobiel toestel gestart.

5.1.2.e **onzichtbaar voor aanmelder** 1 november 2021 16:18
Meneer heeft terug gebeld en gemeld dat de telefoon niet meer te traceren is. De telefoon was via zijn iPad te traceren. Meneer zag dat de iPhone richting Rotterdam ging en vervolgens in het centrum van Rotterdam zijn verbinding verloor. De telefoon is nu echt verloren.

5.1.2.e **onzichtbaar voor aanmelder** 29 oktober 2021 18:02
We weten inmiddels van zijn persoonlijke medewerker dat Toestel op station Roosendaal is (via vind mijn iPhone).
We hebben met NS klantenservice gebeld en die geven aan dat het toestel nog niet bij gevonden voorwerpen ligt.

5.1.2.e **onzichtbaar voor aanmelder** 29 oktober 2021 17:24
@Datalekteam: **Selective wipe** is uitgevoerd.
We kunnen meneer nog steeds niet telefonisch bereiken, we hebben wel een mail gestuurd en verzocht om ons te bellen en ook om NS te bellen en vragen of zijn toestel bij gevonden voorwerpen is terecht gekomen.
Tot nu toe geen reactie.

5.1.2.e Mailimport 29 oktober 2021 17:15
Date sent: Oct 29, 2021 4:00 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: I2110 1207 Spoed; Mobiele telefoon blokkeren svp

LS,

Ik kom er net achter dat ik mijn mobieltje in de trein heb laten liggen.
Kunt u hem blokkeren svp? 5.1.2.e

Thx,
5.1.2.e 5.1.2.e

Sent from my iPad

5.1.2.e **onzichtbaar voor aanmelder** 29 oktober 2021 17:15
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden

gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	29 oktober 2021 17:13		Potentieel datalek
Gerealiseerde doorlooptijd	00:00	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	29 oktober 2021 17:15
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend.
Getroffen maatregelen	Selective wipe is uitgevoerd.
Beschrijving inbreuk	Mobiele telefoon verloren.

Overige Opmerkingen

5.1.2.e 21 juli 2022 12:12

Betrokkene heeft inmiddels nieuwe Iphone gekregen.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2111 0307 Telefoon kwijt

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Dienst Analyse en Onderzoek
Locatie (Aanmelder)	Thuiswerkplek

Details

Korte omschrijving	Telefoon kwijt
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	MT7395
Soort	Mobiel telefoontoestel
Vestiging	Domeinen Roerende Zaken

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	11 november 2021 16:11
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	10 november 2021 13:28
Afgemeld	Ja
Datum afgemeld	10 november 2021 13:28
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 8 november 2021 8:41

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** — 10 november 2021 13:34

Telefoon staat op de planning van wisselproject om gewisseld te worden voor een exemplaar dat Lookout kan draaien

5.1.2.e 9 november 2021 13:20
SD heeft noodzakelijke acties uitgevoerd, zie hieronder.
Geen verdere acties nodig vanuit het datalekteam.
Advies om nieuwe telefoon uit te geven, zodat Lookout kan worden geïnstalleerd.

Datalek incident wordt toegevoegd aan het datalekregister en bij deze gereedgemeld.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 10:56
lookout for work is niet op de telefoon van meneer te installeren (het is al bekend dat dit komt door het verouderde model)
Nadat Datalekteam het incident op gereed heeft gezet, kan dit incident door de SD worden gesloten

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 10:49
In overleg met 5.1.2.e kunnen we de telefoon teruggeven aan de gebruiker (dat is nu gebeurd), de batterij was overigens ook helemaal leeg

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 10:42
Samen met 5.1.2.e gebeld: Uitgelezen in Vodafone portaal, laatste verbruik is op donderdag geweest.
Telefoon is ingeleverd door collega van FD, lag in een zaal in de kamer

5.1.2.e **onzichtbaar voor aanmelder** 8 november 2021 8:56
@Datalekteam: Aanmelder is te bereiken op 5.1.2.e en per mail voor eventuele verdere vragen. Hij gaat eerst rondbellen om te kijken of iemand zijn telefoon gevonden heeft, daarna laat hij een politierapport opstellen (mits deze niet door de beveiliging hier, het restaurantpersoneel of zijn vrienden is gevonden).

5.1.2.e **onzichtbaar voor aanmelder** 8 november 2021 8:53
1. Full Wipe is uitgevoerd voor MT7395.

5.1.2.e **onzichtbaar voor aanmelder** 8 november 2021 8:49
1. Ontgrendelcode is ingewikkeld.
2. Full wipe is gewenst
3. Aanmelder wenst vervangend apparaat.
4. Aanmelder meldt dat hij zijn telefoon mogelijk hier in het pand heeft achtergelaten in de 5.1.2.e en anders op weg naar huis op de fiets of bij een Madame Moustache op de Theresia straat. Aanmelder heeft de telefoon sinds vrijdag 5 november voor het laatst gebruikt in de Tweede Kamer.

5.1.2.e **onzichtbaar voor aanmelder** 8 november 2021 8:41
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden

gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	8 november 2021 8:41		Potentieel datalek
Gerealiseerde doorlooptijd	23:47	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	23:47		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	23:47		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	8 november 2021 8:41
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Telefoon is gevonden en na uitgelezen in Vodafone portaal, teruggegeven aan gebruiker
Getroffen maatregelen	Full wipe
Beschrijving inbreuk	Telefoon kwijt

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2111 0347 Potentieel datalek: iPad niet terecht

Tweede Kamer

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	D66
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek: iPad niet terecht
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2073
Soort	Tablet
Vestiging	Overig

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	12 november 2021 14:41
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	9 november 2021 13:12
Afgemeld	Ja
Datum afgemeld	9 november 2021 13:22
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 8 november 2021 16:44

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 9 november 2021 13:12

Goed dat mevrouw uiteindelijk het verlies toch heeft gemeld. SD heeft alle noodzakelijke acties uitgevoerd, zoals verbruiksactiviteit nagaan. Ipad had geen MDM. Is bekend hoe dat mogelijk is?
Apparaat is in de icloud gewist. Er is niet met 100% zekerheid te zeggen of er onbevoegde toegang

tot de ipad is geweest.
De melding wordt toegevoegd aan het datalekregister. Geen nadere acties vanuit het datalekteam.
Incident wordt gereed gemeld.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 8 november 2021 16:50

Mevr. meldt dat ze haar weinig gebruikte iPad die onderop in de lade (thuis) lag.
mevr. weet niet precies wanneer ze die heeft kwijtgeraakt
in juni/juli geblokkeerd en in oktober opnieuw (vanaf de iphone)
Mevr. heeft het niet direct gemeld aangezien ze ervan overtuigd was dat ze deze iPad bijv. thuis zou kunnen terugvinden.
Mevr. zegt netjes, dat ze er zo lang over heeft gedaan omdat ze zich schuldig zou voelen en ze lang heeft gezocht om de iPad terug te vinden.
Mevr. had hem aangemeld bij de NS, RET en bij de politie. daar kon het niet worden aangegeven (aangezien mevr. geen precieze datum had)
Mevr. had wachtwoord tussendoor al gewijzigd
Mevr. aangegeven dat ze verlies altijd moet melden, dat dat ook niet geeft mocht mevr. het object toch weer terugvinden.

- De vergrendelcode was moeilijk (dus niet serieel of 5.1.2.h = 5.1.2.i)
- mevr. heeft dus tussendoor haar Wachtwoord al gewijzigd
- 5.1.2.e geeft aan dat er al tijden geen verbruiksactiviteit is geweest op het abonnement.
- We zetten nu meteen het abonnement over op een nieuwe simkaart
- Wis het apparaat op icloud gedaan, apparaat stond niet meer in MDM (daar stond alleen een iPhone op naam van mevr.

5.1.2.e heeft nieuwe SIM gekoppeld: 5.1.2.h + 5.1.2.i

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 8 november 2021 16:44

!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:// 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	8 november 2021 16:41		Potentieel datalek
Gerealiseerde doorlooptijd	06:01	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	06:01		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	06:01		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	8 november 2021 16:41
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Ipad gevonden (thuis)
Getroffen maatregelen	Wis het apparaat op icloud gedaan
Beschrijving inbreuk	Ipad kwijt

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2111 0371 Potentieel datalek

5.1.2.e 5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Man
Telefoonnummer	5.1.2.i
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CIO Office
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2308
Soort	Tablet
Configuratie ID	097001396626
Vestiging	Tweede Kamer

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	11 november 2021 9:47
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	10 november 2021 14:04
Afgemeld	Ja
Datum afgemeld	10 november 2021 15:30
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 9 november 2021 13:07

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e — 10 november 2021 14:04

Datalek heb ik 9 november telefonisch met 5.1.2.e besproken.
Geen verdere vragen vanuit het datalekteam. Het incident wordt toegevoegd aan het datalekregister.

Ik meld het datalek gereed.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 13:23
De collega' van connectivity waren:
(5.1.2.e) 5.1.2.e
5.1.2.e
en een 3e collega

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 13:19
In overleg Mevr. 5.1.2.e besloten dat de iPad terug kan, we hebben geen wachtwoordreset nodig geacht, de reden wordt aangevuld door mevr. 5.1.2.e

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 13:15
- Gebruiker is sinds de lunch kwijt, lag in de vensterbank ongeveer een half uur geleden.
- 6 cijfers niet serieel, geen geboortedatum
- Geen synchronisatie in MDM plaatsgevonden
- verbruik voor de hele dag is slechts 6 MB
- eventueel heeft iemand 2 afspraakmeldingen kunnen zien

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 13:08
iPad gevonden in de kantine door collega's van connectivity en ingeleverd bij de SD

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 9 november 2021 13:07
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https:// 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de

gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
    -> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

iPad gevonden in de kantine door collega's van connectivity en ingeleverd bij de SD

Informatie

Aanmelddatum	9 november 2021 12:47		Potentieel datalek
Gerealiseerde doorlooptijd	10:47	Geëscaleerd	Ja
		Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	10:47		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	10:47		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	9 november 2021 12:47
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Mogelijk waren er 2 afspraakmeldingen zichtbaar op de Ipad
Getroffen maatregelen	Ipad na onderzoek terug naar gebruiker
Beschrijving inbreuk	Ipad gevonden in TK gebouw

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2111 0466 Datalek: Ladeblokken

5.1.2.e

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Geslacht	Man
Telefoonnummer	5.1.2.e
Mobiel nummer	5.1.2.e
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	Stafdienst HR
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Datalek: Ladeblokken
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	16 november 2021 11:40
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Nee
Afgemeld	Nee
Geregistreerde tijd	00:00

Verzoek

5.1.2.e — 10 november 2021 14:53

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mailimport, m — Mailimport 10 november 2021 13:40

Sender: fg@tweedekamer.nl
Date sent: Nov 10, 2021 12:36 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
CC: Functionaris gegevensbescherming <fg@tweedekamer.nl>, "5.1.2.e"
<5.1.2.e @tweedekamer.nl>
Subject: FW: formulier_melding_datalek ladeblokken

Beste collega´s van de helpdesk,

Kunnen jullie een datalekmelding in topdesk zetten en hierbij bijgaand formulier bij opnemen?

Dank

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Stafdienst HR
Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA
5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl
Van: 5.1.2.e < 5.1.2.e @tweedekamer.nl>
Verzonden: dinsdag 9 november 2021 14:51
Aan: Functionaris gegevensbescherming <fg@tweedekamer.nl>
Onderwerp: formulier_melding_datalek ladeblokken

Dag 5.1.2.e

Bijgaand het gevraagde formulier. Is dit zo voldoende?

Met vriendelijke groet,
5.1.2.e
5.1.2.e
Programmabureau / Facilitaire Dienst
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(31 5.1.2.e 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Actie

5.1.2.e **onzichtbaar voor aanmelder** 10 november 2021 14:54
@Datalekteam: Op verzoek van datalekteam bij jullie geplaatst.

5.1.2.e **onzichtbaar voor aanmelder** 10 november 2021 14:53
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via
https 5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	10 november 2021 13:40		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	00:00	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	00:00		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	00:00		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt maar nog in behandeling
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	10 november 2021 13:40
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend.
Getroffen maatregelen	Ladenblokken zijn door DJI geleegd. de USB en CD zijn door TK vernietigd.
Beschrijving inbreuk	bij de verhuizing zijn spullen in ladeblokken achter gelaten.

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2111 1199 Melding datalek: DEI Europese Commissie aanpak RESsen

5.1.2.e (Tweede Kamer)

Aanmelder

Naam	5.1.2.h + 5.1.2.i 5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2.i
Geslacht	Vrouw
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	GC Bestuur en Onderwijs
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	Melding datalek: DEI Europese Commissie aanpak RESsen
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	6 december 2021 10:14
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	1 december 2021 16:09
Afgemeld	Ja
Datum afgemeld	2 december 2021 8:53
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 30 november 2021 12:32

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

5.1.2.e Mailimport 30 november 2021 12:14

Date sent: Nov 30, 2021 12:08 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: melding datalek: FW: Aan de Tweede Kamer - Commissie EU - verzoek en agenderingsinput van het DEI voor de EU jaarplanning - bijlage: klacht aan Europese Commissie

Beste collega,

Wij ontvingen deze mail in onze cie.eubox. Ik wil jullie graag wijzen op de PDF klacht DEI Europese

commissie over aanpak RESsen.
In dit documenten staan alle persoongegevens van personen. Ik zou dat willen bestempelen als een datalek (awareness naar de Werkgroep).
Pakken jullie de melding op en wijzen jullie de Werkgroep hierop?

Deze mail is niet voor EU bedoeld maar voor EZK. Kan ik dit doorsturen of moet de PDF eerst aangepast worden door de Werkgroep?
Hoe moet ik hierin handelen?

Dank voor de te nemen moeite

Met vriendelijke groet,
5.1.2.e
Commissie assistent
GC Internationaal en Ruimtelijk
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA s-Gravenhage

T +(5.1.2.e E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: Werkgroep Democratisch Energie Initiatief <5.1.2.e @outlook.com>
Verzonden: dinsdag 30 november 2021 11:12
Aan: Commissie EU <cie.eu@tweedekamer.nl>
Onderwerp: Aan de Tweede Kamer - Commissie EU - verzoek en agenderingsinput van het DEI voor de EU jaarplanning - bijlage: klacht aan Europese Commissie

Vrijdag jl schreven wij: "Is ons schrijven 22/11 in goede orde ontvangen?"

Is het mogelijk te reageren en ons een ontvangstbevestiging te zenden?
Beste groet,

5.1.2.e

5.1.2.e

Begin doorgestuurd bericht:

Van: Werkgroep Democratisch Energie Initiatief <5.1.2.i @outlook.com>
Datum: 22 november 2021 om 17:34:11 CET
Aan: cie.eu@tweedekamer.nl
Kopie: 5.1.2.e <5.1.2.e @gmail.com>, 5.1.2.e <5.1.2.e @gmail.com>
Onderwerp: Aan de Tweede Kamer - Commissie EU - verzoek en agenderingsinput van het DEI voor de EU jaarplanning - bijlage: klacht aan Europese Commissie

Aan: de Tweede Kamer der Staten-Generaal;
Kamercommissie EU

Betreft: verzoek en agenderingsinput in het kader van de EU-jaarplanning

Geachte Tweede Kamer-commissie

Omdat u besloot de behandeling van het EU jaarplan te gaan starten sturen wij u bijgaande informatie over de niet-toepassing van het EU-recht in Nederland.

Het categorisch niet toepassen van de EU-verdragsartikelen (bv Unietrouw), EU-richtlijnen en regelgeving erodeert onze democratische rechtsstaat.

Wij stellen u voor dit onderwerp in uw jaarplanning te agenderen, daarover informatie te verzamelen om te komen tot herstel van het Europees recht in onze rechtsstaat.

Wij leveren alvast input daarvoor aan middels onderstaande korte nota. De bijlagen erbij geven u extra informatie hoe ernstig de situatie is. Reden voor onze klachten aan de Europese Commissie en verzoekschrift aan het EP (zie bijlagen). Maar het is uiteraard veel beter indien u als Tweede Kamer in actie komt.
U mag ons verzoek als een wake-up call zien, die mede wordt gevoed door onze praktijkwaarnemingen.
Wij zijn bereid u verdere informatie aan te leveren.

Namens het Democratisch Energie Initiatief,

5.1.2.e voorzitter
5.1.2.e

Het Europees recht in de knel.

Het Europees recht zit in Nederland in de verdrukking. We geven u in overweging het niet uitvoeren van EU richtlijnen en andere EU regelgeving te onderzoeken en te agenderen.

Bijgaande stukken illustreren de ernst van de situatie. Deze werd/wordt verergerd door de slechte oriëntatie van met name (de hoogste) Nederlandse bestuursrechters op de EU-wetgeving en de rechtspraak van het Hof van Justitie van de EU. Daardoor wordt de onwil/onmacht om de EU-wetgeving en EU-jurisprudentie toe te passen bij de Nederlandse bestuursorganen, zowel bij ministeries, provincies als gemeenten 'gehonoreerd' en versterkt.

Het probleem speelt overheid-breed, van uitvoerende tot en met rechterlijke macht.

Nota van het Democratisch Energie Initiatief

Wij kunnen veel voorbeelden geven over de deplorabele staat van kennis over en ontbrekende bereidheid om EU wetgeving toe te passen maar spitsten ons in

deze nota toe op de rechterlijke macht, ic de bestuursrechters en in het bijzonder de Raad van State.

Wij maken u in dit verband opmerkzaam op het feit dat naar ons oordeel de Raad van State enorme steken heeft laten vallen in relatie tot de tijdige en voortvarende implementatie van het Unierecht. Zonder uitputtend te willen zijn, noemen we een drietal voorbeelden.

• Hoewel deskundigen al langer vraagtekens plaatsten bij de Unierechtelijke rechtsgeldigheid van het "Programma Aanpak Stikstof" uit 2015 duurde het tot mei 2019 voordat de Raad oordeelde dat die regeling inderdaad in strijd was met het Unierecht - en dit pas na een opinie van de Advocaat-generaal van het Europese Hof van Justitie die daarover geen enkel misverstand liet bestaan.
• In de Crisis- en Herstelwet uit 2010 werd de toegang tot de rechter in geschillen over projecten die onder die wet vallen, beperkt tot personen en instanties die eerder in de (politieke) besluitvorming een zienswijze hadden ingediend. De Raad van State accepteerde jarenlang die regeling totdat het Europese Hof in een prejudicieel advies van januari 2021 oordeelde dat het in strijd met het Unierecht is om toegang tot de rechter afhankelijk te stellen van deelname aan het voorafgaande politieke proces.
• Meest recent en wellicht meest aansprekend is de gang van zaken met betrekking tot wettelijke voorschriften en normen voor windturbines, in het bijzonder in relatie tot geluid en slagschaduw. En korte chronologie.
o In 2016 oordeelde het Europese Hof dat windturbinevoorschriften van het Gewest Wallonië in strijd waren met het Unierecht omdat die voorschriften waren vastgesteld zonder voorafgaande milieueffectrapportage ("m.e.r.") zoals geëist wordt door de SMB-richtlijn van 2001.
o Direct daarna werd er in publicaties op gewezen dat die uitspraak ook van belang was voor Nederland omdat het Rijk in 2010 soortgelijke voorschriften had vastgesteld zonder voorafgaande m.e.r.
o Niettemin oordeelde de Raad van State in een uitspraak van 2019 dat er met de Nederlandse windturbinevoorschriften niets mis was omdat, zo stelde de Raad zonder overtuigende motivering, die voorschriften geen "plan" of "programma" waren in de zin van de SMB-richtlijn zodat die richtlijn niet van toepassing zou zijn.
o In de jaren daarna handhaafde de Raad van Staten dat standpunt in tal van zaken die mede daardoor door klagende burgers werden verloren.
o In juni 2021 herhaalde het Europese Hof in niet mis te verstane bewoordingen de uitspraak in de d'Oultremontzaak in een prejudicieel advies over windturbinevoorschriften van Vlaanderen. Ook in

dat advies - de Nevele zaak - oordeelde het Hof dat die voorschriften in strijd zijn met het Unierecht wegens het ontbreken van een voorafgaande m.e.r.
o Toen aan die Nevele uitspraak ook in Nederland de nodige publiciteit was gegeven, besloot de Raad van State in januari 2021 zich opnieuw en nu ten principale te buigen over de vraag of de Nederlandse windturbinevoorschriften wel of niet in overeenstemming waren met het Unierecht.
o Op 30 juni 2021 - dus ruim tien jaar na het vaststellen van die voorschriften en vijf jaar na de d'Oultremontzaak - kwam het verlossende woord: de Raad van State ging om en oordeelde dat ook de Nederlandse windturbinevoorschriften in strijd waren met het Unierecht - en dus buiten toepassing moeten blijven - wegens het ontbreken van een m.e.r. voorafgaand aan de vaststelling van die voorschriften.
o Wat onverlet laat dat in de jaren daarvoor tal van beroepschriften van burgers door de Raad werden afgewezen mede op basis van het oordeel uit 2019 dat er met de Nederlandse windturbinevoorschriften niets aan de hand was.

We voegen daar nog aan toe dat het de civiele rechter - en dus niet de Raad van State - was die in 2015 (rechtbank), 2018 (gerechtshof) en 2020 (Hoge Raad) oordeelde dat internationale verdragen de overheid verplichtten meer te doen om de CO2 uitstoot terug te dringen. Er zijn meer voorbeelden van procedures die welbewust werden voorgelegd aan de civiele rechter en niet aan de bestuursrechter/Raad van State omdat burgers (en hun advocaten) al op voorhand betwijfelden of die bestuursrechter/Raad van State hen recht zou doen.

Uit deze voorbeelden - er zijn er meer - blijkt dat de Raad van State als bestuursrechter in hoogste instantie maar al te vaak pas toepassing geeft aan het Unierecht als het niet anders kan vanwege een eerdere uitspraak van het Europese Hof.

Wij laten in het midden of die opstelling van de Raad eengevolg is van de banden die de Raad en zijn leden hebben met de uitvoerende macht en het openbaar bestuur. Feit is ook dat in een eerdere fase de Raad in de rol van adviseur van regering en parlement niet aan de bel trok met de vraag of de (voorgenomen) wettelijke regelingen die in bovenstaande voorbeelden aan de orde zijn wel in overeenstemming waren met het Unierecht. Terwijl daar, zo bleek later, goede redenen voor waren,

Ons beeld is derhalve dat de Raad van State initieel in zijn adviserende rol de neiging heeft zoveel mogelijk mee te gaan met de wensen en het beleid van de uitvoerende macht ten koste van een correcte en loyale toepassing van Europees recht volgens artikel 4, lid 3 VEU, terwijl in tweede instantiede Raad in zijn bestuursrechtelijke rol pas uitvoering geeft aan artikel 4 als het niet anders kan vanwege een uitspraak van het Europese Hof van Justitie.

Het Democratisch Energie Initiatief

5.1.2.e

Em. hoogleraar internationaal recht

Bijlagen: klacht aan EC en verzoek aan EP

Actie

5.1.2.e 1 december 2021 16:09
Dit is geen incident of melding voor het datalekteam. Het betreft een brief derden die door de betreffende commissie in behandeling moet worden genomen. Het incident wordt door mij gereed gemeld en zal niet worden toegevoegd aan het datalekregister, omdat het geen datalek is.

5.1.2.e **onzichtbaar voor aanmelder** 30 november 2021 12:33
@ DT:
kunnen jullie hier naar kijken? BvD

5.1.2.e **onzichtbaar voor aanmelder** 30 november 2021 12:33
Beste collega,

Wij ontvingen deze mail in onze cie.eubox. Ik wil jullie graag wijzen op de PDF klacht DEI Europese commissie over aanpak RESsen.
In dit documenten staan alle persoongegevens van personen. Ik zou dat willen bestempelen als een datalek (awareness naar de Werkgroep).

Pakken jullie de melding op en wijzen jullie de Werkgroep hierop?

Deze mail is niet voor EU bedoeld maar voor EZK. Kan ik dit doorsturen of moet de PDF eerst aangepast worden door de Werkgroep?
Hoe moet ik hierin handelen?

Dank voor de te nemen moeite

5.1.2.e **onzichtbaar voor aanmelder** 30 november 2021 12:32
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via 5.1.2.h + 5.1.2.i ;
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)

* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	30 november 2021 12:14		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	13:25	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	13:25		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	13:25		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	30 november 2021 12:14
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Na onderzoek, geen datalek
Getroffen maatregelen	Onbekend
Beschrijving inbreuk	PDF klacht DEI Europese commissie over aanpak RESsen in mailbox (incl. persoongegevens)

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2112 0433 Potentieel datalek

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2i
Geslacht	Vrouw
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	PvdA
Locatie (Aanmelder)	5.1.2.i

Details

Korte omschrijving	Potentieel datalek
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	TABL2379
Soort	Tablet
Vestiging	Overig

Planning

Impact	VIP
Urgentie	4. Kan verder met alternatief
Prioriteit	3 Normaal
SLA-streefdatum	14 december 2021 17:49
Doorlooptijd	16 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	24 december 2021 12:00
Afgemeld	Ja
Datum afgemeld	24 december 2021 12:53
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 5.1.2.e — 13 december 2021 11:21

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

mevr. 5.1.2.e belt namens kamerlid.

Actie

5.1.2.e — 24 december 2021 12:00

Incident wordt door datalekteam gereedgemeld.

5.1.2.e — 14 december 2021 13:51

De vraag aan datalekteam is of ww reset moet plaatsvinden. Datalekteam heeft hier (nog) geen criteria voor. Graag advies vragen aan security team of ww reset moet plaatsvinden.

5.1.2.e **onzichtbaar voor aanmelder** 13 december 2021 14:58
Serienummer, IMEI-nummer en TABL nummer opgestuurd, vanuit de 5.1.2.i mailbox.

5.1.2.e **onzichtbaar voor aanmelder** 13 december 2021 14:57
Mevr. 5.1.2.e belt. Ze hebben een iPad gevonden op het vliegfveld in Berlijn en wensen graag het Serienummer te weten om te kunnen verifiëren dat het om de iPad van aanmelder gaat.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 13 december 2021 14:31
-Full whipe ingezet

5.1.2.e **onzichtbaar voor aanmelder** 13 december 2021 14:02
5.1.2.e belt namens aanmelder. Ze geeft aan dat de scherm vergrendelcode moeilijk is om te raden. De sim ontgrendel code is wel 5.1.2.h+5.1.2.i Mevr. 5.1.2.e meldt dat een full wipe kan worden uitgevoerd. Ze hebben contact met de klantenservice van de luchthaven Berlijn.

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 13 december 2021 11:21
@Datalekteam, zien jullie reden voor een ww-reset?

mevr. 5.1.2.e belt namens kamerlid 5.1.2.e
iPad is blijven liggen op luchthaven in Berlijn.

Mevr. heeft contact opgenomen met security aldaar, ipad ligt waarschijnlijk veilig bij sec. op luchthaven Berlijn.
Zaterdag avond 11 dec. is de mail gestuurd aan mevr. 5.1.2.e
Vlucht was 6 uur s avonds afgelopen zaterdag. Er lijkt sinds dien 6.46 uur geen synchronisatie meer geweest te zijn op de ipad (zie onderstaand)

Sinds 9-12-2021 geen dataverbruik op abonnement 5.1.2.h + 5.1.2.i

- Mevr. 5.1.2.e gaat navragen bij Kamerlid 5.1.2.e
- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. ' 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)

- partiele whipe uitgevoerd, Binnendijk gaat navragen of het een full whipe moet zijn.

Knipsel.PNG

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 13 december 2021 11:21
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen 5.1.2.h + 5.1.2i ;
5.1.2.h + 5.1.2i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	13 december 2021 11:19		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	86:11	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	86:11		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	86:11		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	16 uur
Gehaald volgens dienstcontract?	Wel gebruikt en niet gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	13 december 2021 11:19
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Onbekend
Getroffen maatregelen	Full whipe ingezet
Beschrijving inbreuk	Ipad kwijtgeraakt

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

I2112 0913 iPad Kwijtgeraakt op vlucht

5.1.2.e (Tweede Kamer)

Tweede Kamer
DER STATEN-GENERAAL

Aanmelder

Naam	5.1.2.e
Vestiging	Tweede Kamer
Inlognaam netwerk	5.1.2.h + 5.1.2i
Geslacht	Man
E-mail	5.1.2.e @tweedekamer.nl
Afdeling	CDA
Locatie (Aanmelder)	5.1.2.e

Details

Korte omschrijving	iPad Kwijtgeraakt op vlucht
Soort incident	Datalek
Categorie	Datalekken
Subcategorie	Melding datalek

Object

Object ID	Nvt
Soort	Onbekend
Vestiging	Tweede Kamer
Locatie	S 400

Planning

Impact	Persoon
Urgentie	4. Kan verder met alternatief
Prioriteit	4 Laag
SLA-streefdatum	28 december 2021 12:29
Doorlooptijd	36 uur
On hold	Nee
Bewaakt	Nee

Afhandeling

Behandelaar	Datalekteam
Behandelaarsgroep	Datalekteam
Status	In behandeling
Gereed	Ja
Datum gereed	24 december 2021 11:59
Afgemeld	Ja
Datum afgemeld	3 januari 2022 12:55
Geregistreerde tijd	00:00

Verzoek

5.1.2.e 22 december 2021 14:30

Wanneer het vermoeden bestaat dat er een datalek is waarvoor de Tweede Kamer verantwoordelijk is, dan kunnen onderstaande beschrijvingen uitsluitsel geven.
Bij twijfel melding laten beoordelen door het Datalekteam.

1) Iemand is z'n persoonlijk of TK apparaat of datadrager kwijt (Denk aan een USB-stick, ipad, telefoon laptop).
a) Het verloren object wordt gebruikt voor TK exchange gegevens (email/agenda/contactpersonen) en/ of data opslag voor de Tweede kamer? Nee? => Geen Datalek
b) Het verloren object bevat persoonsgegevens (Zie einde pagina voor toelichting)? Nee? => Geen Datalek
c) In andere gevallen het incident behandelen als Datalek.
2) Iemand meldt een gevonden mobiel apparaat => IN ALLE GEVALLEN => behandelen als potentieel Datalek
3) Een leverancier of FAB meldt een potentieel Datalek in zijn organisatie: IN ALLE GEVALLEN => behandelen als potentieel Datalek
4) Iemand meldt een ander issue (bijvoorbeeld: een container met papieren personeels dossiers naast de prullenbak): IN ALLE GEVALLEN => behandelen als potentieel Datalek
5) Iemand geeft aan dat informatie van TK op publiek toegankelijke fora (dropbox, prezi, etc) staat => Meldden als security incident, pas in tweede instantie als potentieel datalek
6) Zet de melding op het datalekteamXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Actie

5.1.2.e 5.1.2.e **onzichtbaar voor aanmelder** 4 januari 2022 15:52

betrof ipad van CDA met nummer 097001737319

5.1.2.e **onzichtbaar voor aanmelder** 4 januari 2022 15:42
Aanmelder belt. Zijn iPad is gevonden door Schiphol en hij kan hem ophalen.

Lijcklama À Nijeholt, Aizo Mailimport 3 januari 2022 12:53
Date sent: 5.1.2.e 3, 2022 12:39 PM
To: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Subject: RE: I2112 0913 - Aanmelding Datalekteam

Goedemiddag,

Het is mij tijdens de drukke feestdagen volledig ontschoten om het formulier in te vullen. Bij deze alsnog in de bijlage, met excuses voor de vertraging.

Met vriendelijke groet,
5.1.2.e
Beleidsmedewerker Energie, Klimaat, Landbouw en Circulaire Economie

CDA-fractie Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
T +(5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.i <5.1.2.i @tweedekamer.nl>
Verzonden: woensdag 22 december 2021 14:39
Aan: 5.1.2.e 5.1.2.e 5.1.2.e tweedekamer.nl>
Onderwerp: I2112 0913 - Aanmelding Datalekteam

Geachte heer 5.1.2.e

Melding met nummer: I2112 0913 is aangemaakt.

Het betreft :iPad Kwijtgeraakt op vlucht

De Dienst Automatisering draagt uw melding ter verdere afhandeling over aan het Datalekteam .

Vertrouwend erop u hiermee voldoende te hebben geïnformeerd.

Indien u nog vragen heeft, kunt u contact opnemen met één van onderstaande personen:

Dhr. 5.1.2.e tst. 5.1.2.e
Mw. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst. 5.1.2.e
Dhr. 5.1.2.e tst 5.1.2.e

Met vriendelijke groet,

Servicedesk
Dienst Automatisering
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T +(5.1.2.i | E 5.1.2.i @tweedekamer.nl

5.1.2.e 24 december 2021 11:59
De noodzakelijke stappen zijn uitgevoerd door de SD, check op ontgrendelcode en PIN codes. En full wipe is uitgevoerd.
Geen nadere vragen vanuit het datalekteam. Incident wordt gereedgemeld.

5.1.2.e **onzichtbaar voor aanmelder** 22 december 2021 14:52
Betreft iPad van CDA. Geen TABL-nummer beschikbaar.

5.1.2.e **onzichtbaar voor aanmelder** 22 december 2021 14:39
@Datalekteam: Aanmelder is in contact met de luchtvaartmaatschappij en gaat nog een verzoek indienen van verlies/diefstal bij de politie.

5.1.2.e **onzichtbaar voor aanmelder** 22 december 2021 14:34
Aanmelder meldt dat hij zijn iPad is kwijtgeraakt Transavia vlucht.

Ontgrendelcodes en PIN codes zijn niet makkelijk te raden.
Aanmelder geeft aan een full wipe te willen. Deze is uitgevoerd.
Ipad is vandaag verloren. Is nog niet duidelijk of deze na verlies online is geweest.

5.1.2.e **onzichtbaar voor aanmelder** 22 december 2021 14:30
!!!!!!! <<<<< LET OP: Verwijder NOOIT een apparaat uit de MDM-omgeving!!! Dan is namelijk alle potentieel beheer niet meer mogelijk!! >>>> !!!!!!!

Acties:
Geen datalek? => Sluit de melding.
Potentieel datalek => Volg onderstaand stappenplan:

* Vermeld dat het ontvreemde mobiel apparaat door de Servicedesk "gewiped" gaat worden via MDM

Wij voeren in eerste instantie een selective wipe uit. Hierbij wordt alleen de Kamerinformatie (E-mail en Kamerapps) gewist. In overleg met de gebruiker kan tot een full wipe worden overgegaan, waarbij de hele telefoon wordt gewist (dus ook eventuele privédata). Bespreek beide opties met de gebruiker!

De MDM-server is voor de Servicedesk te bereiken via mRemote (zie bijgevoegde handleiding) en de daar te openen MDM-server via https: 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i

- Wanneer je de gebruikersnaam opzoekt op de MDM-server, verschijnen alle mobiele apparaten waarop zijn/haar MDM is geïnstalleerd. Vraag goed uit om welk toestel het gaat (Type, uitgegeven door DA of eigen apparatuur) om zo te voorkomen dat het verkeerde apparaat gewist wordt.
- Vraag voor de zekerheid ook of op het apparaat ooit e-mail van de Kamer/MDM gestaan heeft. Dit om te voorkomen dat de gebruiker enkel het verlies van een privétoestel meldt dat geen relevantie voor de Kamer heeft, maar waardoor wel per ongeluk een ander, verkeerd, toestel kan worden gewist.
- Indien je twijfelt welk apparaat het juiste is, kan je IMEI-nummers vergelijken tussen MDM en de apparaten op het grafisch overzicht van de gebruiker. Eigen apparatuur is uiteraard niet in TOPDesk te vinden (ook uit te sluiten via het vergelijken via IMEI's).

Door een IMEI-nummer (bijvoorbeeld vanuit TOPDesk) in te vullen. Let dan wel op het volgende:
o Vul altijd alleen maar de getallen in. Laat 'IMEI' weg!
o Bij Android toestellen houd je dit format aan 5.1.2.h + 5.1.2.i
5.1.2.h + 5.1.2.i
o Bij iPhones/iPads houd je dit format aan 5.1.2.h + 5.1.2.i cijer is. Let op de spaties! Zonder deze spaties, is er geen resultaat).

Vraag verder het volgende uit of controleer dit:

- Is het toestel beveiligd met een serieel code (5.1.2.h + 5.1.2.i of een met identieke cijfers (bv. '5.1.2.h + 5.1.2.i 5.1.2.h + 5.1.2.i ?
- Is het toestel beveiligd met een makkelijk te raden code (bijvoorbeeld het geboortejaar van de gebruiker)
- Is het toestel al online geweest na de ontvreemding/vermissing? (Kan SD checken)

Wij kunnen op de MDM-server wel zien of een wipe is aangezet, maar niet of deze gelukt is. Vergelijk het tijdstip van de wipe-opdracht met de datum waarop een toestel voor de laatste keer online is geweest (een ActiveSync-synchronisatie heeft gehad).

* Inventariseer of de gebruiker een vervangend apparaat nodig heeft en open hiervoor de relevante wijziging.
* Meldt de klant dat het Securityteam de melding in behandeling neemt. Zij nemen contact met de klant op.
* Vraag uit:
-> Hoe ingewikkeld is de ingestelde pincode (geen opeenvolgend cijfers? / allemaal dezelfde cijfers?)
* Beschrijf zo goed mogelijk wat er aan de hand is en welke acties er al zijn ondernomen. (in ieder geval: tijdstip van ontvreemding/kwijt raken, merk & model, wipe-acties & resultaten (maak foto van resultaat wipe-actie & koppel deze aan incident))
* Zet de melding op behandelaar Datalekteam, er wordt een mail gestuurd naar de klant waarbij

het incident wordt overgedragen aan het security team

Informatie

Aanmelddatum	22 december 2021 14:29		Potentieel datalek
		Geëscaleerd	Ja
Gerealiseerde doorlooptijd	16:30	Behandelaar (de-)escaleren	Servicedesk
Doorlooptijd 'On hold'	00:00		
Aangepaste doorlooptijd	16:30		
Doorlooptijd 'Afgerond'	00:00		
Doorlooptijd 'Uitvoering'	16:30		

Contractnummer	Datalekken
Dienst	Datalekken
Korte omschrijving	Datalekken
Dienstenniveau	Storingsafhandeling
SLA-doorlooptijd	36 uur
Gehaald volgens dienstcontract?	Wel gebruikt en gehaald
Servicewindow	Service window

Datalekken

Datalekken

Datum constatering	22 december 2021 14:29
Melding aan AP ja/nee	Nee
Waarom wel/niet melden aan AP	Onbekend
Melding aan betrokkenen ja/nee	Nee
waarom wel/niet melden aan betrokkenen	Onbekend
Mogelijke consequenties	Ipad is weer gevonden
Getroffen maatregelen	Full wipe
Beschrijving inbreuk	Ipad kwijt geraakt

Metadata

Bronnenoverzicht

CC-Connect	0.0
GGM	0.0
IDOL	0.0
SharePoint	0.0
PowerBI	0.0
CC-Connect	Nee
GGM	Nee
IDOL	Nee
SharePoint	Nee
PowerBI	Nee

Docnr129

AUTORITEIT
PERSOONSGEGEVENS

Meldloket

Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	21-12-2016 12:44:29
Uniek nummer	5.1.2.h + 5.1.2.i

Docnr130

Tweede Kamer
DER STATEN-GENERAAL

Procedure melding datalekken Tweede Kamer

Stafdienst Personeel en Organisatie
5.1.2.e

T 5.1.2.e
E 5.1.2.e @tweedekamer.nl

datum 29 maart YYYY

Procedure melding datalekken Tweede Kamer

1. Melden incident hij 5.1.2.i

Elk informatiebeveiligingsincident dat bij een medewerker van de Tweede Kamer bekend wordt, dient te worden gemeld bij 5.1.2.i Dit kan telefonisch, per mail of via het meldingsformulier op Plein 2. Niet alleen informatiebeveiligingsincidenten inzake elektronische data moeten worden gemeld. Ook incidenten met dossiers, documenten, archieven etc. moeten worden verwerkt in Topdesk.

2. Registratie 5.1.2.i

De melder wordt verzocht haar/zijn naam en contactgegevens in het formulier in te vullen naast de informatie over het incident. De 3060-medewerker registreert de incidentmelding in Topdesk en gaat na of er bij het incident persoonsgegevens betrokken zijn. Indien dit het geval is, wordt hiervan via Topdesk melding gemaakt bij de leden van het Datalek team.

3. Beoordeling Datalek team

Het Datalek team - bestaande uit de Security officer, de Beveiligingsambtenaar en de Functionaris Gegevensbescherming - beoordelen of er sprake is van een datalek dat valt onder de meldplicht van de Wbp. Vanwege het gegeven dat de Tweede Kamer binnen 72 uur behoort te melden aan de toezichthouder dient de melding direct en met de hoogste prioriteit te worden behandeld.

3a. Beoordeling: wel datalek

Indien wordt geconstateerd dat er sprake is van een meldenswaardige datalek zorgt de FG ervoor dat de DB&I zo snel mogelijk telefonisch wordt geïnformeerd. In de eerste analyse komen de volgende aspecten aan de orde: categoriseren van het datalek, de impact voor de betrokkenen inschatten, mogelijke maatregelen bespreken om de schade bij betrokkene(n) te beperken en nagaan of ook andere systemen moeten worden onderzocht.

3b. Beoordeling: geen datalek

Indien wordt geconstateerd dat het incident geen datalek is in de zin van de Wbp, wordt deze beoordeling schriftelijk teruggekoppeld aan de DB&I en verwerkt in Topdesk.

4. Advisering FG

Indien wordt geconstateerd dat het incident een datalek is in de zin van de Wbp, stuurt het Datalek team onder eindverantwoordelijkheid van de FG aanvullend een e-mail naar de DB&I met daarin een gemotiveerd advies.

5. Besluit DB&I

Op basis van het advies van het Datalek team besluit de DB&I of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens en/of de betrokkene.

5a. Besluit: wel datalek

Als de DB&I besluit dat er sprake is van een datalek dat gemeld moet worden, dan wordt dit teruggekoppeld aan het Datalek team.

5b. Besluit: geen datalek

Indien de DB&I besluit dat er geen sprake is van een datalek dat gemeld moet worden, dan wordt dit in Topdesk verwerkt en via Topdesk teruggekoppeld aan het Datalek team.

6. Melden

Als de DB&I besluit dat er sprake is van een datalek dat gemeld moet worden, stuurt de FG het meldingsformulier naar de Autoriteit Persoonsgegevens.

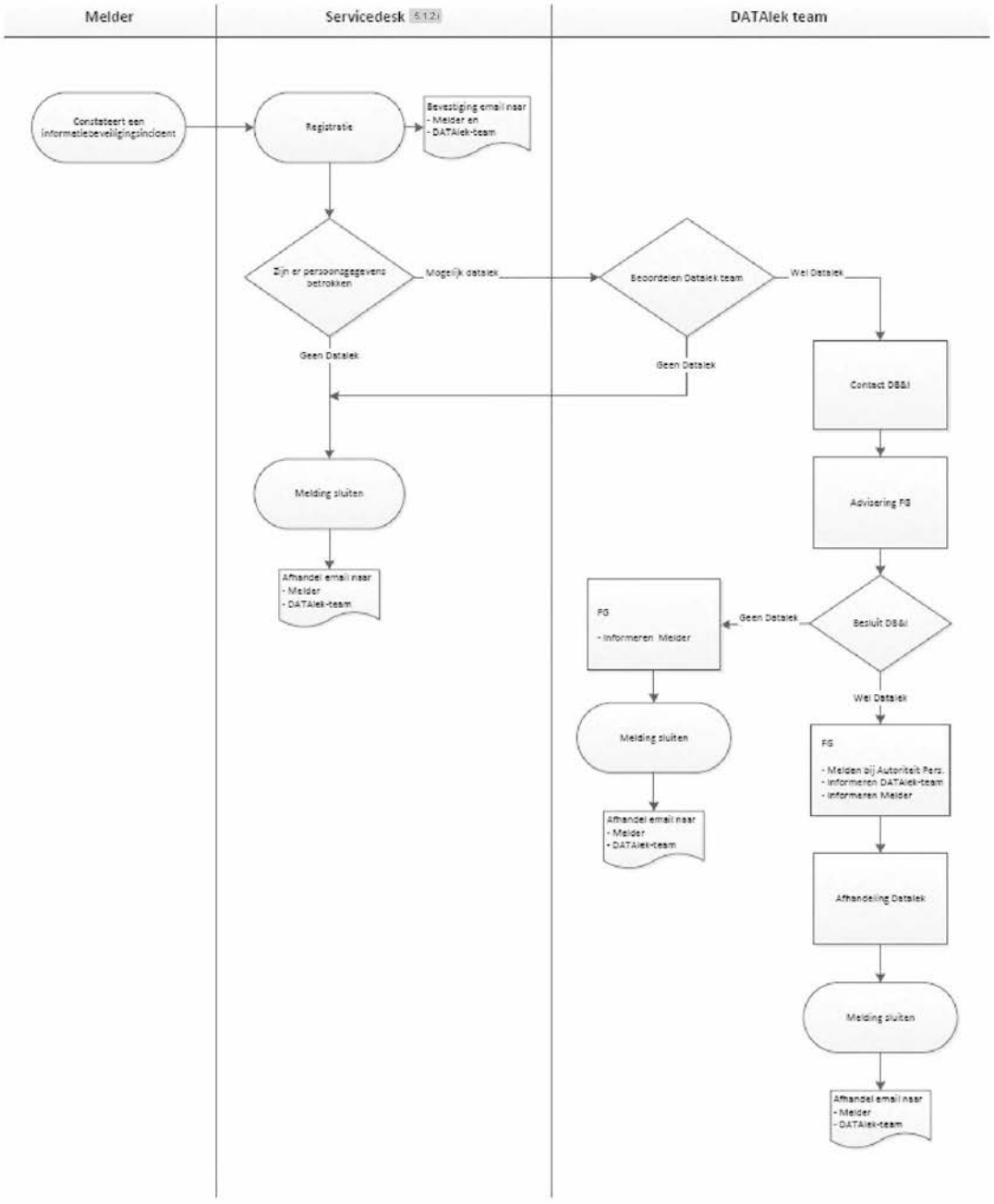
7. Afhandeling datalek

Onder verantwoordelijkheid van het Datalek team wordt de verdere afhandeling van het datalek uitgevoerd. Het gaat hierbij om het:

- veilig stellen van gegevens,
- dichten van het datalek,
- herstellen van schade,
- informeren van betrokkenen,
- inlichten van de stafdienst Communicatie voor een eventuele persverklaring,
- eventueel coördineren van een onderzoek,
- in gang zetten van structurele verbeteringen,
- het rapporteren aan het MT, en
- het evalueren van het incident.

datum 29 maart YYYY

Bijlage 1: Schematische weergave procedure melding datalekken Tweede Kamer



datum 29 maart YYYY

Bijlage 2: Beslisboom melden aan Autoriteit Persoonsgegevens

Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat alleen een inbreuk hoeft te worden gemeld als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.

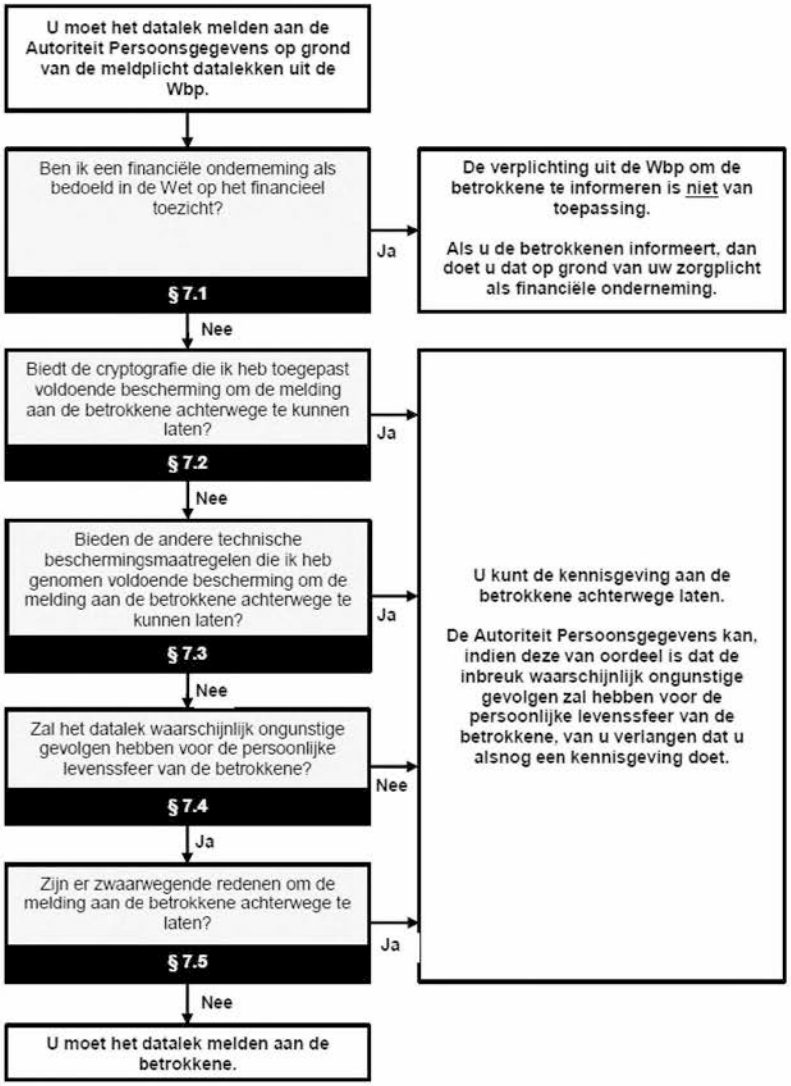
Er moet in ieder geval gemeld worden als één van de onderstaande vragen positief wordt beantwoord:

- Zijn gegevens (definitief) verloren gegaan?
- Zijn de gegevens bijzonder of zeer omvangrijk?
- Zijn de gegevens in onbevoegde handen geraakt?
- Aanmerkelijk risico voor nadelige gevolgen?

datum 29 maart YYYY

Bijlage 3: Beslisboom melden aan betrokkene

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van het datalek. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld.



Bij de vraag of er zwaarwegende redenen zijn om de melding achterwege te laten geldt dat de melding aan de betrokkene achterwege mag blijven als dit noodzakelijk is met het oog op de belangen die worden genoemd in artikel 43, onder e, Wbp.

datum 29 maart YYYY

Bijlage 4: Contactgegevens datalekteam

Functionaris Gegevensbescherming
Naam: 5.1.2.e
Tel: (5.1.2.e
Mobiel: 5.1.2.e
E-mailadres: 5.1.2.e @tweedekamer.nl

Bij afwezigheid Functionaris Gegevensbescherming
Naam: 5.1.2.e
Tel: (5.1.2.e
Mobiel: 5.1.2.e
E-mailadres: 5.1.2.e @tweedekamer.nl

Beveiligingsambtenaar
Naam: 5.1.2.e
Tel: (5.1.2.e
Mobiel: 5.1.2.e
E-mailadres: 5.1.2.e @tweedekamer.nl

Bij afwezigheid Beveiligingsambtenaar
Naam: 5.1.2.e
Tel: (5.1.2.e
Mobiel: 5.1.2.e
E-mailadres: 5.1.2.e @tweedekamer.nl

Security officer
Naam: 5.1.2.e
Tel: (5.1.2.e
Mobiel: 5.1.2.e
E-mailadres: 5.1.2.e @tweedekamer.nl

Bij afwezigheid Security officer
Naam: 5.1.2.e
Tel: (5.1.2.e
Mobiel: 5.1.2.e
E-mailadres: 5.1.2.e @tweedekamer.nl

Docnr131

Omschrijving incident	2020	2021
Verloren/gestolen/gevonden gegevensdrager (telefoon, i-Pad, laptop, usb-stick)	16	18
P-document in verkeerd P-dossier	4	3
Foutieve machtigingen	1	10
e-mail met persoonsgegevens naar verkeerder ontvanger gestuurd	1	4
Document met persoonsgegevens onbedoeld gepubliceerd op internet	2	3
Printincidenten met persoonsgegevens	1	2
Hack incident met persoonsgegevens/telefoonoplichting (spoofing)	4	0
Documenten met persoonsgegevens onbeheerd gevonden	1	1
Datalek fractie/Kamerlid/andere organisatie dus geen datalek voor Tweede Kamerorganisatie	8	4
Geen datalek want geen persoonsgegevens betrokken bij incident	1	0
Totaal	**39**	**45**