Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3306

Vragen van de leden **Rahimi** en **Ellian** (beiden VVD) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister voor Rechtsbescherming over *het bericht «Ambtenaar vervalste meerdere rapporten over beveiliging DigiD-aansluiting»* (ingezonden 21 juni 2023).

Antwoord van Minister **Weerwind** (Rechtsbescherming), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 26 juli 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 3231.

Vraag 1
Bent u bekend met het bericht «Ambtenaar vervalste meerdere rapporten over beveiliging DigiD-aansluiting» van security.nl van 14 juni 2023?[1]

Antwoord 1
Ja.

Vraag 2
In opdracht van wie heeft deze ambtenaar deze taken uitgevoerd?

Antwoord 2
De betreffende ambtenaar voerde zijn taken uit in dienst van Justis. De vervalsing van rapporten maakte daar vanzelfsprekend geen onderdeel van uit.

Vraag 3
Is hier het vierogenprincipe gebruikt door een andere persoon? Zo ja, is deze persoon in zicht en zo nee, kunt u uitleggen waarom geen gebruik is gemaakt van het vierogenprincipe?

[1] Security (2023). Ambtenaar vervalste meerdere rapporten over beveiliging DigiD aansluiting. Zie https://www.security.nl/posting/799578/Ambtenaar+vervalste+meerdere+rapporten+over+beveiliging+DigiD-aansluiting.

ah-tk-20222023-3306
ISSN 0921 - 7398
's-Gravenhage 2023

Antwoord 3
Voor het betreffende proces binnen Justis werd tot maart 2023 geen gebruik gemaakt van het vierogenprincipe. De invoering van het vierogenprincipe is wel één van de verbeteracties die naar aanleiding van dit incident is doorgevoerd.

Vraag 4
Heeft de desbetreffende ambtenaar ook op andere ministeries gewerkt? Zo ja, op welke?

Antwoord 4
Nee.

Vraag 5
Is er aan de hand van het digitaal forensisch onderzoek aanleiding om ook binnen andere ministeries en uitvoeringsorganisatie te onderzoeken of daar ook dergelijke praktijken plaatsvinden of hebben gevonden?

Antwoord 5
Er is naar aanleiding van het uitgevoerde digitaal forensisch onderzoek geen reden om aan te nemen dat bij andere ministeries of uitvoeringsorganisaties dergelijke praktijken plaatsvinden of hebben gevonden. Zie voor de volledigheid ook het antwoord op vraag 6.

Vraag 6
Welke structurele oplossingen ziet u om dit in de toekomst te voorkomen?

Antwoord 6
Op dit moment is het zo dat organisaties bij het gebruik van DigiD jaarlijks moeten aantonen dat zij aan 21 informatieveiligheidseisen voldoen. Sinds 1 januari 2023 vindt digitale ondertekening plaats op de elektronisch ingediende assessments door de onafhankelijke auditor. Zonder deze digitale ondertekening neemt Logius de assessments niet in behandeling. Elke vorm van bewerking in het digitale document, nadat er is getekend, zorgt ervoor dat de geldigheid van de digitale handtekening komt te vervallen. In de afgelopen assessmentronde werd 98% van de assessments digitaal ingediend. Vanaf 1 januari 2024 kunnen assessments uitsluitend digitaal worden ingediend. Hiermee wordt manipulatie van assessments, of rapporten daarover, zo goed als onmogelijk gemaakt. Na de constatering van de manipulatie is bij Justis het auditproces verbeterd en aangescherpt, zo is bijvoorbeeld het vierogenprincipe ingevoerd (zie ook de beantwoording van de vragen 3 en 10).

Vraag 7
Wat is er in het rapport voor Suwinet van 2020 aangepast en waarom?

Antwoord 7
In de aangepaste versies zijn meerdere bevindingen van de Suwinet-auditrapportages afgezwakt of weggelaten. Hierbij zijn sommige negatieve bevindingen aangepast zodat deze positiever overkomen of zijn deze bevindingen volledig weggelaten. Voor meer specifieke informatie verwijs ik naar de managementsamenvatting van het forensisch digitaal onderzoek van Fox-IT, dat ik uw Kamer eerder toestuurde.[2] De vraag waarom deze wijzigingen op de originele auditrapportage van de ADR zijn gemaakt, is geen onderdeel geweest van het digitaal forensisch onderzoek van Fox-IT.

Vraag 8
Wat zijn de verschillen tussen de beveiligingsassessments van DigiD die de Auditdienst Rijk (ADR) aan Justis levert en de beveiligingsassessments die Justis naar Logius stuurt? Is de informatieveiligheid in gevaar geweest en/of zijn er gegevens gelekt?

[2] Kamerstuk 26 643, nr. 1035

Antwoord 8
In de rapporten zijn oordelen van de ADR dat de toepassing van een beveiligingsnorm «niet voldoet» aangepast naar «voldoet». Op dit moment zijn er geen signalen die wijzen op concreet gevaar voor de informatieveiligheid of het lekken van gegevens. In de tweede fase van het onderzoek wordt een risico-inschatting gemaakt naar aanleiding van de gemaakte wijzigingen in de DigiD-auditrapportages. Na het afronden van deze fase zal naar verwachting meer duidelijk zijn over de risico's die op het gebied van informatieveiligheid hebben bestaan.

Vraag 9
Kan de Staatssecretaris ons mededelen of de weggestuurde persoon betrokken was bij de opzet van de exploited audit en zo ja, welke andere personen in een identieke rol betrokken waren, of mogelijk betrokken zijn? En zijn deze personen ook betrokken bij het implementeren van de reparatie van deze exploit?

Antwoord 9
Voor de beantwoording van deze vraag interpreteer ik de term «exploited audit» als «het (frauduleus) aanpassen van de bedoelde rapportages». In die context kan ik bevestigen dat de bedoelde persoon inderdaad was betrokken. Zoals ook uit het onderzoek van Fox-IT blijkt, zijn er echter geen sporen aangetroffen die aantonen dat anderen op de hoogte zijn geweest van de aanpassingen of betrokken zijn geweest bij het aanpassen of namaken van de rapporten. Bij de implementatie en reparatie zijn dus geen medewerkers betrokken die ook betrokken waren bij de aanpassing of het namaken van rapporten.

Vraag 10
Zien de toegezegde vervolgacties op de verbetering van de interne auditfunctie of op de compliance office bij Justis zelf?

Antwoord 10
De vervolgacties zien op het aanscherpen en verbeteren van het auditproces binnen Justis, om manipulatie van assessments, of rapporten daarover, zo goed als onmogelijk te maken (zie ook mijn antwoorden op vragen 3 en 6). Er vinden op dit moment nog twee onderzoeken plaats: het onderzoek naar risico's zoals benoemd in het antwoord op vraag 8 en een onderzoek naar hoe dit heeft kunnen gebeuren. Het is mijn verwachting dat ook hieruit concrete aanbevelingen komen voor verdere verbeteringen om soortgelijke situaties in de toekomst te voorkomen.

Vraag 11
Is er vastgesteld of de betrokken fraudeur ook andere mogelijke exploits heeft gezocht bij Justis en bij Suwinet in die vijf jaren?

Antwoord 11
Voor de beantwoording van deze vraag interpreteer ik de term «exploits» als «het (frauduleus) aanpassen van rapportages». In die context kan ik u melden dat uit het digitaal forensisch onderzoek niet is gebleken dat dit het geval is.

Vraag 12
Heeft het onderzoek kunnen vaststellen of deze medewerkers ook zicht en vermoedens hebben gehad dat deze medewerker deze vervalsingen kon en wilde aanleggen?

Antwoord 12
Voor de beantwoording van deze vraag interpreteer ik de term «deze medewerkers» als «alle medewerkers van Justis behalve betrokkene». Tijdens het onderzoek van Fox-IT zijn geen sporen aangetroffen die erop wijzen dat anderen dan betrokkene op de hoogte waren van de aanpassingen in de rapporten, of betrokken waren bij het aanpassen of namaken van de rapporten.