Auditdienst Rijk
Ministerie van Financiën

Onderzoek beveiliging C2000

Onderzoeksopdracht

Definitief

Colofon

Titel	Onderzoek beveiliging C2000
Uitgebracht aan	Programmadirecteur Meldkamer, C2000 en 112
Datum	13 maart 2017
Kenmerk	2017-0000052403

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

C2000 is het landelijke communicatiesysteem voor de handhaving van de openbare orde en veiligheid in Nederland. De minister van Veiligheid en Justitie (VenJ) is eigenaar van het C2000 netwerk. De aangewezen gebruikers van C2000 zijn Politie, Brandweer, Ambulancezorg en Defensie. Een ongestoorde, betrouwbare werking van C2000 is van cruciaal belang, een adequate beveiliging van C2000 is hiermee onlosmakelijk verbonden.
Om te komen tot een adequate beveiliging van C2000 is ondermeer het "Beveiligingsbeleid C2000" opgesteld dat in 2012 is gepubliceerd[1].
De beveiliging van C2000 is een ketenaangelegenheid. Dit betekent dat de zwakste schakel in de keten het uiteindelijke niveau van de gehele keten bepaalt.

Aan de beveiligingsmaatregelen zoals beschreven in het hiervoor genoemde beveiligingsbeleid dienen alle betrokken partijen (gebruikers) zich te conformeren. Er heeft de afgelopen jaren geen toetsing van dit beleid vanuit VenJ plaatsgevonden zoals het beveiligingsbeleid voorschrijft. Met de vernieuwing van de infrastructuur van C2000 die momenteel plaatsvindt is het van belang dat er dit jaar een goed beeld ontstaat van de werking van het beveiligingsbeleid C2000. De ADR is daarom gevraagd een onderzoek uit te voeren naar de beveiliging van (onderdelen van) C2000.

Voor dit onderzoek hebben wij in overleg met de gedelegeerd opdrachtgever een aantal thema's uit het beveiligingsbeleid geselecteerd. Daarbij is bij een beperkt aantal gebruikers onderzoek gedaan. Dit onderzoek doet daarom geen algehele uitspraak over de beveiliging van C2000 als geheel, desalniettemin levert dit onderzoek inzichten op waarmee de beveiliging van C2000 verder kan worden verbeterd. Voor een nadere toelichting over de wijze waarop de thema's zijn geselecteerd, de scope en diepgang verwijzen wij naar hoofdstuk 7 in dit rapport.

Uit ons onderzoek blijkt dat beveiliging van C2000 niet altijd de aandacht heeft gekregen die het nodig heeft. Belangrijke oorzaken hiervoor zijn de focus op de capaciteit, dekking en gebruik van het C2000-systeem, de vernieuwing van het systeem (project Implementatie Vernieuwing C2000), maar ook het feit dat het hele veld van de veiligheidsregio's nog in beweging is; de meldkamers worden samengevoegd tot één landelijke meldkamerorganisatie en de politie verkeert nog in transitie. Deze ontwikkelingen hebben ook hun weerslag op de mate waarin het beveiligingsbeleid wordt nageleefd: de mate waarin het beleid wordt nageleefd verschilt per organisatie. We zien op diverse gebieden achterstanden, zo zien we ondermeer dat:

- Taken, bevoegdheden en verantwoordelijkheden met name op strategisch niveau binnen organisaties niet altijd duidelijk zijn belegd.
- De Afhankelijkheids- en kwetsbaarheidanalyse (A&K-analyse) die is opgesteld voor de vernieuwing van de C2000-infrastructuur nog niet is doorvertaald in (vernieuwd) beleid en eisen aan beheer en eindgebruikers.
- De toezichthoudende rol op papier wel is beschreven, maar in de praktijk nauwelijks ingevuld wordt.
- De controle op juistheid en volledigheid van de inventaris van randapparatuur in de praktijk maar zeer beperkt plaats vindt en de koppeling met de personeelsadministratie niet overal aanwezig is.

1 . Het beveiligingsbeleid C2000 is gepubliceerd op 21 maart 2012 in De Staatscourant (NR. 5393).

- Bij de uitreiking van C2000-randapparatuur beveiligingsaspecten niet altijd kenbaar worden gemaakt aan eindgebruikers.
- Beveiliging van C2000 nauwelijks aandacht krijgt in trainingen en/of awareness programma's.

Uit ons onderzoek komt tegelijkertijd het beeld naar voren van een sterk "vakmanschap" op operationeel niveau en blijkt dat, ondanks dat eindgebruikers niet expliciet op de hoogte zijn van de geldende voorschriften, er doorgaans wel intrinsiek een relatief hoog beveiligingsbewustzijn aanwezig is; er zijn veel 'ongeschreven' regels. Onder andere bij het proces rondom cryptografie zien we dat door de kennis en inzet van deskundige medewerkers er kwalitatief goed werk wordt geleverd. Het nadeel hiervan is dat de beveiliging wel (te) sterk afhangt van betrokken personen.

Met de komst van een nieuwe C2000 infrastructuur is dit *het* moment om hernieuwde aandacht aan beveiliging van C2000 te geven. Dit onderzoek laat zien dat dit nodig is. Daarbij moet wel worden gerealiseerd dat een communicatiemiddel zoals C2000 inherent risico's met zich mee zal (blijven) brengen; het ongekend aantal (verschillende) gebruikers en de eisen aan een hoge beschikbaarheid en bereikbaarheid staan veelal op gespannen voet met de beveiliging. Het is daarom naar onze mening niet van belang al deze risico's af te dekken, maar te zoeken naar een optimum waarbij beschikbaarheid en beveiliging en preventieve en repressieve maatregelen met elkaar in balans zijn en waarbij, indien nodig, bewust risico's worden geaccepteerd (bepalen van de risk appetite). Dit zal niet van de ene op de andere dag worden gerealiseerd. Wij adviseren om te komen tot een roadmap waarbij, samen met de verschillende C2000-partijen, vanuit een risicogerichte benadering wordt bezien welke maatregelen nog (opnieuw) getroffen moeten worden en in welke volgorde. Daarbij dient rekening te worden gehouden met het "rendement" dat deze aanbevelingen bieden op het gebied van informatiebeveiliging en de capaciteit die hiervoor vrijgemaakt kan worden, aangezien meerdere geïnterviewden hebben aangegeven dat er voor het uitvoeren van sommige controlewerkzaamheden nu onvoldoende personele capaciteit beschikbaar is. Voor een verbeterde beveiliging van C2000 stellen wij voor de volgende elementen mee te nemen in de roadmap:

1. *Het expliciet benoemen van verantwoordelijkheden voor de beveiliging van C2000 bij de verschillende gebruikers op strategisch en tactisch niveau (volgens een piramidestructuur), waarbij verantwoording wordt afgelegd over een beperkt, maar cruciaal aantal onderwerpen.* Deze onderwerpen kunnen gedurende de tijd worden aangepast aan nieuwe trends. Bespreek deze trends ook ten minste jaarlijks met alle partijen. Daarmee wordt beveiliging aantoonbaar en kan beleid worden geëvalueerd en aangescherpt indien nodig.
2. *Het actualiseren van het beveiligingsbeleid op basis van de A&K-analyse.* De nieuwe (technische) omgeving van C2000 brengt mogelijke andere risico's met zich mee. Deze zijn reeds inzichtelijk gemaakt met een A&K-analyse die in 2014 is uitgevoerd. Wij adviseren bij het actualiseren van het beveiligingsbeleid rekening te houden met de verschillende classificatieniveaus van de informatie en de karakteristieken van de verschillende kolommen met bijbehorende gelieerde diensten. Neem daarbij in overweging of BIR-TNK voldoende recht doet aan de eisen van C2000, bijvoorbeeld als het gaat over de beschikbaarheid. Een (geactualiseerd) beleid is vooral van belang voor het maken van afspraken tussen partijen en voor het doorvertalen naar praktische instructies voor de eindgebruikers ('de man op straat').

3. *Gebruik interne controle of audits om de toereikendheid van bovengenoemd stelsel periodiek te toetsen en waar nodig te verbeteren.*
4. *Verbeter de registratie van de inventaris van C2000 randapparatuur.* Om effectief te monitoren is een actuele registratie cruciaal. Porto op de man is "standaard tenzij". Een periodieke inventarisatie is hierbij een onderdeel. Sluit voor deze inventarisatie aan op de momenten waarop portofoons naar beheer moet worden gebracht zoals bij een update van de fleetmap of een actualisatie van de softwareversie. Informeer beheerders van de C2000 randapparatuur over uitdiensttredingen en functiewijzigingen van medewerkers die beschikken over C2000 apparatuur, zodat inzicht bestaat in welke medewerker zijn of haar portofoon moet inleveren of moet laten aanpassen.
5. *Monitor actief op verdachte patronen van randapparatuur. Evalueer naar aanleiding van incidenten of patronen kunnen worden aangescherpt.* Bepaalde patronen van C2000-randapparatuur kunnen duiden op misbruik, het monitoren van deze patronen kan bijdragen aan het signaleren hiervan.
6. *Vertaal het beleid naar een aantal praktische instructies voor de C2000 eindgebruikers.* Hierbij dient rekening te worden gehouden met de soort organisatie waarvoor de eindgebruiker werkt. Zorg dat de eindgebruiker deze instructies ontvangt op het moment dat deze de C2000 randapparatuur in ontvangst neemt. Verwerk deze instructies ook in een awareness programma; maak ze onderdeel van de verplichte jaarlijkse trainingen.
7. *Maak inzichtelijk in welke mate beveiligingsbewustzijn leeft onder de eindgebruikers.* Het adequaat inrichten van het toezichtsinstumentarium is daarvoor een middel. Een startpunt kan een breed onderzoek zijn naar de perceptie bij eindgebruikers van C2000 randapparatuur.

Tot slot willen wij opmerken dat voor bovengenoemde maatregelen al deels good-practices aanwezig zijn bij de diverse partijen. Wij doen daarom de suggestie om deze in kaart te brengen en te bezien of dergelijke maatregelen kunnen worden hergebruikt bij andere partijen.

De rest van het rapport is als volgt ingedeeld: Hierna volgt de beleidsreactie op ons rapport. In de hoofdstukken 1 tot en met 6 worden de verschillende thema's in meer detail behandeld. Elk hoofdstuk begint met een korte toelichting over het beleid, gevolgd door de bevindingen, risico's en adviezen. In hoofdstuk 7 is de onderzoeksverantwoording opgenomen en in hoofdstuk 8 ten slotte de ondertekening.

Beleidsreactie onderzoek beveiliging C2000

Met de vernieuwing van de infrastructuur van C2000 die momenteel plaatsvindt, is het van belang dat er een goed beeld ontstaat van de werking en naleving van het Beveiligingsbeleid op het huidige C2000 systeem om bij het in gebruik nemen van het nieuwe netwerk een goed passend beveiligingsbeleid en bijbehorende maatregelen te nemen. De Auditdienst Rijk is daarom door VenJ gevraagd een onderzoek uit te voeren naar de beveiliging van (onderdelen van) C2000 om daarmee een beeld te krijgen van de naleving van het beveiligingsbeleid C2000. De uitkomsten van het onderzoek zullen worden betrokken bij de inrichting van het beveiligingsbeleid op het nieuwe C2000 systeem.

De ADR constateert een focus op capaciteit en dekking van het netwerk, organisatorische wijzigingen, het gebruik en de vernieuwing van het systeem waardoor beveiliging niet altijd de aandacht heeft gehad die het nodig heeft. Zowel VenJ, de beheerder als de gebruikers van het systeem hebben onderhoudsachterstand te verrichten op de naleving van het beveiligingsbeleid C2000.

De ADR adviseert om de verbeterpunten te verwerken in een roadmap waarbij, samen met de verschillende C2000-gebruikers, vanuit een risicogerichte benadering wordt bezien welke maatregelen nog (opnieuw) getroffen moeten worden en in welke volgorde. Zij geven daarbij aan dat gekeken moet worden naar een optimaal niveau van beveiliging. Het maken van keuzes hierin is onontbeerlijk.

Ik onderschrijf de bevindingen en aanbevelingen uit het rapport. De komende periode zal VenJ samen met de C2000-gebruikers werken aan een roadmap "beveiliging C2000". Hierin zal gekeken worden welke maatregelen (opnieuw) getroffen moeten worden en in welke volgorde en met welke prioriteit dit wordt uitgevoerd. Het is de doelstelling om deze roadmap voor de zomer 2017 gereed te hebben om vervolgens de maatregelen zoals benoemd in de roadmap op te kunnen volgen.

Op korte termijn zal ik in ieder geval met de implementatie van een aantal prioritaire en of snel te realiseren maatregelen starten:

- Het actief monitoren op verdachte patronen van randapparatuur. Ik heb de politie / MDC gevraagd hiervoor een aantal pragmatische voorstellen voor te doen waarbij rekening wordt gehouden met effectiviteit, kosten en vigerend informatiebeveiligingsbeleid van de gebruikersorganisaties.
- Het verbeteren van het zicht op de randapparatuur door middel van een regelmatig uit te voeren inventarisatie en controle van de registratie van de randapparatuur. Ik zal de gebruikers verzoeken hier aandacht aan te besteden.
- Het verduidelijken van de incidentenprocedure voor C2000, zodat bij eventuele beveiligingsincidenten het bekend is bij wie eindgebruikers melding kunnen maken van verlies of diefstal van apparatuur. Ik zal de gebruikers verzoeken hier aandacht aan te besteden.

VenJ zal daarnaast bezien of de beleidsregels van het beveiligingsbeleid C2000 (2012) nog aanpassing behoeven en waar nodig deze aanpassen.

Ik dank de Auditdienst Rijk voor het onderzoek dat zij hebben verricht en heb er vertrouwen in dat wij samen met de C2000 gebruikers de beveiliging van (het vernieuwde) C2000 zo optimaal mogelijk gaan organiseren.

Programmadirecteur Meldkamer, C2000 en 112

1 Governance

In §2.0 van de beleidsregels over de beveiliging van C2000 worden algemene beveiligingsmaatregelen beschreven. In de beleidsregels is ondermeer opgenomen dat de taken, verantwoordelijkheden en bevoegdheden van werknemers, ingehuurd personeel en externe eindgebruikers voor de informatiebeveiliging van C2000 is vastgesteld en gedocumenteerd en dat toezicht op het nakomen van het C2000 beleid is ingeregeld. Verder zijn eisen beschreven voor screening van medewerkers.

1.1 Leg taken, verantwoordelijkheden en bevoegdheden op alle niveaus vast

1.1.1 *Aangetroffen situatie*

Het hele veld van de veiligheidsregio's is nog in beweging; de meldkamers worden samengevoegd tot één Landelijke meldkamerorganisatie en de politie verkeert nog in transitie. Bij de herziening van het beveiligingsbeleid in 2012 is wel het beveiligingsbeleid gericht op de gebruiker beschreven (de beleidsregels). Beveiligingsbeleid voor de beheersorganisatie is echter niet beschreven.
Bovendien zijn taken, bevoegdheden en verantwoordelijkheden met name op strategisch niveau niet altijd duidelijk belegd.
Wie eindverantwoordelijk is voor het C2000 beveiligingsbeleid is niet duidelijk. Het is per kolom (politie, brandweer, ambulancedienst, KMAR) anders ingericht en ook per veiligheidsregio zijn er verschillen.
Op operationeel niveau is het wel duidelijk wat de taken, bevoegdheden en verantwoordelijkheden zijn op het gebied van het C2000 beveiligingsbeleid. Niet omdat dit formeel is vastgelegd, maar doordat in de loop van de jaren een praktijk is gegroeid die werkt voor de organisaties.

1.1.2 *Risico*

Of alle taken conform het beleid worden uitgevoerd is van verschillende factoren afhankelijk, waaronder het 'vakmanschap' van de medewerkers, beschikbare capaciteit en prioriteit die er aan taken wordt gegeven. Het risico bestaat dat beslissingen niet (op het juiste niveau) worden genomen en verantwoordelijkheden niet zijn belegd, waardoor ze tussen wal en schip raken.

1.1.3 *Aanbeveling & handelingsperspectief*

Alhoewel lastig in een veranderende organisatie, waarin verschillende kolommen met elkaar moeten samenwerken, adviseren wij de taken, bevoegdheden en verantwoordelijkheden met het oog op het vernieuwde C2000-netwerk formeel vast te leggen, bekend te maken en uit te dragen. Daarbij moet men ervoor waken vakmanschap in procedures te willen vastleggen.

1.2 Actualiseer het beveiligingsbeleid op basis van de uitgevoerde A&K-analyse

1.2.1 *Aangetroffen situatie*

Bij het beveiligingsbeleid C2000 is geen sprake van een gesloten beleidscyclus. Er zijn veel wijzigingen in de omgeving van C2000. Het huidige beveiligingsbeleid dateert uit 2012 en is daarmee niet actueel. De Afhankelijkheids- en kwetsbaarheidanalyse (A&K-analyse) die is opgesteld in 2014 voor de vernieuwing van de C2000-infrastructuur is nog niet doorvertaald in beleid en eisen aan beheer en eindgebruikers. In het Programma van Eisen is de nieuwe

C2000 omgeving beschreven als departementaal vertrouwelijk, maar uit de A&K analyse blijkt dat er drie informatiestromen zijn die hoger moeten worden geclassificeerd, zoals GARA (aanbesteding van randapparatuur voor geheime communicatie), verkeersgegevens van bijzondere gebruikers en voicelogs van de ambulancezorg. Dit is echter niet als zodanig in het programma van eisen van deze aanbestedingen opgenomen, waardoor leveranciers hier niets voor hoeven in te richten. BIR TNK is volgens geïnterviewden het belangrijkste normenkader voor de beveiliging van C2000. Dit is een goede basis, alleen het BIR tactisch normenkader (TNK) is voor andere doeleinden ontwikkeld dan voor C2000, en zegt bijvoorbeeld onvoldoende over de beschikbaarheid van C2000.

1.2.2 *Risico*

Het risico bestaat dat mogelijk niet alle risico's door maatregelen worden afgedekt, of dat op onderdelen te veel maatregelen zijn getroffen.

1.2.3 *Aanbeveling & handelingsperspectief*

Actualiseer op basis van de in 2014 uitgevoerde A&K-analyse het beveiligingsbeleid en vertaal dit ook in concrete eisen richting beheer en eindgebruikers. Maak hierbij onderscheid naar de verschillende gebruikers. Het verdient de aanbeveling om de A&K-analyse waar nodig te actualiseren.

1.3 Stem de maatregelen uit het beveiligingsbeleid meer af op de verschillen per kolom

1.3.1 *Aangetroffen situatie*

Omdat gevoelige informatie wordt uitgewisseld via C2000 is een adequaat informatiebeveiligingsbeleid voor de gehele keten noodzakelijk. De mate van gevoeligheid van de informatie die wordt uitgewisseld verschilt echter per kolom. Bij de blauwe kolom en de groene kolom (Defensie, inclusief Kmar) kan het gaan over opsporingsinformatie. In de witte kolom is er o.a. sprake van medisch geheim. In de rode kolom is informatie minder vertrouwelijk omdat het veelal gaat over calamiteiten in de publieke ruimte. Daarnaast zijn er gelieerde partijen die gebruik maken van C2000. De gevoeligheid van de informatie in deze laatste categorie is zeer beperkt.
Er is momenteel één uniform informatiebeveiligingsbeleid met een basisset aan maatregelen vastgesteld voor de gehele keten. Een uitzondering geldt hierbij voor de Gara randapparatuur waar zwaardere maatregelen voor zijn getroffen. Verschillende geïnterviewden geven aan dat de maatregelen uit het informatiebeveiligingsbeleid te zwaar zijn in relatie tot de vertrouwelijkheid van de informatie die wordt uitgewisseld.

1.3.2 *Risico*

Het gevolg van deze beleidskeuze is dat voor sommige kolommen het beveiligingsregime te zwaar kan zijn en voor andere kolommen te licht. Dit wordt ook wel aangeduid als respectievelijk overrubriceren en onderrubriceren. Overrubricering leidt tot het treffen van te veel en/of te zware maatregelen, deze maatregelen kunnen een nadelig effect hebben op het gebruik van C2000 of onnodige beheerlast en kosten met zich mee brengen. Onderrubricering leidt tot het treffen van te weinig en/of te lichte maatregelen waarmee het risico op uitlekken van gevoelige informatie groter is.

1.3.3 *Aanbeveling & handelingsperspectief*

In samenhang met een nieuwe risicoanalyse (§1.2.3) en als onderdeel van het actualiseren van het beveiligingsbeleid adviseren wij om meer inzicht te verkrijgen in de classificatie van de informatie per kolom of per functie. Geef

daarbij aandacht aan de verschillen in classificatie en houd hier waar mogelijk rekening mee bij het herijken van de maatregelen in het beveiligingsbeleid.

1.4 Geef meer invulling aan toezichtsinstrumenten

1.4.1 Aangetroffen situatie

De toezichthoudende rol is op papier wel beschreven, maar in de praktijk wordt er nauwelijks aandacht aan gegeven. Instrumenten waarmee toezicht kan worden gehouden zijn niet aanwezig, of worden beperkt gebruikt. Zo signaleren wij dat:

- Volgens het C2000-beveiligingsbeleid elke gebruiker een C2000-beveiligingsfunctionaris dient aan te stellen. Of er een beveiligingsfunctionaris is, verschilt per organisatie. Ook de wijze waarop deze functionaris zijn rol invult verschilt.
- Er bij de meeste organisaties geen sprake is van reguliere (kwartaal)rapportages over beveiligingsincidenten.
- In de praktijk, voor zover wij hebben kunnen nagaan, nauwelijks audits plaatsvinden bij de regio's op het naleven van C2000 beveiligingsbeleid. Er is ook geen instantie die toezicht houdt op het uitvoeren van audits.
- De Multidisciplinair Adviseur C2000 (MAC) degene is die de belasting van het netwerk kan monitoren. Deze toezichthoudende rol is heel divers ingericht. Bij de ene organisatie is deze rol wel ingevuld, bij de andere niet.
- De mate waarin zicht is op de awareness bij gelieerde partijen verschilt per organisatie. Organisaties erkennen dat deze apparatuur mogelijk buiten beeld is.

1.4.2 Risico

Doordat het toezichthoudende instrumentarium beperkt is ingericht, is niet aantoonbaar in hoeverre het C2000 beveiligingsbeleid wordt nageleefd. Hoe effectief de beleidsmiddelen zijn die worden ingezet om de beveiliging van C2000 te bevorderen is daardoor niet bekend, noch kan hierdoor adequaat worden bijgestuurd.

1.4.3 Aanbeveling & handelingsperspectief

Geef actief invulling aan de in de beleidsregels opgenomen toezichtsinstrumenten (C2000 beveiligingsfunctionaris, rapportages en audits).
De aangewezen gebruiker ziet toe op de naleving van de maatregelen om zo invulling te geven aan zijn verantwoordelijkheid. Maak beleidsafspraken over de situaties waarin het C2000 netwerk gemonitord moet worden en organiseer deze monitoring.

1.5 Maak eisen rondom screening van personeel duidelijk

1.5.1 Aangetroffen situatie

De verschillende kolommen hebben verschillende regels en wettelijke bepalingen voor het screenen van medewerkers. Er zijn ook verschillen tussen de veiligheidsregio's. Wat precies de regels zijn voor de screening van medewerkers die gebruik maken van C2000 randapparatuur, kunnen geïnterviewden niet aangeven.
Niet alle medewerkers worden gescreend. Bij de politie en de KMAR is een screening gebruikelijk. Bij de brandweer is een screening niet gebruikelijk omdat er geen wettelijke basis voor is. Over het algemeen wordt wel een VOG aangevraagd, ook voor vrijwilligers en uitzendkrachten.

Het kan gebeuren dat medewerkers lang in dienst zijn en bij indiensttreding gescreend zijn, maar dat een nieuwe screening niet plaatsvindt terwijl zij wel een vertrouwensfunctie zijn gaan uitoefenen (verandering van omstandigheden in de functie). Het zou dan in de rede liggen een herhaalonderzoek uit te laten voeren. Dat gebeurt echter niet altijd.

1.5.2 Risico

Het risico van het niet adequaat screenen van medewerkers die toegang hebben tot vertrouwelijke informatie en een vertrouwensfunctie vervullen is dat vertrouwelijke informatie gelekt wordt en het C2000 systeem mogelijk gecorrumpeerd wordt door 'foute medewerkers'.
Hoe groot het aantal medewerkers is dat niet gescreend is en wel een vertrouwensfunctie bekleedt of toegang heeft tot vertrouwelijke informatie, is niet bekend.

1.5.3 Aanbeveling & handelingsperspectief

Stel een lijst op van vertrouwensfuncties en inventariseer in hoeverre medewerkers die een vertrouwensfunctie bekleden gescreend zijn.
Ook adviseren wij te bepalen welke screening medewerkers dienen te hebben en te inventariseren in hoeverre deze medewerkers aan het juiste screeningsniveau voldoen.
Wij adviseren medewerkers die nog niet (op het juiste niveau) gescreend zijn, en die dat wel zouden moeten zijn, te laten screenen. Daarbij is het wellicht nodig om op basis van risicoanalyse te bepalen in welke volgorde functiegroepen gescreend dienen te worden.

2 Configuratie en cryptobeheer

In de beleidsregels staan maatregelen waarin is vastgelegd dat alle beheerde C2000-randapparatuur dient te worden bijgehouden in een actuele inventaris en afdoende dient te worden gecontroleerd op juistheid en volledigheid. Ook is vastgelegd dat bij uitdiensttredingen of functiewisselingen portofoons moeten worden ingeleverd en gespreksgroepen moeten worden aangepast.

2.1 Controleer de inventaris van C2000 randapparatuur periodiek en monitor actiever op verdachte patronen

2.1.1 *Aangetroffen situatie*

De controle op juistheid en volledigheid van de inventaris van randapparatuur vindt in de praktijk maar zeer beperkt plaats. Veel geïnterviewden geven aan dat hiervoor onvoldoende capaciteit beschikbaar is en dat beheer van de inventaris complex en omslachtig is. Slechts bij één organisatie hebben wij vastgesteld dat er periodiek een sample werd genomen van de lijst met uitgegeven randapparaten die vervolgens één voor één werden nagelopen op kenmerken als Landelijk kader Fleetmap versie; patch versie en status. Afwijkingen werden hiermee gesignaleerd en teruggekoppeld.
Wij signaleren grote verschillen tussen organisaties op dit gebied.
Bij brandweer en ambulancezorg wordt bij elke dienstoverdracht gecontroleerd of alle apparatuur aanwezig is omdat de randapparatuur daar gekoppeld is aan een voertuig.

Door netwerk monitoring kan inzicht verkregen worden in het aantal actieve randapparaten per C2000 zendmast. Dit gebeurt echter niet continu, maar met name bij evenementen en betreft een verantwoordelijkheid van de meldkamer. Hierdoor kunnen afwijkingen in portofoongebruik die kunnen duiden op misbruik gesignaleerd worden. Het betreft hier dan bijvoorbeeld portofoons van medewerkers die op dat moment geen dienst hebben, of die in een andere regio aangemeld zijn dan daar waar ze werkzaam zijn.

2.1.2 *Risico*

Het gevolg van de afwezigheid van periodieke controles op juistheid en volledigheid van de inventaris is dat afwijkingen niet worden gesignaleerd. Het risico dat hierdoor ontstaat is bijvoorbeeld dat diefstal of vermissing van randapparatuur niet wordt opgemerkt.

2.1.3 *Aanbeveling & handelingsperspectief*

Controleer periodiek de inventaris van C2000-randapparatuur. Combineer dit zoveel mogelijk met momenten waarop de apparatuur moet worden bijgewerkt, zoals voor de Landelijk kader Fleetmap of patches. De periodiciteit van controle kan variëren op basis van het risicoprofiel van de randapparatuur.
Ook kan mogelijk monitoring actiever worden ingezet om verdachte patronen te detecteren.
Hierin zal de opdrachtgever moeten bepalen hoeveel tijd en middelen zij beschikbaar wil stellen om het hiervoor beschreven risico te mitigeren.

2.2 Zorg voor inzicht in uitdiensttredingen en functiewisselingen en de koppeling met uitgegeven portofoons en gespreksgroepen

2.2.1 *Aangetroffen situatie*

Wanneer een medewerker de dienst verlaat of een andere functie gaat vervullen moet hij of zij de portofoon respectievelijk inleveren of moeten gespreksgroepen op de portofoon hierop worden aangepast. Uit de interviews ontstaat het beeld dat dit niet in alle gevallen gebeurt.
Dit speelt met name bij de politie waar er geen koppeling is tussen het personeelssysteem en Topdesk (waarin de portofoons geregistreerd worden). Beheerders worden daardoor niet geïnformeerd welke portofoons ingeleverd zouden moeten worden en op welke portofoons gespreksgroepen aangepast moeten worden. Over het inleveren van de portofoon bij functiewisseling of uitdiensttreding zijn volgens geïnterviewden geen duidelijke afspraken gemaakt.

2.2.2 *Risico*

Doordat er geen juist en volledig overzicht is van de in te leveren portofoons , bestaat het risico dat portofoons in circuits buiten de veiligheidsregio's terechtkomen en dat er illegaal in gehandeld wordt. Ook levert het materiële schade op, doordat portofoons mogelijk niet optimaal worden ingezet.
Het niet aanpassen van gespreksgroepen na een functiewisseling leidt ertoe dat medewerkers ongeautoriseerd kennis kunnen nemen van gevoelige informatie.

2.2.3 *Aanbeveling & handelingsperspectief*

Wij adviseren te bezien op welke wijze er een koppeling gemaakt kan worden tussen de registratie van portofoons en de personeelsadministraties van de organisaties.

3 Fysieke beveiliging

In §2.2 van de beleidsregels over de beveiliging van C2000 worden maatregelen beschreven op het gebied van Lokaal beheer C2000, waaronder maatregelen op het gebied van fysieke beveiliging en maatregelen die beschrijven hoe te handelen bij onderhoud, inbouw, uitbouw en reparatie van randapparatuur in voertuigen.

3.1 Zorg voor aansluiting tussen maatregelen voor fysieke beveiliging en de regelgeving en zie toe op de naleving

3.1.1 Aangetroffen situatie

Op de bezochte locaties lijkt veel aandacht te zijn gegeven aan fysieke beveiliging door maatregelen zoals zonering, toegangscontroles, afgesloten radiowerkplaatsen en opslagplaatsen, camera's en paslezers met logging. De geïnterviewde beheerders geven blijk van een hoge mate van awareness op het gebied van fysieke beveiliging.

Wanneer wordt gevraagd of de getroffen maatregelen in overeenstemming zijn met de maatregelen zoals omschreven in het beveiligingsbeleid, is men vaak niet op de hoogte van deze richtlijn. Bij geen van onze gesprekken kon men aangeven of aantonen dat aan deze of andere richtlijnen wordt voldaan. Een uitwerking van regelgeving naar fysieke beveiligingsmaatregelen is niet aangetroffen. Als er al gerefereerd wordt aan richtlijnen voor fysieke beveiliging dan betreft dit organisatie-eigen richtlijnen (Bijvoorbeeld KMar - of Politierichtlijnen). Tevens blijkt er weinig aandacht voor audits op het gebied van fysieke beveiliging. Eén geïnterviewde gaf aan een intern politie onderzoek naar fysieke beveiliging te hebben meegemaakt. De aanbevelingen die hier uit voort zijn gekomen bleken echter nooit opgevolgd.

3.1.2 Risico

Van verschillende fysieke beveiligingsmaatregelen hebben wij de aanwezigheid kunnen vaststellen, maar of hiermee wordt voldaan aan de eisen uit de beleidsregels is niet aantoonbaar en herleidbaar vastgelegd, noch is dit bekend bij de betrokkenen. Hierdoor bestaat de kans dat niet alle vereiste maatregelen op het gebied van fysieke beveiliging juist en volledig zijn geïmplementeerd. Het risico bestaat hierdoor dat ongeautoriseerden kennis kunnen nemen van, of misbruik kunnen maken van gevoelige informatie die via C2000 randapparatuur wordt uitgewisseld.

3.1.3 Aanbeveling & handelingsperspectief

Herijk de voorschriften uit de beleidsregels op het gebied van fysieke beveiliging en breng deze, indien mogelijk in lijn met beschikbare richtlijnen uit het veld, bijvoorbeeld van Politie of Veiligheidsregio's. Vertaal deze regelgeving door naar maatregelen voor de fysieke beveiliging; het toezicht op de naleving van de regelgeving dient geborgd te worden (bijvoorbeeld door periodieke audits).

3.2 Doe nader onderzoek of randapparatuur bij onderhoud aan voertuigen wel wordt gedeactiveerd

3.2.1 *Aangetroffen situatie*

Wanneer een voertuig onderhoud of reparatie behoeft, is er een afdeling of medewerker voor wagenparkbeheer die dit verzorgt. Op het moment dat het voertuig voor onderhoud weggaat dient dit te worden gemeld bij meldkamerbeheer of de verantwoordelijk beheerafdeling zodat zij de mobilofoon in het voertuig op afstand kunnen deactiveren. In voorkomende gevallen wordt de randapparatuur uitgebouwd, dit verschilt per voertuig.

Geïnterviewden geven aan dat zij door deze werkwijze geen uitspraak kunnen doen of in alle gevallen deze procedure wordt gevolgd. Immers zij ontvangen enkel de aanvragen voor deactivering, maar zij hebben geen totaalbeeld van het aantal voertuigen dat voor reparatie of onderhoud de organisatie verlaat. Dit is namelijk een verantwoordelijkheid van wagenparkbeheer. Wel geven enkele geïnterviewden aan dat zij uit ervaring weten dat voertuigen voor onderhoud extern gaan, waarbij de randapparatuur niet gedeactiveerd is.

3.2.2 *Risico*

Wanneer de randapparatuur in een voertuig niet wordt gedeactiveerd tijdens onderhoud of reparatie bestaat het risico dat medewerkers van onderhouds- en reparatiebedrijven kunnen meeluisteren en kennis kunnen nemen van de informatie die via de C2000 randapparatuur wordt uitgewisseld.

3.2.3 *Aanbeveling & handelingsperspectief*

Onderzoek hoe vaak voertuigen voor onderhoud of reparatie worden aangeboden en controleer of dit afwijkt van het aantal maal dat een verzoek tot deactivering van randapparatuur wordt ingediend.

Indien de ontvangen signalen in dit onderzoek correct zijn adviseren wij om te borgen dat bij alle voertuigen die voor onderhoud of reparatie weggaan de aanwezige randapparatuur is gedeactiveerd. Het geven van bekendheid aan de procedure is één van de beschikbare middelen.

4 Incident procedures

In de beleidsregels zijn in §2.0 maatregelen opgenomen ten aanzien van een procedure voor beveiligingsincidenten. Hierin is vastgelegd dat een procedure vastgesteld moet zijn en dat deze beschikbaar is voor alle werknemers. In de procedure moeten o.a. contactpersonen worden opgenomen.

4.1 Zorg voor een heldere incidentprocedure die bij alle betrokken bekend is

4.1.1 *Aangetroffen situatie*

Door onder andere beheerders is veelvuldig aangegeven dat eindgebruikers precies weten hoe zij moeten handelen in het geval van vermissing van een randapparaat. Wanneer gevraagd wordt naar een incidentprocedure waarin deze werkwijze is vastgelegd blijkt dat veel organisaties niet beschikken over een actuele, vastgestelde, en voor eindgebruikers beschikbare incidentprocedure.

4.1.2 *Risico*

Wanneer eindgebruikers niet voldoende op de hoogte zijn van de procedure, bestaat de kans dat incidenten niet juist, volledig en tijdig worden gemeld bij de daartoe aangewezen autoriteit. Het risico hiervan is dat, indien vermiste randapparatuur in verkeerde handen belandt, dit niet gesignaleerd en/of geregistreerd wordt waardoor onbevoegden kennis nemen van vertrouwelijke informatie die uitgewisseld wordt via de C2000 randapparaten.

4.1.3 *Aanbeveling & handelingsperspectief*

Zorg voor een heldere incidentprocedure die bij iedereen bekend is en stimuleer eindgebruikers om (mogelijke) vermissingen direct te melden.

4.2 Zorg voor herkenbare aanspreekpunten voor incidenten op zowel lokaal als landelijk niveau

4.2.1 *Aangetroffen situatie*

In hoofdstuk 1 is beschreven dat de taken en verantwoordelijkheden ten aanzien van sturing, beheersing, verantwoording en toezicht niet helder en eenduidig zijn belegd. Dit is ook van toepassing op de verantwoordelijkheid voor het beveiligingsincidentenproces. Op lokaal niveau is de rol van beveiligingsfunctionaris op bepaalde plekken niet belegd. Daarnaast is de verantwoordelijkheid voor beveiligingsincidenten op landelijk niveau niet belegd. Dit laatste blijkt onder andere uit het voorbeeld dat wanneer C2000 randapparatuur op Marktplaats wordt aangeboden, het niet duidelijk is wie opvolging moet geven aan deze signalen.

4.2.2 *Risico*

Het gevolg van de onduidelijkheid in verantwoordelijkheden is dat wanneer beveiligingsincidenten zich voordoen het niet helder is wie deze incidenten moet signaleren en moet opvolgen met als gevolg dat incidenten niet of te laat worden opgevolgd.

4.2.3 *Aanbeveling & handelingsperspectief*

Leg de rol van beveiligingsfunctionaris op landelijk niveau formeel vast en beleg deze expliciet bij één of meerdere medewerkers. Dit geldt ook voor lokaal niveau, voor zover daar nog geen beveiligingsfunctionaris is aangewezen. Op deze wijze ontstaan er herkenbare aanspreekpunten voor beveiligingsincidenten op landelijk en lokaal niveau.

5 Awareness van beveiligingsbeleid

In bijlage 2 van de beleidsregels over de beveiliging van C2000 worden maatregelen beschreven die ingaan op de awareness van eindgebruikers van C2000, waaronder het opstellen en communiceren van gedragsregels en training en regelmatige bijscholing.

5.1 Benoem praktische maatregelen op het gebied van beveiliging en maak deze kenbaar bij de uitreiking van randapparatuur

5.1.1 Aangetroffen situatie

De inhoud van het beveiligingsbeleid is niet in alle gevallen bij de geïnterviewden bekend. Het beveiligingsbeleid is veelal niet doorvertaald in praktische regels of verouderd. Wel zijn er 'ongeschreven' regels waarnaar men in de praktijk handelt. Deze worden bij sommige organisaties van persoon op persoon overgebracht.

De mate waarin aandacht wordt besteed aan risico's vanuit beveiligingsperspectief levert een diffuus beeld op.

- Sommige organisaties reiken bij het overhandigen van een portofoon dienstinstructies, of een gebruikersovereenkomst uit, of er wordt gebruik gemaakt van e-learning. Bij andere organisaties is men gestopt met het uitreiken van gebruikersovereenkomsten.
- Vanuit de beheerorganisatie (MDC) worden incidenteel beveiligingsgerelateerde zaken onder de aandacht gebracht veelal naar aanleiding van incidenten.
- Organisaties erkennen dat niet alle informatie even goed terug te vinden is op het intranet.

5.1.2 Risico

Het gevolg van een verminderde awareness zorgt mogelijk voor het niet naleven van regels voor gebruik van C2000 randapparatuur.

5.1.3 Aanbeveling & handelingsperspectief

Benoem een aantal praktische maatregelen op het gebied van beveiliging en maak deze kenbaar bij de uitreiking van randapparatuur. Deze kunnen per soort gebruiker(sgroep) verschillen. Deze maatregelen vormen ook de basis voor trainingen en periodieke bijscholing.

5.2 Maak omgang met C2000-randapparatuur onderdeel van trainingen

5.2.1 Aangetroffen situatie

Bijna geen enkele organisatie kent awareness programma's ten aanzien van de beveiliging van C2000. Awareness staat niet regelmatig geagendeerd voor overleggen. Op ad-hoc basis wordt wel eens een presentatie gegeven. Trainingen of presentaties over het gebruik van portofoons zijn veelal meer een 'knoppentraining' en zijn vaak niet gericht op het bevorderen van risicobewustzijn ten aanzien van beveiliging. Het programma 'portogewoon' heeft wel veel bijgedragen aan de awareness van een juist gebruik van randapparatuur. Van regelmatige bijscholing met daarin aandacht voor awareness voor informatiebeveiliging is echter geen sprake.

5.2.2 *Risico*

Eventuele opgedane kennis ten aanzien van informatiebeveiliging van randapparatuur en procedures van de organisatie kunnen bij onvoldoende bijscholing in de loop van de tijd bij de eindgebruikers wegzakken. Veilig gebruik van C2000-randapparatuur is dan in het geding.

5.2.3 *Aanbeveling & handelingsperspectief*

Maak de bewuste omgang met C2000-randapparatuur onderdeel van verplichte terugkerende trainingen of toets de omgang periodiek middels een (verplichte) e-learning. De hiervoor beschreven maatregelen kunnen als basis dienen.

6 Perceptie van beveiligingsbeleid

In dit onderzoek gaan wij uit van de veronderstelling dat het belang dat eindgebruikers hechten aan het beveiligingsbeleid voor een groot deel de bereidheid bepaalt om het beveiligingsbeleid na te leven. Ook wat zij meekrijgen van hun collega 's en leidinggevenden heeft invloed op de naleving van beveiligingsbeleid. Ten slotte is het gevoel dat de eindgebruikers hebben over de uitvoerbaarheid van het beleid van belang voor de naleving van de regelgeving.

6.1 Maak de kloof die er lijkt te bestaan tussen beleid en praktijk kleiner

6.1.1 Aangetroffen situatie

Medewerkers geven blijk van een hoge mate van beveiligingsbewustzijn. Men vindt het belangrijk dat het C2000 netwerk en randapparatuur goed beveiligd zijn en neemt daarvoor ook maatregelen. De koppeling met het beveiligingsbeleid wordt daarbij niet expliciet gemaakt.
Het gevoel bij de geïnterviewden is dat ook de eindgebruikers die op straat met portofoon en mobilofoon werken zich redelijk bewust zijn van het belang van beveiliging. Ook hier is waarschijnlijk geen expliciete koppeling te maken met het beveiligingsbeleid. "Goed omgaan met je portofoon is vooral een kwestie van persoonlijke veiligheid en veiligheid voor je collega", is een vaak gehoorde uitspraak.
Het feit dat de organisatie als geheel het belang van beveiligingsbeleid niet overal even actief uitdraagt naar de eindgebruikers en het toezichtsinstrumentarium (beveiligingsfunctionaris, audits en rapportages) niet adequaat heeft ingericht maakt dat er een kloof lijkt te bestaan tussen het belang dat op strategisch niveau wordt gehecht aan beveiligingsbeleid en het belang dat er op operationeel niveau aan wordt gehecht.

6.1.2 Risico

In hoeverre de eindgebruikers belang hechten aan de naleving van het beveiligingbeleid kunnen wij op basis van dit onderzoek niet zeggen. Op de naleving van het beveiligingsbeleid wordt niet actief gestuurd en toegezien. Dat heeft tot gevolg dat naleving van het beveiligingsbeleid afhankelijk is van de professionaliteit van de medewerkers. Bij het ontbreken van deze professionaliteit kan dit tot grote risico 's leiden.

6.1.3 Aanbeveling & handelingsperspectief

Maak inzichtelijk in welke mate beveiligingsbewustzijn leeft onder medewerkers. Het adequaat inrichten van het toezichtsinstumentarium (zoals beschreven in § 1.4) is daarvoor een middel. Een startpunt kan een breed onderzoek zijn naar de perceptie bij eindgebruikers van C2000 randapparatuur.

7 Verantwoording onderzoek

7.1 Algemeen

Dit onderzoek is uitgevoerd in overeenstemming met de opdrachtbevestiging (ADR-kenmerk: 2016-0000158830, d.d. 27 september 2016), in opdracht van Programmadirecteur Meldkamer C2000 en 112

7.2 Type onderzoek

Deze onderzoeksopdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (IIA standaarden 2200-2600).

Voor alle duidelijkheid geven wij aan dat dit geen assurance-opdracht is en wij derhalve geen zekerheid verstrekken over het object van onderzoek. Dit houdt in dat geen algehele eindconclusie is geformuleerd. Het is aan de opdrachtgever zelf om op basis van de uitkomsten van ons onderzoek zich een oordeel te vormen.

7.3 Doelstelling en onderzoeksvragen

De doelstelling van dit onderzoek is het verschaffen van inzicht in de naleving van (onderdelen van) het C2000 beveiligingsbeleid, alsmede het verschaffen van inzicht in de perceptie van betrokken partijen over het C2000 beveiligingsbeleid teneinde in de toekomst waar mogelijk verbeteringen te kunnen doorvoeren in het C2000 beveiligingsbeleid en de naleving hiervan.

Bij dit onderzoek staan de volgende onderzoeksvragen centraal:

- Welke bevindingen signaleren wij ten aanzien van de naleving van (onderdelen van) het C2000 beveiligingsbeleid?
- Welke perceptie hebben de betrokken partijen over het C2000 beveiligingsbeleid?

7.4 Object van onderzoek, afbakening en definities

Het object van onderzoek betreft de beveiligingsmaatregelen uit het beveiligingsbeleid C2000 bij een aantal (geselecteerde) partijen. Omdat alle maatregelen van het beveiligingsbeleid te omvangrijk zijn om binnen de gestelde termijn te onderzoeken, is een selectie gemaakt van thema's (onderwerpen) en daarmee samenhangende beveiligingsmaatregelen[2]. De volgende thema's zijn onderzocht:

- Governance van beveiliging
- Configuratie- en cryptobeheer
- Incidentprocedure
- Awareness
- Fysieke beveiliging

In de bijlage is een koppeling gemaakt vanuit deze thema's naar de beveiligingsmaatregelen uit het C2000 Beveiligingsbeleid.

2 Om te komen tot deze selectie zijn gesprekken gevoerd met verschillende functionarissen binnen C2000, dit betreft ondermeer een beleidsmedewerker van VenJ/DGPOL, een beheerder van MDC en de voorzitter en secretaris van het Gemeenschappelijke Gebruikersoverleg C2000.

Naast deze thema's is onderzoek gedaan naar de perceptie van de medewerkers over het C2000 Beveiligingsbeleid. Daarbij is ondermeer ingegaan op de bekendheid en toepasbaarheid van het kader.

De hierboven genoemde thema's zijn onderzocht bij de volgende partijen:

- VenJ als eigenaar en strategisch beheerder
- De beheerder van het C2000 netwerk (MDC)
- De volgende C2000 Gebruikers: De gemeenschappelijke meldkamers, De Nationale Politie, de gemeentelijke brandweer, de regionale ambulance voorziening, de landelijke meldkamer ambulancezorg, en de Koninklijke marechaussee. Voor elk van deze gebruikers geldt dat een of twee onderdelen (bijvoorbeeld twee veiligheidsregio's) zijn onderzocht. Selectie van de gebruikers heeft plaatsgevonden in overleg met de opdrachtgever.

Om focus aan te brengen bij dit onderzoek is er voor gekozen de leveranciers buiten beschouwing te laten en deze in een hierop volgend onderzoek mee te nemen
Dit onderzoek is indicatief en geeft geen oordeel over het algehele beveiligingsniveau en beheer van C2000. Bij dit onderzoek is een selectie aan beveiligingsmaatregelen onderzocht bij een selecte groep van betrokken partijen. Indien wij andere beveiligingsmaatregelen zouden hebben meegenomen en/of andere partijen hadden geselecteerd zouden wij mogelijk tot andere bevindingen komen. Inherent aan een beveiligingsonderzoek is dat een aanvaller met onbeperkte tijd en middelen een grotere kans zal hebben om tekortkomingen in de beveiliging te signaleren (en te misbruiken). Daarnaast spelen de continu voortschrijdende technologische ontwikkelingen en wijzigingen op de C2000 infrastructuur en apparatuur een rol. Daarom blijft een constante alertheid ten aanzien van de beveiliging noodzakelijk.

7.5 Referentiekader

Het referentiekader is een selectie van beveiligingsmaatregelen uit het beveiligingsbeleid C2000 zoals deze op 21 maart 2012 is gepubliceerd in de Staatscourant (NR. 5393).

7.6 Uitgevoerde werkzaamheden

Voor dit onderzoek zijn de volgende werkzaamheden verricht. In afstemming met de opdrachtgever is een selectie gemaakt van thema's (onderwerpen) en daarmee samenhangende beveiligingsmaatregelen. Deze zijn beschreven in 7.4 van dit rapport. Vervolgens is in afstemming met de opdrachtgever ook een selectie gemaakt van C2000 gebruikers.
Voor dit onderzoek zijn vervolgens, op basis van de thema's, interviews gehouden met de in 7.4 beschreven partijen. Tijdens de interviews is, ter onderbouwing van beweringen, aanvullende documentatie opgevraagd. Deze documentatie is na het interview doorgenomen. Van alle interviews zijn gespreksverslagen gemaakt, deze zijn voor hoor- en wederhoor teruggelegd bij de geïnterviewden. Eventuele op- of aanmerking van geïnterviewden zijn verwerkt. Op basis van de interviews en de ontvangen documentatie hebben wij een analyse uitgevoerd die de basis vormt voor deze rapportage.

7.7 Overige bepalingen

De opdrachtgever is eigenaar van de rapportage. Het definitieve rapport is uitsluitend bestemd voor de opdrachtgever.

De ADR is de interne auditdienst van het Rijk. Het rapport over dit onderzoek is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

Gelet op de mogelijke vertrouwelijkheid van de informatie in het rapport inzake specifieke risico's en bevindingen die mogelijk inzicht geven in specifieke kwetsbaarheden in de beveiliging van C2000 betekent dit dat het ministerie van VenJ kan besluiten delen van het rapport of het gehele rapport niet te publiceren.

8 Ondertekening

13 maart 2017

Auditmanager

Bijlage(n)

			Onderzoeksvragen / normen
Nr	Focus	Norm	1. Naleving (selectie van) beveiligingskader. Selectie onderwerpen:
1	**Awareness**	**2.1.3**	Er behoren regels te worden vastgesteld voor aanvaardbaar gebruik van C2000-randapparatuur. Deze gedragsregels bevatten ten minste dat: • C2000-randapparatuur is bestemd voor persoonlijk gebruik • C2000-randapparatuur niet onnodig onbeheerd wordt achtergelaten. • De C2000-randapparatuur voor zakelijk gebruik is en niet bestemd is voor privé doeleinden. • Alle pogingen tot het misbruik van de apparatuur, zoals het (trachten van) herprogrammeren, openbreken en anderszins manipuleren van het apparaat of de (cryptografische) informatie hierin, strikt verboden is. • De instructies van de fabrikant ter bescherming van de apparatuur worden opgevolgd (bijvoorbeeld bescherming legen het blootstellen aan elektromagnetische velden). • De instructies van de beheerder die betrekking hebben op de beveiliging van het C2000- netwerk worden opgevolgd. Verder bevatten de gedragsregels instructies voor eindgebruikers hoe te handelen in het geval van vermissing van C2000-randapparatuur alsmede de regels voortkomend uit het Landelijk Kader Fleetmap.
2	**Awareness**	**2.1.4**	De bovenstaande gedragsregels (2.1.3) zijn gecommuniceerd naar en voor akkoord verklaard door personen bij eerste ontvangst van C2000-randapparatuur. Daarna zijn zij eenvoudig voor deze personen beschikbaar.
3	**Awareness**	**2.1.6**	Alle personen die C2000-randapparatuur gebruiken krijgen geschikte training en regelmatige bijscholing met betrekking tot informatiebeveiliging en procedures van de organisatie.
4	**Configuratie- en cryptobeheer**	**2.2.1.**	Alle beheerde C2000-randapparatuur wordt geregistreerd in een actuele inventaris. Hieruit is inzichtelijk welke randapparaten aan welke functionaris en aan welk voertuig is uitgegeven en in welke gespreksgroepen het randapparaat actief kan zijn.
5	**Configuratie- en cryptobeheer**	**2.1.2.**	De C2000-randapparatuur wordt tenminste één keer per week gecontroleerd op juistheid en volledigheid. Ontbrekende randapparaten dienen onverwijld aan operationeel beveiligingsbeheer te worden gemeld.
6	**Configuratie- en cryptobeheer**	**2.2.2.**	Er wordt geregistreerd welke randapparatuur zich buiten de directe controle van de gebruiker (bijvoorbeeld in het geval van onderhoud, inbouw en reparatie) bevindt.
7	**Configuratie- en cryptobeheer**	**2.2.12**	Slechts C2000 geaccrediteerde randapparatuur mag worden gebruikt. Randapparatuur mag alleen worden aangeschaft van een geaccrediteerde leverancier, met een TEA2 supplier licentie.

8	**Configuratie- en cryptobeheer**	**2.2.14**	Randapparaten die aan een organisatie of persoon worden verstrekt die niet geautoriseerd is voor het gebruik van C2000, zijn uitgeschakeld in het netwerk of bevatten geen geldige cryptosleutel.
9	**Configuratie- en cryptobeheer**	**2.2.16**	Het uitvoeren van cryptografische handelingen aan C2000-randapparatuur (laden/verwijderen van sleutels en het programmeren van C2000-randapparatuur) is in overeenstemming met de instructies, in de Documentatieset Lokaal
10	**Fysieke beveiliging**	**2.1.7 (&2.2.6)**	De (tijdelijk) niet in gebruik zijnde C2000-randapparatuur (i.e. voorraad, defect) is ondergebracht in afgesloten kasten in een beveiligde ruimte(n). Toegang tot deze ruimte is beperkt tot hiervoor bevoegde personen.
11	**Fysieke beveiliging**	**2.2.13**	Er is een procedure aanwezig voor de in- en uitbouw van randapparatuur uit voer-, vaar- en vliegtuigen. In- en uitbouw geschiedt enkel bij geaccrediteerde bedrijven.
12	**Fysieke beveiliging**	**2.3.3**	De apparatuurruimte(n) waarin C2000-systeemapparatuur is ondergebracht (exclusief de radio bedienterminals en -werkplekken) dienen te voldoen aan de eisen gesteld in het document Programma van eisen apparatuurruimtes t.b.v. C2000 radiobediensystemen
13	**Fysieke beveiliging**	**2.2.7.**	De toegang tot de beveiligde ruimte(n) wordt geregistreerd.
14	**Governance**	**2.0.2**	De taken, verantwoordelijkheden en bevoegdheden van werknemers, ingehuurd personeel en externe eindgebruikers ten aanzien van de informatiebeveiliging van C2000 moeten worden vastgesteld en gedocumenteerd.
15	**Governance**	**2.0.3**	Elke gebruiker stelt een C2000-beveiligingsfunctionaris aan, die als centraal aanspreekpunt voor en naar de beheerder en eigenaar fungeert op het gebied van informatiebeveiliging. Deze functionaris geeft tevens uitvoering aan de beveiligingsincidenten- en implementatierapportage naar de beheerder
16	**Governance**	**2.2.5**	Alle C2000-randapparatuur heeft binnen de organisatie een formele eigenaar die managementverantwoordelijkheid heeft voor het gebruik en informatiebeveiliging van de randapparatuur en die optreedt als centraal aanspreekpunt voor de C2000-apparatuur
17	**Governance**	**2.0.4**	De toegangsrechten (zowel logisch als fysiek) van alle werknemers, ingehuurd personeel en externe eindgebruikers tot C2000-voorzieningen worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of wordt na wijziging van zijn/haar taak aangepast.
18	**Governance**	**2.2.10**	De achtergrond van alle lokale beheerders is geverifieerd via een screening equivalent met die voor een Vertrouwensfunctie niveau C, in de zin van de wet Veiligheidsonderzoeken van 10 oktober 1996.
19	**Incidentprocedure**	**2.1.5**	Er is een procedure ingericht die het melden van vermissing, verlies en diefstal van randapparatuur beschrijft. Hierin zijn de contactpersonen en escalatiepaden uitgeschreven. De procedure voorziet in het uitschakelen door de beheerder van vermiste, verloren en gestolen randapparatuur.

			2. Perceptie gebruikers tav beveiligingskader (effectivteit)
25	**Perceptie - Attitude**	**nvt**	Kent u de gedragsregels en de beveiligingsvoorschriften voor het gebruik van C2000 apparatuur en netwerk? (C2000 beveiligingskader)
26	**Perceptie - Attutde**	**nvt**	Ziet u de voordelen van het C2000 beveiligingskader? Welke?
27	**Perceptie - Attutde**	**nvt**	Hoe belangrijk vindt u het deze gedragsregels en beveiligingsvoorschriften na te leven? Welk deel is daarbij voor u het belangrijkst, welke het minst belangrijk?
28	**Perceptie - Subjective norm**	**nvt**	Laten personen in uw omgeving (collega's, leidinggevenden) zien dat ze de gedragsregels en beveiligingsvoorschriften belangrijk vinden? (elkaar aanspreken, voorbeeldgedrag, bespreekbaar maken) Heeft u daarvan voorbeelden?)
29	**Perceptie - Subjective norm**	**nvt**	Is er in praktijk ook aandacht voor het kader? Bijvoorbeeld door presentaties, berichten op intranet, afdelingsbijeenkomsten of bij functioneringsgesprekken?
30	**Perceptie - Subjective norm**		Op welke wijze vindt afstemming / communicatie plaats met andere C2000 organisaties over de naleving van het C2000 beveiligingskader?
31	**Perceptie - Percieved Behavrioural Control**	**nvt**	Bent u in staat de gedragsregels en beveiligingsvoorschriften na te leven? Welke belemmeringen ervaart u hierbij?

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00