3E TERTAALRAPPORTAGE 2022 NCTV

Januari 2023
NCTV - KBV/KS

Inhoud

N.B. Pagina's 2-6, 10 en 13 zijn niet meegenomen want vallen buiten de reikwijdte van de Kamervraag.

3.5 Integrale beveiliging

Informatiebeveiliging is een van de pijlers onder de bedrijfsvoering van de NCTV. Voor de NCTV is het VIR-Bi van toepassing. Voor de aanpak van de centrale sturing en beheersing van de informatiebeveiliging wordt het

De NCTV detecteert het optreden van beveiligingsincidenten op de eigen netwerken. In 2022 is de verdere professionalisering van een eigen Security Information Center (SOC) voorzien dat zal bijdragen aan analyse en respons. Hierbij zal worden samengewerkt met het SOC van JenV.

In samenspraak met SOC JenV is het inkoopproces voor de aanschaf van een nieuwe Siem gestart met een verwachte levering en implementatie in 2023. Verder is logging en monitoring op het eigen NCTV-netwerk verbeterd.

Informatiebeveiliging staat of valt met het veiligheidsbewustzijn van medewerkers. Dit bewustzijn wordt versterkt door het opzetten van campagnes (aansluitend op landelijke, rijksbrede- of departementale campagnes) en door voorlichting bij het introductieprogramma voor nieuwe medewerkers.

Onderstaand de concrete acties en de stand van zaken. De rapportage kritieke systemen is op orde.

Te realiseren resultaten 2022 NCTV Integrale beveiliging	Stand van zaken 2e tertaal 2022	Stand van zaken 3e tertaal 2022
Afronding SRA 2021	De enquête met vragen is voorbereid voor T3.	De enquête is in T3 uitgezet maar nog niet alle resultaten zijn binnen. Het rapport zal in T1 2023 worden opgesteld.
TBB/KWAS rapportage	De enquête met vragen is voorbereid voor T3.	idem
Afronding	Op dit moment nog geen bij de NCTV daar de huidige opzet van het onvoldoende tegemoetkomt aan de beveiligings- en privacyaspecten. De werving van een is gestart. zal ook belast worden met de implementatie van het bij de NCTV.	Op 2-1-2023 is de gestart met als prio het .
BIO rapportages vanuit de	BIO-maatregelen zijn ingevoerd. De beoordeling wordt conform toezegging voor 1 oktober afgerond. Vervolgens zal zonodig gestart worden met de implementatie van maatregelen. Dit zal in een plan met tijdspad worden opgenomen. Verwachting is dat - gelet op capaciteitstekort – dit eind 2023 geheel op orde is (is mede afhankelijk van de eventueel te treffen maatregelen).	We ondervinden problemen met de leverancier en het product om rapportages op te leveren. De te nemen maatregelen zijn wel inzichtelijk.
Rapportage kritieke systemen	Op orde	Op orde
Aansluiting DCC JenV en implementatie beleid	Wachten op doorstart van DCC JenV.	Wachten op doorstart van DCC JenV.

3.6 Informatiehuishouding

3.6.5 Baseline IV

Door uitval van medewerkers is de voortgang in het verbeteren van de compliancy vertraagd. Dit leidt niet tot nieuwe risico's of verhoogd risico.

5. Informatiehuishouding		
a. Baseline Informatiehuishouding Rijksoverheid	T1: De Baseline Informatiehuishouding Rijksoverheid wordt gehanteerd bij het herinrichten van de informatiehuishouding van de NCTV. Dit gaat nog niet overal goed. De BIR wordt in T2 op een aantal onderdelen verder uitgewerkt. Momenteel nog niet volledig compliant T2: In T2 is geen voorgang gerealiseerd. Er is prioriteit gegeven aan afronden schoning, processen in kaart brengen, opleidingsplan en het informatieplan.	Geen specifieke resultaten bereikt. We passen waar mogelijk de regelgeving toe als leidend uitgangspunt. Er is overleg met de architecten J&V om aan te sluiten bij de J&V brede standaarden.

b. Verantwoordelijkheden	In T1 is vastgelegd per kern/programma hoe de informatie wordt verwerkt en opgeslagen en welke systemen daarbij worden gebruikt. Vervolgstappen is in T2 de toegankelijkheid van informatie te verbeteren. T2: Dit wordt meegenomen in de aanpassing van [redacted] en in de [redacted]	In functioneel ontwerp [redacted] zijn autorisaties meegenomen. In procesanalyse [redacted] is gekeken wie wat mag en is dit vastgelegd. Bij het Beleidsdocument zijn de verantwoordelijkheden vastgelegd en is het programma in gesprek met [redacted] wat verdere uitwerking betekent.
[redacted]		
e. Informatieontwerp	T1: Informatieontwerp met geprioriteerde classificatie: Gedeeltelijk compliant Er is een Enterprise Architectuur, echter nog geen geprioriteerde classificatie. In T2 Wordt dit verder opgepakt. T2: Architectuur wordt als onderdeel van 'de processen in kaart brengen' aangepast in de tool. Deze activiteit loopt met de analyse van processen bij 4 afdelingen.	Analyse processen loopt. In T3 is de analyse van de impact voor de [redacted] van de nieuwe grondslagen gestart. Resultaten worden vastgelegd in architectuurplaten. Actie loopt om dit op een manier te doen zodat het daarna ook regulier beheerd kan worden.
f. Informatiesysteem	T1: Gedeeltelijk compliant. Voor niet gerubriceerde informatie wordt gebruik gemaakt van [redacted]. Voor NCTV-applicaties waarin informatie wordt opgeslagen is [redacted] opgeleverd. Informatie moet worden overgebracht van netwerkschijven naar [redacted] In T2 wordt hiermee een begin gemaakt. T2: geen wijzigingen in de status.	Geen wijzigingen.
[redacted]		
6. Informatiebeveiliging	De aansluiting SOC JenV is geëvalueerd en levert geen actiepunten op.	

Ministerie van Justitie en Veiligheid

3e tertaalrapportage 2023 NCTV

N.B. Pagina's 4-17 en 22-26 zijn niet meegenomen want vallen buiten de reikwijdte van de Kamervraag.

Inhoudsopgave

6 Toekomstvaste informatievoorziening

6.1 Vernieuwings/legacy aanpak

Ambitie Jaarplan 2023
De NCTV volgt voor de systemen die door de concerndienstverleners worden geleverd het gevoerde beleid m.b.t. lifecycle management van het kerndepartement.

Voor de *die de NCTV zelf beheerd wordt jaarlijks op basis van het life cycle management proces een (financieel) meerjarenbestedingsplan opgesteld om deze omgevingen actueel te houden. Dit plan wordt in T3 2023 geactualiseerd.*

De toepassingen die NCTV zelf ontwikkelt en beheert, worden continu doorontwikkeld zodat de functionaliteit steeds aansluit bij de werkprocessen. De toepassingen worden tevens gemigreerd naar de meest recente versie van de ontwikkeltool.

Stand van zaken 1e tertaalrapportage 2023
In het eerste tertaal 2023 is gestart met de vervanging van de Security Information Event Monitoring (SIEM) oplossing voor de van de NCTV. Dit zal in T2het tweede tertaal 2023 worden afgerond.
Tevens is in het eerste tertaal 2023 gestart met het gefaseerd vervangen van de . Het implementeren van een Privileged Access Management (PAM) oplossing is in het eerste tertaal 2023 afgerond.

Stand van zaken 2e tertaalrapportage 2023
De vervanging van de Security Information Event Monitoring (SIEM) oplossing voor de eigen systemen van de NCTV is in T2 2023 afgerond. De gefaseerde vervanging van de is in T2 voortgezet en zal in T3 worden afgerond.
In T3 zal een herontwerp van de architectuur van worden gemaakt, welke in 2024 zal worden vervangen. Er zijn diverse voorbereidingen getroffen voor een migratie in T3 2023 naar voor de . Tevens zal een start worden gemaakt met de hardware vervanging van de .

3e tertaalrapportage 2023
De geplande – zoals bij 2e tertaalrapportage 2023 aangegeven – zijn uitgevoerd. De upgrade van het ontwikkelplatform naar de meest recente versie loopt nog en zal in T1 2024 afgerond worden.

6.2 Informatiebeveiliging

Ambitie Jaarplan 2023
Informatiebeveiliging is een van de pijlers onder de bedrijfsvoering van de NCTV.
NCTV rapporteert hierover middels de BIO en gaat in 2023 rapporteren met het nieuwe Informatiebeveiligingsbeeld. Voor de NCTV is het VIR-Bi van toepassing.
Voor de aanpak van de centrale sturing en beheersing van de informatiebeveiliging wordt het gebruikt.

De NCTV zal incidentmanagement verder professionaliseren en het Information Security Management System Governance, Risk and Compliance (ISMS GRC) verder inrichten en verbeteren in samenwerking met . In 2023 zal de Disaster response en het Security Risk Assessment (SRA) verder geoptimaliseerd worden.
De verwachting is dat eind 2023 diverse beleidsdocumenten zijn geactualiseerd.

Informatiebeveiliging staat of valt met het veiligheidsbewustzijn van medewerkers. Dit bewustzijn wordt versterkt door het opzetten van campagnes (aansluitend op landelijke, rijksbrede- of departementale campagnes) en door voorlichting bij het introductieprogramma voor nieuwe medewerkers. Voor eind 2023 verwacht de NCTV een gereed te hebben. Iedere medewerker van de NCTV zal hieraan deelnemen.

Concrete activiteiten:
Tertaal 1:
- *Afronding SRA 2023*
- *TBB/KWAS rapportage*
- *BIO rapportages vanuit de*
- *Informatiebeveiligingsbeeld*

Tertaal 2:
Rapportage kritieke systemen
Aansluiting DCC JenV en implementatie beleid

Tertaal 3:
- *gerealiseerd*
- *Inrichting ism*
- *Alle medewerkers hebben de e-learning Weerbaar JenV gevolgd*
- *Afronding*

Stand van zaken 1e tertaalrapportage 2023
Per 1 januari is een ingehuurd voor ondersteuning op de diverse te behalen projecten/onderdelen van IB. Er is een bijgestelde jaarplanning gemaakt. Ook is extra budget toegekend door voor het wegwerken van achterstallig werk. De werving is gestart.

De werving is gestart, echter ook wij hebben te maken met krapte op de arbeidsmarkt. Niet al de achterstand zal weggewerkt kunnen worden. Dit betekent dat niet alle doelen voor 2023 zullen worden gerealiseerd. Het achterstallig werk betreft beschrijvingen van beleid en producten. Dit heeft geen gevolgen voor de organisatie in die zin dat er toenemende technische risico's op treden.

De afronding van de SRA is niet gelukt in het eerste tertaal, dit is doorgeschoven naar het derde tertaal. Ook de TBB is vertraagd en zal in het tweede tertaal worden afgerond. Helaas is het door een aantal bugs in het systeem niet mogelijk om de BIO-rapportage op te leveren. Er wordt door de leverancier aan gewerkt om dit op te lossen.

Het informatiebeveiligingsbeeld is ingevuld (bijlage). De rapportage over kritieke systemen staat in een van .

Aanvulling nav vragen bij 1e tertaalrapportage.
Vraag: Eerder is aangegeven dat de is aangetrokken met de prioriteit van het en de weerbaarheidstrainingen. Ik lees hier geen voortgang over in T1, liggen jullie nog op schema om dit jaar de cursus aan te bieden en alle medewerkers deze hebben afgerond

Antwoord NCTV: op dit moment worden gesprekken gevoerd met leveranciers (offerte fase). De verwachting is dat alle medewerkers de weerbaarheidstraining niet dit jaar hebben afgerond.

Stand van zaken 2e tertaalrapportage
De werving is afgerond, de externen zijn gestart.

De TBB-inventarisatie is afgerond. Het rapport dient nog worden opgesteld.

De bugs in het zijn nog niet opgelost daardoor is het niet mogelijk de BIO-rapportage op te leveren. Er wordt door de leverancier aan gewerkt om dit op te lossen.

Het informatiebeveiligingsbeeld is ingevuld (bijlage).

Het loopt achter in de doorontwikkeling. Hierdoor is er nog geen strategisch beleid dat door vertaald kan worden door de organisatieonderdelen. De verwachting is dat dit pas in 2024 aangeboden wordt.

De offertes voor het zijn net binnen. De externe ISO is begin september begonnen. De verwachting is dat het inkoopproces verder doorgezet kan worden maar dat de oplevering van het LMS op zijn vroegst pas in Q1 2024 plaats zal vinden. Als gevolg van deze vertraging zullen de weerbaarheidstraining niet dit jaar worden gevolgd.

3e tertaalrapportage 2023

In 2023 is binnen de NCTV een project Informatiebeveiliging gestart met als doel om het weerbaarheidsniveau van de NCTV op het gestelde weerbaarheidsniveau te krijgen. Op dit moment voldoet de NCTV nog niet aan het gestelde ambitieniveau (weerbaarheidsniveau) van 2023. Voor de aanpak van de centrale sturing en beheersing van de informatiebeveiliging wordt het

De afgelopen jaren heeft NCTV in de jaarplannen de ambitie uitgesproken om voor vier domeinen een volwassenheid in het NBA model op niveau vier te behalen. Voor 2024 is de NCTV voornemens onderstaande acties uit te voeren om tot de gestelde weerbaarheidsniveaus te komen:

a) NCTV in 2024 naar een volwassenheid te brengen;
b) De funderende elementen leggen om de overige NBA domeinen in 2024 en 2025 naar te brengen;
c) Inzicht krijgen in de huidige volwassenheid van de overige elf NBA-domeinen;
d) Werken aan de verplichtingen ten aanzien van de BIO waarbij focus is op aantoonbaar risico gebaseerd werken met een werkende PDCA-cyclus aan Informatiebeveiligingsbeleid (H5), Organiseren Informatiebeveiliging (H6), Beveiliging bedrijfsvoering (H12) en leveranciersrelaties (H15).
e) Een PDCA cyclus waarmee niveau voor de vier domeinen in 2025 te behalen.

Het strategisch en tactisch informatiebeveiligingsbeleid en de beleidsregels IB zijn eind 2023 opgesteld en in januari 2024 vastgesteld door het MT NCTV. Hiermee is de basis gelegd om in T1-T2 2024 de IB-producten te maken en te implementeren en om de PDCA-cyclus voor Informatiebeveiliging in werking te krijgen.

Inrichting
De NCTV is sinds 2023 aangesloten bij het JenV-brede traject en afhankelijk van JenV voor verdere ontwikkeling. De verwachte oplevering van het project JenV is 2024. De

technische-, procesmatige en beleidsmatige producten worden daarom in 2024 ontwikkelt, oplevering van de producten is in Q4 2024. De NCTV heeft in Q4 2024 een werkend volledig geïmplementeerd, dit is wel afhankelijk van het JenV-project.

De NCTV was voornemens het in 2023 (tertaal 3) geïmplementeerd te hebben. Helaas is dit wegens recent incident niet gelukt. Hierdoor hebben de medewerkers de verplichte niet uitgevoerd.

Medewerkers krijgen bij indiensttreding een verplichte cursus ‘Veilig werken’, gegeven door de . Daarnaast geeft het cluster van de NCTV jaarlijks een roadshow veilig werken bij iedere afdeling. Deze roadshow is verplicht voor alle medewerkers van de NCTV. Middels deze twee opleidingen op het gebied van weerbaarheid verhoogt de NCTV de (digitale) weerbaarheid van het personeel. Dit is een tijdelijke beheersmaatregel.

In november 2023 is er binnen het managementteam een besluit genomen over te gaan tot implementatie van het . De verwachting is dat het Q4 2024 volledig is geïmplementeerd inclusief het beleid. Het eigenaarschap ligt bij de . In 2025 wordt gestart met het uitvoeren van door alle medewerkers van de NCTV.

Ministerie van Justitie en Veiligheid

2e tertaalrapportage 2024 NCTV

Inhoud

N.B. Pagina 4-6, 9-14, 18-20 en 22-29 zijn verwijderd uit dit document omdat die buiten de reikwijdte van de Kamervraag vallen.

Herzien informatiebeveiligingsbeleid.	De implementatie loopt vertraging op door (1) indien er een knelpunt op de capaciteit ontstaat bij betrokken afdelingen en (2) afhankelijkheid	Indien er niet tijdig geworven kan worden, worden doelstellingen niet (tijdig) gerealiseerd.	Medium	Leiderschap is nodig op alle niveaus om de benodigde capaciteit beschikbaar te maken. Voor andere processen extra capaciteit inhuren.

	van de uitwerking van andere processen (zoals de Wet CoTNV).			

De doorlooptijd van VGB`s is terug op het oude niveau. Op dit moment is de NCTV bezig met het maken van een inhaalslag van de herhaalonderzoeken. De verwachting is dat deze inhaalslag in 2024 is afgerond. Daardoor wordt dit nu niet meer als risico gezien. Bovenstaande risico`s berusten voor een groot deel op capaciteitsproblemen. Dit is nog onverminderd van kracht.

In het najaar 2024 verschijnt naar verwachting het rapport van het onafhankelijk onderzoek dat de ADR in opdracht van de Minister van Justitie en Veiligheid uitvoert bij de NCTV en de politie naar het beveiligen van bijzondere informatie. Aanleiding voor dit onderzoek is de aanhouding van twee (oud-) medewerkers van de NCTV.

In T1 heeft de NCTV een accreditatie verkregen voor her ingebruikname van van de SG, op advies van de Daarbij werkt de NCTV door aan het vernieuwde informatiebeveiligingsbeleid. De ontwikkeling hiervan was al in januari 2023 in gang gezet via de werkgroep digitale weerbaarheid. De uitkomsten van het ADR-rapport zullen worden meegenomen in de verdere doorontwikkeling van het informatiebeveiligingsbeleid- en de uitvoering. Daarnaast is er hard gewerkt aan de onderliggende processen om de informatiebeveiliging van de NCTV op een hoger niveau te krijgen. Dit werk zal in de komende periode worden vervolgd.

Stand van zaken 2e tertaalrapportage 2024

In T2 zijn er geen wijzigingen met betrekking tot de risico`s.
De NCTV werkt uitsluitend met geldende VGB`s. Op dit moment is er nog een klein aantal herhaalonderzoeken welke uitgevoerd worden. Dit maakt de oude VGB`s echter niet minder geldig. De verwachting is dat de inhaalslag eind 2024 is afgerond.

2.3 Cyberweerbaarheid

Ambitie Jaarplan 2024

In 2023 is binnen de NCTV een project gestart met als doel om het weerbaarheidsniveau van de NCTV op het gestelde weerbaarheidsniveau te krijgen.

Het gestelde weerbaarheidsniveau is het niveau van alle te nemen maatregelen bij elkaar (organisatorisch, preventief, detectief, repressief en correctief) om pogingen van kwaadwillende om toegang te krijgen te verhinderen en onbewuste fouten te verminderen. Het gestelde weerbaarheidsniveau dient ook in overeenstemming te zijn met geldende (o.a. BIO) en toekomstige (o.a. NIS) wet- en regelgeving.

Het project levert producten op (informatiebeveiligingsbeleid en informatiebeveiligingsregels) die door NCTV-breed geïmplementeerd moeten worden in de processen en procedures om te komen tot het gestelde weerbaarheidsniveau

Voor de tijdelijke versterking van behoeve van het project Informatiebeveiliging is een aanvraag voor middelen gedaan bij het JenV programma IB 2.0.

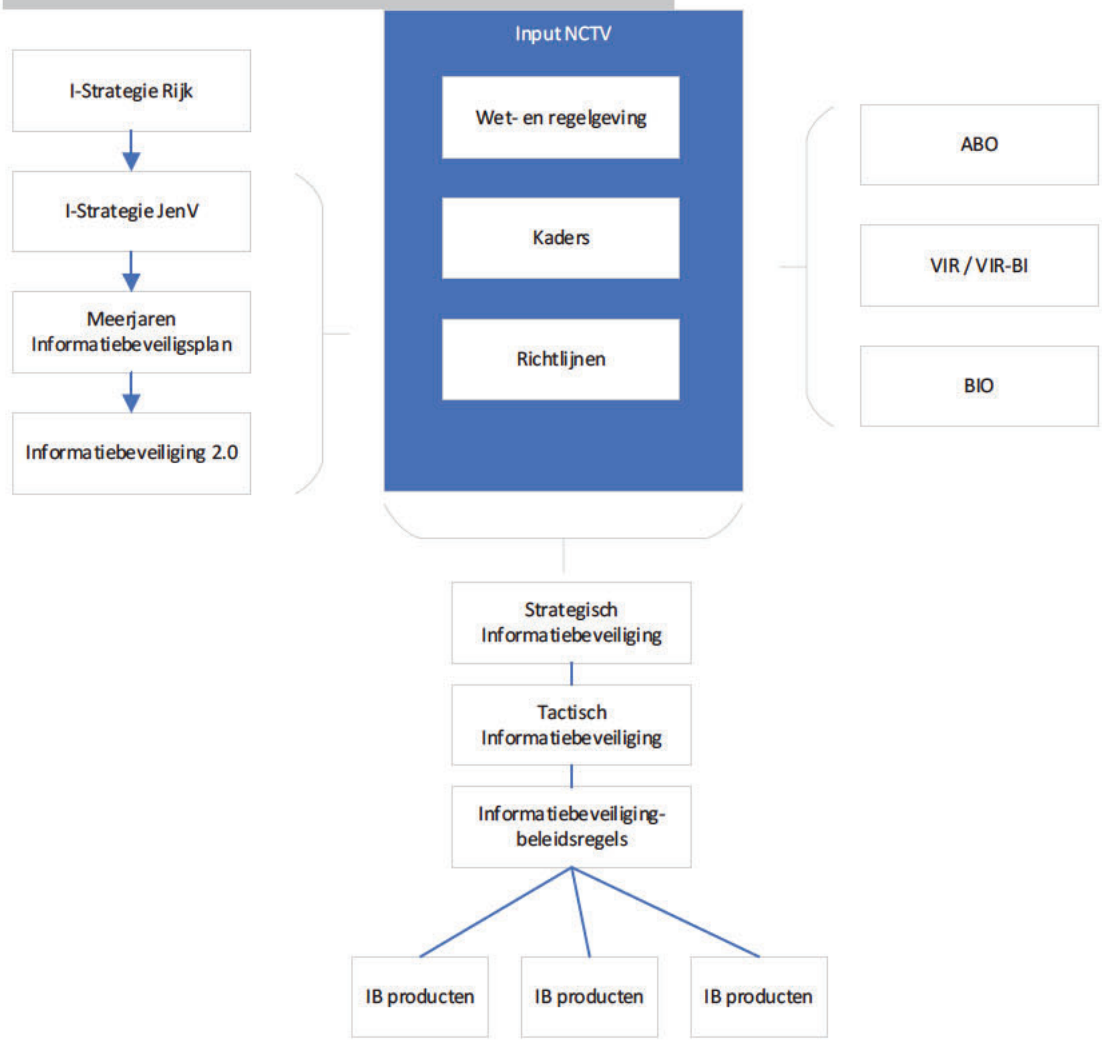
Zie voor een detailplanning de bijlage 2. Informatiebeveiliging

---

Stand van zaken 1e tertaalrapportage 2024

September 2023 is de volledige projectgroep IB 2.0 gestart met 5 externe specialisten informatiebeveiliging. In het laatste tertaal van 2023 is een eerste gap-analyse gedaan op 4 van de 11 domeinen van de i-Strategie JenV. Dit is ook gerapporteerd in de Tertaalrapportage T3 2023.

Daarop is de conclusie getrokken dat een grondige herziening van het beleid op het gebied van informatiebeveiliging noodzakelijk is.



De NCTV gebruikt de uitgangspunten van de i-Strategie JenV, meerjaren IB plan en het programma IB 2.0 en koppelt die aan een toetsingskader dat bestaat uit Algemene Beveiligingseisen Defensie Opdrachten (ABDO), Voorschrift Informatiebeveiliging Rijk – Bijzondere Informatie (VIR-BI) en de Baseline Informatiebeveiliging Overheid (BIO).

Op basis daarvan zijn in T1 2024 de volgende documenten vastgesteld door de NCTV:

- Strategische informatiebeveiligingsbeleid
- Tactische informatiebeveiligingsbeleid
- Informatiebeveiligingsbeleidsregels – dit zijn de 1 op 1 uitwerking van de totale set van maatregelen van het toetsingskader

Om implementatie mogelijk te maken en invulling te geven aan de richtlijn om risico gedreven te werken is het onderstaande door de NCTV vastgesteld:

- Governance Informatiebeveiliging
- Risicomanagement

In het eerste tertaal 2024 is verder gewerkt aan de informatiebeveiligingsproducten, waarin steeds de IB aspecten van een onderwerp worden opgesteld. Na vaststelling worden deze gebruikt voor implementatie in de primaire processen van de afdelingen. Realisatie van alle IB producten staat gepland voor T2 2024. IB producten die zijn

vastgesteld moeten door de afdelingen in hun processen geïmplementeerd worden. Daarvoor is gestart met een implementatieproject dat loopt vanaf T2 2024 tot T1 2025. Elk product wordt vastgelegd in [redacted] en wordt voorzien van een leeswijzer die op Intranet geplaatst wordt.

Zie bijlage 2. Informatiebeveiliging voor een detailplanning

Zie bijlage 3. Informatiebeveiligingsproducten voor een lijst met informatiebeveiligingsproducten.

Stand van zaken 2e tertaalrapportage 2024

In het tweede tertaal lag de nadruk op de afronding van de IB-producten en daarnaast de vraag hoe informatiebeveiligingsproducten geïmplementeerd kunnen en moeten worden bij afdelingen. De IB-producten zijn grotendeels afgerond, het laatste deel moet afgerond worden in T3. Informatiebeveiliging gaat over:

- Mensen / medewerkers en hun rollen, taken en verantwoordelijkheden
- (Primaire) processen
- Bedrijfsmiddelen die nodig zijn binnen de processen

Aspecten van informatiebeveiliging worden als (beleids-)eisen toegevoegd aan de manier waarop er met deze drie onderwerpen wordt omgegaan. Afdelingshoofden zijn als eigenaar verantwoordelijk voor de implementatie van de IB-eisen. Om de implementatie zo effectief en efficiënt te laten verlopen is in het tweede tertaal een implementatieplan gemaakt. In dit plan wordt toegelicht op welke wijze de implementatie van IB-producten zal plaatsvinden en welke planning daarbij aangehouden worden. In plaats van de implementatie van elk afzonderlijk IB-product is gekozen voor een thematische aanpak. Elk thema omvat meerdere IB-producten. Door een thematische aanpak te hanteren wordt de implementatie voor afdelingen begrijpelijk en behapbaar. De vertaalslag van wat er in het beleid staat naar hoe het binnen afdelingsprocessen en -systemen toegepast moet worden, wordt op deze manier eenvoudiger. Ook zorgt de thematische aanpak voor een aanpak waarin de implementatie van verschillende beleidsdocumenten gebundeld wordt.

Bij het maken van het implementatieplan en in het werken met de IB-producten met de afdelingen is de conclusie dat het veel capaciteit vergt om de implementatie uit te voeren. Verminderde capaciteit is een risico dat implementatie kan vertragen. Daarnaast betekent implementatie van de IB-producten tevens een nieuwe werkwijze voor veel afdelingen, wat ook impact op de realisatie kan hebben.

Bij de eerste tertaalrapportage werd aangegeven dat verwacht werd dat [redacted] voor de vier aandachtsgebieden governance, organisatie, risicomanagement en incidentemanagement, dit jaar behaald zal worden. Dit is bijgesteld naar zomer 2025. De verwachting is dat [redacted] later in 2025 wordt behaald voor de vier aandachtsgebieden. [redacted] wordt daarna gezien als stip op de horizon, als ambitie om informatiebeveiliging continu te blijven verbeteren.

2.7 Baseline IV 2023

Ambitie Jaarplan 2024

NCTV heeft onvoldoende in beeld in welke mate wordt voldaan aan alle kaders van de Baseline IV 2023. De planning is dat dit in 2024 in de volle breedte wordt geïnventariseerd, echter is wel afhankelijk of een geschikte kandidaat voor de huidige vacature wordt gevonden. Bij de inventarisatie zal worden bepaald welke achterliggende regelgeving, beleid, voorschriften, kaders, handreikingen e.d. voor de NCTV relevant zijn. De thema's van de Baseline 2023 die betrekking hebben op informatiehuishouding zullen worden geadresseerd in het project Informatiehuishouding (zie ook onder paragraaf 2.6).

Stand van zaken 1e tertaalrapportage 2024

De NCTV heeft nog niet volledig in beeld in welke mate wordt voldaan aan alle kaders van de Baseline IV 2024. Een inventarisatie van de mate van compliance loopt.
Binnen NCTV is in 2023 het project Digitale Weerbaarheid van start gegaan.
In T1 2024 is besloten om een afdeling te vormen die zich richt op het versterken van governance, compliance en risicomanagement volgens het 3-lines model. Ook het programma informatiehuishouding valt onder deze afdeling.
De structuren, kaders en processen die door dit project worden geïnitieerd leiden ertoe dat op meer punten aan de Baseline IV 2024 zal worden voldaan.

Stand van zaken 2e tertaalrapportage 2024

In T1 2024 zijn de voorbereidingen getroffen voor het inrichten van de afdeling Governance, Risk en Compliance (GRC). In T2 is een , en een concept- O&F-rapport opgesteld.
In T2 heeft de voorbereiding plaatsgevonden van het project Digitale Weerbaarheid, dit wordt in T3 gestart. De kaders en richtlijnen vanuit de afdeling GRC en de inrichting van processen door het project Digitale Weerbaarheid zullen ertoe leiden dat in toenemende mate aan de Baseline IV 2024 zal worden voldaan.
In T3 zal worden geïnventariseerd op welke punten de NCTV kan verbeteren in relatie tot de Baseline IV 2024.

Bijlage 2 Informatiebeveiliging NCTV

 # Digitale weerbaarheid

Hieronder wordt ingegaan op de activiteiten die de NCTV komend jaar oppakt met IB-beleid.

De prioritering en planning van de mijlpalen en beheersmaatregelen op NCTV worden mede bepaald door de ontwikkelingen van de aanhouding van de medewerker van de NCTV. Hierdoor kunnen bepaalde producten versneld geïmplementeerd en afgerond worden.

Werkende detectie- en responsediensten op ICT-kwetsbaarheden;(a)

In 2023 is in het kader van het life cycle management een nieuw product ingekocht. Daarbij is gebruik gemaakt van de aanwezige kennis van het security operation centre (SOC) JenV. De technische-, procesmatige en beleidsmatige onderdelen van het nieuwe product worden in 2023 en 2024 ontwikkelt, oplevering van de producten is voorzien in Q4 2024. De NCTV heeft het nieuwe security incident event management SIEM in Q4 2024 volledig geïmplementeerd.

Voor alle derde partijen zijn beleidsregels opgesteld die gebruikt kunnen worden in het toezicht.

Momenteel is het oude SIEM-systeem nog in werking. Het huidige gebruik van dit systeem is niet geborgd in beleid. Ontwikkelen van beleid is in scope bij de implementatie van de nieuwe SIEM.

Werkend identity & access management (IAM) voor toegangsbeheer; (a)

De NCTV is zoals aangegeven in Jaarplan 2023 sinds 2023 aangesloten bij het IAM-project van JenV (centraal project). De verwachte oplevering van het project JenV is 2024. De technische-, procesmatige en beleidsmatige producten worden in 2024 ontwikkeld, oplevering van de producten is in Q4 2024. De NCTV volgt het project IAM van JenV. Binnen dit project is een haalbaarheidsstudie uitgevoerd van de gekozen richting. Dat betekent dat de oplevering van IAM door JenV waarschijnlijk niet in 2024 gerealiseerd gaat worden. Het is in ieder geval zeker dat de NCTV dan niet al in 2024 kan aansluiten maar dat dit in 2025 wordt opgepakt.

Werkend privileged access management (PAM) voor accountbeheer; (a)

Er is technisch al een start gemaakt met de inrichting van een PAM . Parallel is de NCTV gestart met het opstellen van het beleid, proces, RASCI (response, accountable, support, consulted, informed), rapportage en PCDA (plan, do, check, act). Verwachte oplevering van de producten is Q3 2024. De NCTV heeft voor het een volledig operationeel PAM systeem. Voor PAM bij de toepassingen bij de teams wordt PAM een onderdeel van de thema gestuurde implementatie van IB in 2024.

Stand van zaken 2e tertaalrapportage 2024

Voor PAM bij NCTV is, , een beleidsdocument opgesteld en vastgesteld. In het derde tertaal van 2024 start de NCTV met de implementatie van dit beleid als onderdeel van thema “Toegang”.

Beschikken over IT-herstelplannen van kritieke systemen voor business continuïteit; (c)

De huidige IT-herstelplannen worden in 2024 geactualiseerd. De NCTV zoekt daarvoor aansluiting bij het project van JenV in de eerste helft van 2024. Verwachte oplevering is eind Q2 2024 voor het beleid. De planning is dat eind 2024 de implementatie gereed is.

Stand van zaken 2e tertaalrapportage 2024

In eerste tertaal 2025 start NCTV met het opstellen van een business continuity management (BCM) plan. Los daarvan wordt voor het gebruik gemaakt van de expertise van programma IB 2.0 om een IT-herstelplan op te stellen voor het .

Het uitvoeren of herhalen van een red team onderzoek; (a) / (c)

De NCTV maakt gebruik van de ADR voor het laten uitvoeren van (pen)testen. De huidige toegezegde capaciteit bij JenV volstaat niet. De NCTV is in afwachting van ontwikkelingen op dit gebied bij JenV. De NCTV ontwikkeld in 2024 beleid voor het uitvoeren en opstellen van auditrapportages (intern en extern), de beoogde oplevering van de beleidsmatige en procesmatige producten is Q4 2023. Verwachte volledige implementatie is Q4 2024.

Stand van zaken 2e tertaalrapportage 2024

Red Teaming zal pas worden gepland na implementatie van het nieuwe IB-beleid.

Het volgen van opleidingen op het gebied van weerbaarheid van personeel; (b)

Bij indiensttreding wordt de cursus ‘veilig werken’ gegeven door . Deze is verplicht voor alle nieuwe medewerkers. Daarnaast geeft het jaarlijks een roadshow veilig werken bij iedere afdeling. Deze roadshow is verplicht voor alle medewerkers van de NCTV. Middels deze twee opleidingen op het gebied van weerbaarheid verhoogt de NCTV de (digitale) weerbaarheid van het personeel.

Tevens is de NCTV voornemens een te implementeren. Hierover is in november 2023 binnen het managementteam het besluit genomen over te gaan tot implementatie.

Stand van zaken 2e tertaalrapportage 2024

In augustus 2024 is gestart met de technische oplevering van het . Als eerste module wordt de bewustwording Wet CoTNV ontwikkeld, direct gevolgd door bewustwording IB. Het beleidsdocument dat ten grondslag ligt aan bewustwording IB is ontwikkeld en vastgesteld.

Het structureel hebben van inzicht in: (c)

Op basis van de in Q4 2023/Q1 2024 uitgevoerde GAP-analyse door het NCTV-project Digitale weerbaarheid kan worden vastgesteld op welk de organisatie zich bevindt. Op basis van de uitkomsten van deze gap-analyse wordt de uitvoeringsplanning van 2024 vastgesteld.

Stand van zaken 2e tertaalrapportage 2024

Er is voor 2024 en 2025 een implementatieprogramma ontwikkeld om informatiebeveiliging binnen de organisatie te versterken. Dit brengt de NCTV organisatie onder andere tot op de aandachtsgebieden governance, organisatie, risicomanagement en incidentmanagement uit het NBA-LIO Volwassenheidsmodel in zomer 2025. Door borging in de PDCA tijdens uitrol kan later dat jaar later worden bereikt (herhaalbaar).

---

het naleven van de BIO als norm voor de informatiebeveiliging;

Eind 2023 is gestart met de herziening van informatiebeveiligingsbeleid op basis van de Baseline Informatiebeveiliging Overheid (BIO). In januari zijn daarvoor de beleidsdocumenten vastgesteld en vanaf dat moment wordt BIO gebruikt als kader voor alle risico's en maatregelen. De baseline is een niet door de overheid vastgelegd kader. NCTV heeft daarvoor een eigen kader opgesteld. Dat kader wordt vanaf heden gebruikt bij IB onderwerpen.

Stand van zaken 2e tertaalrapportage 2024

Het door de NCTV opgestelde kader is uitgebreid met eisen EU, NAVO, BIO 2.0 en de geplande herziening van VIR-BI (besluit voorschrift informatiebeveiliging rijksdienst-bijzondere informatie) en algemene beveiligingseisen Defensie opdrachten (ABDO) en algemene beveiligingseisen rijksopdrachten (ABRO). Dit complete kader wordt in derde tertaal 2024 vastgesteld.

---

de (grootste) incidenten met inbreuk op de BIO compliance*;*

De NCTV is nog niet volledig 'in control' aangaande BIO-maatregelen. We hebben een BIO-overzicht van de organisatie uit 2021, maar geen actueel overzicht. Daarnaast zijn niet op de BIO-maatregelen getoetst. We hebben geen actueel beeld van de BIO-beheersmaatregelen op de organisatie en systemen.

Stand van zaken 2e tertaalrapportage 2024

De implementatie van informatiebeveiliging zal ervoor zorgen dat de NCTV in control is aangaande compliance aan de BIO.

---

de kritieke en bedrijfskritische systemen;

De NCTV beschikt over kritieke en bedrijf kritische systemen. Deze systemen zijn aangemeld bij de CISO JenV. Afhankelijk van voortgang van het vaststellen van het proces accreditatie door [redacted] is de NCTV voornemens in Q1 2024 te starten met het accrediteren van [redacted]

Naast de inventarisatie van bedrijfskritieke- en kritieke systemen heeft de NCTV werkt de NCTV aan beleid, proces, RASCI, PDCA en rapportage voor deze kritieke systemen. De NCTV zal in Q4 2024 de genoemde producten opleveren, om vervolgens zo spoedig mogelijk het beleid/proces zo volledig mogelijk te implementeren.

de grootste risico's voor beschikbaarheid, integriteit en vertrouwelijkheid van de kritieke systemen.

Middels een Quickscan Informatiebeveiliging (QS-IB) zijn de BIV-aspecten van de kritieke systemen in kaart gebracht. Deze worden drie jaarlijks of bij significante wijzigingen van de functionaliteiten uitgevoerd. Een aantal kritieke systemen behoeven in 2024 een nieuwe QS-IB. Er is een backlog voor het uitvoeren van QS-IB maar door een nieuwe methode kan die achterstand worden ingelopen in T3.

Risicobeheer is ingericht en de eerste risicoanalyses hebben geleid tot het instellen van een risicoregister. Er is een opzet voor behandelplannen voor alle risico's die binnen acceptatieniveau vallen die door risico eigenaren moet worden gebruikt en waarop toezicht wordt gehouden.

Stand van zaken 2e tertaalrapportage 2024

Door een gecomprimeerde QS-IB en risicoanalyse kan de achterstand in de uitvoering van quickscans worden weggewerkt.

Het (doen) uitvoeren van een volwassenheidsmeting van het SOC; (c) / (a)

Middels VIR (besluit voorschrift informatiebeveiliging rijksdienst) en VIR-BI. NCTV voert jaarlijks interne securitytesten uit op [redacted]. Beleidsmatig wordt dit voor Q4 2024 vastgelegd middels intern auditbeleid. In 2024 is de security test uitgevoerd op basis van het nieuwe NCTV kader.

Aansluiten op de [redacted]. (a) / (c) Onbekend

De NCTV maakt deel uit van de JenV projectorganisatie die de implementatie van [redacted] begeleidt. Daarmee is geborgd dat de NCTV alle stappen doorloopt om aan te kunnen sluiten op het [redacted]

Integrale Beveiliging
De NCTV voert ondanks druk op de bezetting en hoge werkdruk, de noodzakelijke processen uit om de integrale veiligheid van de organisatie te waarborgen. Hierbij heeft door de toenemende digitalisering en complexiteit, informatiebeveiliging lange tijd prioriteit gekregen. Mede door de werving van een extra medewerker kunnen we vanaf T2/T3 2024 meer aandacht geven aan de integrale beveiliging.

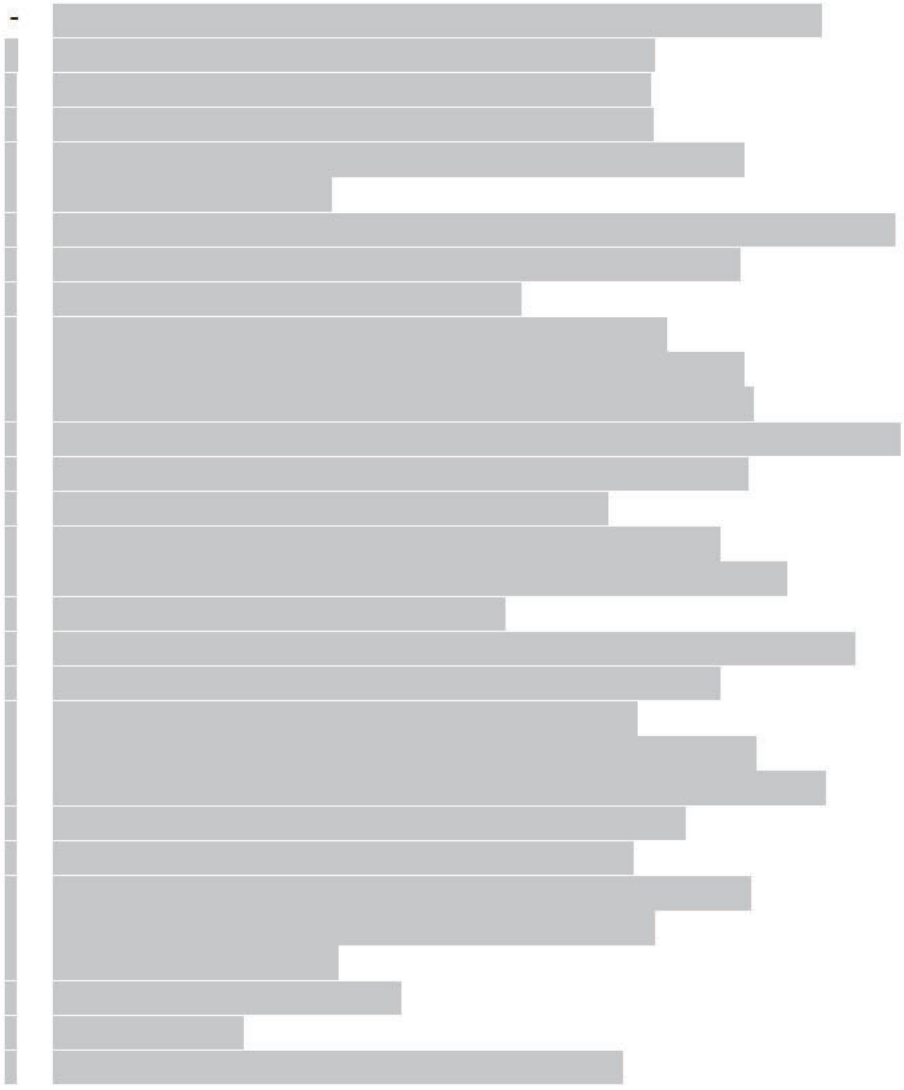
De NCTV beschikt over veel documentatie over integrale beveiliging, dit moet geactualiseerd worden. De NCTV is daarom voornemens het beleid en processen van integrale beveiliging in T2 en T3 2024 te vernieuwen en waar nodig te verbeteren. Dit hoopt de NCTV te doen middels ingehuurde capaciteit.

Binnen dit project wordt de jaarlijkse drie-fasen-toezichtcyclus (SRA, TBB en implementatieplan) opnieuw opgepakt en wordt het proces verder uitgeschreven en geïmplementeerd. Binnen dit project zal eerst een GAP-analyse uitgevoerd worden met de geldende wet- en regelgeving en normenkaders van JenV.

Bijlage 3 Informatiebeveiligingsproducten NCTV

Hierbij een lijst met producten waar aan wordt gewerkt (willekeurige volgorde):

-



Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~DEP. VERTROUWELIJK~~

ICV BIR NCTV 2015

Datum	21 januari 2016
Status	Concept

Colofon

Afzendgegevens	[redacted]
	Turfmarkt 147 2511 DP Den Haag Postbus 16950 2500 BZ Den Haag www.nctv.nl
Contactpersoon	[redacted]
	T [redacted]
Projectnaam	Beveiliging
Ons kenmerk	-
Auteurs	[redacted]

Inhoud

1 Inleiding

1.1 VIR

Het Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007) vraagt van elk DG een in control verklaring (ICV) wat betreft informatiebeveiliging. Dit geschiedt op basis van het BIR-ICV model 2015. Hierin verklaart het management van de NCTV, aan de hand van de BIR, dat zij 'in control' zijn als het gaat om informatiebeveiliging.

1.2 Leeswijzer

Deze nota levert een overzicht van de status van de implementatie van de BIR bij de NCTV per eind 2015 voor de kritieke ICT-systemen als vervolg op het overzicht van 2014.

Allereerst is in de 'In Control Verklaring' aangegeven wat de belangrijkste risico's van de NCTV zijn door het nog niet operationeel zijn van enkele BIR-maatregelen. De opzet van het bijbehorend managementsysteem wordt nader toegelicht met een overzicht van taken van de NCTV, de te Beschermen Belangen van de NCTV en de kritieke informatiesystemen die de NCTV zelf beheert.
Als laatste wordt een update gegeven van de GAP-analyse BIR waarin een overzicht van de status van de BIR-maatregelen per einde 2015 is opgenomen. In bijlage A staan de openstaande maatregelen met degene die verantwoordelijk is voor invoering hiervan met de geplande einddatum.

2 Inleiding

De NCTV verklaart dat over 2015:

De NCTV in control is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007). Dit houdt het volgende in:

De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee in voldoende mate op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd.
De implementatie van maatregelen is gebaseerd op de Baseline Informatie-beveiliging Rijksdienst (BIR:2012);
De interne beheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 / BIR 2012 en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's. Deze risico's zijn van zodanig belang dat ze worden opgenomen in de bedrijfsvoeringmededeling van de NCTV.

De belangrijkste (hoge) risico's die daarbij nog worden onderkend zijn:

- [redacted]

Voor de uitvoering van haar taken gebruikt de NCTV de volgende kritieke informatiesystemen:

- [redacted]

Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse.

Naast deze systemen maakt de NCTV gebruik van diverse standaard applicaties op het VenJ-net dat gebruik maakt van de Haagse Ring. Deze generieke diensten voor infrastructuur, kantoorautomatisering en ICT systeembeheer vallen buiten de scope van deze ICV omdat ze onder de verantwoordelijkheid vallen van BZK. De NCTV

gaat er van uit dat zowel het VenJ-net als de Haagse Ring voldoen aan de BIR en dat de daarin opgeslagen TBB's van de NCTV adequaat zijn beveiligd.

Het MT NCTV heeft de GAP-analyse BIR over 2014 met bijbehorende risico's en het beveiligingsplan voor 2015 vastgesteld. De voortgang van dit jaarplan wordt periodiek besproken met het [redacted] en bijgesteld indien nodig.
Om de jaarlijkse PDCA-cyclus te kunnen uitvoeren heeft het MT NCTV het plan van aanpak voor de 'controle interne risicobeheersing 2015' vastgesteld. Maandelijks stelt de [redacted] een managementrapportage op waarin wordt gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten.

De belangrijkste resultaten die de NCTV in het kader van de BIR in 2015 heeft behaald, zijn:

- Uitvoeren Quick scan BIR voor de volgende informatiesystemen met (indien nodig) een aanvullende risicoanalyse:
  - [redacted]
- Benoemen van systeemeigenaren met taken en bevoegdheden. Deze systeemeigenaren hebben bovenstaande quick scans BIR vastgesteld.
- Vaststellen en testen van het continuïteitsplan NCTV.
- Implementeren van een beveiligde uitwijkvoorziening voor het [redacted] van het NCSC bij [redacted]
- Implementeren van logging en monitoring in het [redacted] en [redacted] gekoppeld aan een SIEM.
- Opstellen van ICT-beheerprocedures waaronder patchmanagement, back-up en restore procedure, meldingenbeheer.
- Verhelpen van kwetsbaarheden die de ADR heeft geconstateerd in de externe websites van de NCTV.
- Quick win: Instructie medewerkers [redacted] en aanpassing van de internet-koppeling van [redacted] 'anoniem' met een 'standaard' browserprofiel om te voorkomen dat medewerkers herleidbare sporen achterlaten op internet.
- Beschrijven, vaststellen en uitvoeren van diverse processen bij de afdeling [redacted] waaronder indiensttreding en uitdiensttreding van medewerkers.
- Diverse workshops om het beveiligingsbewustzijn van de medewerkers te bevorderen.
- Controle op het autorisatiebeleid wordt periodiek voorgelegd aan de lijnmanagers (eigenaren/verantwoordelijken)
- Aanbrengen anti-inkijkfolie in vergaderzalen NCTV.

Ondertekening NCTV

[redacted]

Drs. H.W.M. Schoof, NCTV

3 TBB NCTV

3.1 Missie NCTV

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is binnen de Rijksoverheid dé organisatie die verantwoordelijk is voor terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing. Samen met partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland. De focus ligt op voorkomen en beperken van maatschappelijke ontwrichting.

3.2 Taken NCTV

De NCTV heeft de volgende taken:

- Het identificeren en duiden van dreigingen en risico's;
- Het bewaken en beveiligen van personen, objecten, diensten en evenementen;
- Het (doen) verhogen van cyber security;
- Het (doen) verhogen van de weerbaarheid van vitale sectoren, burgers, bedrijven, structuren en netwerken;
- Het realiseren van optimale crisisbeheersing en crisiscommunicatie.

3.3 Kritieke informatiesystemen NCTV

Voor uitvoering van bovenstaande taken gebruikt de NCTV de volgende kritieke informatiesystemen:

- [redacted]

De NCTV is een netwerkorganisatie met een coördinerende taak. De kritieke informatiesystemen maken geen deel uit van een keten.

3.4 TBB NCTV

Te beschermen belangen (TBB) zijn de belangen die door de NCTV worden beschermd omdat compromittering hiervan de primaire processen kan aantasten.

[redacted]

Voor bovenstaande TBB zijn de kritieke informatiesystemen van de NCTV van belang. Naast deze kritieke informatiesystemen maakt de NCTV voor opslag van TBB gebruik van diverse standaard applicaties op het VenJ-net.

4 Status BIR maatregelen

4.1 IB thema's

4.1.1 PDCA cyclus

Voor de kritieke informatiesystemen bij de NCTV bestaat een actuele risicoafweging (niet ouder dan 3 jaar).

In 2014 is een quick scan BIR uitgevoerd aangevuld met een risicoanalyse op [redacted] Deze risicoanalyses zijn in 2015 vastgesteld door de systeemeigenaar. De maatregelen die in deze risicoanalyses zijn benoemd worden ingevoerd met de upgrade naar [redacted] en zullen gereed zijn in Q1 van 2016.

In 2015 is een quick scan BIR uitgevoerd op het anoniem [redacted] en het [redacted] Ook deze risicoanalyses zijn vastgesteld door de systeemeigenaar. De quick wins in [redacted] zijn in 2015 ingevoerd, de aanvullende maatregelen worden met de upgrade naar [redacted] ingevoerd in 2016.

Tevens heeft de NCTV in 2015 een self assessment uitgevoerd in het kader van de KWAS. De benoemde risico's zijn opgenomen in het risicoregister KWAS.

De NCTV heeft een plan van aanpak voor de 'controle interne risicobeheersing 2015' vastgesteld om de effectiviteit van de integrale risicobeheersing te controleren.

Maandelijks stelt de [redacted] een managementrapportage op waarin wordt gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten en verbeterpunten.

4.1.2 Beveiliging externe koppelvlakken

De NCTV heeft meer dan 30 websites met een extern koppelvlak naar het internet. Om na te gaan of de websites kwetsbaarheden vertonen heeft de ADR pentesten uitgevoerd op een groot deel van deze websites. De geconstateerde kwetsbaarheden zijn verholpen.
In het verleden zijn de externe koppelvlakken van de NCTV getest. In 2016 worden de externe koppelvlakken van de NCTV-netwerken weer onderworpen aan een pentest.

4.1.3 Patchmanagement

In 2015 is een gecombineerde procedure voor patchmanagement opgesteld voor alle netwerken binnen de NCTV. Deze procedure is vastgesteld door hoofd bedrijfsvoering.

4.1.4 Beheer van medewerkers en toegang

De afdeling [redacted] heeft het indiensttreding- en uitdiensttreding proces van medewerkers beschreven, vastgesteld en ingevoerd. Daarnaast zijn autorisatiematrices goedgekeurd. In 2016 wordt het verouderde autorisatiesysteem in het [redacted] vervangen. De controle op het autorisatiebeleid wordt periodiek voorgelegd aan de lijnmanagers (eigenaren/verantwoordelijken).

[redacted]

3 [redacted]

4 [redacted]

4.1.5 *Logging en monitoring*

In 2015 is logging en monitoring in het [redacted] geïmplementeerd. Eind 2015 zijn hiervan de eerste resultaten beschikbaar gekomen. In 2015 is een start gemaakt met logging en monitoring van het [redacted]. In 2016 wordt de logging in het [redacted] gekoppeld aan een SIEM.

4.2 Resultaten GAP-analyse

Ook is in 2015 een aanvullende GAP-analyse BIR uitgevoerd. In deze GAP-analyse is nagegaan in welke mate een BIR-maatregel is ingevoerd voor de kritieke informatiesystemen van de NCTV.

4.2.1 *Scope GAP-analyse*

De BIR is opgedeeld in 11 hoofdstukken met totaal ongeveer 240 maatregelen.

De GAP-analyse uit 2014 was gericht op de volgende 3 onderdelen waar de NCTV zelf verantwoordelijk voor is:

1. Organisatorische en fysieke maatregelen die NCTV-breed zijn ingericht in het kader van informatiebeveiliging (hoofdstuk 5 t/m 9 en 13 t/m 15 van de BIR met ca. 105 maatregelen);
2. ICT-basis beveiligingsmaatregelen die zijn ingericht voor beveiliging van informatie op het [redacted], met name in de bedrijfskritieke systemen [redacted] (hoofdstuk 10 t/m 12 van de BIR met ca. 135 maatregelen) en [redacted];
3. ICT-basis beveiligingsmaatregelen die zijn ingericht voor beveiliging van informatie op het [redacted] (hoofdstuk 10 t/m 12 van de BIR).

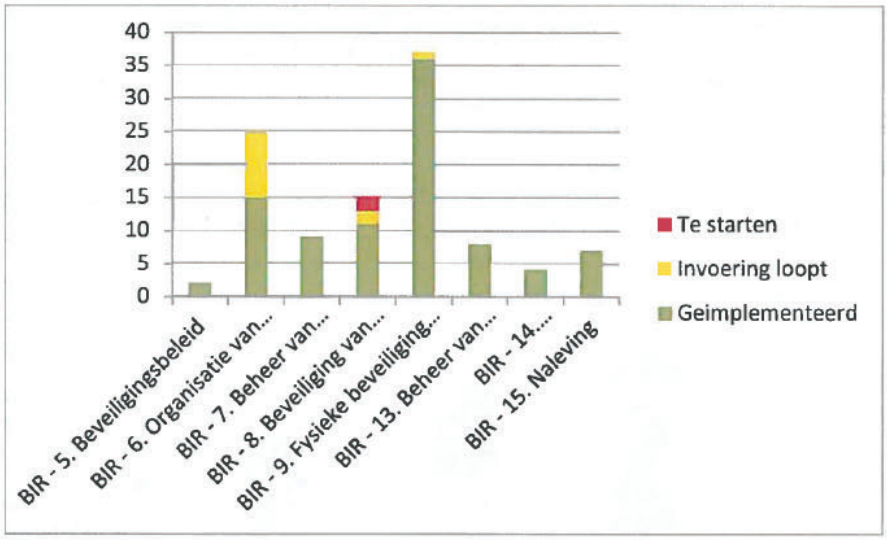
4.2.2 *Status informatiebeveiliging 2015*

4.2.2.1 Status organisatorische en fysieke maatregelen NCTV

In 2015 heeft het MT in het kader van het BIR-project diverse beleidsdocumenten en procedures vastgesteld waarmee een aantal basisbeveiligingsmaatregelen uit de BIR is geïmplementeerd.
Dit zijn onder andere:

- Opstellen en testen continuïteitsplan NCTV
- Invoeren van diverse processen bij de afdeling [redacted] waaronder indiensttreding en uitdiensttreding van medewerkers.
- Diverse workshops om het beveiligingsbewustzijn van de medewerkers te bevorderen.

In onderstaand overzicht is de status van de organisatorische en fysieke beveiligingsmaatregelen weergegeven.



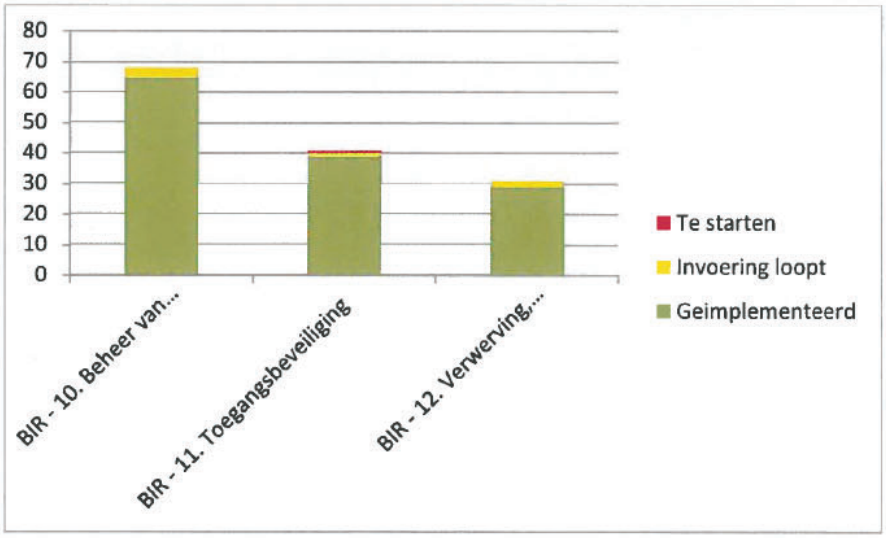
Per eind december 2015 is ongeveer 91% van de organisatorische en fysieke beveiligingsmaatregelen geïmplementeerd bij de NCTV, de implementatie van 7% loopt nog en de implementatie van 2% moet nog starten.

Twee maatregelen om informatiebeveiliging op te nemen in de functieomschrijving van NCTV-medewerkers (BIR eis 8.1.1.1 en 8.1.1.3) zullen in 2016 starten in samenhang met de evaluatie van het O&F-rapport.

4.2.3 Status ICT-beveiligingsmaatregelen

4.2.3.1 [redacted]

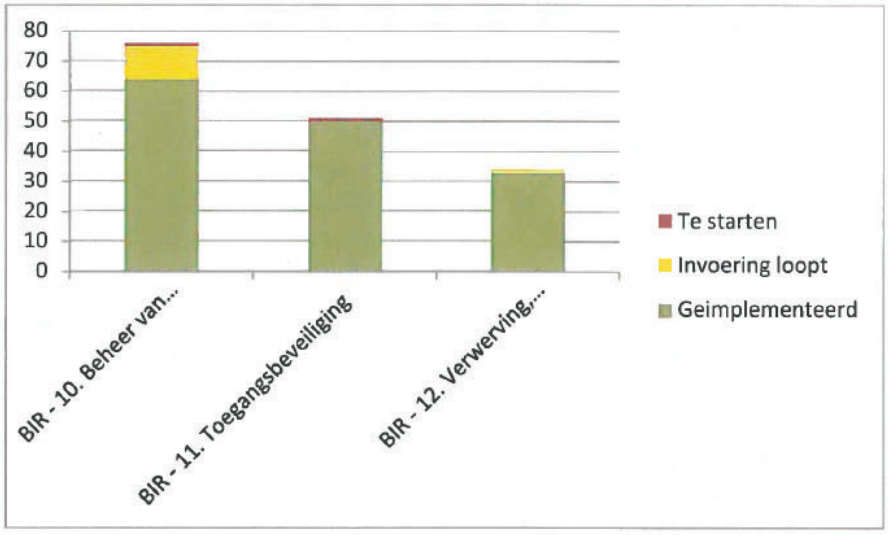
In onderstaand overzicht is de status van de ICT-beveiligingsmaatregelen die van toepassing zijn voor het [redacted] weergegeven.



Per eind december 2015 is ongeveer 93% van de ICT-beveiligingsmaatregelen geïmplementeerd bij de NCTV, de implementatie van 6% loopt nog. Eén maatregel is niet gestart omdat invoering hiervan in het [redacted] niet mogelijk is en het bijbehorend risico laag is.

4.2.3.2 [redacted]

In onderstaand overzicht is de status van de ICT-beveiligingsmaatregelen die van toepassing zijn voor het [redacted] weergegeven.



Per eind december 2015 is ongeveer 91% van de ICT-beveiligingsmaatregelen geïmplementeerd bij de NCTV, de implementatie van 8% is gestart en één maatregel moet nog starten. Eén maatregel is niet gestart omdat invoering hiervan in het [redacted] niet mogelijk is en het bijbehorend risico laag is.

De belangrijkste ICT-maatregelen die in 2016 moeten worden ingevoerd in het [redacted] zijn:

- Verdere inrichten logging en monitoring van het netwerk en applicaties en deze logging koppelen aan een Security Incident en Event Managementsysteem (SIEM door ICT-beheer [redacted]).

Bijlage A

1. **Explainformulieren organisatorische en fysieke maatregelen NCTV**

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
6.1.4.1	Er is een goedkeuringsproces voor nieuwe IT voorzieningen en wijzigingen in IT voorzieningen.	Gestart	Middel	**Risico:** Door het ontbreken van deze maatregel bestaat het risico dat binnen de NCTV nieuwe informatiesystemen worden geïnitieerd zonder afstemming met de [redacted] office en daardoor gekozen wordt voor een voor de NCTV suboptimale oplossing. Bovendien bestaat het risico dat vooraf onvoldoende is nagedacht over de vereiste beveiligingsmaatregelen in het informatiesysteem.	MT NCTV heeft een besluit genomen dat voorstellen voor nieuwe informatiesystemen en i-gerelateerde projecten moeten worden voorgelegd aan het [redacted] en pas in het MT kunnen worden behandeld als de [redacted] er een advies over heeft uitgebracht. In 2016 wordt deze procedure verder geborgd in de organisatie.	[redacted] ism Senior adviseur [redacted]		Q4 2106
6.2.1.6	Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de	Gestart	Middel	**Risico:** [redacted] p	[redacted]	[redacted]		[redacted]

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.							
6.2.3 6.2.3.1 t/m 6.2.3.8	Beveiliging behandelen in overeenkomsten met een derde partij In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.	Gestart	Hoog			systeem-eigenaar in overleg met [redacted] en eventueel diensten-centrum		Q2 2016

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
7.1.2.1	Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.							
8.1.1.1	De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving (zie ook de Ambtenarenwet) en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan: • uitvoering van het informatiebeveiligingsbeleid • bescherming van bedrijfsmiddelen • rapportage van beveiligingsincidenten		Laag	In de functiebeschrijvingen wordt niet expliciet aandacht geschonken aan informatiebeveiliging, maar in de bewustwording-campagnes wordt hieraan wel aandacht besteed. **Risico:** Indien medewerkers niet formeel op de hoogte zijn van hun plichten en de procedures kunnen ze zich daaraan onttrekken of van mening zijn dat ze daar niet op aangesproken kunnen worden. Dit actiepunt is opgenomen in brief aan OR (d.d. 22/10/2015) van zaken die bij evaluatie van het O&F-rapport aan de orde moeten komen.	Dit actiepunt is opgenomen in brief aan OR (d.d. 22/10/2015) van zaken die bij evaluatie van het O&F-rapport aan de orde moeten komen. Verder in overleg met de P-adviseur en de projectleider O&F evaluatie bezien		Q4 2015	Q2-2016

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
8.1.1.3	(R) Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.		Midden	**Risico**: indien medewerkers niet op de hoogte zijn van de verantwoordelijkheden kunnen ze door fouten gerubriceerde informatie lekken.	Dit actiepunt is opgenomen in brief aan OR (d.d. 22/10/2015) van zaken die bij evaluatie van het O&F-rapport aan de orde moeten komen. Verder in overleg met de P-adviseur en de projectleider O&F evaluatie bezien		Q4 2015	Q2-2016
8.2.1.1	Het lijnmanagement heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van rijksambtenaren en ingehuurd personeel (die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.	Gestart	Midden	Zie P-visie NCTV. **Risico** is dat door vertrek van enkele externe medewerkers alle beveiligingskennis verdwijnt. Dit risico is midden omdat in geval van nood de NCTV kan terugvallen op de expertise van de	Strategie voor behouden van kennis en vaardigheden van NCTV is opgenomen in HRM-plan 2016, tevens bezig te bezien hoe bij afdeling bedrijfsvoering kennis kan worden geborgd		Q2-2015	Q4 2016
8.3.1.3	Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het	Gestart	Midden	**Risico**: door het niet correct toekennen en intrekken van autorisaties kan stapeling van autorisaties ontstaan waardoor need to know en functiescheiding in geding	Processen voor indienst-, uitdiensttreding en verandering van functie zijn gedefinieerd. Deze verder in laten opnemen.			Q2 2016

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.			kan komen. Bovendien is gestart met een periodieke controle van autorisaties.				
9.1.2.8	(R) Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	Gestart	Hoog	[redacted]	[redacted]	iom [redacted] en [redacted]	01-04-2014	Q2-2016
10.8.2.1	Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid, waaronder traceerbaarheid en	Gestart	Midden	**Risico:** de externe partij gaat onzorgvuldig om met de door de NCTV aangeleverde informatie waardoor deze kan lekken.	Afspraken over uitwisseling van gegevens met ketenpartijen via [redacted] en fileshareportal zijn vastgelegd; afspraken met bijv. [redacted]	Lijnmanager		Q2 2016

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	onweerlegbaarheid, van gegevens te waarborgen zijn beschreven en getoetst.				[redacted] worden opgesteld			
10.8.2.3	Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd.				Systeemeigenaren zijn benoemd			
14.1.1.1	(R) Calamiteitenplannen worden gebruikt in de jaarlijkse bewustwording-, training- en testactiviteiten.				Zie continuïteitsplan NCTV			
14.1.2.1	Er is een Business Impact Analyse (BIA) waarin de gebeurtenissen worden geïdentificeerd die kunnen leiden tot discontinuïteit in het bedrijfsproces. Aan de hand van een risicoanalyse zijn de waarschijnlijkheid en de gevolgen van de discontinuïteit in kaart gebracht in termen van tijd, schade en herstelperiode.				Zie continuïteitsplan NCTV			
14.1.3.1	In de continuïteitsplannen wordt minimaal aandacht				Zie continuïteitsplan NCTV			

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	besteed aan: • Identificatie van essentiële procedures voor bedrijfscontinuïteit. • Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie). • Prioriteiten en volgorde van herstel en reconstructie. • Documentatie van systemen en processen. • Kennis en kundigheid van personeel om de processen weer op te starten.							
14.1.5.1	(R) Er worden minimaal jaarlijks oefeningen en testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.				Zie continuïteitsplan NCTV			

2. Explainformulieren ICT-maatregelen Stg-net met ZOT en NEO

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
10.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: • het administreren van significante wijzigingen • impactanalyse van mogelijke gevolgen van de wijzigingen • goedkeuringsprocedure voor wijzigingen	Gestart	Midden	**Risico:** Door ontbreken van de procedure kan de informatievoorziening uitvallen	Procedure opnemen in	Senior adviseur		Q1 2016
10.4.1.5	Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.							
10.5.1.1	Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.	Gestart	Midden	**Risico:** Door ontbreken van geteste restore procedure kan de informatievoor-ziening niet tijdig worden hersteld of kan dataverlies optreden	Procedure restore en recovery is opgesteld en moet nog worden getest	Senior adviseur		Q1 2016
10.6.1.1	Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of							

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.							
10.10.1 t/m 10.10.5	Aanmaken en beschermen logbestanden en controle systeemgebruik							
11.4.5.4	(R) Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.							
11.4.5.5	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).	Gestart	Laag	**Risico:** Niet gebruikte services die default zijn ingeschakeld bij installatie kunnen door een kwaadwillende worden misbruikt. Aangezien het [redacted]: geen informatie naar het internet kan sturen is het risico laag	Niet gebruikte services voor zover mogelijk uitschakelen met update van [redacted]	Coördinator [redacted]		Q2 2016
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of		Laag	**EXPLAIN:** deze functionaliteit is niet ingebouwd in het [redacted], Gezien het feit dat de gebruiker in moet loggen met een [redacted]	**Geen actie** Gezien het feit dat de medewerkers in moeten loggen met een [redacted] is de kans dat een account succesvol kan worden misbruikt laag en **het risico** van het	Geen		

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	misbruik van het systeem.			wordt dit **risico** laag geschat.	ontbreken dan deze maatregel ook laag.			
12.1.1.1	In projecten worden een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.							
12.4.1.3	Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.	Gestart	Laag	**Risico:** geen correct overzicht van geïnstalleerde programmatuur met corresponderende licenties en documentatie	De apparatuur is al opgenomen in een CMDB, contract en licentiemanagement inrichten	Senior adviseur		Q2 2016
12.5.1.1	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL .	Gestart	Midden	**Risico:** het met applicaties kan uitvallen of gecompromitteerd worden door ongeautoriseerde wijzigingen	Het wijzigingsproces wordt in 2016 geoptimaliseerd	Coördinator		Q2 2016

2. Explainformulieren ICT-maatregelen CERT-netwerk

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
10.1.2.2	(R) Instellingen van informatiebeveiligingsfunctie s (b.v. security software) op het koppelvlak tussen vertrouwde en onvertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.	gestart	Midden	**Risico:** niet (tijdig) signaleren verstoringen en/of beveiligingsissues	Project Monitoring en logging met een SIEM inrichten volgens Plan van Aanpak			Q4 2015
10.2.2.2	De in dienstverlenings-contracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld met audits of rapportages en gebeurt minimaal eens per drie maanden.			Nvt voor het				
10.4.1.5	Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.	Gestart	Midden	Back-up aanwezig, recoveryprocedure moet nog worden aangepast.	Procedure restore en recovery is opgesteld en moet nog worden getest			Q2 2016
10.6.1.1	Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld	Gestart	Hoog		Project Monitoring en logging inrichten volgens Plan van Aanpak			Q4 2016

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.							
10.6.1.4	Er zijn procedures voor beheer van apparatuur op afstand.	Gestart	Midden	Procedure beheer uitwijk ontbreekt. **Risico:** de uitwijkvoorziening van het [redacted] valt uit door beheerfouten.	Procedure beheer uitwijk opstellen als onderdeel van uitwijk project	[redacted]		Q2 2016
10.10.1 t/m 10.10.5	Aanmaken en beschermen logbestanden en controle systeemgebruik	Gestart	Hoog	[redacted] niet tijdig kunnen signaleren van een verstoring / aanval en correctieve actie kunnen nemen	Project Monitoring en logging met een SIEM inrichten volgens Plan van Aanpak	[redacted]		Q4 2016
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.		Laag	**EXPLAIN:** deze functionaliteit is niet ingebouwd in het [redacted] Gezien het feit dat de gebruiker in moet loggen met een persoonlijk wachtwoord en token wordt dit **risico** laag geschat.	**Geen actie** Gezien het feit dat de medewerkers in moeten loggen met een [redacted] is de kans dat een account succesvol kan worden misbruikt laag en **het risico** van het ontbreken dan deze maatregel ook laag.	Geen		
11.6.1.2	(R) Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.							

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
12.5.1.1	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices zoals ITIL .	Gestart	Midden	**Risico:** het [redacted] met applicaties kan uitvallen of gecompromitteerd worden door ongeautoriseerde wijzigingen	Het wijzigingsproces wordt in 2016 geoptimaliseerd	[redacted]		Q2 2016
12.4.1.3	Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.			Software, configuraties en documentatie [redacted] wordt geregistreerd in [redacted]				

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~DEP. VERTROUWELIJK~~

ICV BIR NCTV 2016

Datum	18 januari 2017
Status	Definitief

Colofon

Afzendgegevens	[redacted]
	Turfmarkt 147 2511 DP Den Haag Postbus 16950 2500 BZ Den Haag www.nctv.nl
Contactpersoon	[redacted]
	T [redacted]
Projectnaam	Beveiliging
Ons kenmerk	-
Auteurs	[redacted]

Inhoud

1 Inleiding

1.1 VIR

Het Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007) vraagt van elk DG een in control verklaring (ICV) wat betreft informatiebeveiliging. Dit geschiedt op basis van het BIR-ICV model 2016. Hierin verklaart het management van de NCTV, aan de hand van de BIR, dat zij 'in control' zijn als het gaat om informatiebeveiliging.

1.2 Leeswijzer

Deze nota levert een overzicht van de status van de implementatie van de BIR bij de NCTV per eind 2016 voor de informatievoorziening inclusief de kritieke ICT-systemen in beheer van de NCTV.

Allereerst is in de 'In Control Verklaring' aangegeven wat de belangrijkste risico's van de NCTV zijn door het nog niet operationeel zijn van een aantal BIR-maatregelen.
De opzet van het bijbehorend managementsysteem (planning en control) wordt nader toegelicht met een overzicht van taken van de NCTV, de Te Beschermen Belangen (TBB) van de NCTV en de kritieke informatiesystemen die de NCTV zelf beheert.
Als laatste wordt een update gegeven van de GAP-analyse BIR waarin een overzicht van de status van de BIR-maatregelen per einde 2016 is opgenomen. In bijlage A staan de openstaande maatregelen met degene die verantwoordelijk is voor invoering hiervan met de geplande einddatum.

2 In Control Verklaring NCTV

2.1 ICV

De NCTV verklaart dat over 2016:

> De NCTV in control is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007).

Dit houdt het volgende in:

De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee in voldoende mate op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd.
De implementatie van maatregelen is gebaseerd op de Baseline Informatiebeveiliging Rijksdienst (BIR:2012);
De interne beheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 / BIR 2012 en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's. Deze risico's zijn van zodanig belang dat ze worden opgenomen in de bedrijfsvoeringmededeling van de NCTV.

[redacted]

Voor de uitvoering van haar taken gebruikt de NCTV de volgende kritieke informatiesystemen:

- [redacted]

Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse.
De ICV op de informatiebeveiliging omvat de gehele informatievoorziening waarvoor de NCTV verantwoordelijk is inclusief het gerubriceerde deel.

Naast deze systemen maakt de NCTV gebruik van diverse standaard applicaties op het VenJ-net die gebruik maken van de Haagse Ring. Deze generieke diensten voor infrastructuur, kantoorautomatisering, ICT systeembeheer en toegangscontrole vallen buiten de scope van deze ICV omdat deze beheerd worden door de concerndienstverleners onder verantwoordelijkheid van BZK. De NCTV gaat er van uit dat zowel het VenJ-net als de Haagse Ring voldoen aan de BIR en dat de daarin opgeslagen Te Beschermen Belangen (TBB) van de NCTV adequaat zijn beveiligd.

Het MT NCTV heeft de ICV over 2015 met bijbehorende risico's en het beveiligingsjaarplan voor 2016 vastgesteld. De voortgang van dit jaarplan wordt periodiek besproken met het hoofd SB en bijgesteld indien nodig.
Om de jaarlijkse PDCA-cyclus te kunnen uitvoeren heeft het MT NCTV het plan van aanpak voor de 'controle interne risicobeheersing 2016' vastgesteld. Maandelijks stelt de BVC een managementrapportage op waarin wordt gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten.

De belangrijkste resultaten die de NCTV in het kader van de BIR in 2016 heeft behaald, zijn:

- Testen en in gebruik nemen van een beveiligde uitwijkvoorziening voor het van het NCSC bij .
- Implementeren van logging en monitoring in het gekoppeld aan Security Information and Event Management (SIEM) en inregelen van een proces om de logging dagelijks te doorlopen.
- Implementeren van logging en monitoring van .
- Opstellen van ICT-beheerprocedures waaronder encryptiebeleid, back-up procedure en een procedure voor aanmelding van een nieuwe informatievoorziening.
- Opheffen websites die gebruik maken van Flash en verhelpen van kwetsbaarheden die de ADR in 2016 heeft geconstateerd in de externe websites van de NCTV.
- Implementeren quick wins om de beveiliging van te verbeteren.
- Optimaliseren van diverse processen bij de .
- Diverse activiteiten om het beveiligingsbewustzijn van de medewerkers te bevorderen zoals bijvoorbeeld een introductie veilig werken bij de NCTV voor nieuwe medewerkers en een presentatie over ransomware.
- Periodiek controleren autorisaties door de lijnmanagers (eigenaren/ verantwoordelijken).
- Opstellen uitgangspunten document voor de integrale beveiliging van de op de .
- Actualiseren diverse beleidsdocumenten met betrekking op integrale beveiliging bij de NCTV.
- Opnemen van beveiligingsafspraken in contracten voor nieuwe ICT-diensten.

Ondertekening NCTV

Drs. H.W.M. Schoof, NCTV

3 TBB NCTV

3.1 Missie NCTV

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is binnen de Rijksoverheid dé organisatie die verantwoordelijk is voor terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing. Samen met partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland. De focus ligt op voorkomen en beperken van maatschappelijke ontwrichting.

3.2 Taken NCTV

De NCTV heeft de volgende taken:

- Het identificeren en duiden van dreigingen en risico's;
- Het bewaken en beveiligen van personen, objecten, diensten en evenementen;
- Het (doen) verhogen van cyber security;
- Het (doen) verhogen van de weerbaarheid van vitale sectoren, burgers, bedrijven, structuren en netwerken;
- Het realiseren van optimale crisisbeheersing en crisiscommunicatie.

3.3 Kritieke informatiesystemen NCTV

Voor uitvoering van bovenstaande taken gebruikt de NCTV de volgende kritieke informatiesystemen:

- [redacted]

De NCTV is een netwerkorganisatie met een coördinerende taak. De kritieke informatiesystemen maken geen deel uit van een van de ketens binnen VenJ.

3.4 TBB NCTV

Te Beschermen Belangen (TBB) zijn de belangen die door de NCTV worden beschermd omdat compromittering hiervan de primaire processen kan aantasten. De NCTV heeft in de KWAS van 2016 de volgende belangen als TBB benoemd:

1. [redacted]

Voor bovenstaande TBB zijn de kritieke informatiesystemen van de NCTV van belang. Naast deze kritieke informatiesystemen maakt de NCTV voor opslag van TBB gebruik van diverse standaard applicaties op het VenJ-net.

4 Status BIR maatregelen

4.1 IB thema's

4.1.1 PDCA cyclus

Voor de kritieke informatiesystemen bij de NCTV bestaat een actuele risicoafweging (niet ouder dan 3 jaar). De te nemen maatregelen die voortvloeiden uit de risicoanalyses van [redacted] zijn in 2016 afgerond.

In 2015 is een quick scan BIR uitgevoerd op het anoniem [redacted] Deze risicoanalyses zijn vastgesteld door de systeemeigenaar. De quick wins voor [redacted] zijn in 2016 ingevoerd, de aanvullende maatregelen worden met de upgrade naar Surfnet 2.0 ingevoerd in 2017. In het [redacted] worden nog enkele openstaande maatregelen in 2017 ingevoerd.

Tevens heeft de NCTV in 2016 een KWAS uitgevoerd.

De NCTV heeft een plan van aanpak voor de 'controle interne risicobeheersing 2016' vastgesteld om de effectiviteit van de integrale risicobeheersing te controleren.

Maandelijks stelt de [redacted] een managementrapportage op waarin wordt gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten en verbeterpunten.

4.1.2 Beveiliging externe koppelvlakken

De NCTV had meer dan 30 websites met een extern koppelvlak naar het internet. Om na te gaan of de websites kwetsbaarheden vertonen heeft de Audit Dienst Rijk (ADR) pentesten uitgevoerd op een groot deel van deze websites. De door de ADR geconstateerde kwetsbaarheden in de geteste websites zijn verholpen.
Een deel van de geteste e-learningsites maakte gebruik van Flash.
Beveiligingsexperts zoals de ADR en het NCSC, raden het gebruik van Flash af omdat kwetsbaarheden in Flash player op grote schaal worden misbruikt.
Daarom heeft de NCTV in 2016 8 e-learningsites opgeheven en wordt 1 e-learningsite omgebouwd.

4.1.3 Patchmanagement

In 2015 is een procedure voor patchmanagement opgesteld voor alle netwerken binnen de NCTV. Met de invoering van SIEM kan de status van de geïnstalleerde software in relatie tot de vereiste patches worden bewaakt.

4.1.4 Beheer van medewerkers en toegang

De afdeling bedrijfsvoering heeft het indiensttreding- en uitdiensttreding proces van medewerkers geïmplementeerd in [redacted]. Daarnaast zijn autorisatie-matrices goedgekeurd. In 2016 is het verouderde autorisatiesysteem voor [redacted] in het [redacted] vervangen. In 2017 worden de resterende applicaties naar de nieuwe centrale database van het [redacted] gemigreerd. Tevens worden in 2017 in het [redacted] de Linux applicaties aan de centrale database gekoppeld.
De controle op het autorisatiebeleid is periodiek voorgelegd aan de lijnmanagers (eigenaren/verantwoordelijken) en de aanpassingen zijn verwerkt.

[redacted]

4.1.5 *Logging en monitoring*

In 2016 is logging en monitoring in het [redacted] en [redacted] gekoppeld aan SIEM (Security Information en Event Management). Eind 2016 is de implementatie van SIEM in het [redacted] afgerond en is een proces ingeregeld om de logging dagelijks te doorlopen. De logging van [redacted] wordt in 2017 gekoppeld aan een monitoringtool.

4.2 Resultaten analyse

In 2016 is een controle uitgevoerd op de openstaande maatregelen van de BIR die in de GAP-analyse van 2015 waren geconstateerd.

4.2.1 *Scope*

De BIR is opgedeeld in 11 hoofdstukken met totaal ongeveer 240 maatregelen.

De GAP-analyse was gericht op de volgende 3 onderdelen waar de NCTV zelf verantwoordelijk voor is:

1. Organisatorische en fysieke maatregelen die NCTV-breed zijn ingericht in het kader van informatiebeveiliging (hoofdstuk 5 t/m 9 en 13 t/m 15 van de BIR met ca. 105 maatregelen);
2. ICT-basis beveiligingsmaatregelen die zijn ingericht voor beveiliging van informatie op het Stg-net, met name in de bedrijfskritieke systemen [redacted] en [redacted] (hoofdstuk 10 t/m 12 van de BIR met ca. 135 maatregelen) en [redacted];
3. ICT-basis beveiligingsmaatregelen die zijn ingericht voor beveiliging van informatie op het [redacted] (hoofdstuk 10 t/m 12 van de BIR).

4.2.2 *Status informatiebeveiliging 2016*

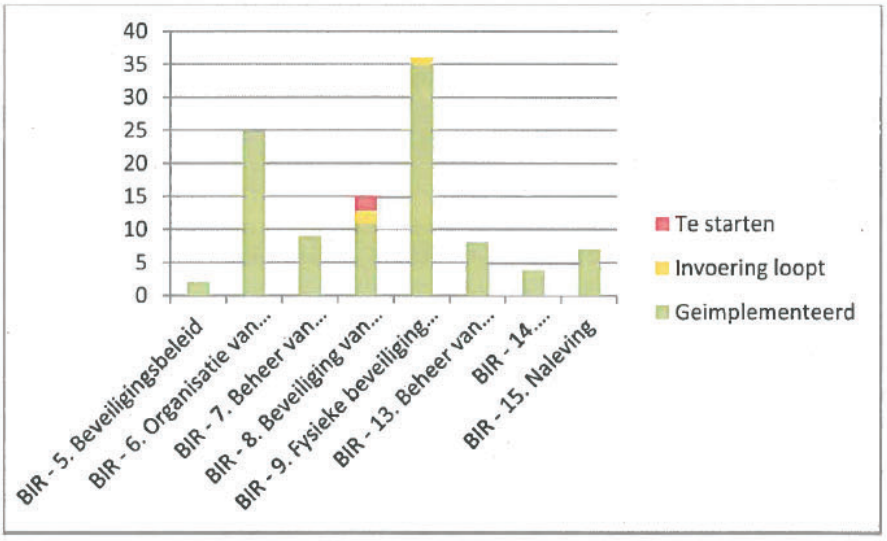
4.2.2.1 Status organisatorische en fysieke maatregelen NCTV

De NCTV heeft in 2016 enkele documenten van het Programma Integrale Beveiliging, in het kader van voortschrijdend inzicht en ontwikkelingen, geactualiseerd. Dit betreft:

- Tactisch kader integrale beveiliging;
- Informatiebeveiligingsbeleid;
- Beleid beveiligingsbewustzijn;
- Toegangscontrole netwerken en elektronische informatie.

In het kader van de meldplicht datalekken heeft de NCTV een inventarisatie uitgevoerd van de verwerking van persoonsgegevens bij de NCTV en is een procedure voor het melden van datalekken opgesteld.
De [redacted] heeft in 2016 een encryptiebeleid, back-up procedure en een procedure voor aanmelding van een nieuwe informatievoorziening vastgesteld.
De implementatie van enkele organisatorische maatregelen is vertraagd en is nu voorzien in 2017.

In onderstaand overzicht is de status van de organisatorische en fysieke beveiligingsmaatregelen weergegeven.



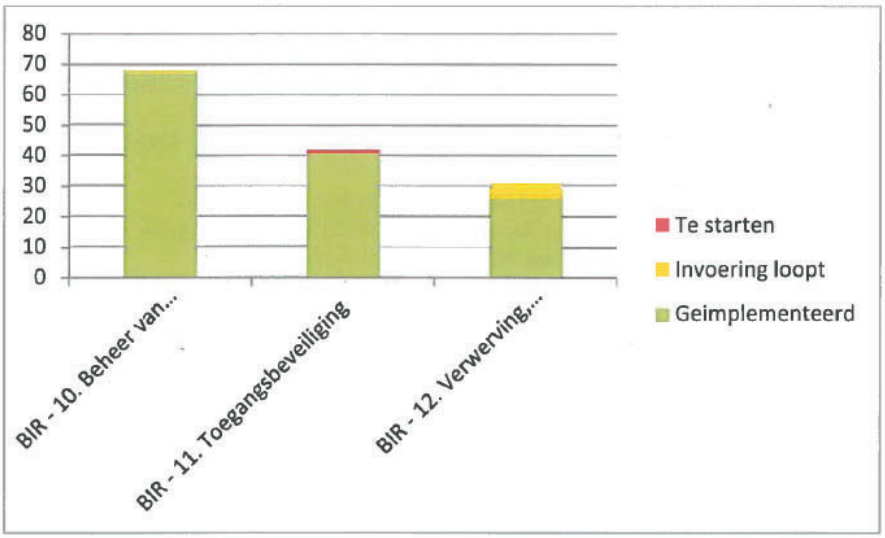
Per eind december 2016 is ongeveer 95% van de organisatorische en fysieke beveiligingsmaatregelen geïmplementeerd bij de NCTV, de implementatie van 3% loopt nog en de implementatie van 2% moet nog starten.

Twee maatregelen om informatiebeveiliging op te nemen in de functieomschrijving van NCTV-medewerkers (BIR eis 8.1.1.1 en 8.1.1.3) zullen in 2017 in samenhang met het O&F-rapport worden afgerond.

4.2.3 Status ICT-beveiligingsmaatregelen

4.2.3.1 [redacted]

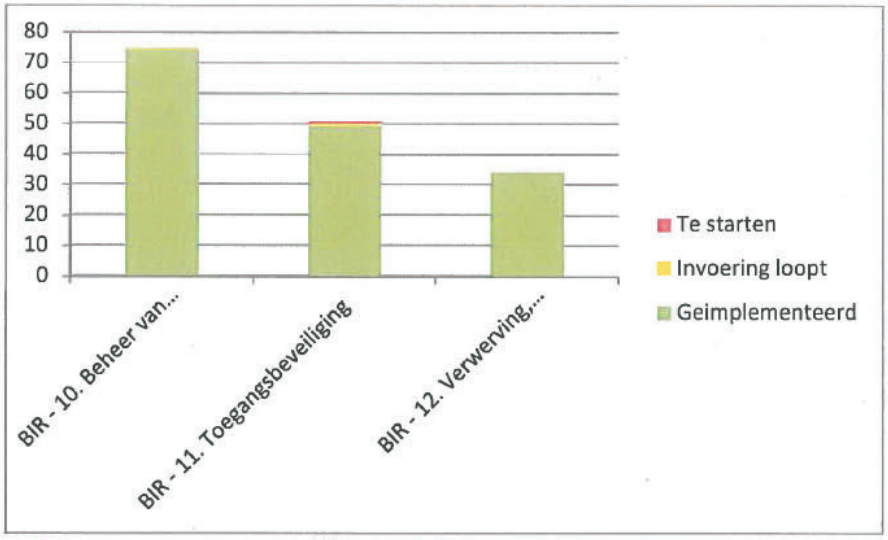
In onderstaand overzicht is de status van de ICT-beveiligingsmaatregelen die van toepassing zijn voor het [redacted] weergegeven.



Per eind december 2016 is ongeveer 93% van de ICT-beveiligingsmaatregelen geïmplementeerd bij de NCTV, de implementatie van 6% loopt nog. Eén maatregel is niet gestart omdat invoering hiervan in het [redacted] niet mogelijk is en het bijbehorend risico laag is.

4.2.3.2 [redacted]

In onderstaand overzicht is de status van de ICT-beveiligingsmaatregelen die van toepassing zijn voor het [redacted] weergegeven.



Per eind december 2016 is ongeveer 97% van de ICT-beveiligingsmaatregelen geïmplementeerd bij het [redacted] de implementatie van 2% is gestart. Eén maatregel is niet gestart omdat invoering hiervan wacht op een besluit over een wijziging van de wachtwoordpolicy en het bijbehorend risico laag is (zie bijlage).

De belangrijkste ICT-maatregelen die in 2017 nog moeten worden ingevoerd in het [redacted] zijn:

- Naar aanleiding van de risicoanalyse van het [redacted] wordt in 2017 een studie naar aanvullende DDoS maatregelen gestart.
- De koppeling van Linux applicaties met de centrale database is nog onderhanden.
- Tonen van het aantal loginpogingen aan gebruikers.
- Invoeren wijzigingsformulier voor de besluitvorming van wijzigen waarbij ook kosten en beheerlast worden meegewogen.

Bijlage A

1. Explainformulieren organisatorische en fysieke maatregelen NCTV

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
6.1.4.1	Er is een goedkeuringsproces voor nieuwe IT voorzieningen en wijzigingen in IT voorzieningen.							
6.2.1.6	Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en							

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	hoe het toezicht is geregeld.							
6.2.3 6.2.3.1 t/m 6.2.3.8	Beveiliging behandelen in overeenkomsten met een derde partij In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.							
8.1.1.1	De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving (zie ook de Ambtenarenwet) en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan: • uitvoering van het informatiebeveiligingsbeleid		Laag	In de functiebeschrijvingen wordt niet expliciet aandacht geschonken aan informatiebeveiliging, maar in de bewustwording-campagnes wordt hieraan wel aandacht besteed. **Risico:** Indien medewerkers niet formeel op de hoogte zijn van hun plichten en de procedures kunnen ze zich daaraan onttrekken of van	Dit actiepunt is opgenomen in brief aan OR (d.d. 22/10/2015) van zaken die bij evaluatie van het O&F-rapport aan de orde moeten komen. Verder in overleg met de P-adviseur en de projectleider O&F evaluatie bezien		Q4 2015	Q2-2017

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	• bescherming van bedrijfsmiddelen • rapportage van beveiligingsincidenten			mening zijn dat ze daar niet op aangesproken kunnen worden. Dit actiepunt is opgenomen in brief aan OR (d.d. 22/10/2015) van zaken die bij evaluatie van het O&F-rapport aan de orde moeten komen.				
8.1.1.3	(R) Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.		Midden	**Risico**: indien medewerkers niet op de hoogte zijn van de verantwoordelijkheden kunnen ze door fouten gerubriceerde informatie lekken.	Dit actiepunt is opgenomen in brief aan OR (d.d. 22/10/2015) van zaken die bij evaluatie van het O&F-rapport aan de orde moeten komen. Verder in overleg met de P-adviseur en de projectleider O&F evaluatie bezien		Q4 2015	Q2-2017
8.2.1.1	Het lijnmanagement heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van rijksambtenaren en	Gestart	Midden	Zie P-visie NCTV. **Risico** is dat door vertrek van enkele externe medewerkers alle beveiligingskennis verdwijnt. Dit risico is	Strategie voor behouden van kennis en vaardigheden van NCTV is opgenomen in HRM-plan 2016, tevens bezig te bezien hoe bij afdeling		Q2-2015	Q2 2017

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	ingehuurd personeel (die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.			midden omdat in geval van nood de NCTV kan terugvallen op de expertise van de	bedrijfsvoering kennis kan worden geborgd			
8.3.1.3	Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.	Gestart	Midden	**Risico**: door het niet correct toekennen en intrekken van autorisaties kan stapeling van autorisaties ontstaan waardoor need to know en functiescheiding in geding kan komen. Bovendien is gestart met een periodieke controle van autorisaties.	Processen voor indienst-, uitdiensttreding en verandering van functie zijn beschreven. Deze processen moeten nog worden ingevoerd in Topdesk als ondersteunende tool.		Q2-2015	Q2 2017
9.1.2.8	(R) Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	Gestart	Hoog	:		iom	01-04-2014	Q2-2017

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum

2. Explainformulieren ICT-maatregelen Stg-net met ZOT en BeBOs

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
10.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: • het administreren van significante wijzigingen • impactanalyse van mogelijke gevolgen van de wijzigingen • goedkeuringsprocedure voor wijzigingen	Gestart	Midden	**Risico:** Door niet goed uitvoeren van de procedure kan de informatievoorziening uitvallen of beveiliging verminderen	Procedure is beschreven en wordt opgenomen in	Senior adviseur	Q2-2015	Q1 2017
10.5.1.1	Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.			Zie back-up procedure				
11.4.5.5	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).			Niet gebruikte services zijn voor zover mogelijk uitgeschakeld met de update van				
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker		Laag	**EXPLAIN:** deze functionaliteit is niet ingebouwd in het Gezien het feit dat de	**Geen actie** Gezien het feit dat de medewerkers in moeten loggen met een token is de kans dat een account succesvol kan	Geen		

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.			gebruiker in moet loggen met een persoonlijk wachtwoord en token wordt dit **risico** laag geschat.	worden misbruikt laag en **het risico** van het ontbreken dan deze maatregel ook laag.			
12.4.1.3	Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.			De apparatuur is al opgenomen in een CMDB, het overzicht van licenties wordt in 2017 in [redacted] ingevoerd.				

2. Explainformulieren ICT-maatregelen CERT-netwerk

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
10.1.2.2	(R) Instellingen van informatiebeveiligingsfunctie s (b.v. security software) op het koppelvlak tussen vertrouwde en onvertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.			Implementeren van logging en monitoring in het [redacted] gekoppeld aan Security Information and Event Management (SIEM) en inregelen van een proces om de logging dagelijks te doorlopen				
10.4.1.5	Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.							
10.6.1.1	Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.			Implementeren van logging en monitoring in het [redacted] gekoppeld aan Security Information and Event Management (SIEM) en inregelen van een proces om de logging dagelijks te doorlopen				
10.6.1.4	Er zijn procedures voor beheer van apparatuur op afstand.			Zie procedure [redacted]				

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
10.10.1 t/m 10.10.5	Aanmaken en beschermen logbestanden en controle systeemgebruik			Implementeren van logging en monitoring in het [redacted] gekoppeld aan Security Information and Event Management (SIEM) en inregelen van een proces om de logging dagelijks te doorlopen				
11.2.1.2 (R).	Authenticatiegegevens worden bijgehouden in één bronbestand) zodat consistentie is gegarandeerd	Gestart	Laag	**Risico:** oude accounts kunnen achterblijven bij vertrek medewerker. Risico is laag omdat het netwerk account wordt bij vertrek wel wordt ingetrokken.	De koppeling van Linux authenticatie aan de centrale database is nog onderhanden	[redacted]	Q4 2016	Q1 2017
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.		Laag	**EXPLAIN:** deze functionaliteit is niet ingebouwd in he[redacted] Gezien het feit dat de gebruiker in moet loggen met een persoonlijk wachtwoord [redacted] wordt dit **risico** laag geschat.	Tonen loginpogingen aan gebruikers (ook n.a.v. wens tot wijziging wachtwoordpolicy)	[redacted]		Q1 2017

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~DEP. VERTROUWELIJK~~ - CONCEPT

ICV BIR NCTV 2017
Programma Integrale Beveiliging

Datum	15 januari 2018
Status	Definitief

Colofon

Afzendgegevens	[redacted]
	Turfmarkt 147 2511 DP Den Haag Postbus 16950 2500 BZ Den Haag www.nctv.nl
Contactpersoon	[redacted]
	T [redacted]
Projectnaam	ICV BIR 2017 Programma Integrale Beveiliging
Ons kenmerk	-
Auteurs	[redacted]

Inhoud

1 Inleiding

1.1 VIR

Het Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007) vraagt van elk DG een in control verklaring (ICV) wat betreft informatiebeveiliging. Dit geschiedt op basis van het BIR-ICV model 2017. Hierin verklaart het management van de NCTV, aan de hand van de Baseline Informatiebeveiliging Rijksdienst (BIR:2012), dat zij 'in control' zijn als het gaat om informatiebeveiliging.

1.2 Leeswijzer

Dit rapport geeft een overzicht van de status van de implementatie van de BIR bij de NCTV per eind 2017 voor de informatievoorziening inclusief de kritieke ICT-systemen in beheer van de NCTV.

Allereerst is in de 'In Control Verklaring' aangegeven wat de belangrijkste risico's van de NCTV zijn door het nog niet operationeel zijn van een aantal BIR-maatregelen.
De opzet van het bijbehorend managementsysteem (planning en control) wordt nader toegelicht met een overzicht van taken van de NCTV, de Te Beschermen Belangen (TBB) van de NCTV en de kritieke informatiesystemen die de NCTV zelf beheert.
Als laatste wordt een update gegeven van de GAP-analyse BIR waarin een overzicht van de status van de BIR-maatregelen per einde 2017 is opgenomen. In bijlage A staan de maatregelen die afgelopen jaar gereed zijn gemeld en de openstaande maatregelen met degene die verantwoordelijk is voor invoering hiervan met de geplande einddatum.

2 In Control Verklaring NCTV

2.1 ICV

De NCTV verklaart dat over 2017:

> De NCTV in control is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007).

Dit houdt het volgende in:

De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee in voldoende mate op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd. De implementatie van maatregelen is gebaseerd op de Baseline Informatie-beveiliging Rijksdienst (BIR:2012)
De interne beheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 / BIR:2012 en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's. Deze risico's zijn van zodanig belang dat ze worden opgenomen in de bedrijfsvoeringmededeling van de NCTV.

In 2017 heeft de NCTV er bij [redacted] aangedrongen op een [redacted] heeft een projectleider benoemd die dit project nog moet oppakken.

[redacted]

Voor de uitvoering van haar taken gebruikt de NCTV de volgende kritieke informatiesystemen:

[redacted]

Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse.
De ICV op de informatiebeveiliging omvat de gehele informatievoorziening waarvoor de NCTV verantwoordelijk is inclusief het gerubriceerde deel.

Naast deze systemen maakt de NCTV gebruik van diverse standaard applicaties op het VenJ-net die gebruik maken van de Haagse Ring. Deze generieke diensten voor infrastructuur, kantoorautomatisering, ICT systeembeheer en toegangscontrole

vallen buiten de scope van deze ICV omdat deze beheerd worden door de concerndienstverleners onder verantwoordelijkheid van BZK. De NCTV gaat er van uit dat zowel het VenJ-net als de Haagse Ring voldoen aan de BIR:2012 en dat de daarin opgeslagen Te Beschermen Belangen (TBB) van de NCTV adequaat zijn beveiligd.

Het MT NCTV heeft de ICV over 2016 met bijbehorende risico's en het beveiligingsjaarplan voor 2017 vastgesteld. De voortgang van dit jaarplan wordt periodiek besproken met het [redacted] en bijgesteld indien nodig.
Om de jaarlijkse PDCA-cyclus te kunnen uitvoeren heeft het MT NCTV het plan van aanpak voor de 'controle interne risicobeheersing 2017' vastgesteld. Maandelijks stelt de [redacted] een managementrapportage op waarin wordt gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten.

De belangrijkste resultaten die de NCTV in het kader van de BIR:2012 in 2016 heeft behaald, zijn:

- Het ondersteunen van de bedrijfsvoeringprocessen met [redacted];
- Uitvoeren en opvolgen van de adviezen van de peer reviews op [redacted];
- Opstellen van een intakeproces voor invoering van nieuwe informatievoorzieningen incl. beveiliging daarvan;
- Inventarisatie van de verwerking van persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming;
- Het project [redacted] is begonnen met het in kaart brengen van de huidige informatiehuishouding van de NCTV;
- Diverse activiteiten om het beveiligingsbewustzijn van de medewerkers te bevorderen zoals bijvoorbeeld de Week van de Veiligheid;
- Periodieke controle autorisaties door de leidinggevenden (eigenaren/ verantwoordelijken);
- Actualiseren van beleidsdocumenten Programma Integrale Beveiliging;
- Opnemen van beveiligingsafspraken in contracten voor nieuwe ICT-diensten.
- Begeleiding van Auditdienst (ADR) bij het uitvoeren van een audit over de ICV BIR 2016. De audit was zonder tekortkomingen.
- Opnemen taken en verantwoordelijkheden van een medewerker ten aanzien van informatiebeveiliging in diverse beleidstukken.
- Vanaf 1 november 2017 is de NCTV gestart met het uitvoeren van herhaalonderzoeken voor de vertrouwensfuncties om de 'basis op orde' te krijgen.

Ondertekening NCTV

[redacted]

Drs. H.W.M. Schoof, NCTV

3 TBB NCTV

3.1 Missie NCTV

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is binnen de Rijksoverheid dé organisatie die verantwoordelijk is voor terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing. Samen met partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland. De focus ligt op voorkomen en beperken van maatschappelijke ontwrichting.

3.2 Taken NCTV

De NCTV heeft de volgende taken:

- Het identificeren en duiden van dreigingen en risico's;
- Het bewaken en beveiligen van personen, objecten, diensten en evenementen;
- Het (doen) verhogen van cyber security;
- Het (doen) verhogen van de weerbaarheid van vitale sectoren, burgers, bedrijven, structuren en netwerken;
- Het realiseren van optimale crisisbeheersing en crisiscommunicatie.

3.3 Kritieke informatiesystemen NCTV

Voor uitvoering van bovenstaande taken gebruikt de NCTV de volgende kritieke informatiesystemen:

- [redacted]

De NCTV is een netwerkorganisatie met een coördinerende taak. De kritieke informatiesystemen maken geen deel uit van een van de ketens binnen VenJ.

3.4 TBB NCTV

Te Beschermen Belangen (TBB) zijn de belangen die door de NCTV worden beschermd omdat compromittering hiervan de primaire processen kan aantasten. De NCTV heeft in de KWAS van 2016 de volgende belangen als [redacted]

- [redacted]

Voor bovenstaande TBB zijn de kritieke informatiesystemen van de NCTV van belang. Naast deze kritieke informatiesystemen maakt de NCTV voor opslag van TBB gebruik van diverse standaard applicaties op het VenJ-net.

4 Status BIR maatregelen

4.1 IB thema's 2017

4.1.1 Plan-Do-Check-Act cyclus

Voor de kritieke informatiesystemen bij de NCTV bestaat een actuele risicoafweging (niet ouder dan 3 jaar).

In 2015 is een quick scan BIR uitgevoerd op het anoniem [redacted]. Deze risicoanalyses zijn vastgesteld door de systeemeigenaar. De quick wins voor [redacted] zijn in 2016 ingevoerd. In 2017 is een Proof of Concept gestart voor [redacted] om na te gaan of deze de gewenste functionaliteit biedt voor een upgrade in 2018. In het [redacted] zijn nog enkele openstaande maatregelen in 2017 ingevoerd.

De NCTV heeft een plan van aanpak voor de 'controle interne risicobeheersing 2017' vastgesteld om de effectiviteit van de integrale risicobeheersing te controleren.

Maandelijks stelt de [redacted] een managementrapportage op waarin wordt gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten en verbeterpunten.

4.1.2 Beveiliging externe koppelvlakken

De NCTV had meer dan 30 websites met een extern koppelvlak naar het internet. Om na te gaan of de websites kwetsbaarheden vertonen heeft de Audit Dienst Rijk (ADR) een aantal pentesten uitgevoerd op een deel van deze websites (voornamelijk bij een update van de website).
Daarnaast zijn diverse Responsible Disclosure meldingen ontvangen en binnen de gestelde tijd afgehandeld.

4.1.3 Patchmanagement

In 2015 is een procedure voor patchmanagement opgesteld voor alle netwerken binnen de NCTV. Met de invoering van SIEM wordt nu de status van de geïnstalleerde software in relatie tot de vereiste patches bewaakt.

4.2 Resultaten analyse

In 2017 is een controle uitgevoerd op de openstaande maatregelen van de BIR die in de GAP-analyse van 2016 waren geconstateerd.

4.2.1 Scope

De BIR is opgedeeld in 11 hoofdstukken met totaal ongeveer 240 maatregelen.

De GAP-analyse was gericht op de volgende 3 onderdelen waar de NCTV zelf verantwoordelijk voor is:

1. Organisatorische en fysieke maatregelen die NCTV-breed zijn ingericht in het kader van informatiebeveiliging (hoofdstuk 5 t/m 9 en 13 t/m 15 van de BIR met ca. 105 maatregelen);
2. ICT-basis beveiligingsmaatregelen die zijn ingericht voor beveiliging van informatie op het [redacted];
3. ICT-basis beveiligingsmaatregelen die zijn ingericht voor beveiliging van informatie op het [redacted] (hoofdstuk 10 t/m 12 van de BIR).

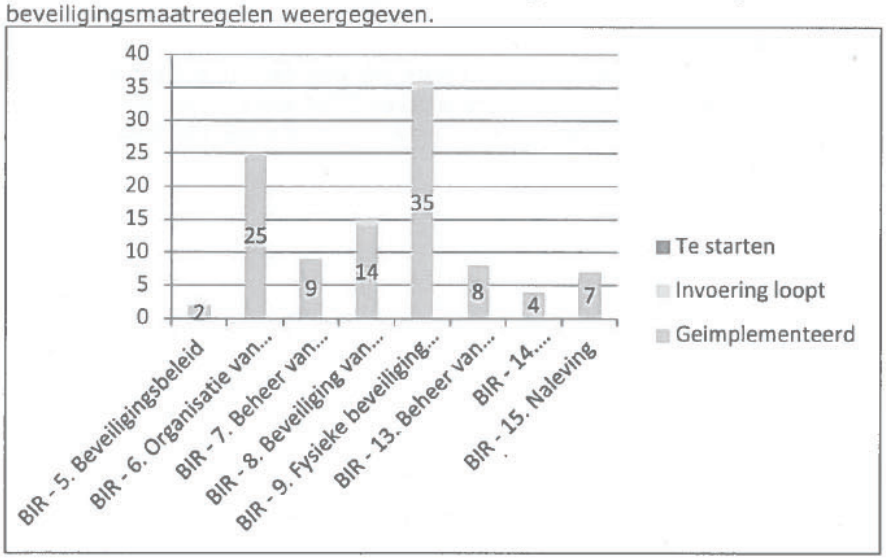
4.2.2 Status informatiebeveiliging 2017

4.2.2.1 Status organisatorische en fysieke maatregelen NCTV

De NCTV heeft in 2017 enkele documenten van het Programma Integrale Beveiliging, in het kader van voortschrijdend inzicht en ontwikkelingen, geactualiseerd. Dit betreft:

- Regeling materieelbeheer;
- Rubriceringsmethodiek NCTV;
- Omgaan met vertrouwensfuncties;
- Fysieke beveiliging;

In onderstaand overzicht is de status van de organisatorische en fysieke beveiligingsmaatregelen weergegeven.



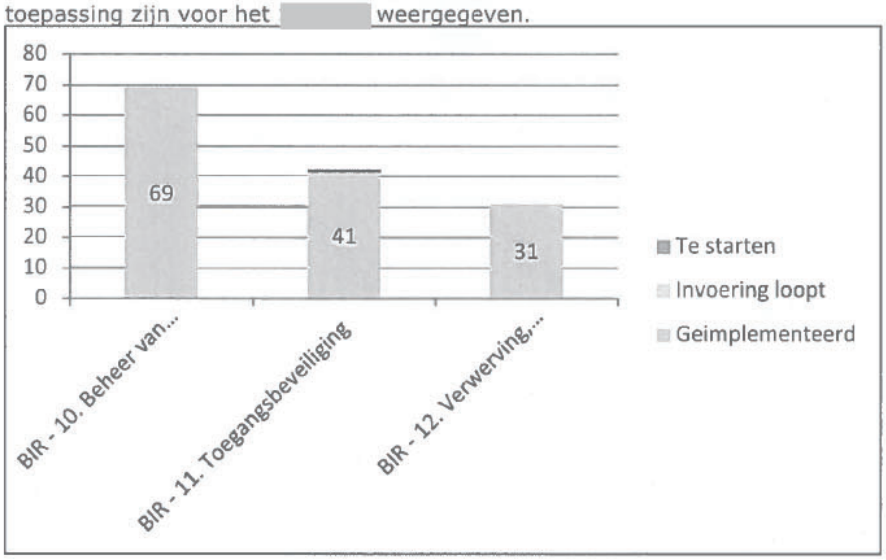
Per eind december 2017 is ongeveer 99% van de organisatorische- en fysieke beveiligingsmaatregelen geïmplementeerd bij de NCTV, de implementatie van 1% loopt (dit zijn 8.2.1.1 en 9.1.2.8 zie bijlage A) nog.

Twee maatregelen om informatiebeveiliging op te nemen in de functieomschrijving van NCTV-medewerkers (BIR eis 8.1.1.1 en 8.1.1.3) zijn opgenomen in de beleidsdocumenten van de NCTV, niet in de functieomschrijving, met uitzondering van de BVC/CISO.

4.2.3 Status ICT-beveiligingsmaatregelen

4.2.3.1 [redacted]

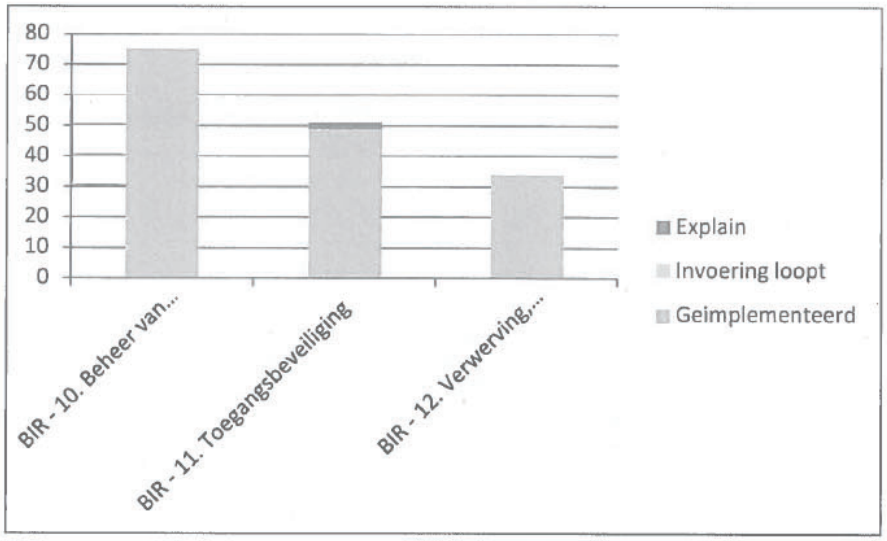
In onderstaand overzicht is de status van de ICT-beveiligingsmaatregelen die van toepassing zijn voor het [redacted] weergegeven.



Per eind december 2016 is ongeveer 99% van de ICT-beveiligingsmaatregelen geïmplementeerd bij de NCTV. Voor één maatregel (11.5.1.4 zie bijlage A) is een explain opgesteld, omdat invoering hiervan in het [redacted] niet mogelijk is en het bijbehorend risico laag is.

4.2.3.2 CERT-netwerk

In onderstaand overzicht is de status van de ICT-beveiligingsmaatregelen die van toepassing zijn voor het [redacted] weergegeven.



Per eind december 2017 is ongeveer 97% van de ICT-beveiligingsmaatregelen geïmplementeerd bij het [redacted]. Voor twee maatregelen is een explain opgesteld omdat invoering hiervan nog niet mogelijk is en het bijbehorend risico laag is (zie bijlage A).

De risicoanalyse van het [redacted] heeft de vraag opgeworpen of de huidige maatregelen tegen een DDoS aanval voldoende zijn. Daarom wordt in 2018 een studie uitgevoerd naar aanvullende DDoS maatregelen.

Bijlage A

1. Explainformulieren organisatorische en fysieke maatregelen NCTV

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
8.1.1.1	De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving (zie ook de Ambtenarenwet) en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan: • uitvoering van het informatiebeveiligingsbeleid • bescherming van bedrijfsmiddelen • rapportage van beveiligingsincidenten			In de functiebeschrijvingen wordt niet expliciet aandacht geschonken aan informatiebeveiliging, maar in de bewustwording-campagnes wordt hieraan wel aandacht besteed. In alle beleidsstukken mbt (informatie)beveiliging worden de taken en verantwoordelijkheden van alle betrokken partijen benoemd.	Gereed			
8.1.1.3	(R) Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor			Zie ook pt 8.1.1.1. Voor een beperkt aantal functies is een expliciete verantwoordelijkheid t.a.v. Informatiebeveiliging	Gereed			

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.			benoemd in de beleidsstukken.				
8.2.1.1	Het lijnmanagement heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van rijksambtenaren en ingehuurd personeel (die kritische bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.	Gestart	Midden	Zie P-visie NCTV. Risico is dat door vertrek van enkele externe medewerkers alle beveiligingskennis verdwijnt. Dit risico is nu nog midden omdat in geval van nood de NCTV kan terugvallen op de expertise van de . Zonder aanvullende maatregelen kan risico groter worden door meer afstand van .	In 2017 is gestart met een verkenning rond het outsourcen van het beheer van het bij een andere overheidspartij en lopen gesprekken met over beheer van het . Tevens is een aanvang gemaakt om processen in Sharepoint vast te leggen.		Q2-2015	Q4 2018
8.3.1.3	Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen			Processen voor indienst-, uitdiensttreding en verandering van functie zijn gedefinieerd en in opgenomen. Daarnaast laat afdeling bedrijfsvoering periodieke controles van autorisaties uitvoeren.	Gereed			

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
	van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.							
9.1.2.8	(R) Er vindt minimaal één keer per half jaar een periodieke controle/evaluatie plaats op de autorisaties voor fysieke toegang.	Gestart	Hoog				01-04-2014	

2. Explainformulieren ICT-maatregelen Stg-net met ZOT en BeBOs en Surfnet

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
10.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: • het administreren van significante wijzigingen • impactanalyse van mogelijke gevolgen van de wijzigingen • goedkeuringsprocedure voor wijzigingen			Inrichting van een Change Advisory Board (CAB). Zie ook de documentatie op [redacted] en in de Teamsite	Gereed			
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.		Laag	**EXPLAIN:** deze functionaliteit is niet ingebouwd in het [redacted]. Gezien het feit dat de gebruiker in moet loggen met een persoonlijk wachtwoord en token wordt dit **risico** laag geschat.	**Geen actie** Gezien het feit dat de medewerkers in moeten loggen met een token is de kans dat een account succesvol kan worden misbruikt laag en het risico van het ontbreken dan deze maatregel ook laag.	Geen		

2. Explainformulieren ICT-maatregelen CERT-netwerk

BIR-Eis	Omschrijving	status	Risico	Onderbouwing	Omschrijving actie	Actie houder	Start datum	Eind datum
11.2.1.2 (R).	Authenticatiegegevens worden bijgehouden in één bronbestand) zodat consistentie is gegarandeerd		Laag	**Risico:** oude accounts kunnen achterblijven bij vertrek medewerker. Risico is laag omdat het netwerk account bij vertrek wel wordt ingetrokken.	Authenticatiegegevens worden bijgehouden in 1 bronbestand per netwerk. Omdat het			
11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.		Laag	**EXPLAIN:** deze functionaliteit is niet ingebouwd in het of VenJ-net. Gezien het feit dat de gebruiker in moet loggen met een persoonlijk wordt dit **risico** laag geschat.	Aangezien heeft geëvalueerd en deze functie niet noodzakelijk vond is deze functie niet aanwezig.			

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

In Control Verklaring NCTV

De NCTV verklaart dat over 2018:

De NCTV 'in control' is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007).

Dit houdt het volgende in:

1. De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee in voldoende mate op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd. De implementatie van maatregelen is gebaseerd op de Baseline Informatiebeveiliging Rijksdienst (BIR2012). Jaarlijks wordt een jaarverslag opgesteld waarin gerapporteerd wordt over het afgelopen jaar en een jaarplan wordt voorgelegd voor het komende jaar waarin de PDCA cyclus ('Controle interne risicobeheersing') is opgenomen.
   Het MT NCTV heeft de ICV over 2017 met bijbehorende risico's en het beveiligingsjaarplan voor 2018 vastgesteld. De voortgang van dit jaarplan is periodiek besproken met het [redacted] en bijgesteld indien nodig. Maandelijks stelde [redacted] een managementrapportage op waarin werd gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten.

2. Voor de uitvoering van haar taken gebruikt de NCTV de volgende kritieke informatiesystemen:
   [redacted]

   Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse en voldoen aan de VIR 2007 en de BIR2012.

   De interne beheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 en de BIR2012 en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's. Voor de hieronder genoemde risico's is het van belang de voortgang te bewaken en deze op te nemen in het jaarplan van de bedrijfsvoering van de NCTV.

3. In 2018 had de NCTV de risicoanalyses voor de kritieke systemen uit willen voeren. Hiervoor was men afhankelijk van de oplevering, door BZK, van de BIR2017 met [redacted] niveau. De oplevering daarvan is uitgesteld naar 2019. Binnen de NCTV zijn de risico's voor de kritieke systemen besproken. De inventarisatie en beoordeling van deze risico's zijn niet vastgelegd. De NCTV neemt dat als actiepunt mee bij de implementatie van de BIR2017 en zal in 2019 de risicoanalyses uitvoeren.
   In 2017 heeft de NCTV er bij [redacted]
   - [redacted]

- [redacted]

Naast deze systemen maakt de NCTV gebruik van diverse standaard applicaties op het JenV-net die gebruik maken van [redacted]. Deze generieke diensten voor infrastructuur, kantoorautomatisering, ICT systeembeheer en toegangscontrole vallen buiten de scope van deze ICV, omdat deze beheerd worden door de concerndienstverleners onder verantwoordelijkheid van BZK. De NCTV gaat er van uit dat zowel het JenV-net als [redacted] voldoen aan de BIR2012 en dat de daarin opgeslagen Te Beschermen Belangen (TBB) van de NCTV adequaat zijn beveiligd.

4. Een toelichting op de IB activiteiten die de NCTV in het kader van de BIR2012 in 2018 heeft behaald, zijn:
   - Het ondersteunen van de bedrijfsvoeringprocessen met [redacted];
   - Opstellen van een intakeproces voor invoering van nieuwe informatie toepassingen of systemen inclusief de beveiligingsmaatregelen;
   - Inventarisatie van de verwerking van persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming;
   - Het projectteam [redacted] heeft de huidige Enterprise Architectuur van de NCTV in kaart gebracht;
   - Diverse activiteiten om het beveiligingsbewustzijn van de medewerkers te bevorderen;
   - Periodieke controles autorisaties door de leidinggevenden (eigenaren/ verantwoordelijken);
   - Opnemen van beveiligingsafspraken in contracten voor nieuwe ICT-diensten;
   - Het uitvoeren van pentesten door de ADR op projecten en websites.
   - De NCTV is gestart met het uitvoeren van herhaalonderzoeken voor de vertrouwensfuncties om de 'basis op orde' te krijgen.

De reikwijdte van de ICV-IB 2018 omvat de gehele informatieketen binnen de NCTV inclusief de kritieke systemen en het gerubriceerde netwerk. De kritieke informatiesystemen maken geen deel uit van een van de ketens binnen JenV. Voor het gerubriceerde netwerk binnen de NCTV gelden hogere en aanvullende eisen ten opzichte van de BIR2012.
[redacted] Ze zijn daarom niet toegevoegd maar wel ter inzage beschikbaar bij [redacted] NCTV.

Ondertekening wnd NCTV

[redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

ICV-IB 2019

De bestuurder van de NCTV verklaart dat over 2019:

1. De NCTV in control is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) en dat de beoordeling van de bedrijfskritieke systemen onderdeel uit maakt van de beoordeling van de kritieke systemen. Dit houdt het onderstaande in.

2. De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee in voldoende mate op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd. De implementatie van maatregelen is gebaseerd op de Baseline Informatiebeveiliging Rijksdienst (BIR2017).

3. De interne risicobeheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 en de BIR2017 en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's. Deze risico's zijn van zodanig belang dat ze zijn opgenomen in het wegingsverslag bij de managementparagraaf als onderdeel van het jaarverslag van de NCTV. Voor de hieronder genoemde risico's is het van belang de voortgang te bewaken en deze op te nemen in het jaarplan van de bedrijfsvoering van de NCTV.

[redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

[redacted] uit dat zowel het JenV-netwerk als de Haagse Ring voldoen [redacted] adequaat zijn beveiligd. De [redacted] ende beeld van de [redacted]

[redacted] is ontworpen voor de opslag van informatie tot en met niveau Dep. V. (BBN2). De NCTV heeft zelf maatregelen getroffen om de inhoud van alle zaken van de NCTV alleen toegankelijk te maken voor NCTV medewerkers. Op dit moment zijn er voor [redacted] nog onvoldoende maatregelen getroffen om het geschikt te maken voor de opslag van persoonsgegevens, de beschikbaarheid te verhogen en [redacted].
De NCTV beschikt over informatie die interessant is voor statelijke actoren en informatie waaraan hogere eisen van beschikbaarheid worden gesteld zoals bij [redacted], Kamervragen en WOB-verzoeken (bedrijfskritieke informatie). [redacted]
De NCTV zal in 2020 haar processen aanpassen en dit soort informatie opslaan op haar eigen Staatsgeheime netwerk of op een andere wijze de beschikbaarheid van deze informatie garanderen. Het risico is nu aanwezig dat informatie die onder de genoemde categorieën vallen toch is opgeslagen onder [redacted]. De medewerkers hadden onvoldoende kennis over dit risico in het verleden. De NCTV zal in 2020 haar medewerkers wijzen op deze kwetsbaarheid, een handelingsperspectief bieden en vragen om informatie te verplaatsen naar geschikte applicaties. Voor dit soort informatie zal geen gebruik meer worden gemaakt van [redacted].

4. De reikwijdte van de ICV-IB 2019 omvat de gehele informatieketen binnen de NCTV inclusief de kritieke systemen en het gerubriceerde netwerk. De kritieke informatiesystemen maken geen deel uit van een van de ketens binnen JenV. Voor het gerubriceerde netwerk binnen de NCTV gelden hogere en aanvullende eisen ten opzichte van de BIR2017.
   De risicoanalyses van de kritieke systemen zijn [redacted] gerubriceerd. Ze zijn daarom niet toegevoegd maar wel ter inzage beschikbaar bij de [redacted] NCTV.

5. Eind 2019 is het NBA geïntroduceerd als methodiek om het volwassenheidsniveau informatiebeveiliging van een organisatie te meten en hierover te rapporteren. Het volwassenheidsniveau (NBA level) van de NCTV bevindt zich op dit moment op niveau 2 voor wat betreft beleid, organisatie, incidentmanagement en risicomanagement.

[redacted]

Ondertekening NCTV

[redacted]

P.J. Aalbersberg

Toelichting:

1. Jaarlijks wordt een jaarrapportage opgesteld waarin wordt gerapporteerd over het afgelopen jaar. Tevens wordt een jaarplan, Interne controle risicobeheersing NCTV, opgesteld voor het komende jaar waarin de PDCA-cyclus is opgenomen.
   Het MT NCTV heeft, begin 2019, de ICV over 2018 met bijbehorende risico's en de Interne controle risicobeheersing NCTV (jaarplan) voor 2019 vastgesteld. De voortgang van dit jaarplan is periodiek besproken met het [redacted] en bijgesteld indien nodig.
   Maandelijks stelde de [redacted] een managementrapportage op waarin werd gerapporteerd over integrale beveiliging inclusief de opvolging van beveiligingsincidenten. Periodiek werd gerapporteerd over de status van de BIR2017. Op dit moment is de NCTV 'in control' voor wat betreft alle te nemen maatregelen. Sommige maatregelen zijn wel opgestart maar nog niet afgerond omdat deze mede afhankelijk zijn van het handelen van andere partijen. Deze partijen hebben vertraging opgelopen of hebben aangegeven niet in de gevraagde maatregelen te kunnen voorzien. De NCTV heeft hierop haar beleid aangepast en aanvullende maatregelen genomen die nog verdere uitwerking behoeven.

2. Voor de uitvoering van haar taken gebruikt de NCTV de volgende eigen kritieke informatiesystemen:
   [redacted]
   Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse en voldoen aan de VIR 2007 en de BIR2017.

5. Voor de introductie van het volwassenheidsniveau (NBA) is een nulmeting uitgevoerd. De resultaten zijn eerder gedeeld met [redacted]. De meting heeft in het Engels plaatsgevonden en zorgde binnen JenV voor verschillende interpretaties. [redacted] heeft een plan van aanpak opgesteld om alle dienstonderdelen te ondersteunen om in 2022 op niveau 4 uit te komen IB. De NCTV volgt de lijn van JenV [redacted].
   De NCTV heeft zijn processen voldoende ingericht maar het ontbreekt aan een juiste structuur om de goede werking en het bestaan aan te tonen. De huidige status, volgens de methodiek, van de NCTV leidt niet tot hoge risico's.

   Een toelichting op de IB activiteiten die de NCTV in het kader van de BIR2017 in 2019 heeft behaald, zijn:
   - Het ondersteunen van de bedrijfsvoeringprocessen met [redacted];
   - Opstellen van een intakeproces voor invoering van nieuwe informatie toepassingen of systemen inclusief de beveiligingsmaatregelen en AVG;
   - Inventarisatie en implementatie (deels) van de verwerking van persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming;
   - Het projectteam [redacted] heeft de huidige Enterprise Architectuur van de NCTV in kaart gebracht;
   - Diverse activiteiten om het beveiligingsbewustzijn van de medewerkers te bevorderen zoals een week van de veiligheid;
   - Periodieke controles op autorisaties door de leidinggevenden (eigenaren/ verantwoordelijken);
   - Opnemen van beveiligingsafspraken in contracten voor nieuwe ICT-diensten;
   - Het uitvoeren van pentesten door de ADR op projecten en websites.
   - De NCTV heeft 'de basis op orde' ten aanzien van herhaalonderzoeken voor vertrouwensfuncties. Dat betekent dat iedere medewerker een VGB heeft jonger dan 5 jaar.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~Dep. VERTROUWELIJK~~
DI&I

Kern Bedrijfsvoering
KBV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
[redacted]

Datum
8 januari 2021

Ons kenmerk
x

nota

ICV-IB 2020

De bestuurder van de NCTV verklaart dat over 2020:

1. De NCTV in control is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) en dat de beoordeling van de bedrijfskritieke systemen onderdeel uit maakt van de beoordeling van de kritieke systemen. Dit houdt het onderstaande in.

   a. De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd. De implementatie van maatregelen is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).

   b. De interne risicobeheersing heeft zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 en de BIO en - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's.
   Deze risico's zijn van zodanig belang dat ze zijn opgenomen in het wegingsverslag bij de managementparagraaf als onderdeel van het jaarverslag van de NCTV. Voor de hieronder genoemde risico's is het van belang de voortgang te bewaken en deze op te nemen in de bedrijfsvoeringparagraaf van de NCTV.

[redacted]

Kern Bedrijfsvoering
KBV

Datum
8 januari 2021

Ons kenmerk
x

[redacted]

b. [redacted]

c. [redacted]

Kern Bedrijfsvoering
KBV

Datum
8 januari 2021

Ons kenmerk
x

De NCTV zal in 2021 haar processen aanpassen en dergelijke informatie opslaan op haar eigen Staatsgeheime netwerk of op een andere wijze de beschikbaarheid van deze informatie garanderen. Het risico is nu aanwezig dat informatie die onder de genoemde categorieën vallen toch is opgeslagen onder . De medewerkers hadden onvoldoende kennis over dit risico in het verleden. De NCTV zal in 2021 haar medewerkers wijzen op deze kwetsbaarheid, een handelingsperspectief bieden en vragen om informatie te verplaatsen naar geschikte applicaties. Voor dergelijke informatie zal geen gebruik meer worden gemaakt van

2. De reikwijdte van de ICV-IB 2020 omvat de gehele informatieketen binnen de NCTV inclusief de kritieke systemen en het gerubriceerde netwerk. De kritieke informatiesystemen maken geen deel uit van een van de ketens binnen JenV. Voor het gerubriceerde netwerk binnen de NCTV gelden hogere en aanvullende eisen ten opzichte van de BIO.
   De risicoanalyses van de kritieke systemen zijn gerubriceerd. Ze zijn daarom niet toegevoegd maar wel ter inzage beschikbaar bij de NCTV.

3. Eind 2019 is het NBA geïntroduceerd als methodiek om het Volwassenheidsniveau informatiebeveiliging van een organisatie te meten en hierover te rapporteren. Het volwassenheidsniveau (NBA level) van de NCTV bevindt zich op dit moment op niveau 3 (basis op orde) voor wat betreft beleid, organisatie, incidentmanagement en risicomanagement. De eigen ambitie van de NCTV is om eind 2021 niveau 4 te bereiken.

Ondertekening NCTV

P.J. Aalbersberg

Toelichting:

1. Jaarlijks wordt een jaarrapportage opgesteld waarin wordt gerapporteerd over het afgelopen jaar. Tevens wordt een jaarplan, Interne controle risicobeheersing NCTV, opgesteld voor het komende jaar waarin de PDCA-cyclus is opgenomen.
   Het MT NCTV heeft, begin 2020, de ICV over 2019 met bijbehorende risico's en de Interne controle risicobeheersing NCTV (jaarplan) voor 2020 vastgesteld. De voortgang van dit jaarplan is periodiek besproken met [redacted], [redacted], en bijgesteld indien nodig.
   Periodiek werd gerapporteerd over de status van de BIO. Op dit moment is de NCTV 'in control' voor wat betreft alle te nemen maatregelen. Sommige maatregelen zijn wel opgestart maar nog niet afgerond omdat deze mede afhankelijk zijn van het handelen van andere partijen. Deze partijen hebben vertraging opgelopen of hebben aangegeven niet in de gevraagde maatregelen te kunnen voorzien. De NCTV heeft hierop haar beleid aangepast en aanvullende maatregelen genomen die nog verdere uitwerking behoeven.

2. Voor de uitvoering van haar taken gebruikt de NCTV de volgende eigen kritieke informatiesystemen:
   [redacted]
   Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse en voldoen aan het VIR 2007 en de BIO.

5. Voor de introductie van het volwassenheidsniveau (NBA) is een nulmeting uitgevoerd. De resultaten zijn eerder gedeeld met [redacted]. In 2020 heeft periodiek overleg plaatsgevonden met de projectleider van [redacted] voor de implementatie en de voortgang voor het NBA niveau.
   De NCTV heeft zijn processen voldoende ingericht maar het ontbreekt nog aan de juiste structuur om de goede werking en het bestaan aan te tonen. De huidige status van de NCTV processen leidt niet tot (hoge) risico's.

Een toelichting op de IB activiteiten die de NCTV in het kader van de BIO in 2020 heeft behaald, zijn:

- De aansluiting met het SOC JenV is gerealiseerd;
- Uitvoeren van Quickscans en PIA's voor bestaande projecten en systemen;
- Het projectteam Samen Digitaal heeft de ontwikkelingen met beide Documentmanagementsystemen verder doorgevoerd;
- Diverse activiteiten om het beveiligingsbewustzijn van de medewerkers te bevorderen zijn gerealiseerd;
- Periodieke controles op autorisaties door de leidinggevenden (eigenaren/verantwoordelijken) zijn uitgevoerd;
- Het uitvoeren van pentesten door de ADR op projecten en Websites;
- Processen en producten ter verbetering van de kwaliteitsborging zijn ingevoerd;
- De transitie van BIR2017 naar BIO is gerealiseerd;
- Het [redacted] (anoniem surfen op internet) is geïmplementeerd.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~Dep. VERTROUWELIJK~~
DI&I

Kern Bedrijfsvoering
KBV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
10 januari 2022

Ons kenmerk
[redacted]

nota

ICV-IB 2021

De bestuurder van de NCTV verklaart dat over 2021:

1. De NCTV 'in control' is ten aanzien van het Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007) en dat de beoordeling van de bedrijfskritieke systemen deel uit maakt van de beoordeling van de kritieke systemen. Dit houdt het volgende in:

   a. De NCTV heeft een managementsysteem voor informatiebeveiliging op basis van risicobeheer, waarmee op de maatregelen ter borging van de vertrouwelijkheid, integriteit en de beschikbaarheid van informatie wordt gestuurd. De implementatie van maatregelen is gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO).

   b. De interne risicobeheersing heeft in 2021 zodanig gefunctioneerd dat er voldoende zekerheid is verkregen dat de bedrijfsvoering voldoet aan het VIR 2007 en de BIO en dat - waar nodig - aanvullende maatregelen zijn getroffen, behoudens de hieronder genoemde risico's.
   Deze risico's zijn van zodanig belang dat ze zijn opgenomen in het wegingsverslag bij de managementparagraaf als onderdeel van het jaarverslag van de NCTV. Voor de hieronder genoemde risico's is het van belang de voortgang te bewaken en deze op te nemen in de bedrijfsvoeringparagraaf van de NCTV.

[redacted]

Kern Bedrijfsvoering
KBV

Datum
10 januari 2022

Ons kenmerk
[redacted]

[redacted]

b. [redacted]

c. [redacted]

Kern Bedrijfsvoering
KBV

Datum
10 januari 2022

Ons kenmerk
[redacted]

[redacted]

2. De reikwijdte van de ICV-IB 2021 omvat de gehele informatieketen binnen de NCTV inclusief het gerubriceerde netwerk met de kritieke informatiesystemen. Deze informatiesystemen maken geen deel uit van een van de ketens binnen JenV. Voor het gerubriceerde netwerk binnen de NCTV gelden hogere en aanvullende eisen ten opzichte van de BIO.
   De risicoanalyses van de kritieke systemen zijn [redacted] gerubriceerd. Ze zijn daarom niet toegevoegd maar wel ter inzage beschikbaar bij de [redacted].

3. Eind 2019 is het NBA-model (Nederlandse Beroepsorganisatie van accountants) model geïntroduceerd als methodiek om het Volwassenheidsniveau informatiebeveiliging van een organisatie te meten en hierover te rapporteren. Het volwassenheidsniveau (NBA-level) van de NCTV bevindt zich op dit moment op niveau 3 (basis op orde) voor wat betreft beleid, organisatie, incidentmanagement en risicomanagement. De ambitie van de NCTV is om eind 2022 niveau 4 te bereiken.

[redacted]

Ondertekening NCTV

[redacted]

R.J. Aalbersberg

Toelichting:

1. Jaarlijks wordt een jaarrapportage opgesteld waarin wordt gerapporteerd over het afgelopen jaar. Tevens wordt een jaarplan, Interne controle risicobeheersing NCTV, opgesteld voor het komende jaar waarin de PDCA-cyclus is opgenomen.
   Het MT NCTV heeft, begin 2021, de ICV over 2020 met bijbehorende risico's en de Interne controle risicobeheersing NCTV (jaarplan) voor 2021 vastgesteld. De voortgang van dit jaarplan is periodiek besproken met het [redacted], en bijgesteld indien nodig.
   Periodiek werd gerapporteerd over de status van de BIO. Op dit moment is de NCTV 'in control' voor wat betreft alle te nemen maatregelen. Sommige maatregelen zijn wel opgestart maar nog niet afgerond omdat deze mede afhankelijk zijn van het handelen van andere partijen. Deze partijen hebben vertraging opgelopen of hebben aangegeven niet in de gevraagde maatregelen te kunnen voorzien. De NCTV heeft hierop haar beleid aangepast en aanvullende maatregelen genomen die nog verdere uitwerking behoeven.

2. Voor de uitvoering van haar taken gebruikt de NCTV de volgende eigen kritieke informatiesystemen:
   - [redacted]

   Deze kritieke informatiesystemen beschikken over een actuele risicoanalyse en voldoen aan het VIR 2007 en de BIO.

5. Voor de introductie van het volwassenheidsniveau (NBA) is een nulmeting uitgevoerd. De resultaten zijn eerder gedeeld met [redacted]. In 2021 heeft periodiek overleg plaatsgevonden met de projectleider van [redacted] voor de implementatie en de voortgang voor het NBA-niveau.
   De NCTV heeft zijn processen voldoende ingericht maar het ontbreekt nog aan de juiste structuur om de goede werking en het bestaan aan te tonen. De huidige status van de NCTV processen leidt niet tot (hoge) risico's.

Een toelichting op de IB-activiteiten die de NCTV in het kader van de BIO in 2021 heeft behaald, zijn:

- De aansluiting met het SOC JenV is geëvalueerd;
- Uitvoeren van QuickScans en PIA's voor bestaande projecten en systemen;
- Het projectteam Samen Digitaal heeft de ontwikkelingen met beide Documentmanagementsystemen verder voortgezet;
- Diverse activiteiten om het beveiligingsbewustzijn van de medewerkers te bevorderen zijn gerealiseerd;
- Periodieke controles op autorisaties door de leidinggevenden (eigenaren/verantwoordelijken) zijn uitgevoerd;
- Pentesten zijn door de ADR op diverse projecten en websites uitgevoerd;
- Handreiking persoonsbeveiliging opgesteld;
- Het netwerk voor anoniem surfen op internet is geïmplementeerd;
- De nieuwe Front-end van het gerubriceerde netwerk is uitgerold.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
29 januari 2015

Ons kenmerk
[redacted]

nota

Managementrapportage januari 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

Inleiding
In het kader van het Programma Integrale Beveiliging en het rapporteren van de voortgang op lopende zaken, het oplossen van actiepunten en het melden van incidenten gaan we vanaf heden maandelijks rapporteren. Het doel van de rapportage is om de lijnmanagers instrumenten te geven om op te sturen binnen hun directie of afdeling. Graag ontvangen we feedback op het format en de gepresenteerde zaken.

KWAS 2014
Bij het vaststellen van de KWAS 2014 zijn actiepunten benoemd. De volgende punten zijn al in gang gezet.

- Medewerkers hebben behoefte aan meer duidelijkheid voor hun handelingsperspectief in verhouding tot de veiligheid. Verder is er behoefte aan meer duidelijkheid voor het omgaan met privacy en persoonsgegevens. Beide onderwerpen zijn in een workshop besproken met werkgroepleden beveiliging en introducees zoals de [redacted]. Vanaf 16 februari zullen er afspraken gepland gaan worden binnen de afdelingsoverleggen om beide onderwerpen te bespreken met de medewerkers. De verwachting is dat begin april de resultaten met advies aan het MT voorgelegd kunnen worden.
- Medewerkers hadden behoefte aan privacyfolie voor de iPhone, iPad en laptop. De levering is inmiddels binnengekomen. [redacted] NCTV is gestart met de uitgifte.
- Veiligheidsbewustzijn kan versterkt worden. In samenspraak met de afdeling [redacted] is een communicatieplan 2015 opgesteld. Per kwartaal is een thema benoemd en zal er op diverse manieren aandacht worden besteed aan veiligheidsbewustzijn. De informatie over veiligheid en beveiliging wordt op het intranet geplaatst vanuit het

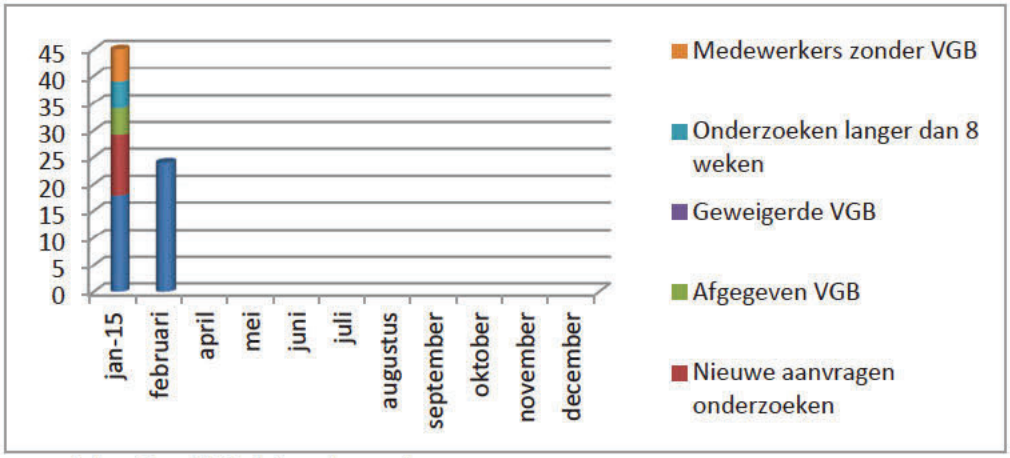
Directie Strategie en Bedrijfsvoering

Datum
29 januari 2015

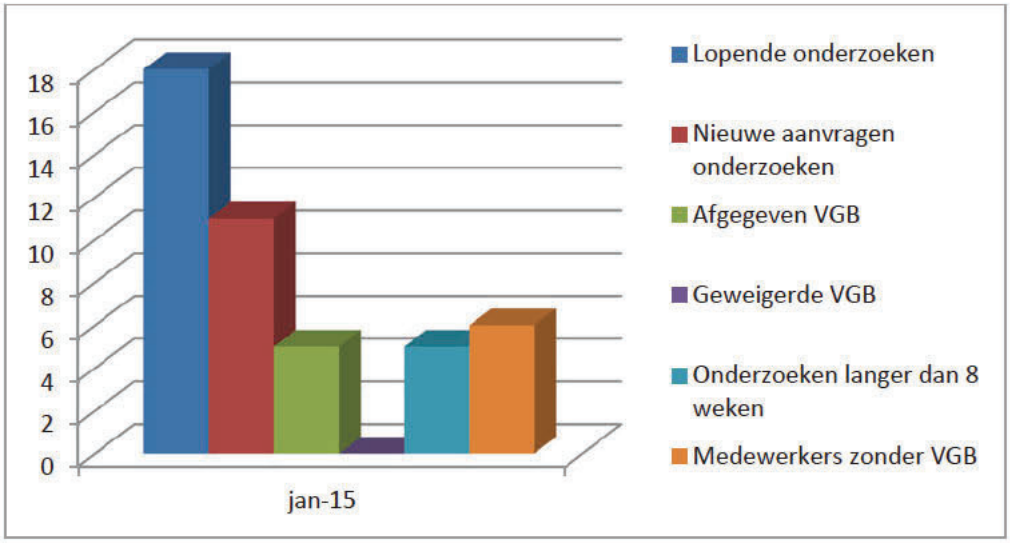
Ons kenmerk
123456

handelingsperspectief van de medewerker en is inmiddels verbeterd en geactualiseerd.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een vereiste om te kunnen werken binnen de NCTV. De afgelopen maand is er een toename te zien van het aantal uitzonderingen om te werken zonder VGB. Verder zijn er 5 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en die dus langer gaan duren dan 8 weken. Het betreft hier veelal onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Zie onderstaand beeld.



Totaal beeld veiligheidsonderzoeken



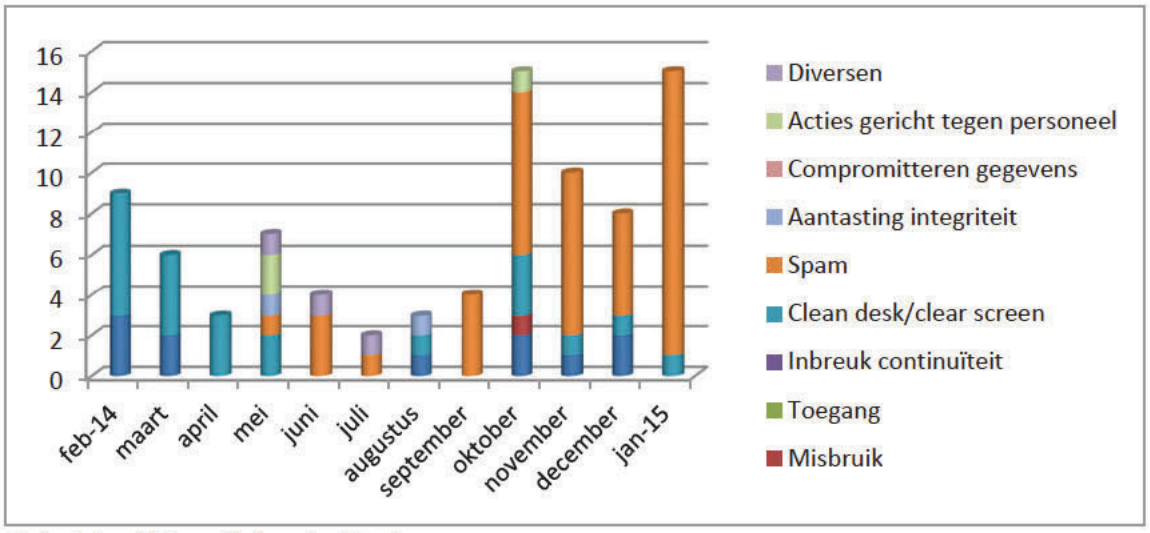
Beeld veiligheidsonderzoeken januari

Directie Strategie en Bedrijfsvoering

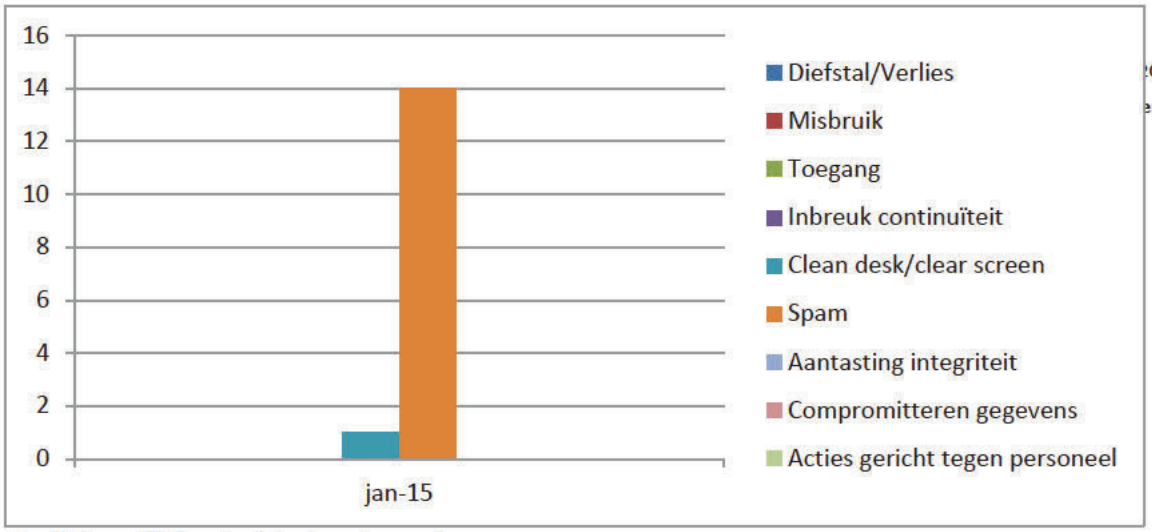
Datum
29 januari 2015

Ons kenmerk
123456

Incidentenregistratie
Binnen de NCTV vinden diverse incidenten plaats. Om een beeld te krijgen over de aard van de incidenten wordt een maandoverzicht gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen. In onderstaand plaatje vindt u het overzicht van de maand januari 2015. Het is de bedoeling om telkens een maand aan het overzicht toe te voegen tot een maximum van twaalf maanden.
In de voorgaande periode hadden we geen softwarepakket om de centrale registratie van incidenten goed bij te houden. Hierdoor is het lastig om trends vanaf 2013 te volgen. In het tweede kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen. Tot op heden werden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Totaal beeld beveiligingsincidenten



Beeld beveiligingsincidenten januari

SPAM/Phising mail
De afgelopen maand hebben we een toename gezien van zowel spam als phising mails. De meldingen zijn doorgezet naar [redacted] Het lijkt er op dat de medewerkers goed omgaan met de bewuste berichten en hiervan op de juiste wijze melding maken.

[redacted]

Hack Twitter
De afgelopen maand hebben er incidenten voorgedaan met het hacken van twitteraccounts. [redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
7 maart 2015

nota

Managementrapportage februari 2015
Programma Integrale Beveiliging

Van

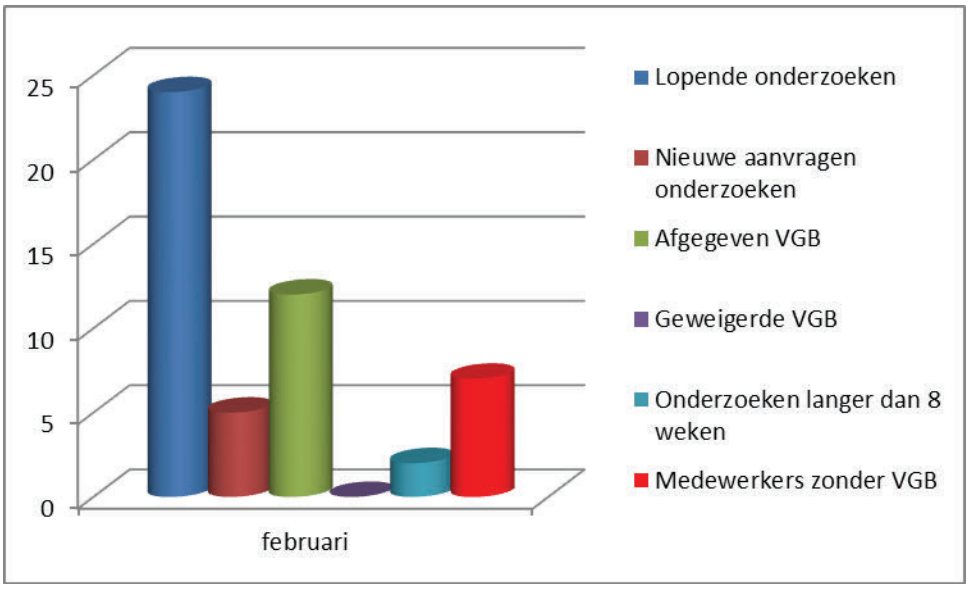
Datum/eindparaaf

Advies
Ter kennisgeving.

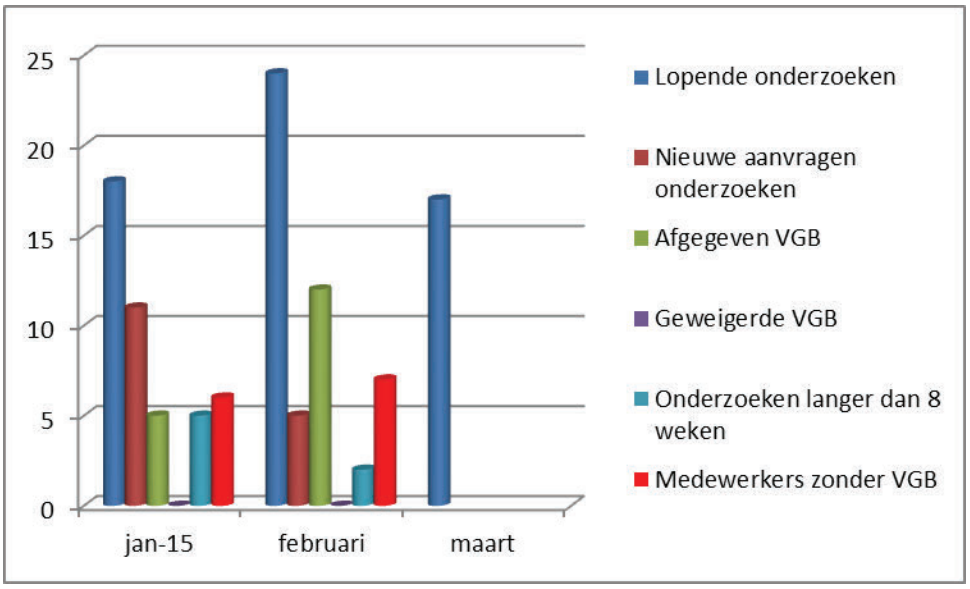
Inleiding
In het kader van het Programma Integrale Beveiliging en het rapporteren van de voortgang op lopende zaken, het oplossen van actiepunten en het melden van incidenten gaan we vanaf heden maandelijks rapporteren. Het doel van de rapportage is om de lijnmanagers instrumenten te geven om op te sturen binnen hun directie of afdeling. Graag ontvangen we feedback op het format en de gepresenteerde zaken.

Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een vereiste om te kunnen werken binnen de NCTV. In tegenspraak tot het bestaande beleid is er in de afgelopen maand een lichte toename te zien van het aantal uitzonderingen om te werken zonder VGB. Verder zijn er 2 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en die dus langer gaan duren dan 8 weken. Het betreft hier veelal onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Zie onderstaand beeld.



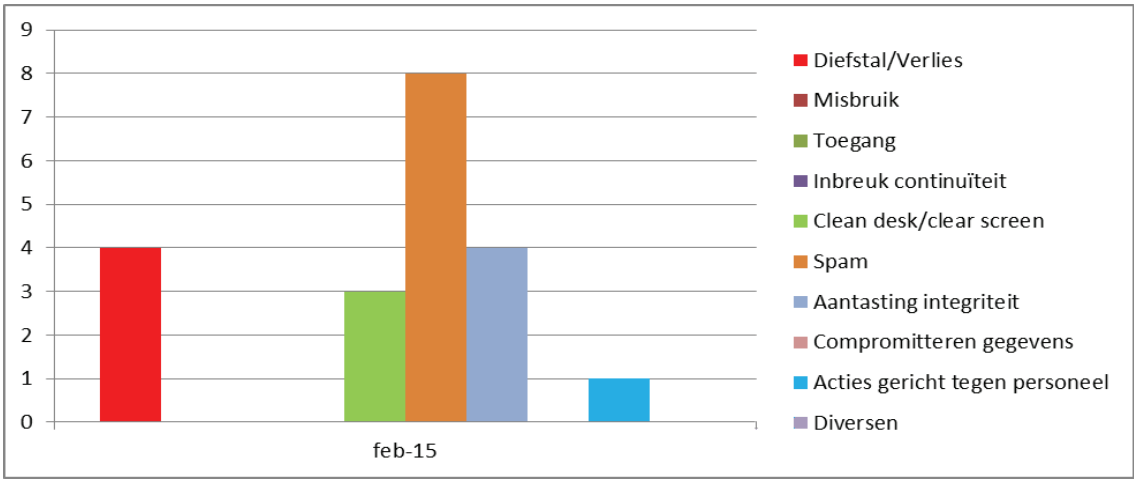
Beeld veiligheidsonderzoeken februari



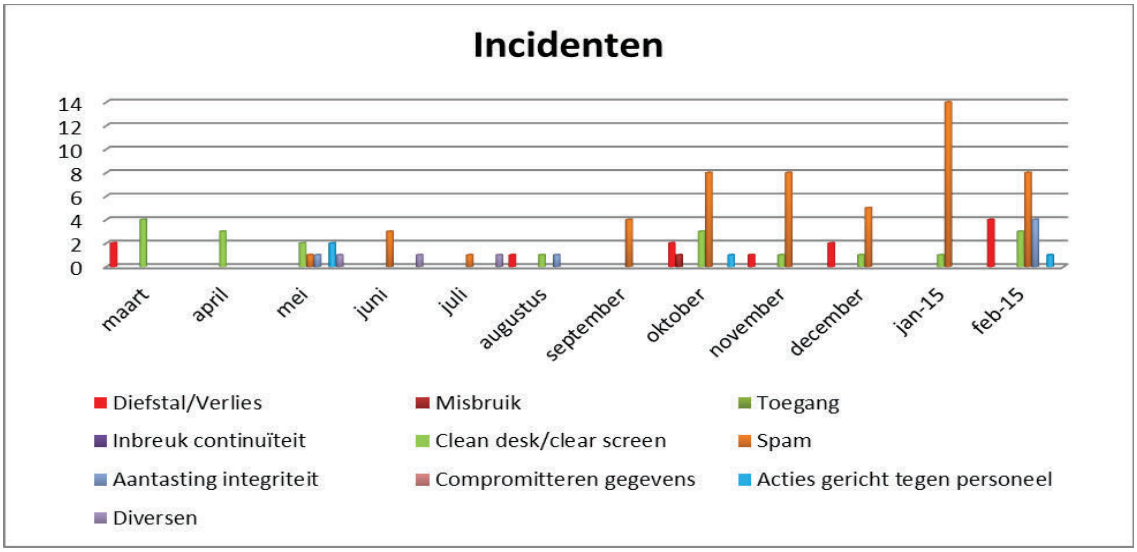
Totaal beeld veiligheidsonderzoeken

Incidentenregistratie

Binnen de NCTV vinden diverse incidenten plaats. Om een beeld te krijgen over de aard van de incidenten wordt een maandoverzicht gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen. In onderstaand plaatje vindt u het overzicht van de maand februari 2015.
Het is de bedoeling om telkens een maand aan het overzicht toe te voegen tot een maximum van twaalf maanden.
In het tweede kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen. Tot op heden werden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Beeld beveiligingsincidenten februari



Totaal beeld beveiligingsincidenten

Toelichting tabellen

SPAM/Phising mail
De afgelopen maand zien we wederom veel spam en phising mails die binnen komen bij medewerkers. De meldingen zijn doorgezet naar [redacted] Het lijkt er op dat de medewerkers goed omgaan met de bewuste berichten en hiervan op de juiste wijze melding maken.

Cleandesk/clear screen
De afgelopen maand zijn er twee sleutelkluizen open aangetroffen en één grote kluis met [redacted]. De betreffende afdelingshoofden zijn geïnformeerd.

Acties gericht tegen personeel
De afgelopen maand heeft er een incident voorgedaan gericht tegen [redacted]

Aantasting integriteit
Er heeft zich een viertal incidenten voorgedaan waarbij; [redacted] De incidenten worden door de betreffende leidinggevenden afgehandeld. Het betreffen incidenten die geen directe dreiging betreffen voor het functioneren van de medewerker.

Diefstal/verlies
Het betreft hier tijdelijk verlies van informatie, verlies van de OV-card, verlies van een [redacted] en verlies van een rijkspas.

Overige incidenten

De trend van toename van digitale incidenten zet zich voort. Binnen de NCTV proberen we zoveel mogelijk preventieve maatregelen te treffen. De meeste kwetsbaarheden worden gemeld door het [redacted]. In het rapport van de KWAS 2014 en CSBN4 wordt al gewaarschuwd voor een toename van nieuwe digitale kwetsbaarheden.

[redacted] interdepartementaal probleem voorgedaan door een DDOS aanval op de website. De werkprocessen van de NCTV zijn niet verstoord door de aanval. Het [redacted] is gedelegeerd eigenaar van de websites van de NCTV. Aan de functioneel beheerder [redacted] is het advies gegeven om voorzorgsmaatregelen te nemen.

[redacted] Er heeft zich geen risico voorgedaan voor de NCTV. Overigens wordt op initiatief van de werkgroep innovatie van de NCTV gezocht naar een oplossing voor de toekomst.

[redacted]

Domeinnaamkaping
Is een probleem dat zich voordoet bij websites die langere tijd niet worden gebruikt en onderhouden worden. Binnen de NCTV loopt nog een project om te onderzoeken of bepaalde [redacted] opgeheven kunnen worden.

[redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
15 april 2015

nota

Managementrapportage maart 2015
Programma Integrale Beveiliging

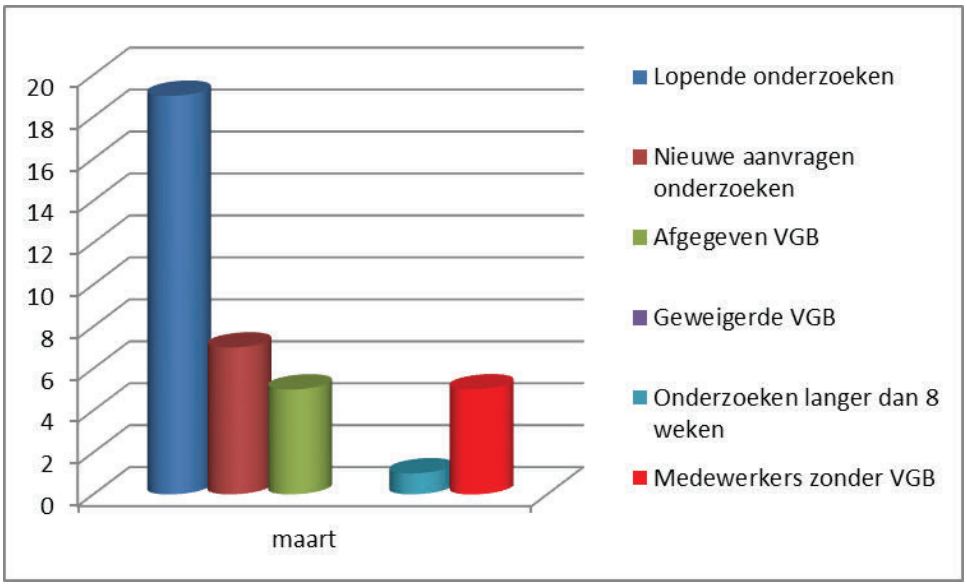
Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

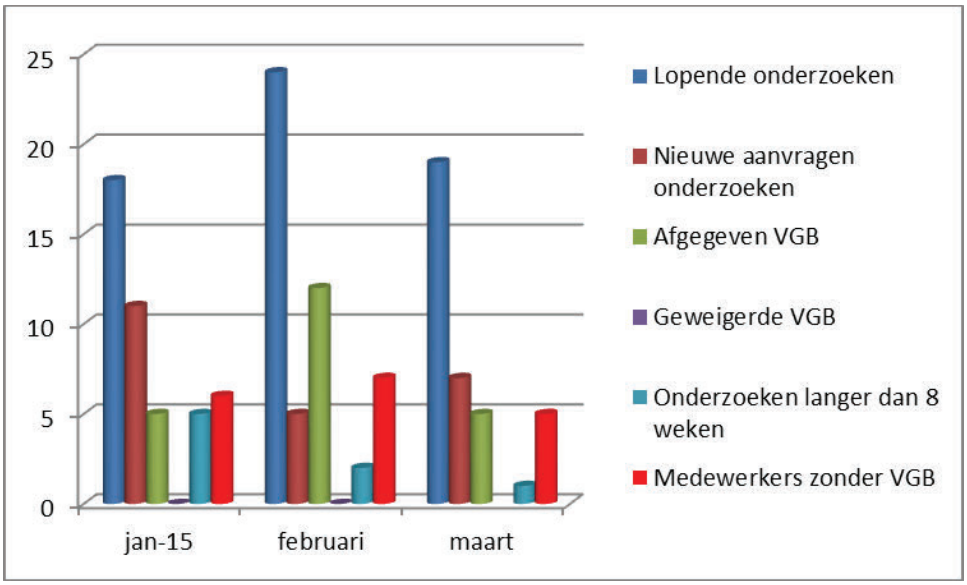
Inleiding
In het kader van het Programma Integrale Beveiliging en het rapporteren van de voortgang op lopende zaken, het oplossen van actiepunten en het melden van incidenten gaan we vanaf heden maandelijks rapporteren. Het doel van de rapportage is om de lijnmanagers instrumenten te geven om op te sturen binnen hun directie of afdeling.

Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een vereiste om te kunnen werken binnen de NCTV. De afgelopen maand was er een afname van het aantal uitzonderingen om te werken zonder VGB. Verder is er 1 onderzoek die niet binnen de gestelde termijn afgerond kon worden en die dus langer gaat duren dan 8 weken. Het betreft hier veelal onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Zie onderstaand beeld.



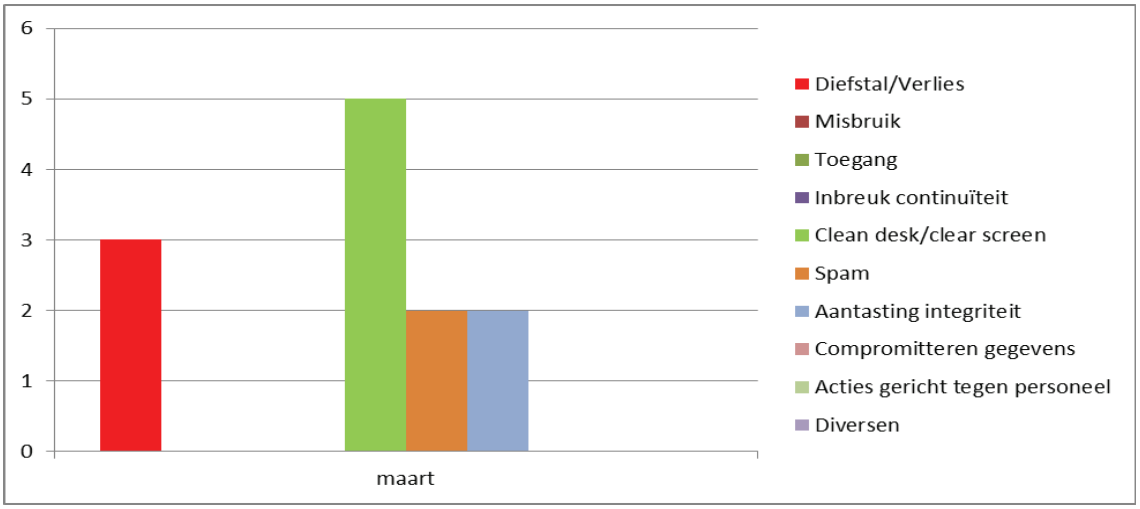
Beeld veiligheidsonderzoeken maart



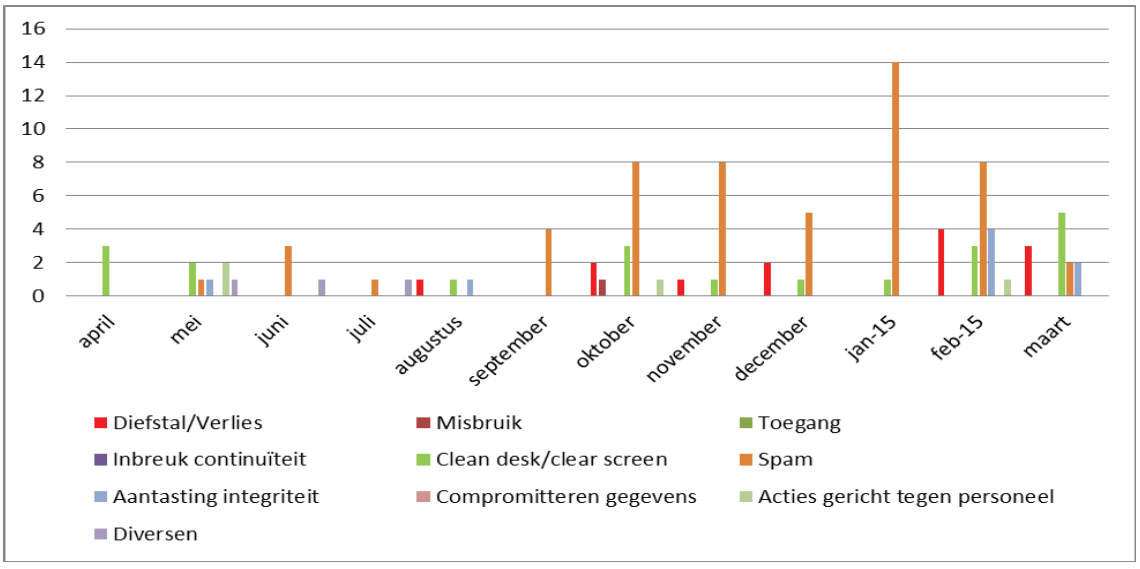
Totaal beeld veiligheidsonderzoeken

Incidentenregistratie

Binnen de NCTV vinden diverse incidenten plaats. Om een beeld te krijgen over de aard van de incidenten wordt een maandoverzicht gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen. In onderstaand plaatje vindt u het overzicht van de maand maart 2015.
Het is de bedoeling om telkens een overzicht te genereren van een maximum van twaalf maanden.
In het tweede kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen.
Tot op heden werden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Beeld beveiligingsincidenten maart



Totaal beeld beveiligingsincidenten

Toelichting tabellen

Diefstal/verlies
Het betreft hier het verlies van een portemonnee binnen de NCTV zone, verlies van de OV-card en het verlies van een [redacted]. De spullen zijn nog niet terug gevonden. De OV-card en het [redacted] zijn geblokkeerd.

Cleandesk/clear screen
De afgelopen maand zijn er twee kluizen open aangetroffen, één bij [redacted] en één bij [redacted]. Er zijn drie incidenten voor wat betreft het aantreffen van [redacted] op de werkplek; [redacted]. De betreffende afdelingshoofden zijn geïnformeerd.

SPAM/Phising mail
De afgelopen maand zien we wederom veel spam en phising mails die binnen komen bij medewerkers. De meldingen zijn doorgezet naar[redacted] [redacted] Het lijkt er op dat de medewerkers goed omgaan met de bewuste berichten en hiervan op de juiste wijze melding maken.

Aantasting integriteit
Er zijn twee computers die na onderzoek besmet met malware bleken te zijn. De computers waren op het [redacted] en in een vergaderzaal in gebruik. De computers zijn onderzocht door het [redacted], maar het is niet meer te achterhalen of door de malware informatie is gecompromitteerd. De computers zijn veilig gesteld.

Overige incidenten

De trend van toename van digitale incidenten zet zich voort. Binnen de NCTV proberen we zoveel mogelijk preventieve maatregelen te treffen. De meeste kwetsbaarheden worden gemeld door het[redacted]. In het rapport van de KWAS 2014 en CSBN4 wordt al gewaarschuwd voor een toename van nieuwe digitale kwetsbaarheden.

Ransomware
Diverse overheidsdiensten hebben al last gehad van e-mailberichten die ransomware (cryptoware) bevatten. Als de attachment wordt geactiveerd dan worden de bestanden in de mappen van de medewerker versleuteld. De huidige oplossing die wordt gebruikt is het verwijderen van de mappen en een backup terug zetten. Binnen de NCTV heeft nog geen besmetting plaats gevonden. (zie ook de NCSC maandmonitor maart)

[redacted]
Er zijn diverse kwetsbaarheden ontdekt in de producten van [redacted]. De NCTV gebruikt ook [redacted] voor het [redacted] Een eerste onderzoek toont aan dat wij nog geen last hebben van de kwetsbaarheden. Verder onderzoek loopt nog.

Social Media
IS bedreigt militairen uit Amerika die op social media uitspraken doen over hun deelname aan de strijd en van wie eenvoudig profielen zijn te vinden. Een soort gelijke actie is in Frankrijk ook op gezet. Gebruik van social media in combinatie met werk gerelateerde informatie dient zorgvuldige afgewogen te worden. Wij nemen dit mee in de uitwerking van de actiepunten van de workshops Veilig werken.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
30 april 2015

nota

Managementrapportage april 2015
Programma Integrale Beveiliging

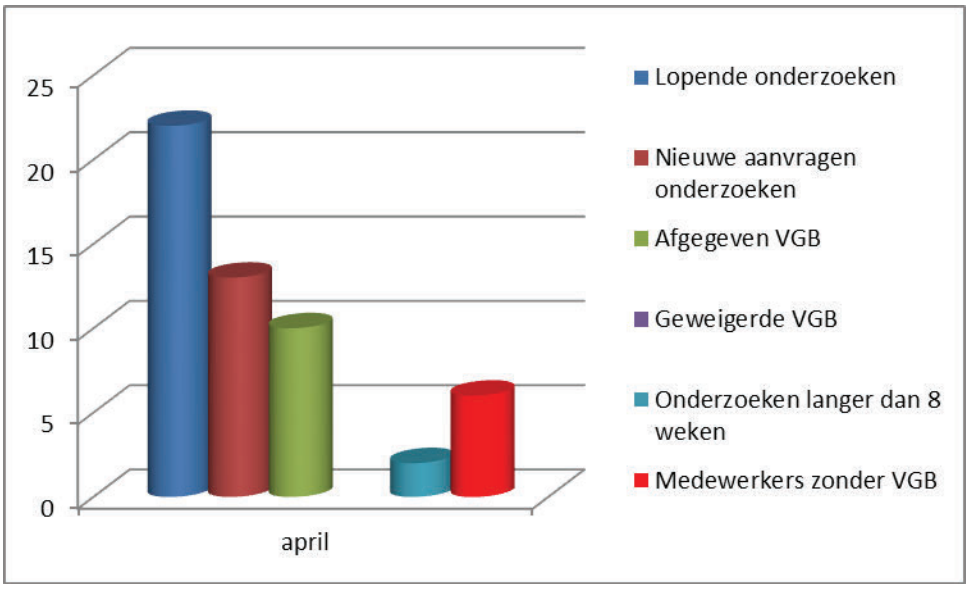
Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

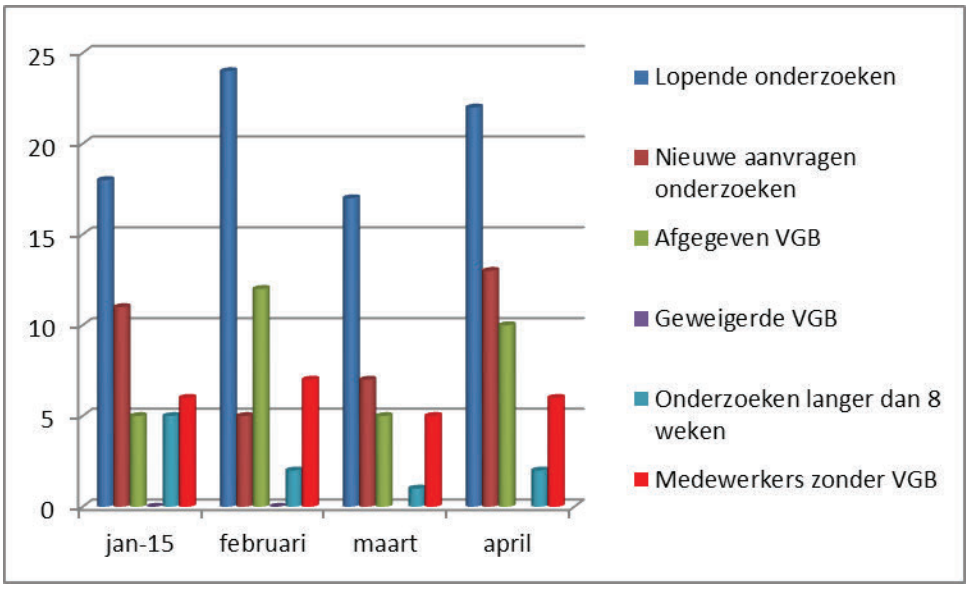
Inleiding
In het kader van het Programma Integrale Beveiliging en het rapporteren van de voortgang op lopende zaken, het oplossen van actiepunten en het melden van incidenten gaan we vanaf heden maandelijks rapporteren. Het doel van de rapportage is om de lijnmanagers instrumenten te geven om op te sturen binnen hun directie of afdeling.

Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een vereiste om te kunnen werken binnen de NCTV. De afgelopen maand was er een toename van het aantal uitzonderingen om te werken zonder VGB. Het betreft hier allemaal ICT medewerkers voor het [redacted] die tijdelijk gaan werken bij het [redacted] Verder zijn er 2 onderzoeken die niet binnen de gestelde termijn afgerond kon worden en die dus langer gaat duren dan 8 weken. Het betreft hier veelal onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Zie onderstaand beeld.



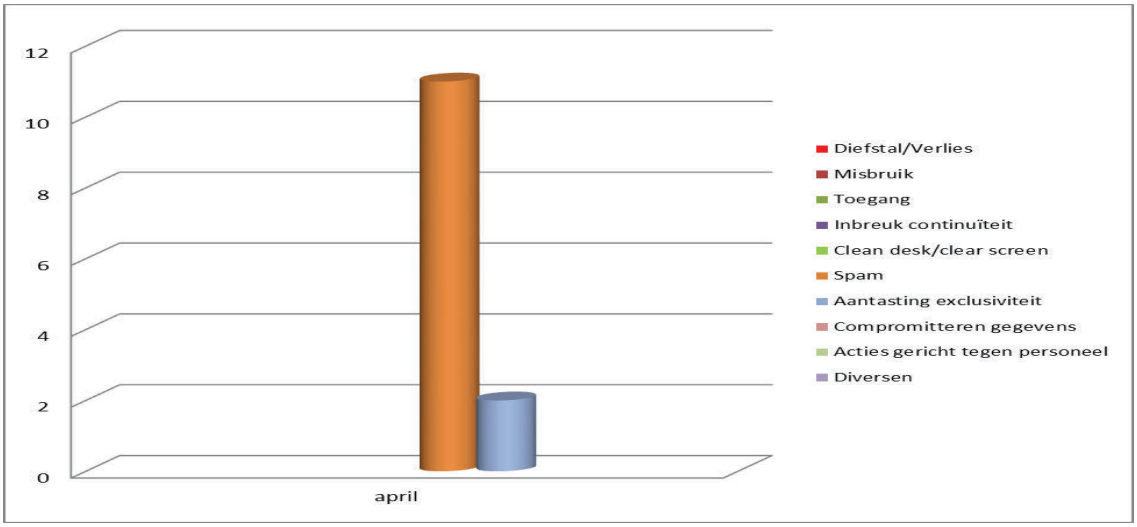
Beeld veiligheidsonderzoeken april



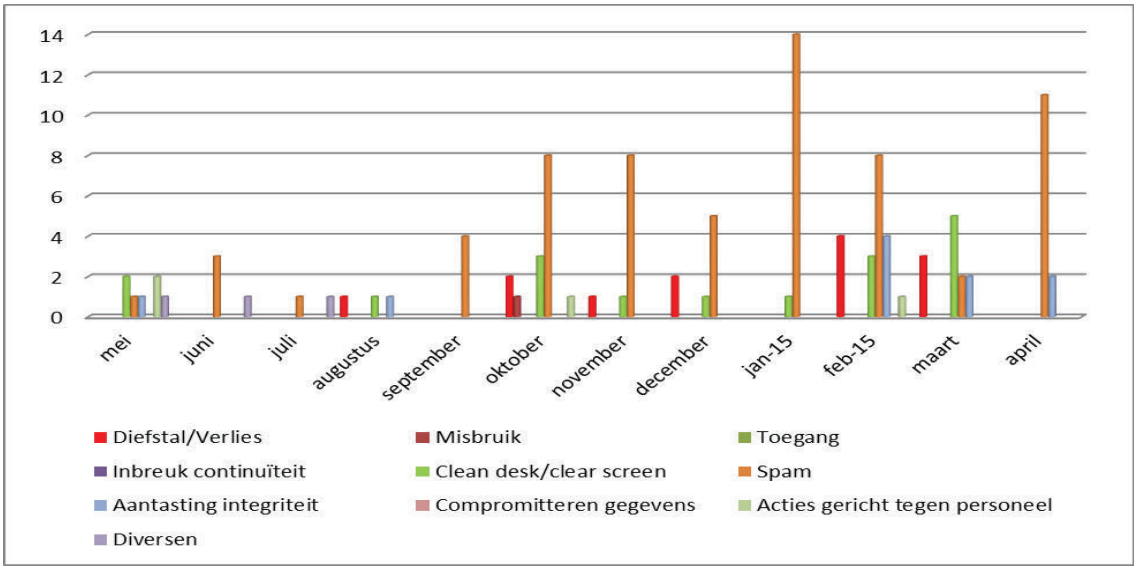
Totaal beeld veiligheidsonderzoeken

Incidentenregistratie

Binnen de NCTV vinden diverse incidenten plaats. Om een beeld te krijgen over de aard van de incidenten wordt een maandoverzicht gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen. In onderstaand plaatje vindt u het overzicht van de maand april 2015.
Het is de bedoeling om telkens een overzicht te genereren van een maximum van twaalf maanden.
In het tweede kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen.
Tot op heden werden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Beeld beveiligingsincidenten april



Totaal beeld beveiligingsincidenten

Toelichting tabellen

Diefstal/verlies
Geen meldingen

Cleandesk/clear screen
Geen meldingen

SPAM/Phising mail
We zien een toename in het aantal meldingen van spam en phising mails die NCTV medewerkers ontvangen. De meldingen zijn doorgezet naar [redacted]. Het lijkt er op dat de NCTV medewerkers goed omgaan met de bewuste berichten en hiervan op de juiste wijze melding maken. Via het intranet NCTV zal aandacht worden besteed aan de toename en risico's van phising mail en ransomware.

Aantasting exclusiviteit
Een externe deelnemer van een overleg twittert een foto van een presentatie over contraterrorisme, cybersecurity en crisisbeheersing. De diverse diensten signaleren het bericht. Imagoschade is beperkt gebleven.
Psychiater die twittert over NCTV en dat hij bij de NCTV werkt. Beiden berichten kloppen niet maar geven wel een beeld over de NCTV en veroorzaken ook reacties bij netwerkpartners.

Overige

De trend van toename van digitale incidenten zet zich voort. Binnen de NCTV proberen we zoveel mogelijk preventieve maatregelen te treffen. De meeste kwetsbaarheden worden gemeld door het [redacted]. In het rapport van de KWAS 2014 en CSBN4 wordt al gewaarschuwd voor een toename van nieuwe digitale kwetsbaarheden.

[redacted]
Er is opnieuw een kwetsbaarheid aangetroffen op de [redacted]. De NCTV gebruikt de [redacted]. De chip is gekraakt waardoor kwaadwillenden toegang hebben tot de informatie op de kaart, het saldo of producten. [redacted] neemt nog geen maatregelen omdat er nog geen fraude is gepleegd met de card. Het risico voor de NCTV is laag omdat de kaarten niet persoonsgebonden zijn en dus geen persoonlijke data van gebruikers bevatten.

Spionage
Het aantal pogingen en daadwerkelijke daden neemt de laatste tijd in de wereld enorm toe. Ook hacktivisten behoren tot de dadergroep. Het risico op spionage komt steeds dichter bij. De noodzaak tot het nemen van passende en soms aanvullende maatregelen wordt belangrijker. Binnen de NCTV zijn we SIEM aan het implementeren waardoor monitoring en logging beter uitgevoerd kan worden op [redacted]. Siem is een product om afwijkend gedrag van gebruikers of systeemverkeer te signaleren. Bij afwijkend gedrag worden incidentmeldingen gegeneerd die resulteren in een nader onderzoek. Bij VenJ wordt het SOC

(security operations centre) ingevoerd. Het SOC is met name bedoeld voor het generieke VenJ netwerk. De producten/maatregelen bevinden zich nog in de implementatiefase. Verder worden in Q2 pentesten uitgevoerd op de websites. Een andere trend die wordt waargenomen is het gebruik van informatie op social media door statelijke actoren en hacktivisten.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
2 juni 2015

nota

Managementrapportage mei 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. Op dit moment zijn er 6 medewerkers werkzaam bij de NCTV zonder VGB. Het betreft hier allemaal [redacted] medewerkers voor het [redacted] die tijdelijk gaan werken bij [redacted] werkzaamheden verricht.
Ik wil er nogmaals op wijzen dat gedogen formeel niet is toegestaan en dat hier sprake is van een kwetsbaarheid voor de NCTV.

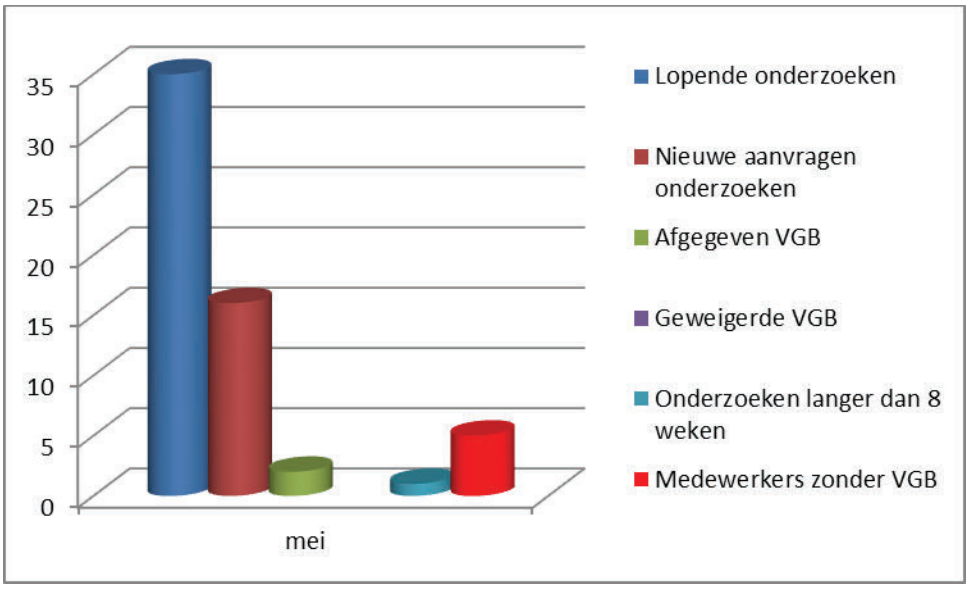
Verder is er 1 onderzoek dat niet binnen de gestelde termijn afgerond kon worden en dus langer duurt dan 8 weken. Het betreft hier veelal onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. In de maand mei is het aantal aanvragen voor een veiligheidsonderzoek fors toegenomen. Hierdoor is het aantal lopende onderzoeken (35) ook hoog.

Een feit is nu dat de doorlooptijd van onderzoeken langer is dan gebruikelijk. In het verleden werden onderzoeken soms met 5 tot 6 weken afgerond. Nu duren die onderzoeken 9 weken. Gezien het feit dat de kosten van de onderzoeken nog niet worden doorbelast en aan de wettelijke termijn van 9 weken wordt voldaan, hebben we ook geen mogelijkheid te klagen.

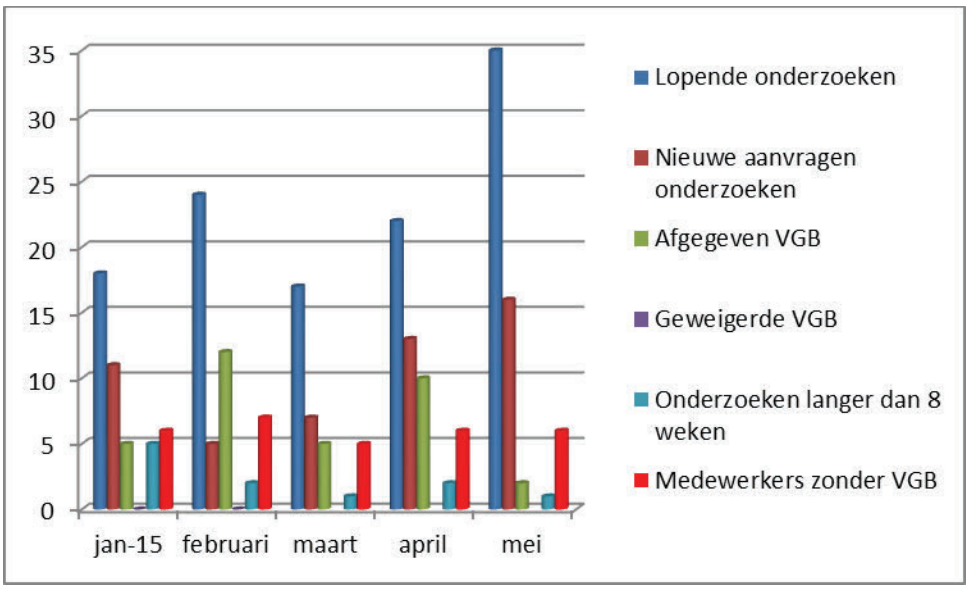
Wat we merken is dat tijdens de selectiegesprekken of arbeidsvoorwaardengesprekken onvoldoende geïnformeerd wordt naar de persoonlijke omstandigheden van kandidaten. Bij het inleveren van de aanvragen van onderzoeken komen we er achter dat de kandidaat of diens partner een verblijf heeft gehad in het buitenland. Deze informatie is van belang omdat dat een mogelijke indicatie is dat het onderzoek langer dan 9 weken gaat duren

(soms maanden). Voor het vervullen van een vacature al dan niet tijdelijk kan dat belangrijke informatie zijn.

Zie onderstaand beeld.



Beeld veiligheidsonderzoeken mei

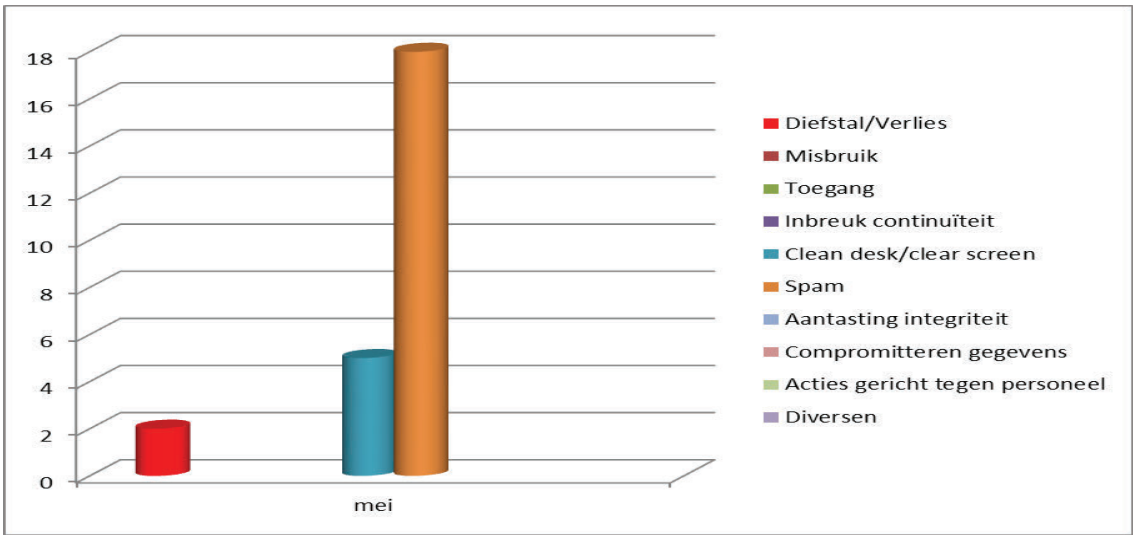


Totaal beeld veiligheidsonderzoeken 2015

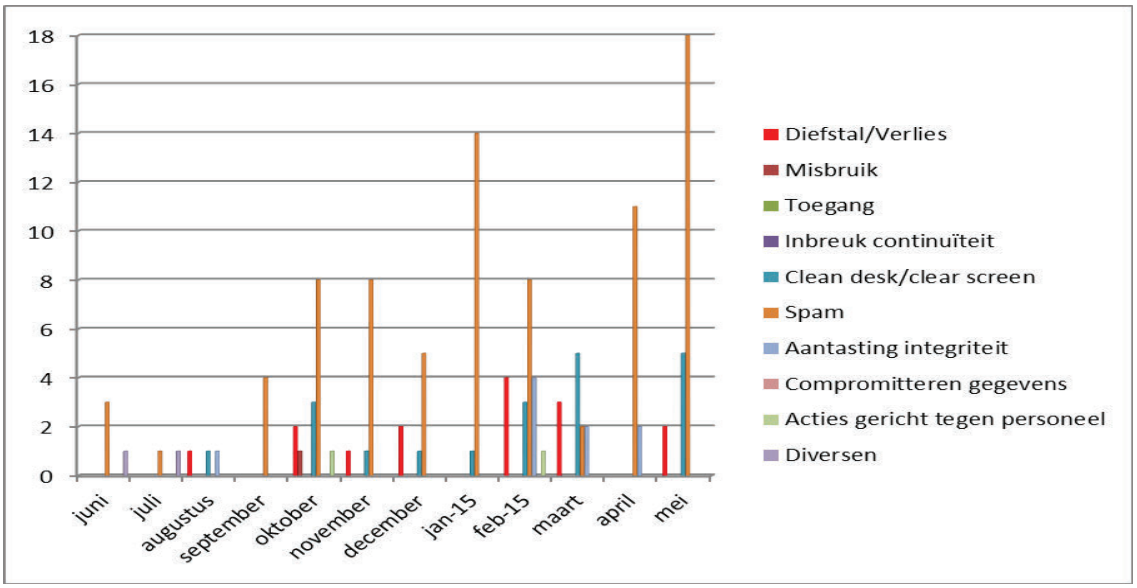
Incidentenregistratie

Om een beeld te krijgen over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.

In het derde kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen. Tot op heden werden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Beeld beveiligingsincidenten mei



Totaal beeld beveiligingsincidenten

Toelichting tabellen

Diefstal/verlies
Van twee medewerkers is de afgelopen maand de iPad gestolen. Beide iPads zijn door het [redacted] op afstand gewist en onbruikbaar gemaakt. Het risico is klein dat de daders informatie van de NCTV hebben gecompromitteerd.

Cleandesk/clear screen
De afgelopen maand hebben 5 medewerkers hun [redacted] voor het [redacted] na gebruik niet opgeborgen. De [redacted] zijn veilig gesteld en in de kluis bij de [redacted] opgeborgen.

SPAM/Phising mail
In de maand mei zijn er 18 meldingen van Spam gedaan door medewerkers. Er zijn twee berichten binnengekomen waarvan vast staat, na onderzoek, dat er sprake was van een phising-mail. [redacted] is verantwoordelijk voor het aanpassen van de filters en het nemen van extra maatregelen om de risico's te beperken. De afgelopen maand is er een artikel over Ransomware geplaatst op het [redacted] NCTV om de medewerkers te wijzen op de mogelijke risico's.

Overige

[redacted]

[redacted] *laptops*
In de maand mei zijn wederom beveiligingslekken ontdekt in de software van [redacted] laptops. [redacted] laptops zijn in gebruik bij de directie [redacted]. [redacted]

[redacted]
In de afgelopen maanden is de [redacted] door de ADR (Auditdienst Rijk) onderworpen aan een penetratietest. Uit de test is gebleken dat de geconstateerde bevindingen zijn verholpen en dat er zich op dit moment geen kwetsbaarheden voordoen.

Medewerkers zonder VGB
Voor medewerkers zonder VGB maar die wel binnen de NCTV werkzaamheden mogen verrichten, worden extra afspraken gemaakt omtrent autorisaties tot ICT mappen en autorisaties voor de rijkspas. Deze medewerkers zijn geen bezoeker en dragen geen herkenbare (bezoekers)pas met koord. Voor de NCTV medewerkers en [redacted] zijn zij niet zichtbaar.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
2 juli 2015

nota

Managementrapportage juni 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

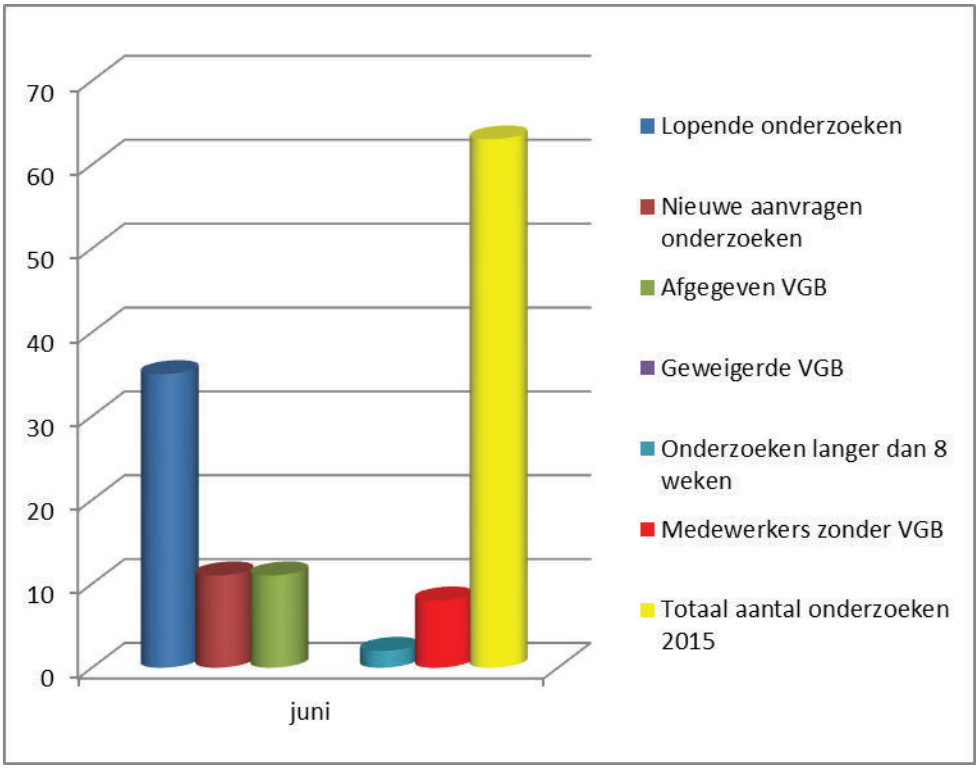
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. Op dit moment zijn er 8 medewerkers (met waiver) werkzaam bij de NCTV zonder VGB. Het betreft hier allemaal [redacted] voor het [redacted] die tijdelijk werken bij het [redacted] werkzaamheden verricht.

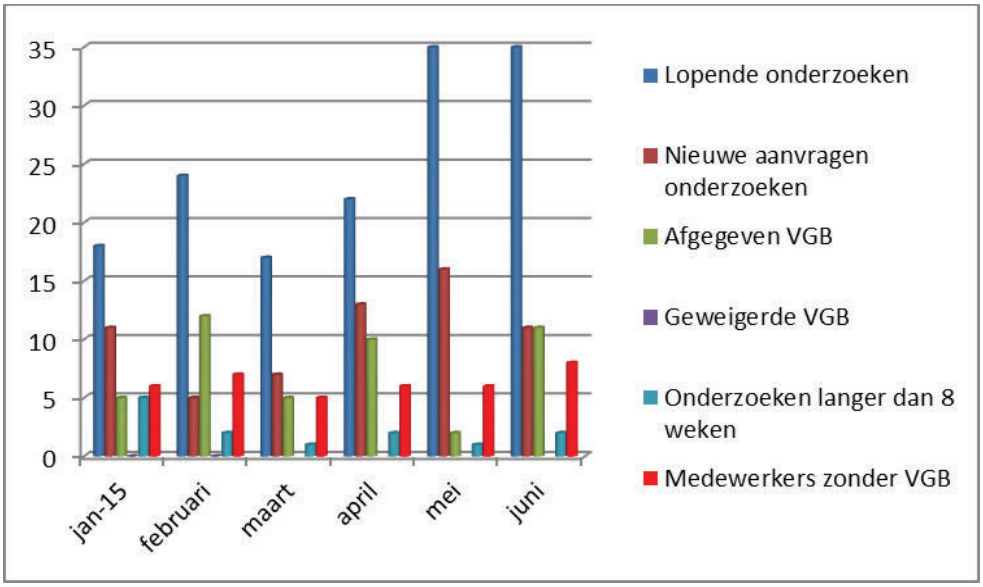
Verder zijn er 2 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en dus langer duren dan 8 weken. Het betreft hier onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Het aantal lopende onderzoeken blijft hoog met 35. In 2015 zijn er 63 aanvragen gedaan voor een veiligheidsonderzoek.

[redacted]

Zie onderstaand beeld.



Beeld veiligheidsonderzoeken juni

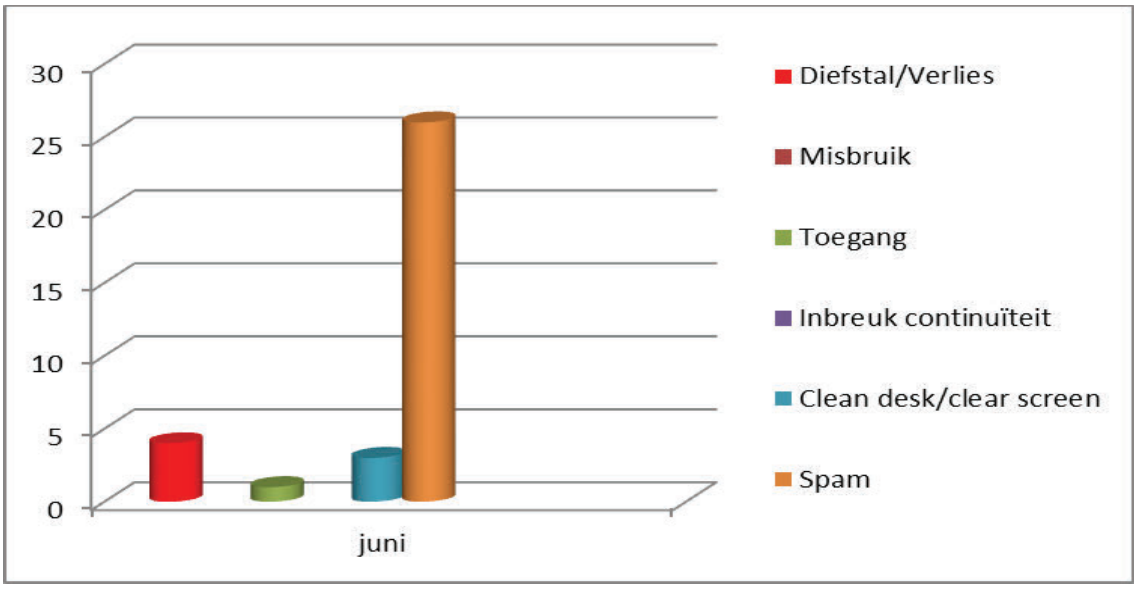


Totaal beeld veiligheidsonderzoeken 2015

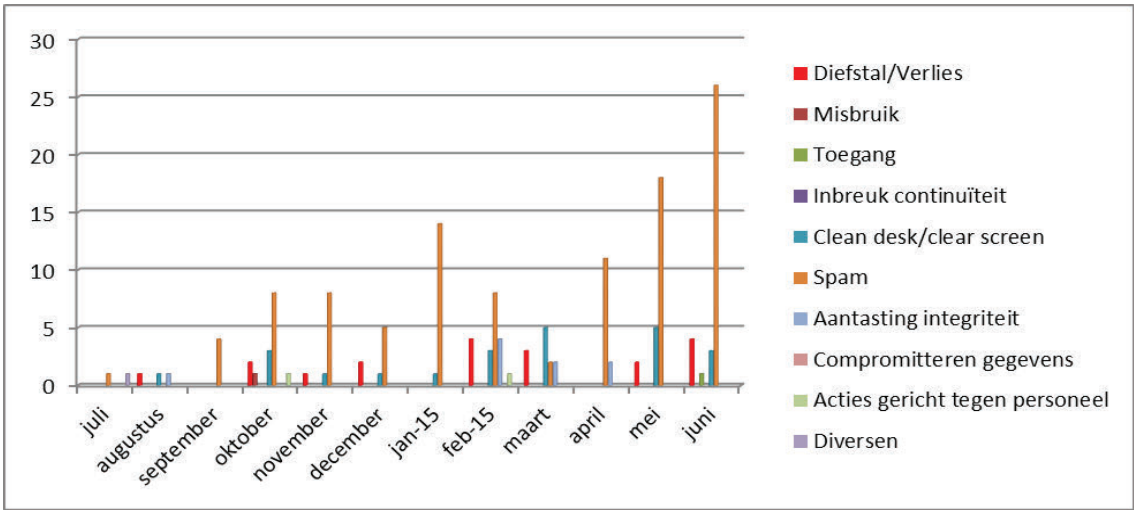
Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.

In het derde kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen. Tot op heden worden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Beeld beveiligingsincidenten juni



Totaal beeld beveiligingsincidenten

Toelichting tabellen

Diefstal/verlies
Van een medewerker is de afgelopen maand de iPad gestolen. De iPad is door het [redacted] op afstand gewist en onbruikbaar gemaakt. Het risico is klein dat de daders informatie van de NCTV hebben gecompromitteerd. Drie medewerkers verloren hun rijkspas die direct na melding inactief is gemaakt voor gebruik.

Toegang
Een niet geautoriseerde beveiligingsmedewerker heeft met een hoofdsleutel de deur van de operationele ruimte op de 4e etage van de NCTV geopend. [redacted]

Cleandesk/clear screen
De afgelopen maand hebben 8 medewerkers [redacted] voor het [redacted] na vertrek niet opgeborgen. De [redacted] zijn door de [redacted] beveiligers veilig gesteld en in de kluis bij de receptie opgeborgen. Het verzoek aan de lijnmanagers is om de medewerkers te attenderen op correct beheer van de [redacted]. Tijdens de cleandesk campagne in september zal er ook extra aandacht aan worden besteed.

SPAM/Phising mail
In de maand mei zijn er 26 meldingen van Spam gedaan door medewerkers. [redacted] is verantwoordelijk voor het aanpassen van de filters en het nemen van extra maatregelen om de risico's te beperken. De komende maand zal er een artikel over Spam geplaatst worden op het intranet NCTV om de medewerkers te wijzen op de mogelijke risico's.

Overige

[redacted]

Jezelf succesvol presenteren op LinkedIn
Via de mail werd een bericht gestuurd naar alle medewerkers met een uitnodiging en tips om je op LinkedIn te presenteren. Deze mail werd door een aantal medewerkers gezien als spam. Het bleek om een actie te gaan van de Directie

Voorlichting VenJ. Het was niet de bedoeling om het naar de NCTV te sturen. De [redacted] heeft hierover overleg gevoerd met de Directie Voorlichting en we hebben afspraken gemaakt voor de toekomst en de behoefte uitgesproken om elkaar te ondersteunen en te versterken.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
2 juli 2015

nota

Managementrapportage juni 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

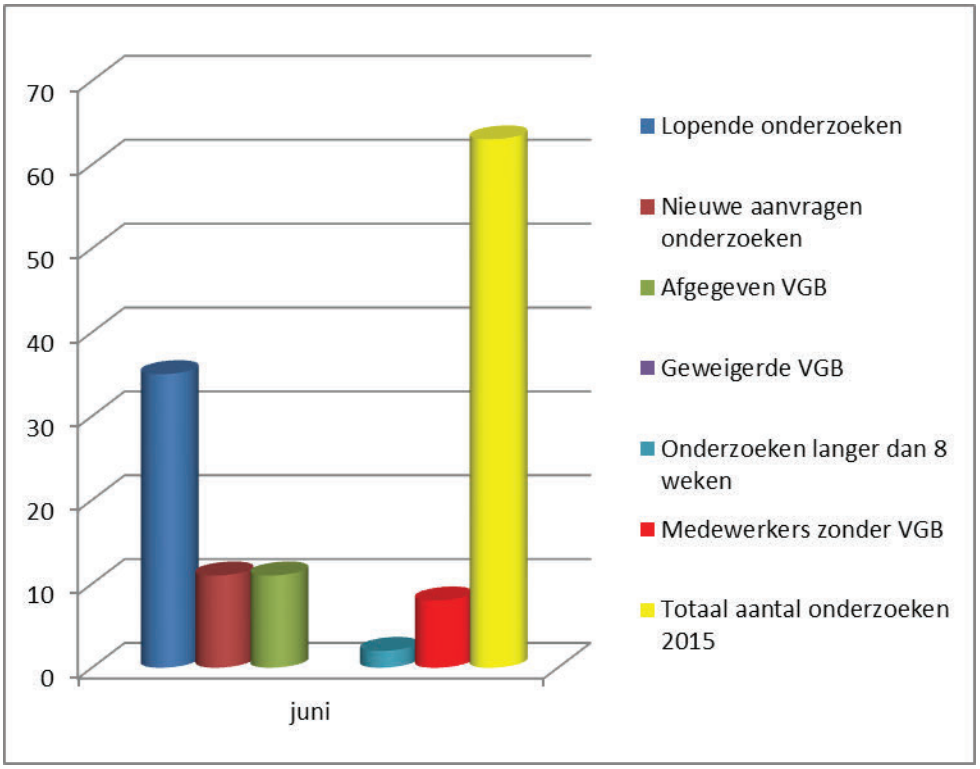
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. Op dit moment zijn er 8 medewerkers (met waiver) werkzaam bij de NCTV zonder VGB. Het betreft hier allemaal [redacted] voor het [redacted] die tijdelijk werken bij het [redacted] werkzaamheden verricht.

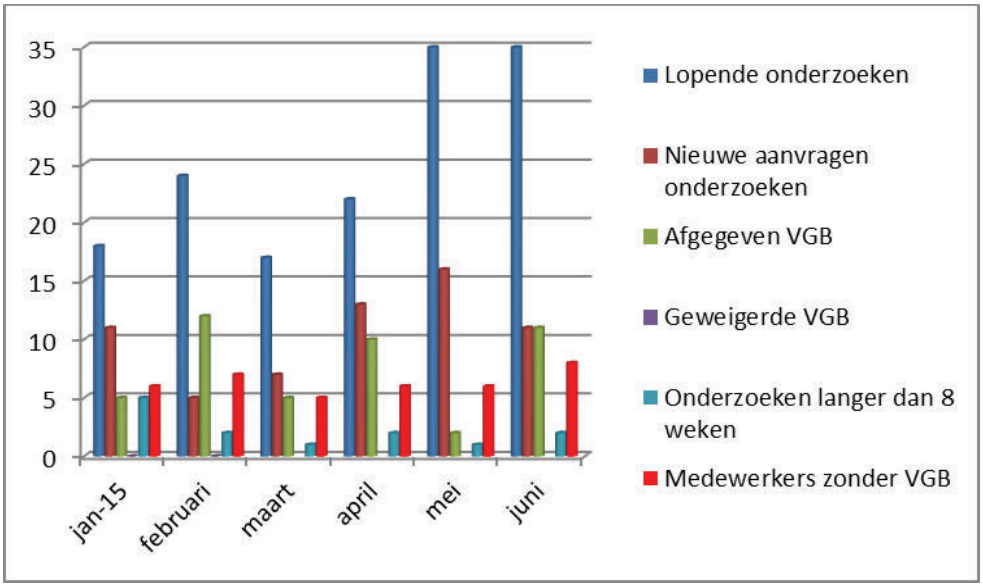
Verder zijn er 2 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en dus langer duren dan 8 weken. Het betreft hier onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Het aantal lopende onderzoeken blijft hoog met 35. In 2015 zijn er 63 aanvragen gedaan voor een veiligheidsonderzoek.

[redacted]

Zie onderstaand beeld.



Beeld veiligheidsonderzoeken juni

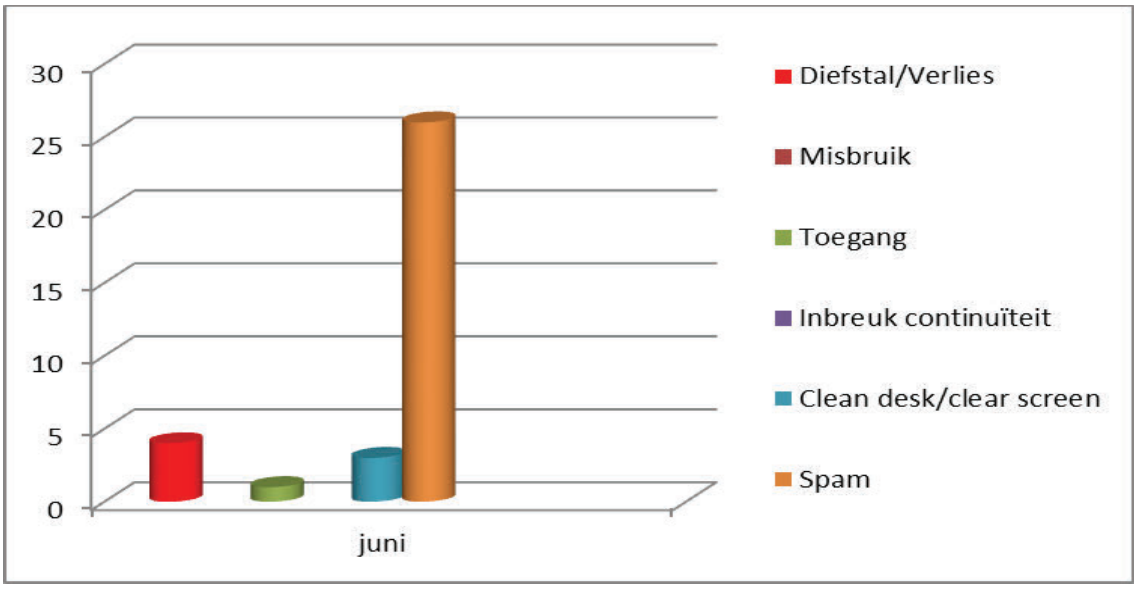


Totaal beeld veiligheidsonderzoeken 2015

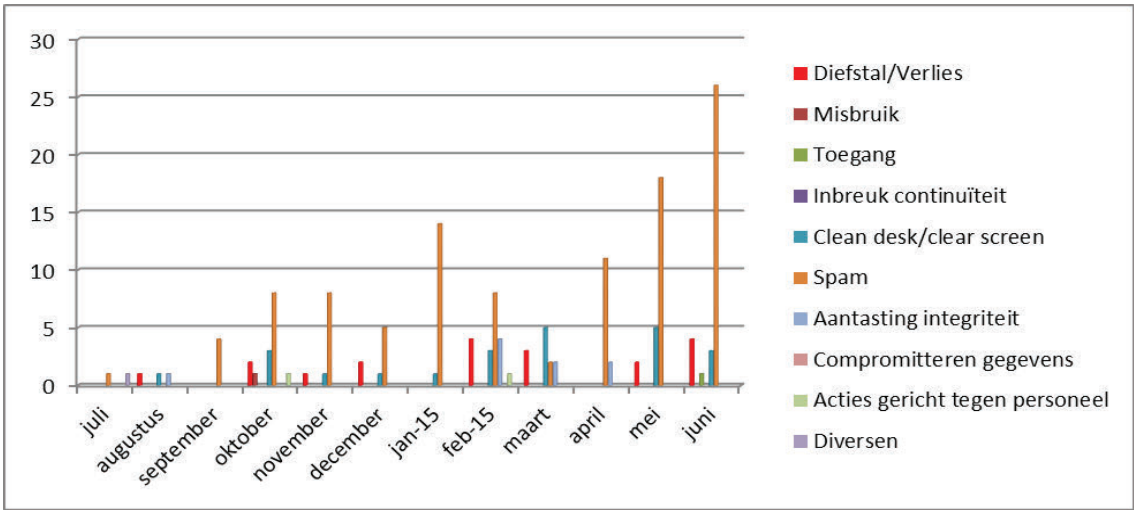
Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.

In het derde kwartaal zal cleandesk meer onder de aandacht worden gebracht en zullen we de lijnmanagers voorzien van informatie waarop zij kunnen sturen. Tot op heden worden alleen ernstige cleandesk incidenten direct aan de lijnmanagers gemeld.



Beeld beveiligingsincidenten juni



Totaal beeld beveiligingsincidenten

Toelichting tabellen

Diefstal/verlies
Van een medewerker is de afgelopen maand de iPad gestolen. De iPad is door het [redacted] op afstand gewist en onbruikbaar gemaakt. Het risico is klein dat de daders informatie van de NCTV hebben gecompromitteerd. Drie medewerkers verloren hun rijkspas die direct na melding inactief is gemaakt voor gebruik.

Toegang
Een niet geautoriseerde beveiligingsmedewerker heeft met een hoofdsleutel de deur van de operationele ruimte op de 4e etage van de NCTV geopend. [redacted]

Cleandesk/clear screen
De afgelopen maand hebben 8 medewerkers [redacted] voor het [redacted] na vertrek niet opgeborgen. De [redacted] zijn door de [redacted] beveiligers veilig gesteld en in de kluis bij de receptie opgeborgen. Het verzoek aan de lijnmanagers is om de medewerkers te attenderen op correct beheer van de [redacted]. Tijdens de cleandesk campagne in september zal er ook extra aandacht aan worden besteed.

SPAM/Phising mail
In de maand mei zijn er 26 meldingen van Spam gedaan door medewerkers. [redacted] is verantwoordelijk voor het aanpassen van de filters en het nemen van extra maatregelen om de risico's te beperken. De komende maand zal er een artikel over Spam geplaatst worden op het intranet NCTV om de medewerkers te wijzen op de mogelijke risico's.

Overige

[redacted]

Jezelf succesvol presenteren op LinkedIn
Via de mail werd een bericht gestuurd naar alle medewerkers met een uitnodiging en tips om je op LinkedIn te presenteren. Deze mail werd door een aantal medewerkers gezien als spam. Het bleek om een actie te gaan van de Directie

Voorlichting VenJ. Het was niet de bedoeling om het naar de NCTV te sturen. De [redacted] heeft hierover overleg gevoerd met de Directie Voorlichting en we hebben afspraken gemaakt voor de toekomst en de behoefte uitgesproken om elkaar te ondersteunen en te versterken.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
3 september 2015

nota

Managementrapportage juli/augustus 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

Toelichting
In verband met de zomervakantie zijn de maandrapportages van juli en augustus samengevoegd.

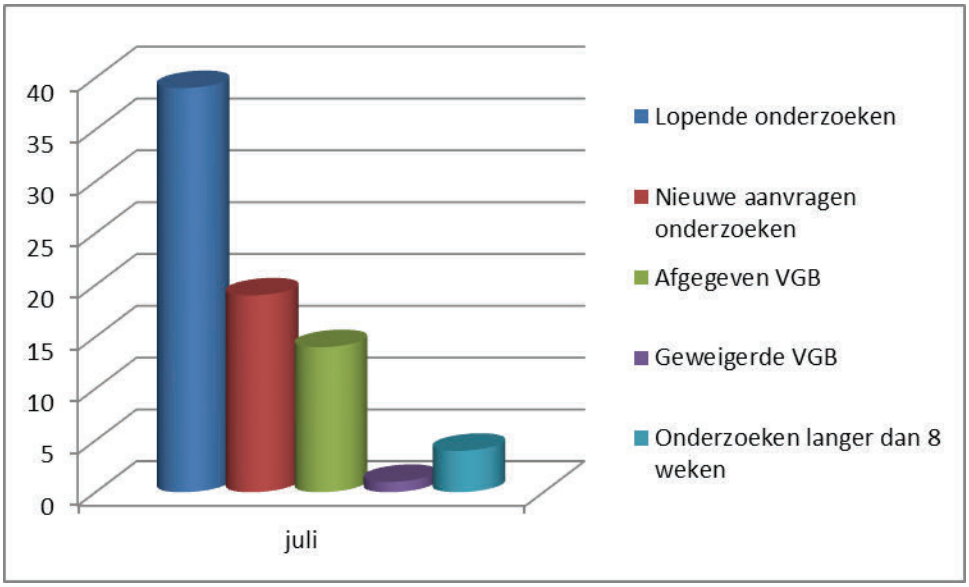
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie.

Er zijn 3 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en dus langer duren dan 8 weken. Het betreft hier onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd. Het aantal verzoeken tot onderzoeken is gestegen door de verwachte komst van trainees, stagiaires en nieuwe medewerkers in september.

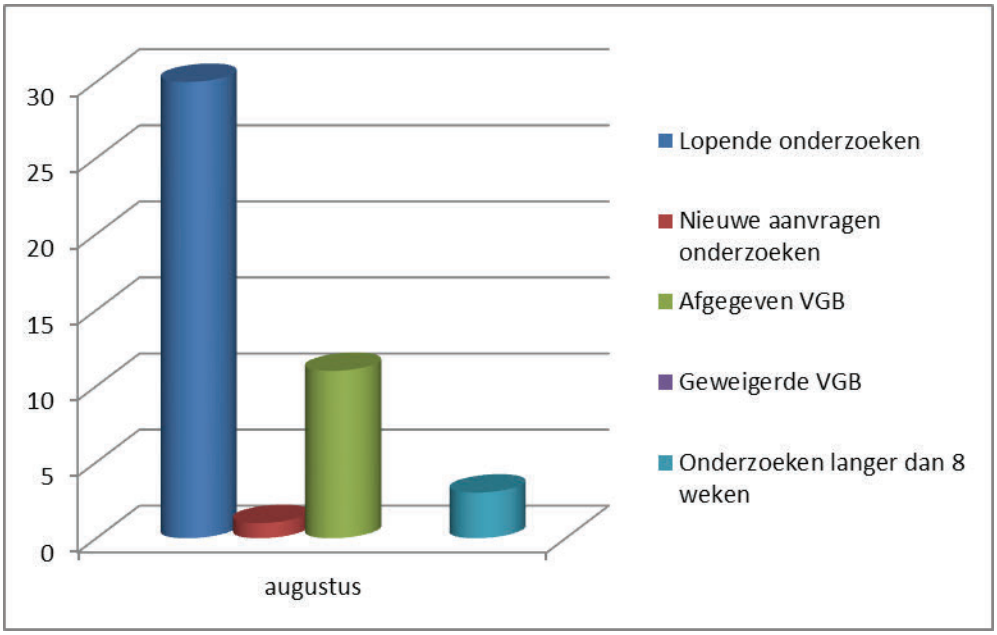
[redacted]

De doorlooptijd van onderzoeken is nog steeds langer dan gebruikelijk, nu 10 tot 12 weken.

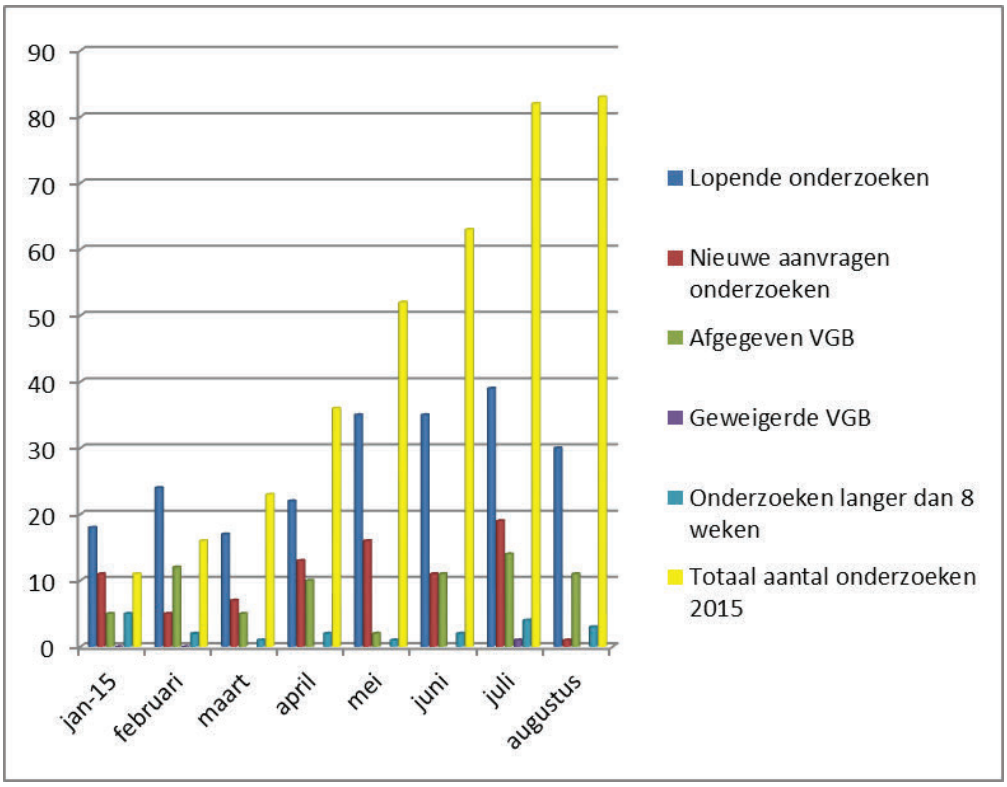
Zie onderstaand beeld.



Beeld veiligheidsonderzoeken juli



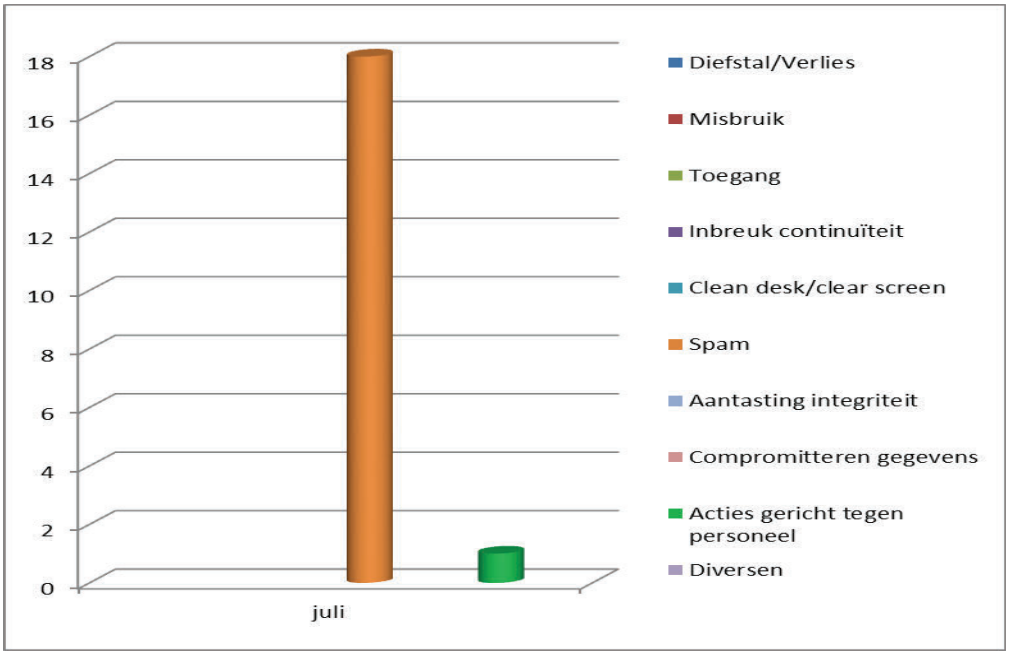
Beeld veiligheidsonderzoeken augustus



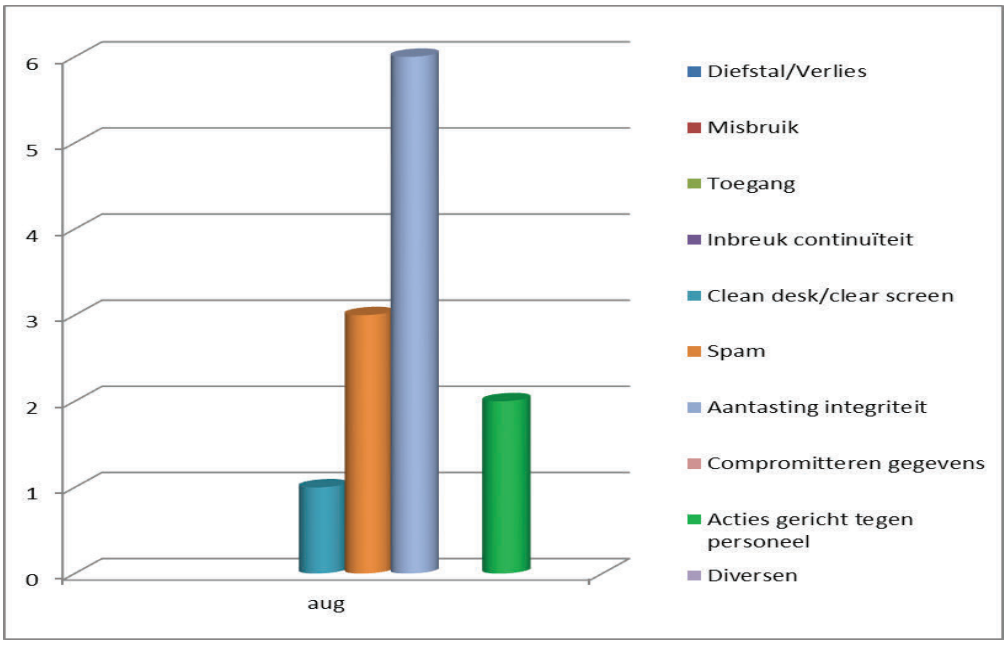
Totaal beeld veiligheidsonderzoeken 2015

Incidentenregistratie

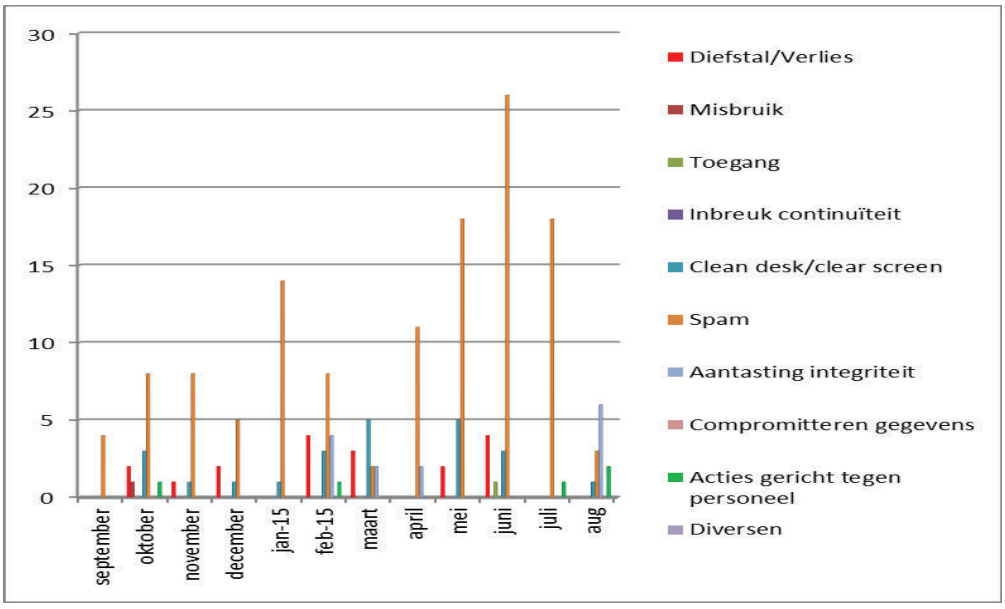
Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten juli



Beeld beveiligingsincidenten augustus



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Diefstal/verlies
Er zijn geen meldingen gemaakt van verlies of diefstal.

Cleandesk/clear screen

Er hebben zich geen ernstige incidenten voorgedaan in het kader van het cleandeskbeleid.

SPAM/Phising mail
In de afgelopen maanden is het aantal meldingen afgenomen.
De komende maand zal er een artikel over Spam geplaatst worden op het intranet NCTV om de medewerkers te wijzen op de mogelijke risico's.

Acties gericht tegen personeel

- In juli heeft zich een incident voorgedaan tijdens een cursus op een externe locatie. In eerste instantie leek er sprake te zijn van een mogelijke dreiging naar de medewerkers NCTV. Na onderzoek door de lokale politie bleek het te gaan om een actie door een verwarde persoon. Het incident is geëvalueerd door de leidinggevende en zijn medewerkers.
- In augustus is er een melding gemaakt, bij de beveiliging, over een mogelijke dreiging tegen
- Er zijn dreigmails ontvangen bij die mogelijk afkomstig zijn van een .

Aantasting integriteit

-
- Een toekomstige medewerker, zonder waiver of VGB, heeft berichten gestuurd naar NCTV medewerkers via gmail. In de berichten werd gebruik gemaakt van een NCTV handtekening (informatie over de organisatie en de persoon). De medewerker is aangesproken op het gedrag door de leidinggevende.
- Er zijn twee nepfacturen ontvangen door VenJ voor de NCTV. Zij hadden de facturen verwerkt. Bij controle door de NCTV is gebleken dat het om nepfacturen ging (o.a. factuur van).
- Er waren 2 werkstations in besmet met malware. Dit is gedetecteerd met SIEM (nieuwe systeem voor logging en monitoring), zijn uit het netwerk gehaald. De worden onderzocht door De afgelopen maand werden meer kwetsbaarheden gevonden ten aanzien van het gebruik . Op korte termijn vindt overleg plaats met het afdelingshoofd. Er zal een voorlichtingssessie gehouden worden voor de medewerkers om ze te wijzen op de mogelijke risico's van hun handelen.
- Bij de werving door een externe projectleider voor een externe projectmedewerker zijn producten en werkwijzen van in de advertentie op internet geplaatst. De projectleider is er op aangesproken.

- Op de website van de NCTV stond een document met naam en contactgegevens van een medewerker. Het document is inmiddels verwijderd.

Overige

Recentelijk is er een kwetsbaarheid gepubliceerd over de . Door deze kwetsbaarheid kan een besmet worden door bijvoorbeeld een . Een besmetting kan leiden tot het verwijderen van bestanden of activeren van de microfoon. Deze kwetsbaarheid kan gebruikt worden in het kader van spionage bijvoorbeeld tijdens vergaderingen waarin gerubriceerde informatie wordt gedeeld.
Inmiddels is er op het intranet een artikel geplaatst voor medewerkers. In het MT van 10 augustus is het besproken en de keuze gemaakt om binnen de NCTV . De werkgroep beveiliging komt met een voorstel.

De nieuwe noodzakelijk zijn voor plaats en tijd onafhankelijk werken zijn de afgelopen weken verspreid. Bij de verspreiding door wordt er onvoldoende aandacht besteed aan de controle op de uitgifte en verzending. Certificaten komen in handen van verkeerde medewerkers of organisatieonderdelen. Het risico op identiteitsfraude is aanwezig. De klachten zijn doorgestuurd naar en worden inmiddels door het management van besproken.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
14 oktober 2015

nota

Managementrapportage september 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisgeving.

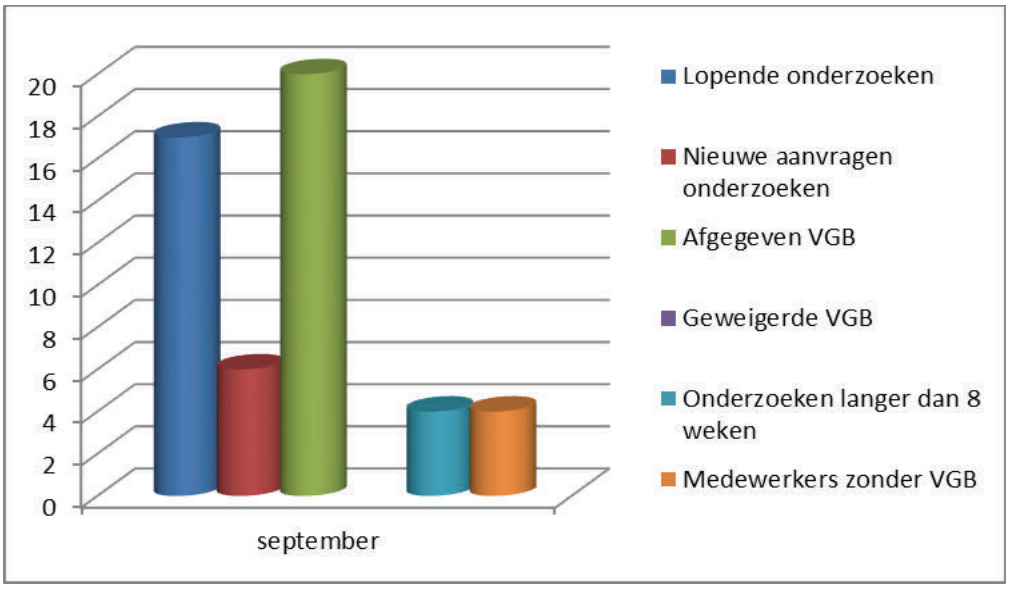
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. Op dit moment zijn er 4 medewerkers (met waiver) werkzaam bij de NCTV zonder VGB. [redacted]

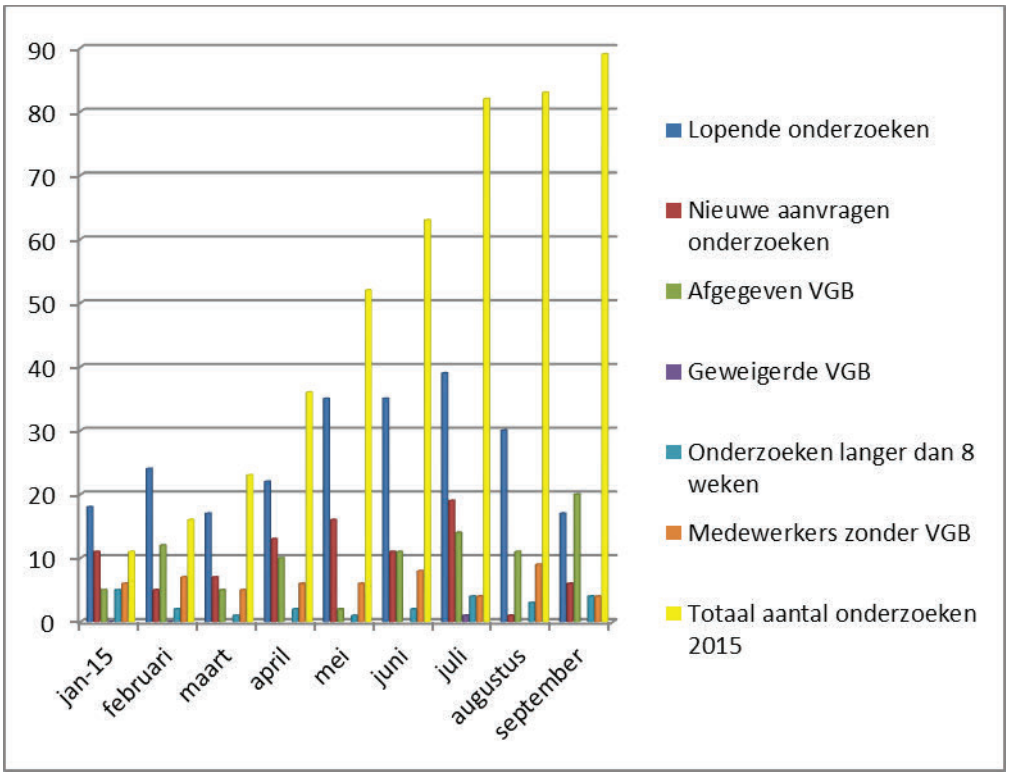
Er zijn 4 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en dus langer duren dan 8 weken. Het betreft hier onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd.

De doorlooptijd van onderzoeken is nog steeds langer dan gebruikelijk, nu 10 tot 12 weken.

Zie onderstaand beeld.



Beeld veiligheidsonderzoeken september

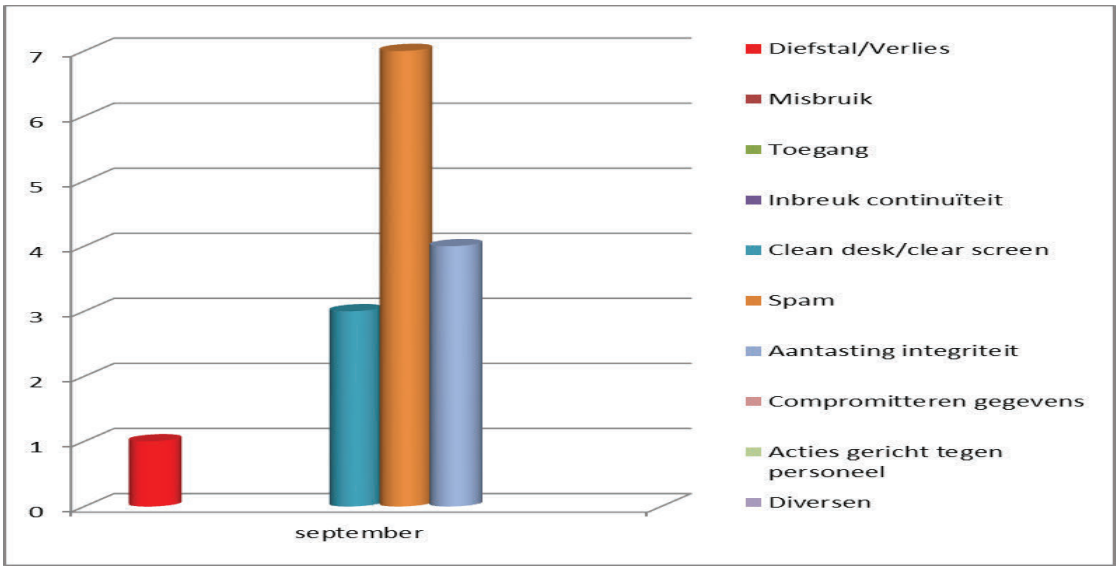


Totaal beeld veiligheidsonderzoeken 2015

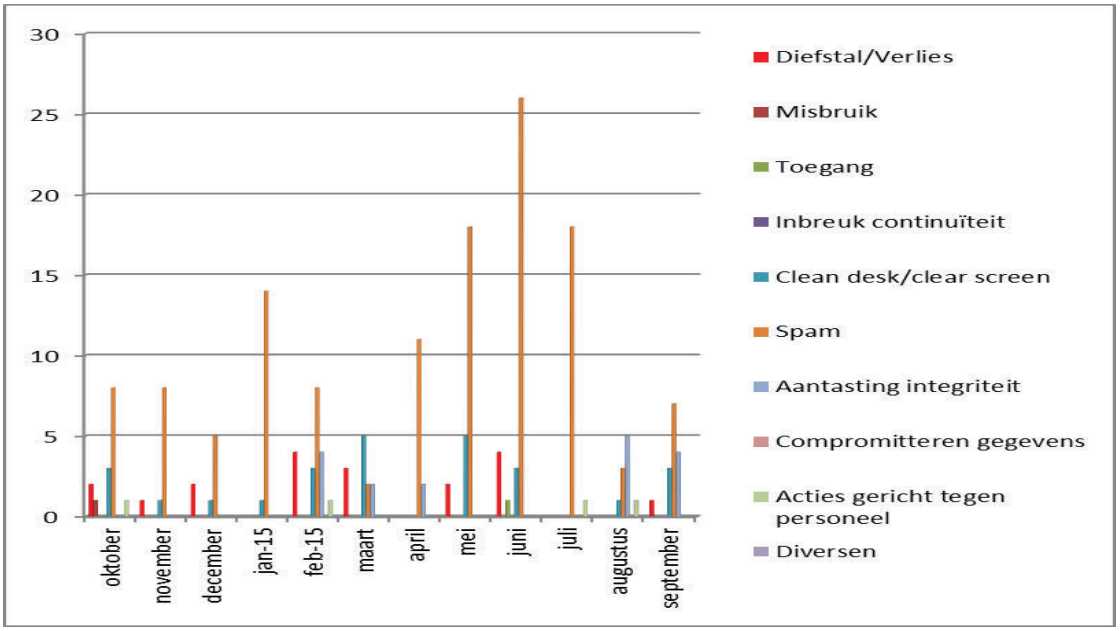
Datum
14 oktober 2015

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten september



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Diefstal/verlies
Op de Turfmarkt is een document gevonden met een mailbericht van de NCTV over Jihadisme. Het bericht is naar diverse netwerkpartners gestuurd en bevat openbare informatie. De netwerkpartners zijn inmiddels door de leidinggevende bij de NCTV gewezen op hun verantwoordelijkheid en het veilig omgaan met informatie.

Cleandesk/clean screen
Er zijn drie [redacted] tijdens cleandeskrondes gevonden en ingenomen door de beveiliging.

SPAM/Phising mail
Het aantal meldingen van spam en phising is beduidend lager. Hier is geen directe verklaring voor te geven.

Aantasting integriteit
Er hebben zich meerdere meldingen voorgedaan waarbij de integriteit van een persoon, informatie of de NCTV is aangetast. Er is een toename van het aantal meldingen in het kader van integriteit.

- Een viertal [redacted] in gebruik bij de NCTV waren niet voorzien van een actuele virusscanner en daarmee voldeden ze niet aan de eisen van de BIR. In overleg met de leidinggevende zijn de medewerkers verzocht hun [redacted] te laten voorzien van een actuele virusscanner door Support NCTV.
- Op de NCTV website was een brief gepubliceerd met naam en contactgegevens van een medewerker in de metadata. Inmiddels is het proces aangepast en het document verwijderd.
- Een medewerker heeft een mail gestuurd naar netwerkpartners met [redacted]. Het incident werd gemeld door de netwerkpartners. [redacted] is hiervan op de hoogte gesteld. De medewerker heeft een gesprek gehad met de leidinggevende. Risico op verlies van informatie is laag omdat het bericht naar een beperkte groep is gestuurd en niet [redacted].
- Een medewerker wilde thuis een document uitprinten dat in zijn VenJ mailbox stond. VenJ heeft er voor gekozen dat er uit veiligheidsoverwegingen bij thuiswerken geen stukken uitgeprint kunnen worden. [redacted]

Overige

[redacted]
Via de [redacted] van [redacted] kunnen app's worden geïnstalleerd die het toestel of de software kunnen compromitteren. Op dit moment zijn er nog geen meldingen bekend bij de NCTV van compromittering van [redacted]. Het risico op compromittering van smartphones, waarbij de microfoon of camera op afstand

kan worden afgeluisterd, neemt verder toe. Door de aanwezigheid van smartphones tijdens besprekingen of vergaderingen kan dit leiden tot een toenemende kans op compromittering van informatie. Inmiddels lopen er initiatieven via de werkgroep beveiliging om aanvullende maatregelen te treffen.

NCTV
In Q2 zijn er door de ADR pentesten uitgevoerd op een aantal .
Dit zijn:

-
-
-
-
-

In de onderzoeken is gekeken naar mogelijke kwetsbaarheden. De geconstateerde kwetsbaarheden zijn grotendeels opgelost. In Q3 en Q4 zullen er nog onderzoeken plaatsvinden op andere van de NCTV.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
3 november 2015

nota

Managementrapportage oktober 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter bespreking. In verband met de huidige actualiteiten wordt voorgesteld bepaalde maatregelen zoals het toekennen van autorisaties aan te scherpen.

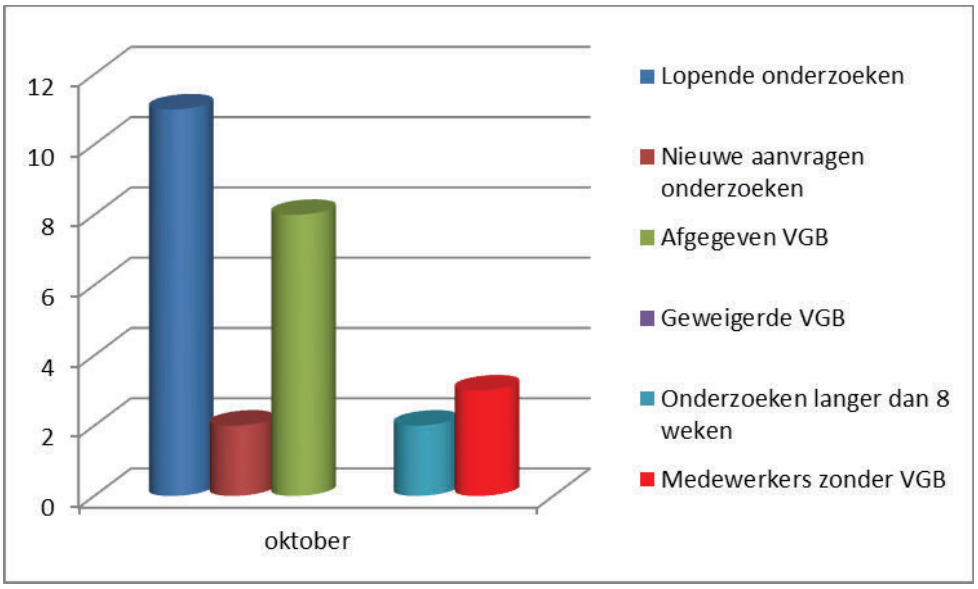
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. Op dit moment zijn er 3 medewerkers (met waiver) werkzaam bij de NCTV zonder VGB. [redacted]

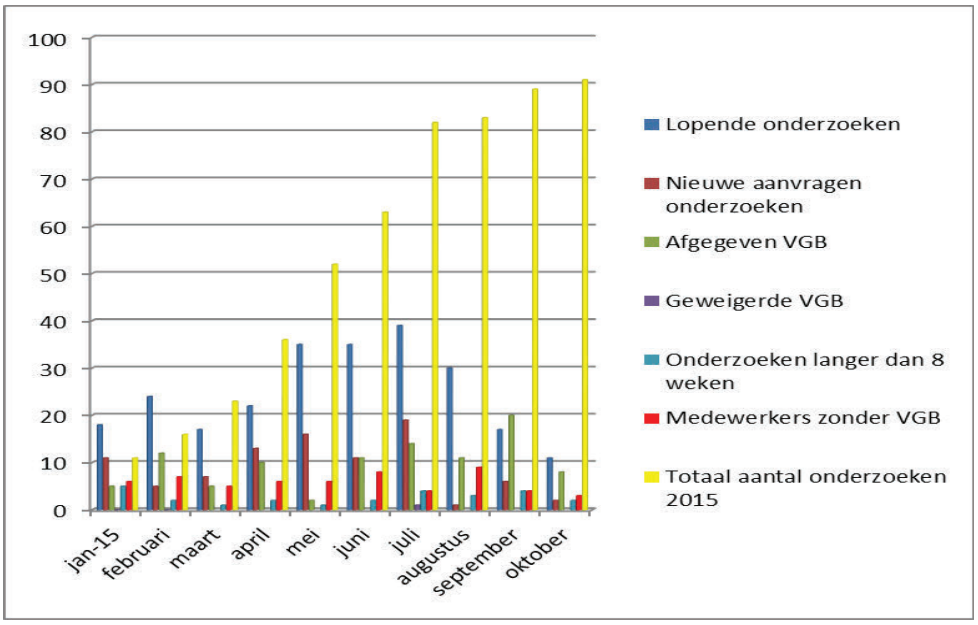
Er zijn 2 onderzoeken die niet binnen de gestelde termijn afgerond konden worden en dus langer duren dan 8 weken. Het betreft hier onderzoeken waarbij informatie van een buitenlandse dienst wordt gevraagd.

[redacted] De NCTV maakt nog steeds uitzonderingen op het tijdelijk werken zonder veiligheidsonderzoek. Dat is strijdig met de wettelijke voorschriften en kan de bestuurder en de NCTV in diskrediet brengen.

Zie onderstaand beeld.



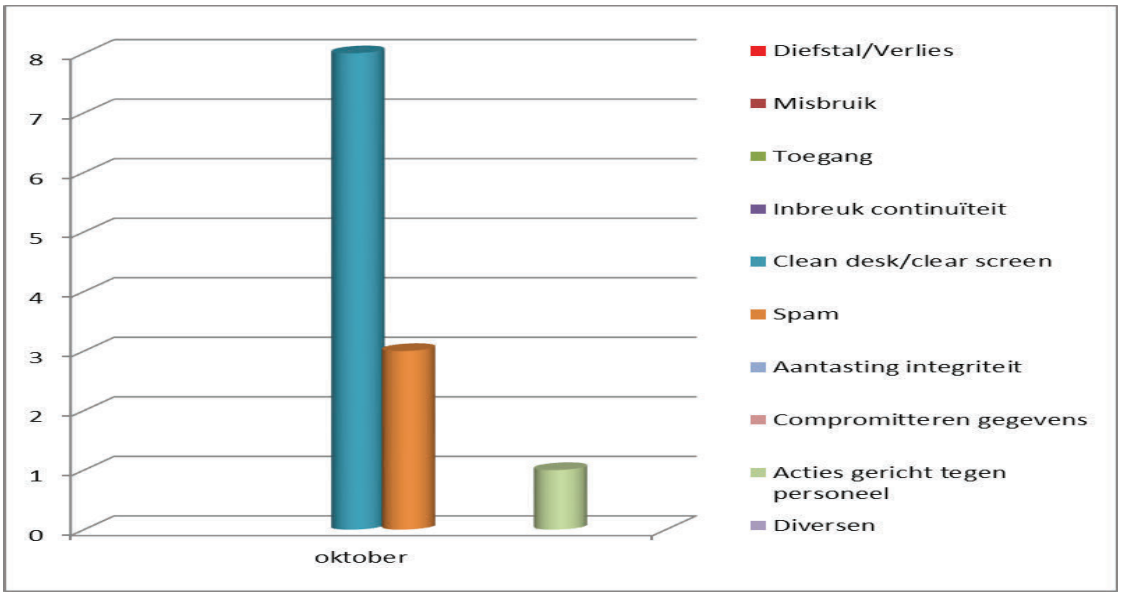
Beeld veiligheidsonderzoeken oktober



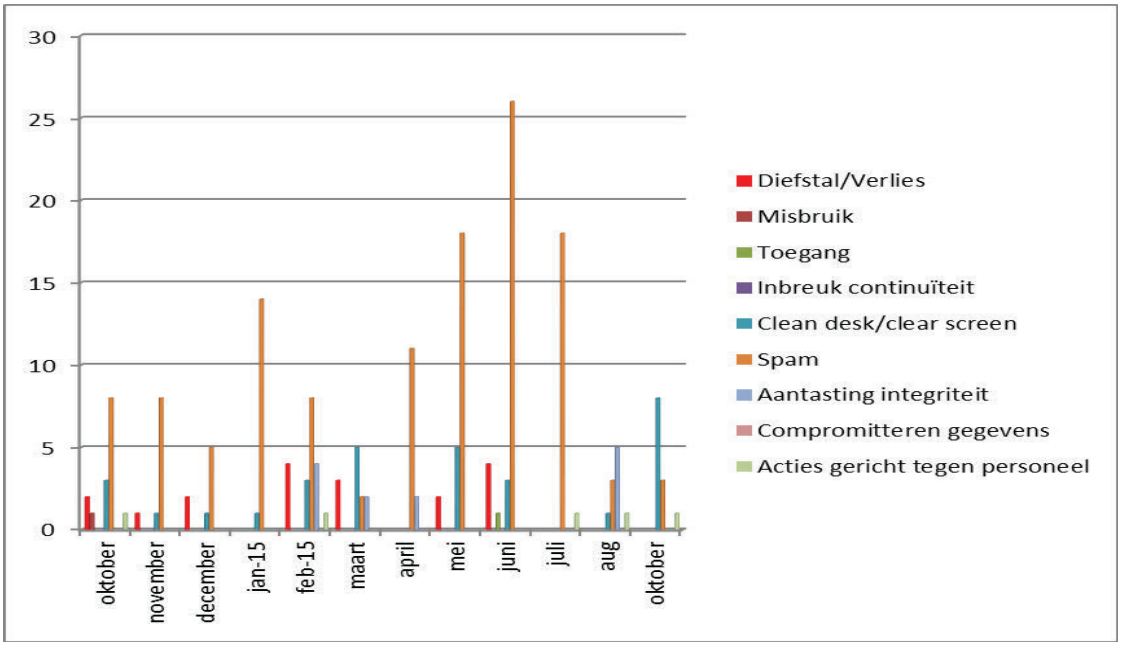
Totaal beeld veiligheidsonderzoeken 2015

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten oktober



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Directie Strategie en Bedrijfsvoering

Datum
3 november 2015

Toelichting tabellen

Cleandesk/clean screen
Er zijn 7 [redacted] aangetroffen op de werkplekken tijdens de cleandeskrondes.

SPAM/Phising mail
Het aantal meldingen van spam en phising is laag.

[redacted]

Overige

[redacted]

Directie Strategie en Bedrijfsvoering

Datum
3 november 2015

[redacted]

Namens de NCTV is er nogmaals bij het [redacted] VenJ en [redacted] op gewezen wat de risico's zijn van het gebruik van de [redacted] met verouderde browser en applicaties. De pSG is eveneens geïnformeerd. De verwachting is nu uitgesproken dat [redacted] voor het eind van het jaar wordt uitgerold.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
3 december 2015

nota

Managementrapportage november 2015
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies
Ter bespreking.

Toelichting

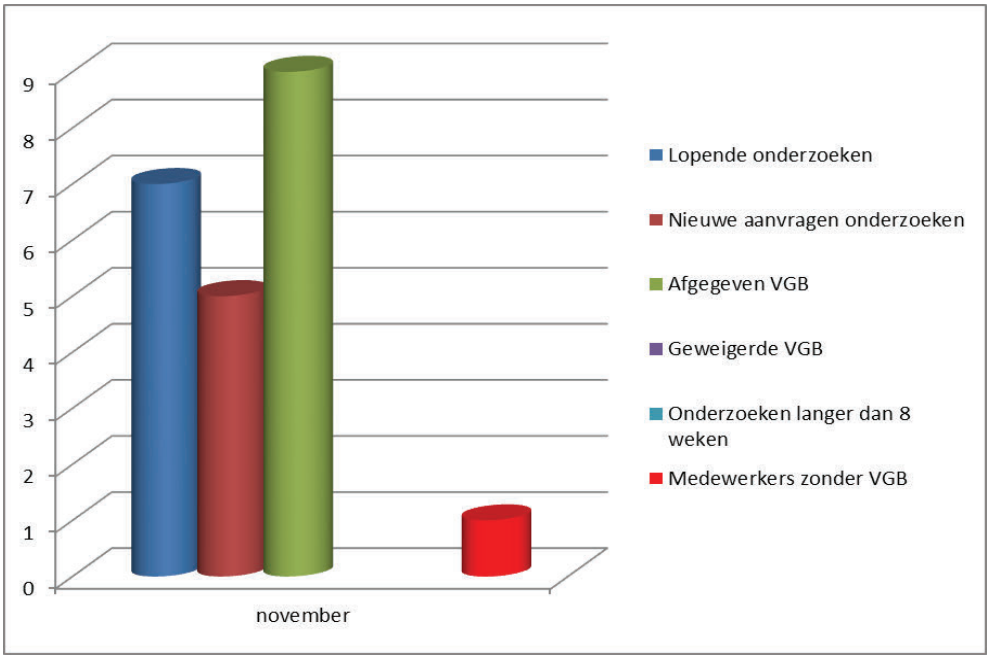
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In november was er 1 medewerker (met waiver) werkzaam bij de NCTV zonder VGB. Het betrof hier een medewerker bij de afdeling [redacted] die ingehuurd is als projectleider.
[redacted]

Op dit moment wordt er in de media gecommuniceerd over medewerkers bij de Nationale Politie die wel of geen VGB hebben.
De situatie bij de NCTV is als volgt;

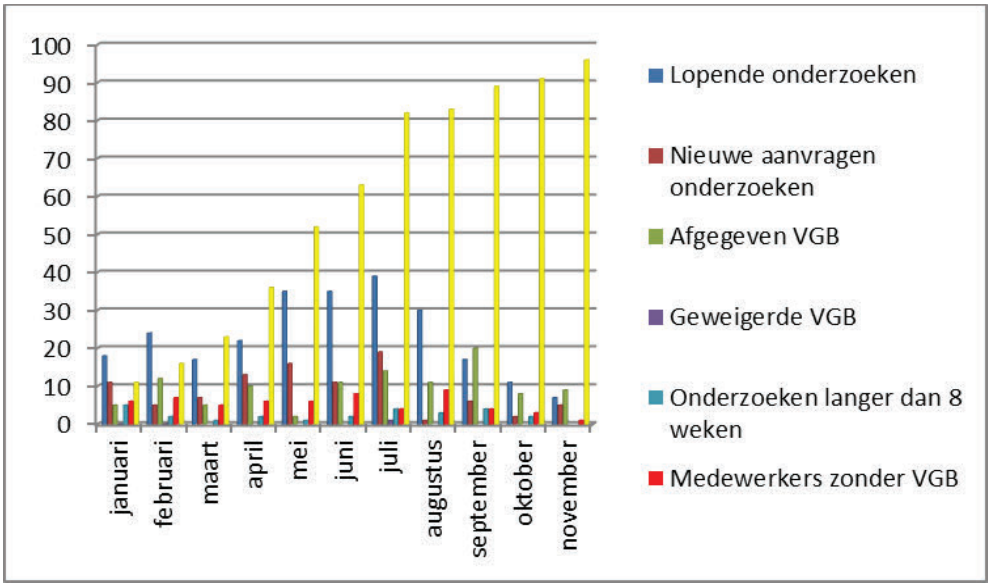
- Inmiddels beschikt iedere persoon die nu werkzaam is binnen de schil van de NCTV over een VGB.
- Als er uitzonderingen worden gemaakt (waiver) voor personen zonder VGB dan krijgen zij beperkte rechten op ICT mappen op het VenJ netwerk en beperkte toegangsrechten tot de [redacted]
- Voorwaarde voor het werken op het [redacted] is dat de medewerker minimaal een VGB B heeft.
- Autorisaties tot het [redacted] worden gegeven op basis van functionele noodzaak.
- Medewerkers die andere werkzaamheden / functies gaan vervullen waarvoor een zwaarder veiligheidsonderzoek noodzakelijk is krijgen een nieuw veiligheidsonderzoek.

Overigens zijn er nog wel verbeteringen te behalen in het beheer van rechten tot mappen op het [redacted] en [redacted]. Door het niet of niet tijdig melden van verplaatsingen of beëindigingen van contracten worden extra rechten die toegekend zijn aan medewerkers niet gewijzigd.

Zie onderstaand beeld.



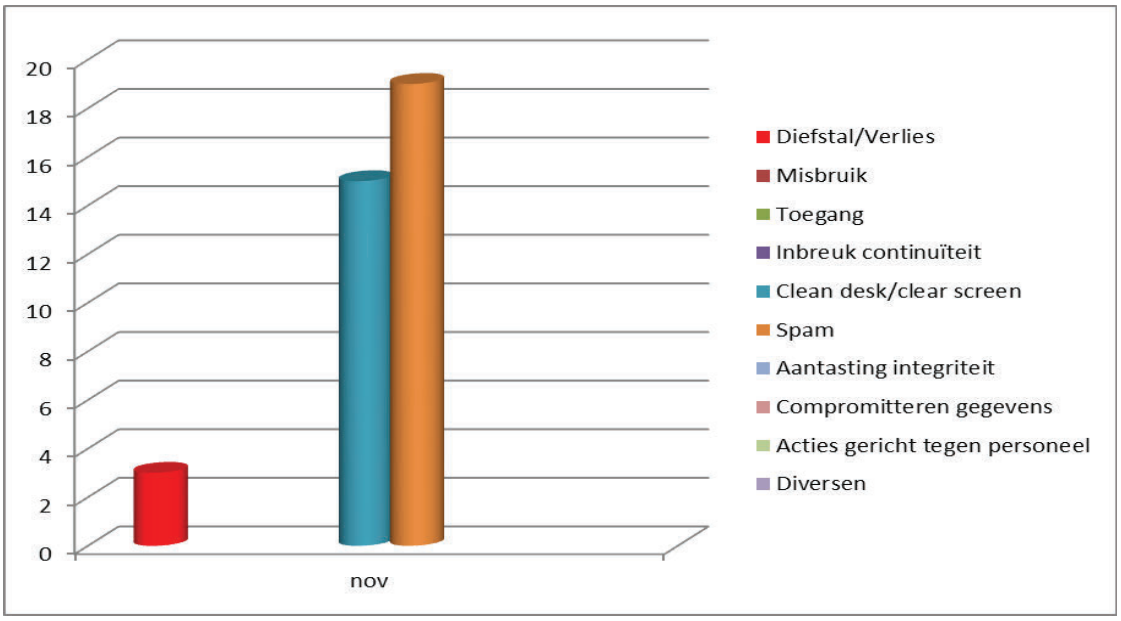
Beeld veiligheidsonderzoeken november



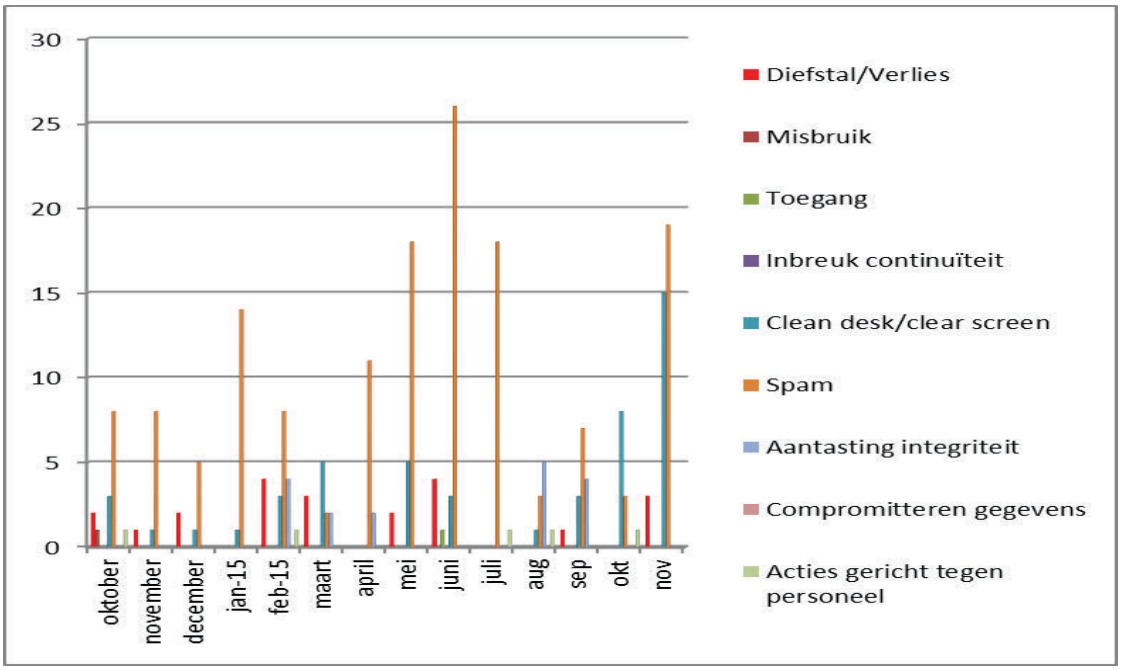
Totaal beeld veiligheidsonderzoeken 2015

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten november



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Diefstal/verlies
Een medewerker heeft zijn iPad verloren. Een medewerker heeft zijn rijkspas verloren en een medewerker is intern zijn) verloren. De iPad is door het op afstand gewist en onbruikbaar gemaakt. Het risico is klein dat de daders informatie van de NCTV hebben gecompromitteerd.

Cleandesk/clean screen
Er zijn 11 aangetroffen op de werkplekken tijdens de cleandeskronden en veilig gesteld. Verder zijn er drie kluizen open aangetroffen bij . Bij zijn aangetroffen. De leidinggevenden zijn hierover geïnformeerd.

SPAM/Phising mail
Het aantal meldingen van spam en phising is weer gestegen. Een aantal medewerkers heeft een telefoontje gekregen van een onbekende beller, na het opnemen schakelt het toestel door naar een buitenlands nummer. De meeste gesprekken zijn direct afgebroken. Een tweetal medewerkers heeft phisingmail gekregen op de smartphone. Bij 1 medewerker is hierdoor 15 euro afgeboekt van de telefoonrekening.

Overige

Economische veiligheid
In de media is bekend gemaakt dat is overgenomen door een Engels bedrijf. Naast de bredere impactanalyse t.a.v. de economische veiligheid over deze verkoop met een korte analyse van

NCTV
In Q3 zijn er door de ADR pentesten uitgevoerd op een aantal .
Dit zijn:

In de onderzoeken is gekeken naar mogelijke kwetsbaarheden. De geconstateerde kwetsbaarheden zijn grotendeels opgelost.
Deze geteste websites, met uitzondering , maken gebruik van .
Beveiligingsexperts raden het gebruik van af omdat kwetsbaarheden in op grote schaal worden misbruikt. Bovendien kunnen systemen met de webapplicaties niet gebruiken omdat deze systemen g .
Voorgesteld wordt om pas om te zetten naar bij een update van de betreffende website.
In Q4 zullen er nog onderzoeken plaatsvinden op andere websites van de NCTV.

Mede door het feit dat de NCTV het VenJ, het en de nogmaals heeft gewezen op de risico's van de , is versneld de in het weekend van 27 november uitgerold. Het grootste deel van de kwetsbaarheden die er waren in de verschillende applicaties met verouderde versies zijn hier mee opgelost. De komende tijd zal de verdere werking van applicaties verbeteren.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
15 januari 2016

nota

Managementrapportage december 2015
Programma Integrale Beveiliging

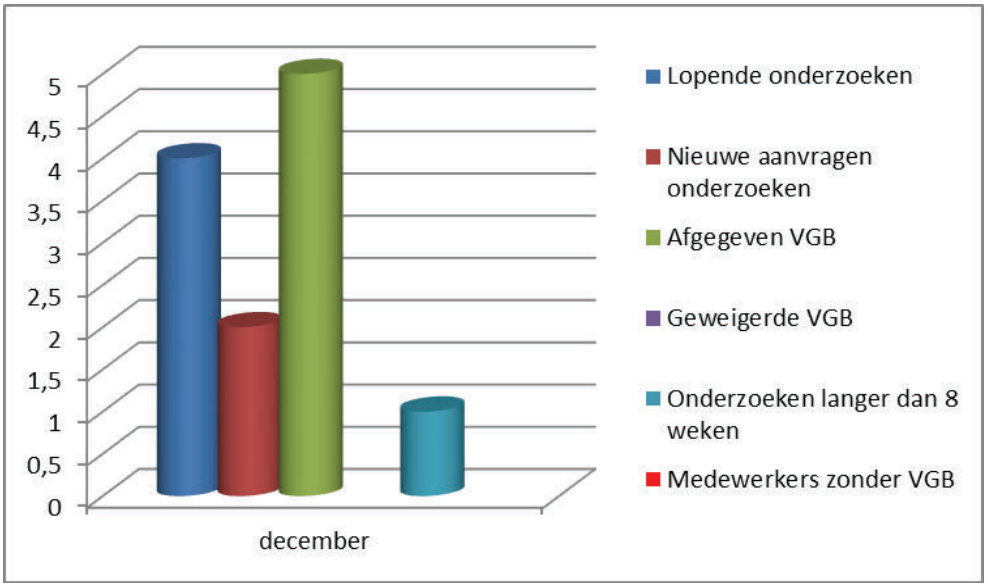
Van
Datum/eindparaaf

Advies
Ter kennisneming.

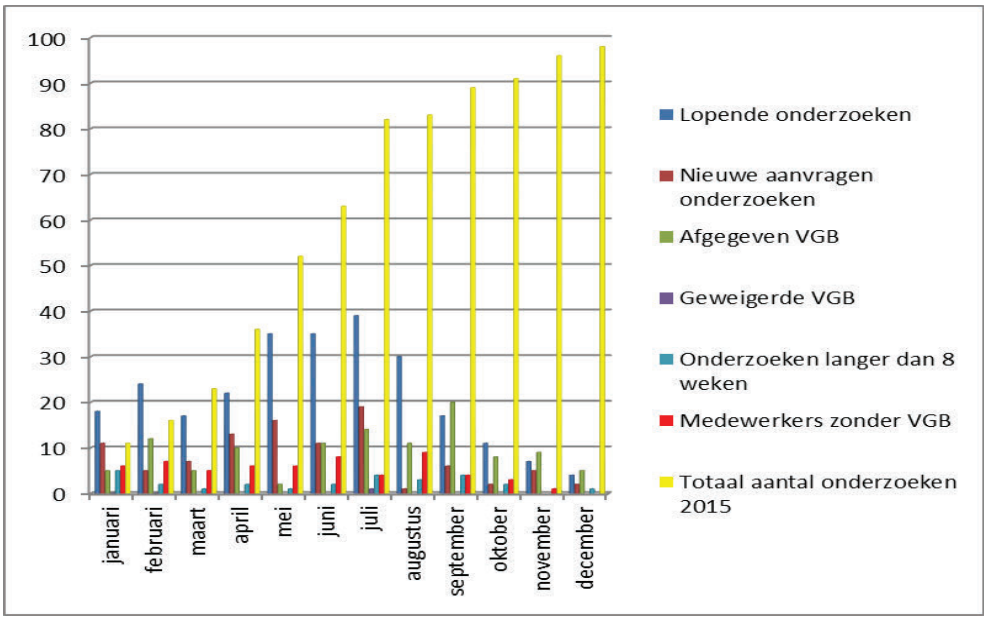
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In december waren er geen uitzonderingen op het werken zonder VGB bij de NCTV. Er loopt nog 1 onderzoek voor een nieuwe medewerker van wie de aanvraag in juni 2015 heeft plaatsgevonden.

Zie onderstaand beeld.



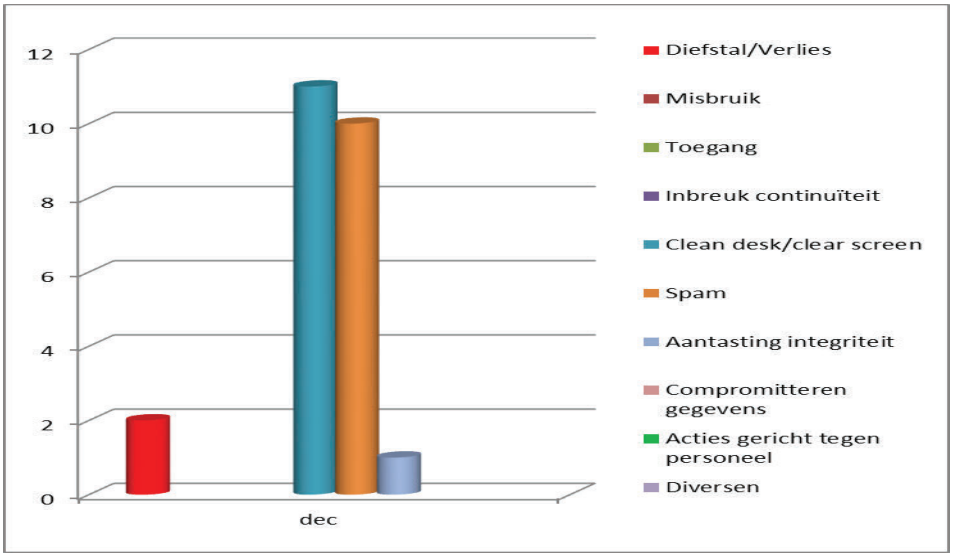
Beeld veiligheidsonderzoeken december



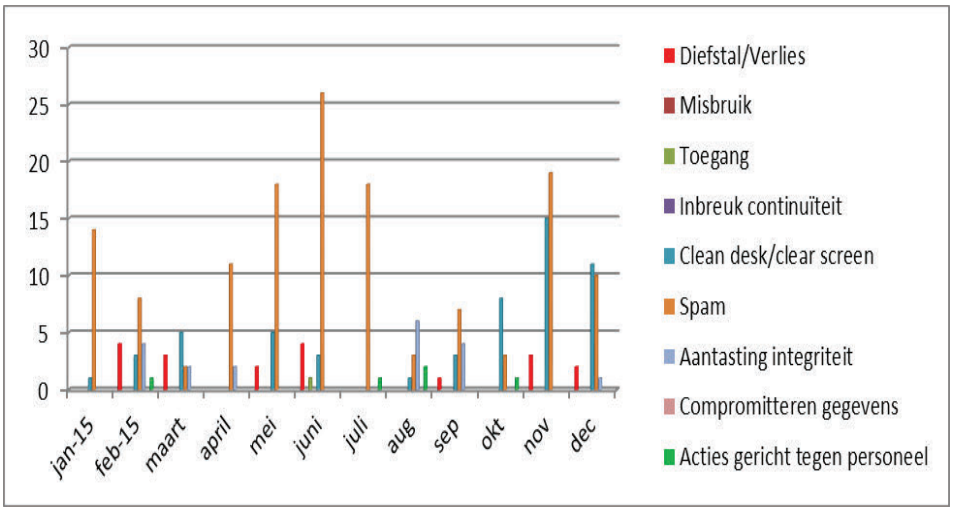
Totaal beeld veiligheidsonderzoeken 2015

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten december



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Diefstal/verlies
Eén medewerker heeft zijn iPhone verloren. Bij de afdeling Inkoop VenJ is een zaklamp van de NCTV die ter reparatie was aangeboden ontvreemd. Het incident wordt met de afdeling Inkoop afgehandeld.

Cleandesk/clean screen
Er zijn 7 [redacted] en twee [redacted] onbeheerd aangetroffen op de werkplekken tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers.

SPAM/Phising mail
Er zijn meldingen gedaan van spam en phising. Tot nu toe zijn er 20 meldingen van medewerkers die een oproep hebben gekregen van een onbekende (buitenlandse) beller, na het opnemen schakelt het toestel door naar een buitenlands nummer. De oproepen zijn niet beantwoord. Er is een artikel op het intranet geplaatst en de meldingen zijn doorgestuurd naar [redacted] . [redacted] heeft de meldingen doorgestuurd naar de telecomprovider maar nog geen terugkoppeling gekregen.

Aantasting Integriteit
[redacted]

Overige

Economische veiligheid
[redacted]

[redacted] *NCTV*
Ook in Q4 zijn er door de ADR pentesten uitgevoerd op een aantal [redacted] .
Dit zijn:
- [redacted]

In de onderzoeken is gekeken naar mogelijke kwetsbaarheden. De geconstateerde kwetsbaarheden zijn grotendeels opgelost.
Deze geteste websites maken [redacted] . Beveiligingsexperts raden het [redacted] af omdat kwetsbaarheden in [redacted] op grote schaal worden misbruikt. Bovendien kunnen systemen met [redacted] de webapplicaties niet gebruiken omdat deze systemen geen [redacted] ondersteunen.

Voorgesteld is om pas om te zetten naar bij een update van de betreffende website.

Terugblik 2015

Het onderzoek heeft voor 11 personen langer geduurd dan de wettelijke termijn van 8 weken. In één geval heeft het onderzoek 14 maanden geduurd in verband met informatie uitwisseling tussen .

In augustus heeft zich een piek voorgedaan voor het aantal uitzonderingen om tijdelijk te werken zonder VGB. Het ging toen om 9 medewerkers van met name

Incidenten
In 2015 heeft de beveiliging 10 maal een niet afgesloten kluis aangetroffen met informatie.
Alle incidenten hebben ondanks het mogelijke hoge risico geen of beperkte schade veroorzaakt voor de NCTV. Na een aantal incidenten heeft de risicoafweging geleid tot aanvullende maatregelen zoals In veel gevallen was er sprake van dat medewerkers zich onvoldoende hielden aan de voorgeschreven regels of zich niet bewust waren van de mogelijke risico's.
Er hebben zich diverse incidenten voorgedaan tegen NCTV medewerkers al dan niet bewust, zoals de , en .

Vooruitblik 2016

Vanaf 1 januari 2016 geldt ook voor de NCTV de meldplicht datalekken. De inventarisatie van verwerking van persoonsgegevens en de bijbehorende risico's is nog niet voltooid. De verantwoordelijkheid ligt hier bij de lijnmanagers. De processen voor het melden van een datalek zijn beschreven.
De verwachting is dat er zich meer digitale incidenten zullen voordoen. Vanuit worden de ontwikkelingen samen met gevolgd en daar waar nodig aanvullende maatregelen getroffen.
Het maken van schriftelijke afspraken over het omgaan met informatie en persoonsgegevens van de NCTV met de dienstverlenende partijen op de Turfmarkt en bij externe partijen zal dit jaar gerealiseerd worden. Binnen VenJ is hier nu ook meer aandacht meer. Er heeft ook een verschuiving plaatsgevonden

ten aanzien van verantwoordelijkheden, taken en rollen bij de dienstverlenende onderdelen zoals , en
De implementatie van de maatregelen uit de BIR zal eveneens in 2016 aandacht vergen van het management en de afdeling bedrijfsvoering. Voor 2016 zijn de volgende thema's van belang;

1. Governance van ICT en Informatiebeveiliging (IB) en aansturing leveranciers;
2. Verder invoeren logging en monitoring;
3. Updaten van inclusief het implementeren van het autorisatiesysteem en bijbehorende autorisatieprocedures.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
8 februari 2016

nota

Managementrapportage januari 2016
Programma Integrale Beveiliging

Van

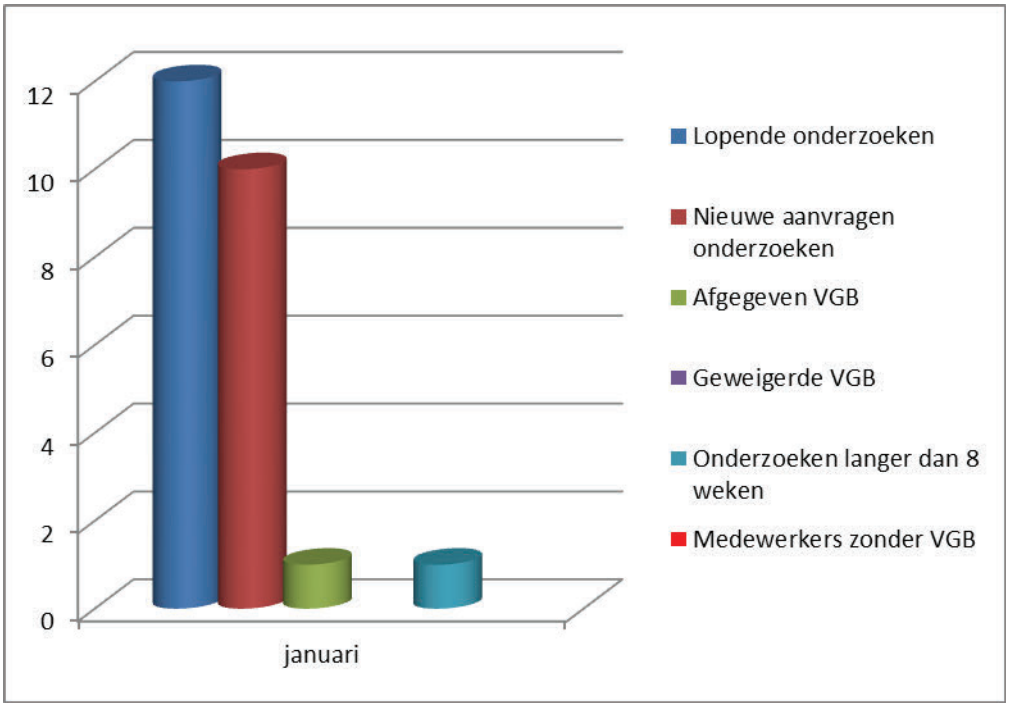
Datum/eindparaaf

Advies
Ter kennisneming.

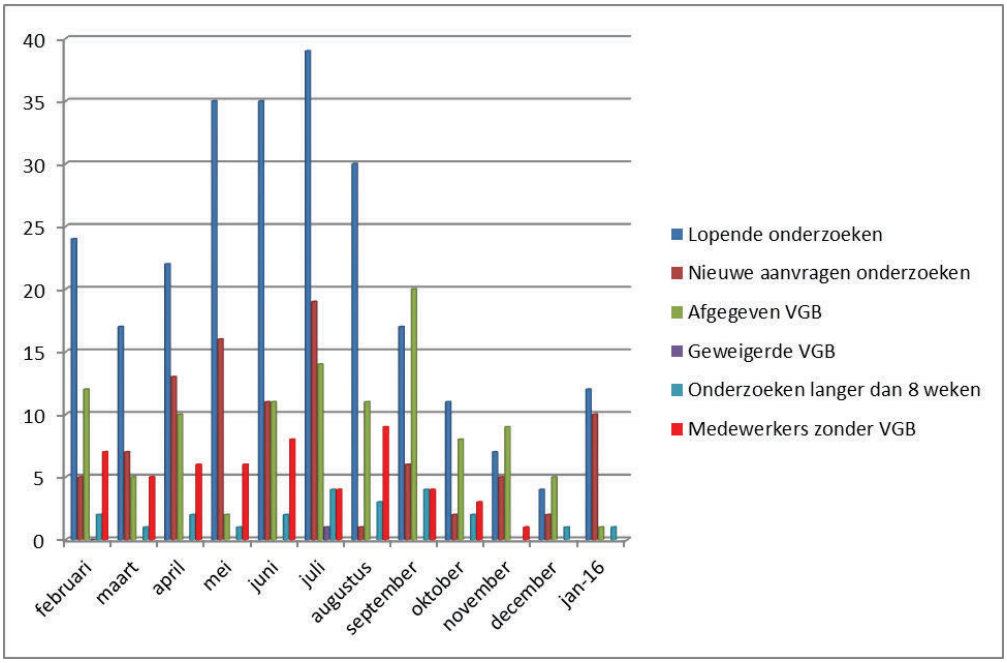
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In januari waren er geen uitzonderingen op het werken zonder VGB bij de NCTV. Er loopt nog 1 onderzoek voor een nieuwe medewerker van wie de aanvraag in juni 2015 heeft plaatsgevonden.

Zie onderstaand beeld.



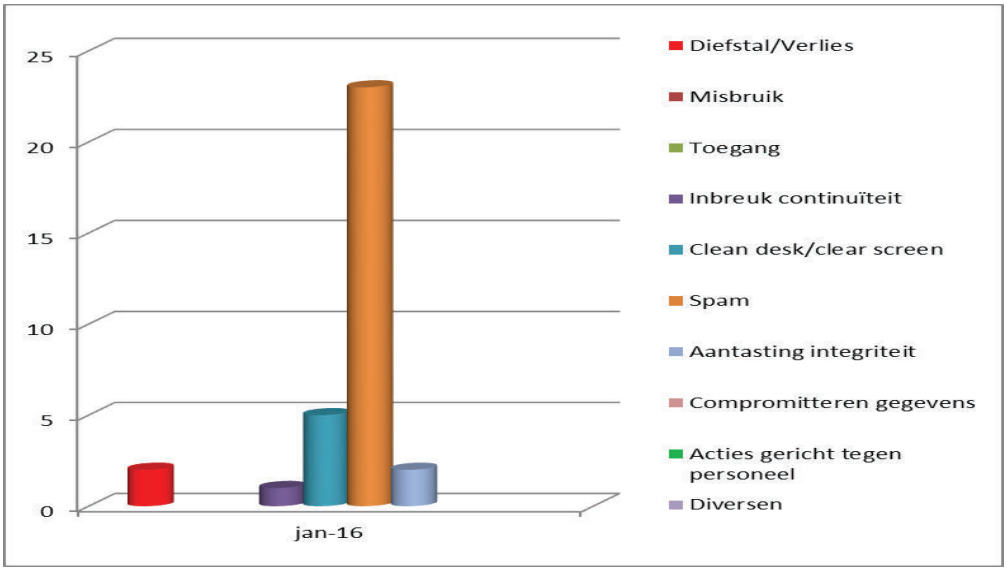
Beeld veiligheidsonderzoeken januari



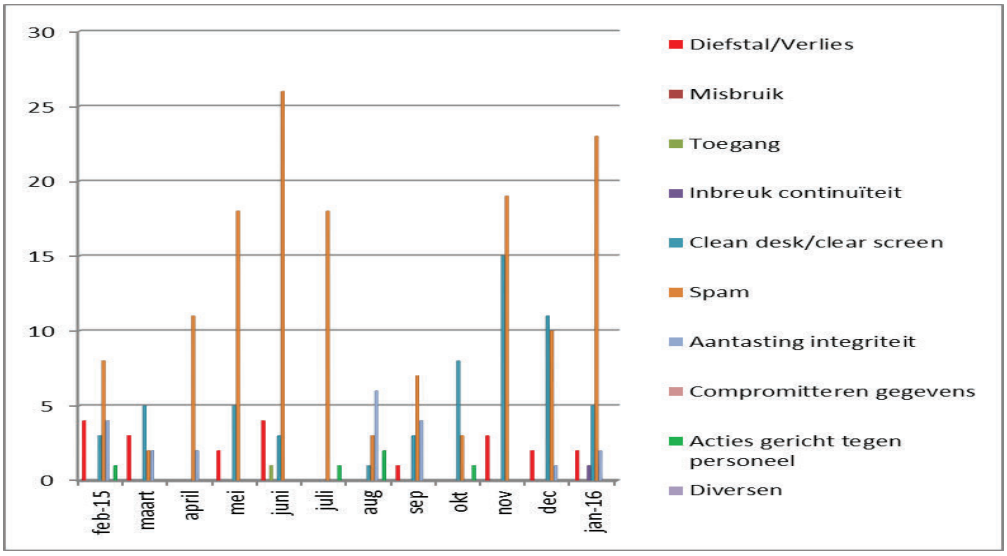
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten januari



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Diefstal/verlies
Eén medewerker heeft zijn iPhone verloren. Het risico op compromittering van informatie op deze telefoon is beperkt doordat de telefoon op afstand is gewist. Eén medewerker is het [redacted] voor het [redacted] intern kwijtgeraakt. Ook hier is het risico laag omdat het [redacted] is geblokkeerd en een nieuw [redacted] is verstrekt.

Cleandesk/clean screen
Er is 1 [redacted] onbeheerd aangetroffen op een werkplek tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers. Tijdens de cleandeskrondes zijn drie [redacted] documenten aangetroffen op de bureaus bij [redacted]. De documenten zijn opgeborgen in de kluis bij de receptie. Er is een notitie achtergelaten voor de eigenaar waar hij het stuk kan ophalen. Verder heeft er 1 medewerker een [redacted] op een [redacted] aangetroffen. Het bleek om een [redacted] te gaan waardoor het risico voor compromittering beperkt was.

Inbreuk continuïteit
We hebben een storing gehad van het mobiele telefonie netwerk van [redacted]. Met name de [redacted] heeft last gehad van het niet bereikbaar zijn via de mobiele telefoon. De oorzaak bleek een foutieve handeling van een persoon te zijn bij [redacted]. Om mogelijke problemen in de toekomst te voorkomen heeft de Waakdienst een extra toestel gekregen met een [redacted].

SPAM/Phising mail
Er zijn 9 meldingen van spam en phising binnengekomen. De meldingen zijn doorgestuurd naar [redacted] De afgelopen maand zijn er weer 14 meldingen binnengekomen van medewerkers die door een onbekend buitenlands nummer zijn gebeld. In dit geval is er wederom melding gemaakt naar [redacted]. Het resultaat van dit onderzoek is nog niet bekend.

[redacted]
In het [redacted] bleken adressen te staan van beveiligde woningen. De [redacted] medewerkers van de Afdeling [redacted] hebben de adressen verwijderd. [redacted]
In [redacted] bleek een [redacted] opgeslagen te zijn in een zaakdossier van [redacted]. Het onderzoek heeft geen duidelijkheid gegeven hoe of wie dit document daar had geplaatst. Mogelijk is het door de postkamer gescand en toegevoegd. Het document is inmiddels verwijderd. Het betrof een offerte voor werkzaamheden op [redacted]. Het risico is beperkt omdat er geen gedetailleerde informatie in stond.

Overige

De NCTV heeft de laten onderzoeken op kwetsbaarheden.
Het onderzoek heeft een aantal kwetsbaarheden opgeleverd die gezamenlijk met beheersbaar worden gemaakt.

Smartboards
Er is een kwetsbaarheid ontdekt in de waarmee de videosignalen worden geschakeld op de smartboards die gebruikt worden in de vergaderzalen van de NCTV.
Het risico dat deze backdoor kan worden gebruikt bij de NCTV is laag omdat deze bij de NCTV geen verbinding heeft met het internet.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
8 maart 2016

nota

Managementrapportage februari 2016
Programma Integrale Beveiliging

Van

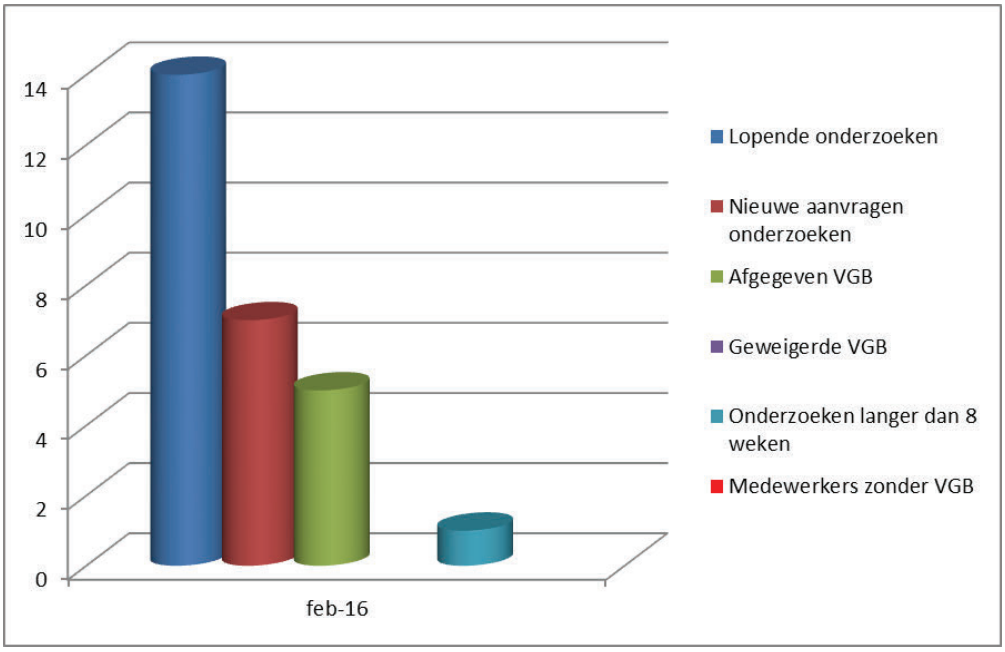
Datum/eindparaaf

Advies
Ter kennisneming.

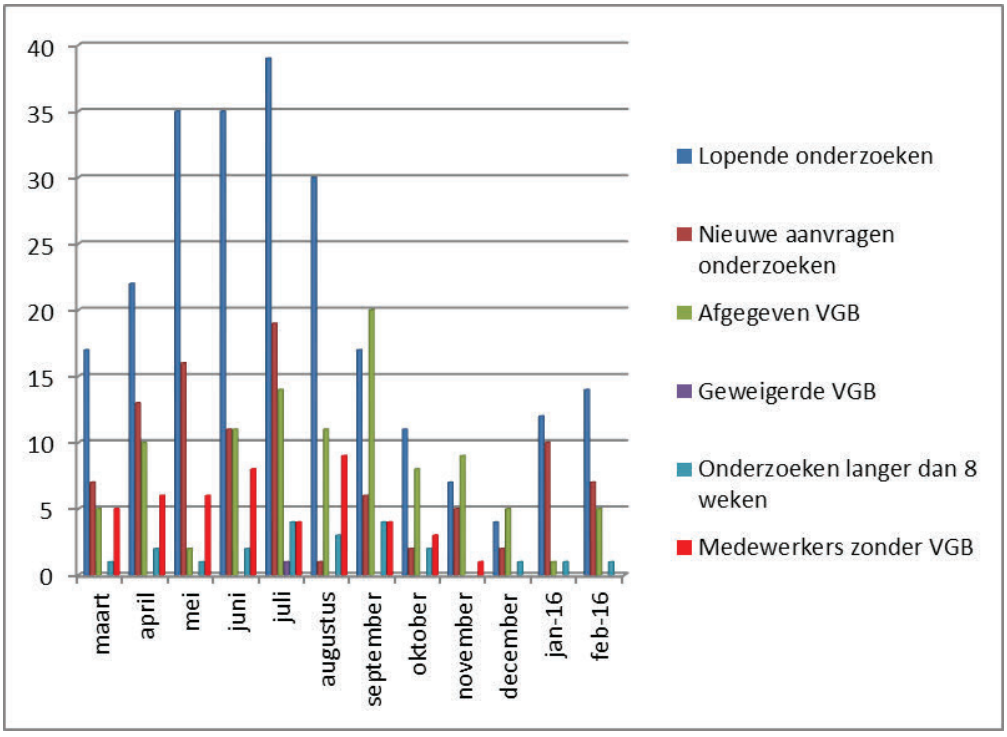
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In februari waren er geen uitzonderingen op het werken zonder VGB bij de NCTV. Er loopt nog 1 onderzoek voor een nieuwe medewerker van wie de aanvraag in juni 2015 heeft plaatsgevonden.

Zie onderstaand beeld.



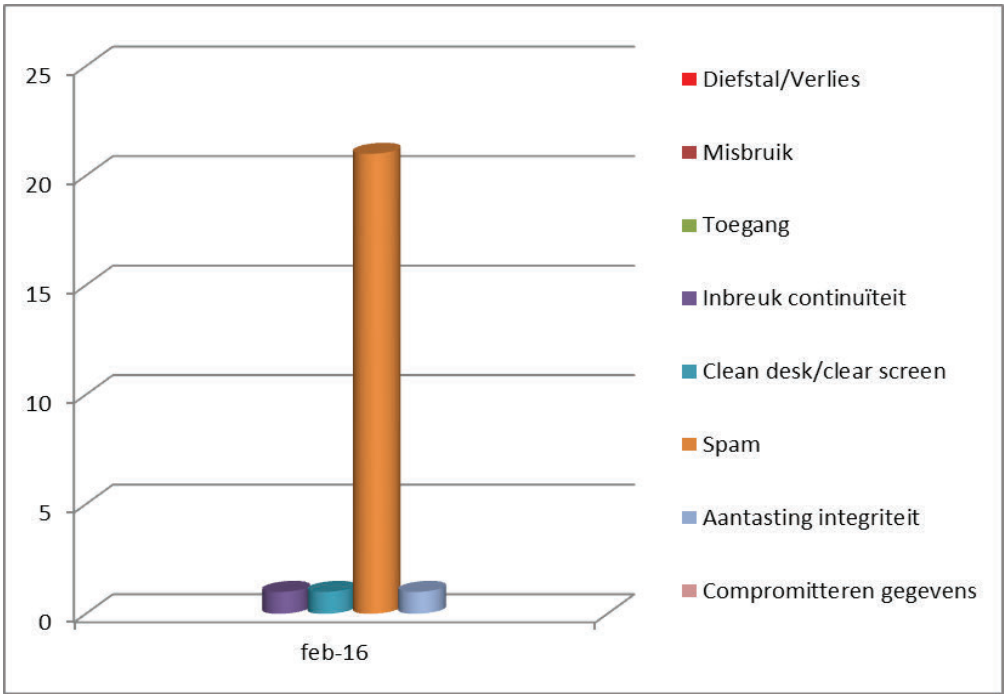
Beeld veiligheidsonderzoeken februari



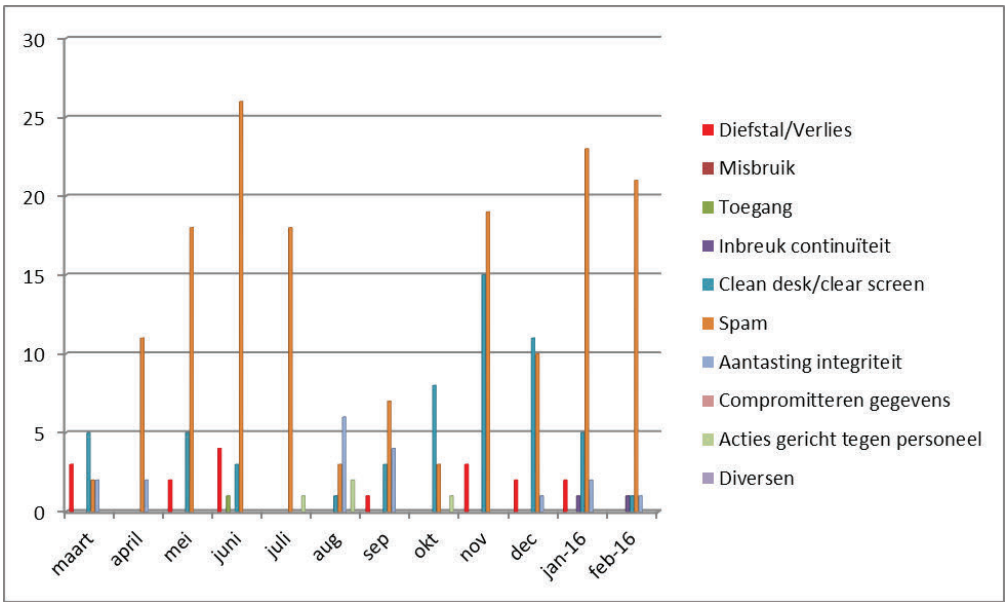
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten januari



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Inbreuk continuïteit primair proces NCTV
We hebben, 3 uur, uitval van het vaste telefonie netwerk gehad. De [redacted] hebben hier het meeste last van ondervonden. De bereikbaarheid was geborgd door de overschakeling naar mobiele telefonie. De oorzaak was een menselijke fout bij [redacted], de beheerder van het telefonie netwerk. De problemen worden besproken met de accountmanager [redacted].

Cleandesk/clean screen
Er is 1 [redacted] onbeheerd aangetroffen op een werkplek tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers. Overigens is het aantal meldingen een substantiële vermindering is ten opzichte van vorige maand.

SPAM/Phising mail
Er zijn 10 meldingen van spam en phising binnengekomen. De meldingen zijn doorgestuurd naar [redacted]. De afgelopen maand zijn er 8 meldingen binnengekomen van medewerkers die door een onbekend buitenlands nummer zijn gebeld. In dit geval is er wederom melding gemaakt naar [redacted]. Een drietal medewerkers heeft melding gemaakt van spam in het SMS verkeer op hun smartphone. Er is contact geweest met Defensie die hier ook in toenemende mate last van heeft. In de media wordt op dit moment ook melding gemaakt van een toenemend aantal meldingen van telefoon oproepen vanuit het buitenland.

Aantasting Integriteit
We hebben een [redacted] melding gehad over een kwetsbaarheid op [redacted]. Als tussen oplossing waren deze [redacted] verwijderd van de website. [redacted] had de kwetsbaarheid niet binnen 60 dagen opgelost waardoor het als incident is geëscaleerd. Inmiddels heeft [redacted] het probleem verholpen en zijn de [redacted] zonder kwetsbaarheid beschikbaar op de website.

Overige

Autorisaties
Vorige maand is er aan alle leidinggevenden een verzoek gedaan om de autorisaties voor de toegang tot ICT mappen op het VenJ netwerk te controleren. Inmiddels zijn de meeste reacties binnen en zijn ze verwerkt. Bij controle van de autorisaties op het [redacted] bleken er onterecht medewerkers voor een bepaalde map geautoriseerd te zijn. De correctie heeft plaatsgevonden in overleg met de leidinggevende.
In januari zijn ook alle rijkspas autorisaties gecontroleerd en daar waar nodig aangepast. Er heeft eveneens een controle plaatsgevonden op de interne lijst van gebruikers van de [redacted].

[redacted] *NCTV*
In februari 2016 heeft de ADR pentesten uitgevoerd op [redacted]. De geconstateerde kwetsbaarheden zijn opgelost.

Roaming kosten
Naar aanleiding van extreem hoge roaming kosten van mobiele data oftewel Internetgebruik in het buitenland van [redacted] heeft de Afdeling [redacted] rapportages opgevraagd bij [redacted]. In de rapportages staat duidelijk voor welke NCTV medewerker een onbeperkt data abonnement voor mobiele devices (dus > 200 euro) is aangevraagd. De Afdeling [redacted] zal deze lijsten aan het management verstrekken met het verzoek deze kritisch te bezien. Voorts zal, in het vervolg, bij de aanvraag door medewerkers gevraagd worden naar de toestemming van de leidinggevende. In de nieuwsberichten van de Afdeling [redacted] zal extra aandacht besteedt worden aan het onderwerp ‘roaming’. Periodiek zal gewaarschuwd worden voor mogelijke hoge roaming kosten in het buitenland en zullen we het handelingsperspectief voor de medewerker schetsen. Het ontstane incident is voorgelegd aan de leidinggevende.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
13 april 2016

nota

Managementrapportage maart 2016
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

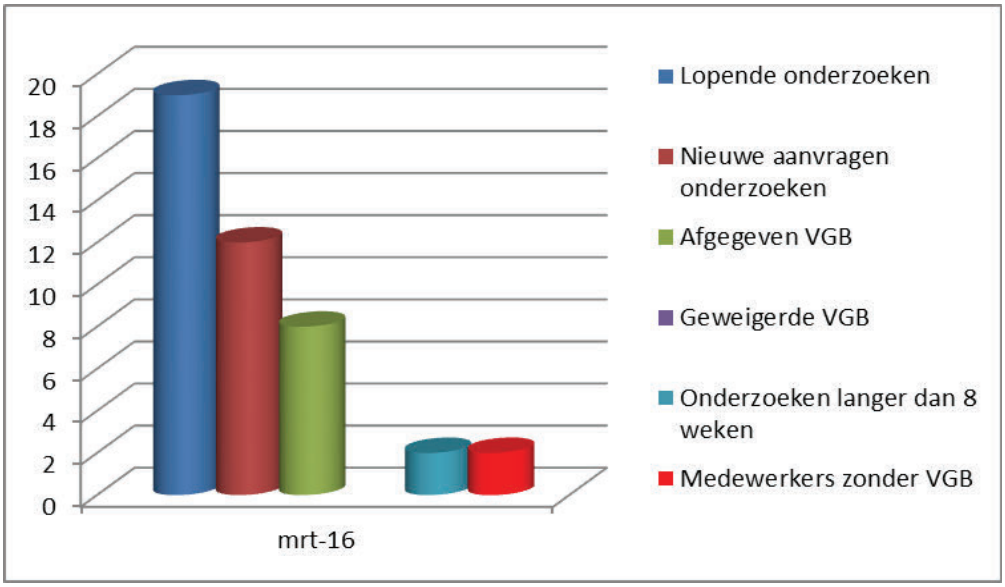
Advies
Ter kennisneming.

Toelichting

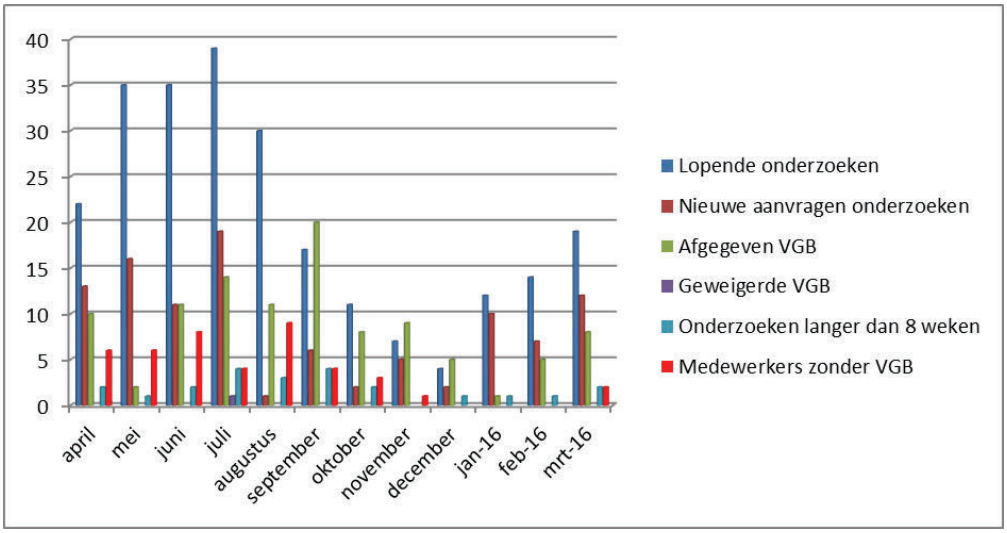
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In maart zijn er twee aanvragen goedgekeurd als uitzonderingen op het tijdelijk werken zonder VGB bij de NCTV (bij [redacted]).

[redacted]

Zie onderstaand beeld.



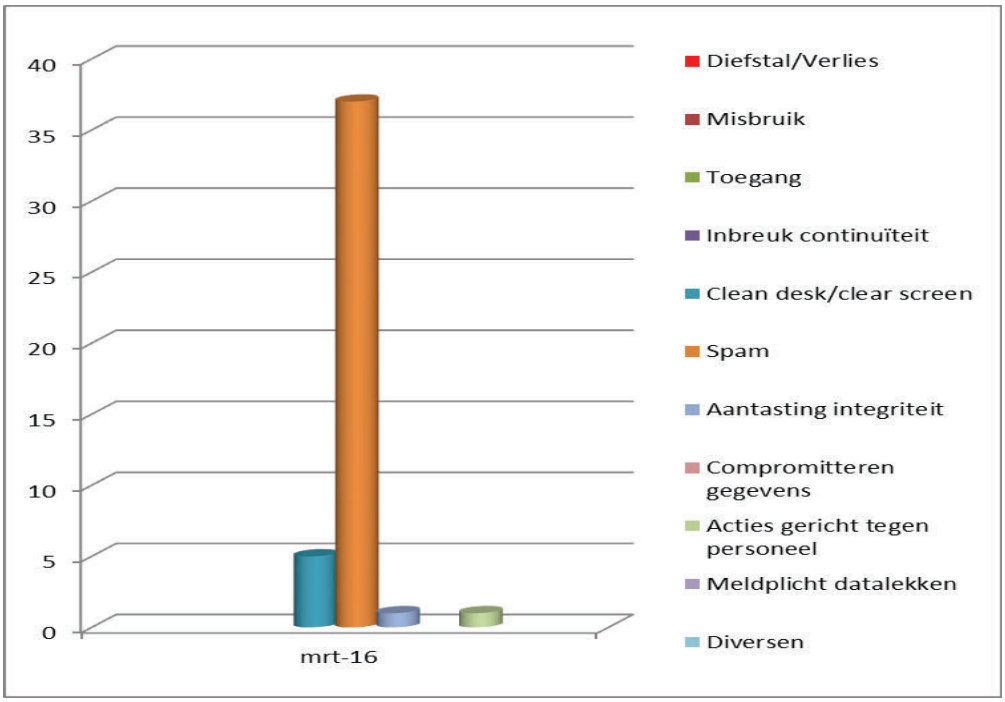
Beeld veiligheidsonderzoeken maart



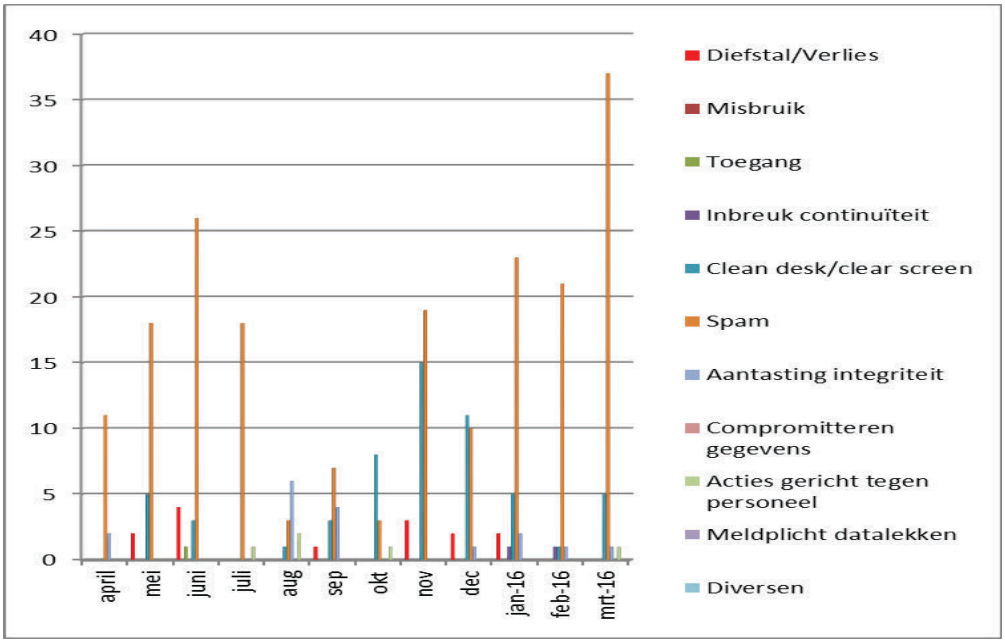
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten januari



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Cleandesk/clean screen
Er zijn 4 [redacted] en één laptop onbeheerd aangetroffen op werkplekken tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers.

SPAM/Phising mail
Er zijn 26 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]. Phishing mails kunnen gebruikt worden voor o.a. het plaatsen van ransomware.
De afgelopen maand zijn er 11 meldingen binnengekomen van medewerkers die door een onbekend buitenlands nummer zijn gebeld. In dit geval is er wederom melding gemaakt naar [redacted]. Een drietal medewerkers heeft melding gemaakt van spam in het SMS verkeer op hun smartphone.

Aantasting Integriteit
Via twitter heeft een burger gemeld dat hij bij een medepassagier gedeeltelijk kon meekijken. Hij zag dat de passagier bij de NCTV werkte. We weten niet om welke medewerker het gaat. In overleg met de afdeling [redacted] is een artikel geplaatst op intranet waarin iedereen nogmaals wordt gewezen op de risico's en dat privacyscreens bij [redacted] verkrijgbaar zijn voor mobiele devices.

Acties gericht tegen personeel
Het secretariaat NCTV had een intimiderend e-mailbericht ontvangen voor [redacted].
Het bericht is gedeeld met [redacted] en toegevoegd aan [redacted]

Overige

[redacted] *NCTV*
In maart is de [redacted] getest en akkoord bevonden door de ADR. Tevens zijn alle [redacted] voorzien van een update in verband met de [redacted]

[redacted]

Meldplicht Datalekken
Afgelopen maanden hebben de directies in het kader van de meldplicht datalekken een inventarisatie uitgevoerd van de verzamelingen persoonsgegevens binnen de NCTV. Ontbrekende verzamelingen van de NCTV zijn op de website van de rijksoverheid geplaatst.
In maart is het "privacy beleidskader VenJ" gepubliceerd en op het rijksportaal geplaatst. Dit privacy beleidskader biedt naast algemene richtlijnen ook een aantal bijzondere richtlijnen voor gegevensverwerking in samenwerkings-verbanden, een stroomschema waarmee een gebruiker kan uitmaken of er sprake is van rechtmatige verwerking van persoonsgegevens en een model van een privacy protocol voor een samenwerkingsverband.
In maart heeft zich ook een incident voorgedaan bij het [redacted]. Dit [redacted] heeft per ongeluk een mail gestuurd waarin

alle geadresseerden van de hele wereld voor elkaar zichtbaar werden. Het bericht [redacted] was ook gericht aan de NCTV en een aantal medewerkers zijn ook zichtbaar geworden. De verzender is geattendeerd op de fout en heeft excuses aangeboden.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage april 2016
Programma Integrale Beveiliging

Datum
11 mei 2016

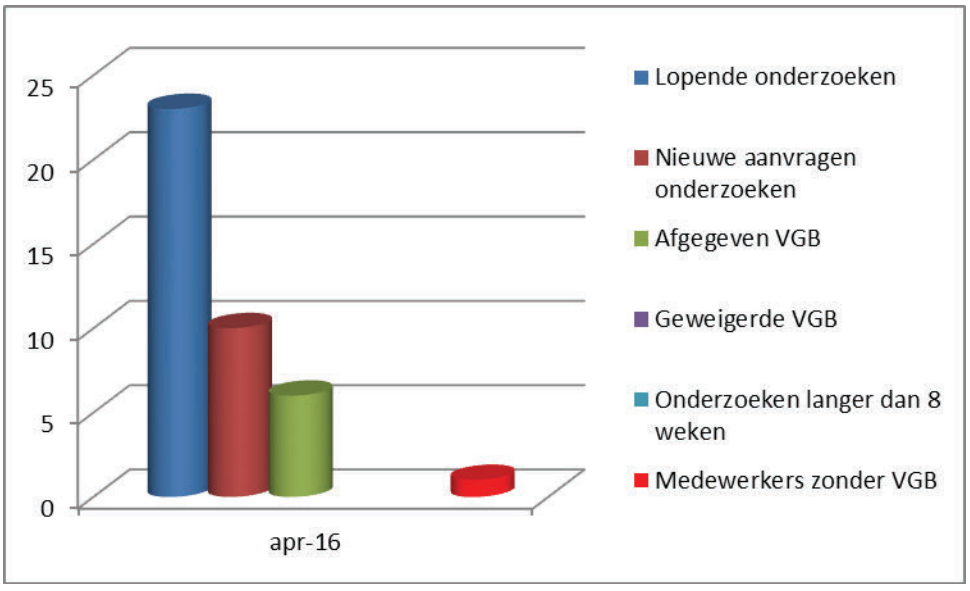
Van
Datum/eindparaaf

Advies
Ter kennisneming.

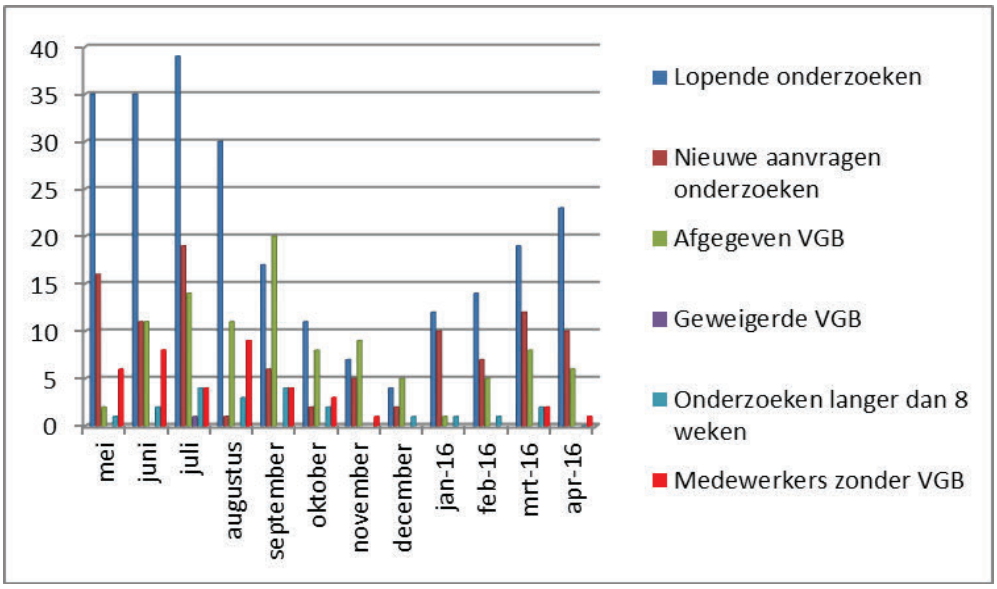
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In april is er één uitzondering op het tijdelijk werken zonder VGB bij de NCTV (bij).

Zie onderstaand beeld.



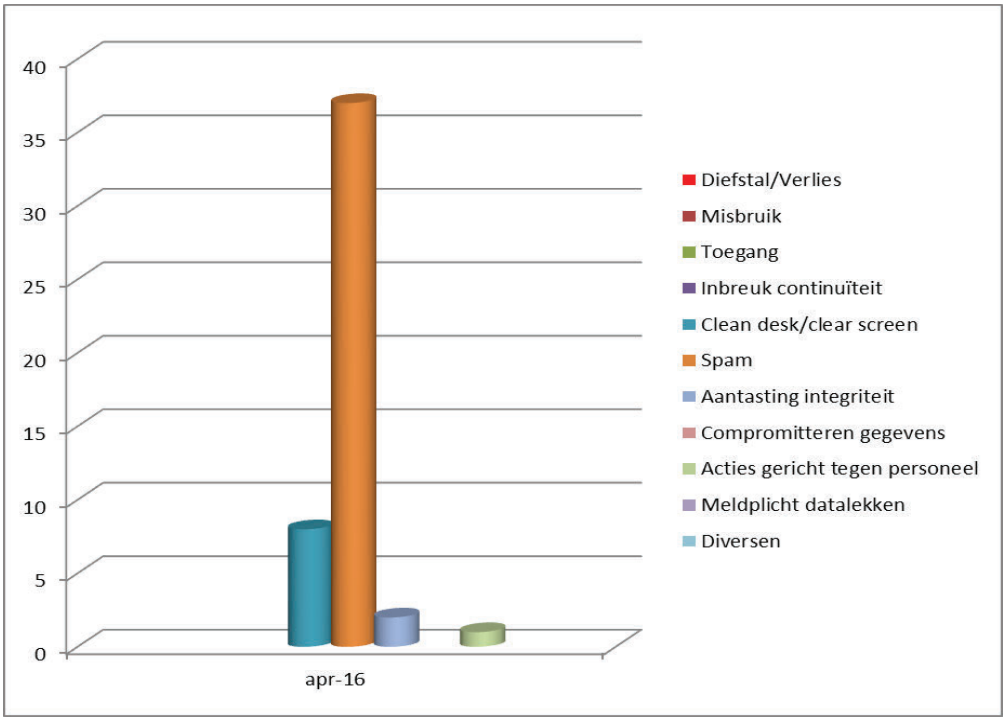
Beeld veiligheidsonderzoeken april



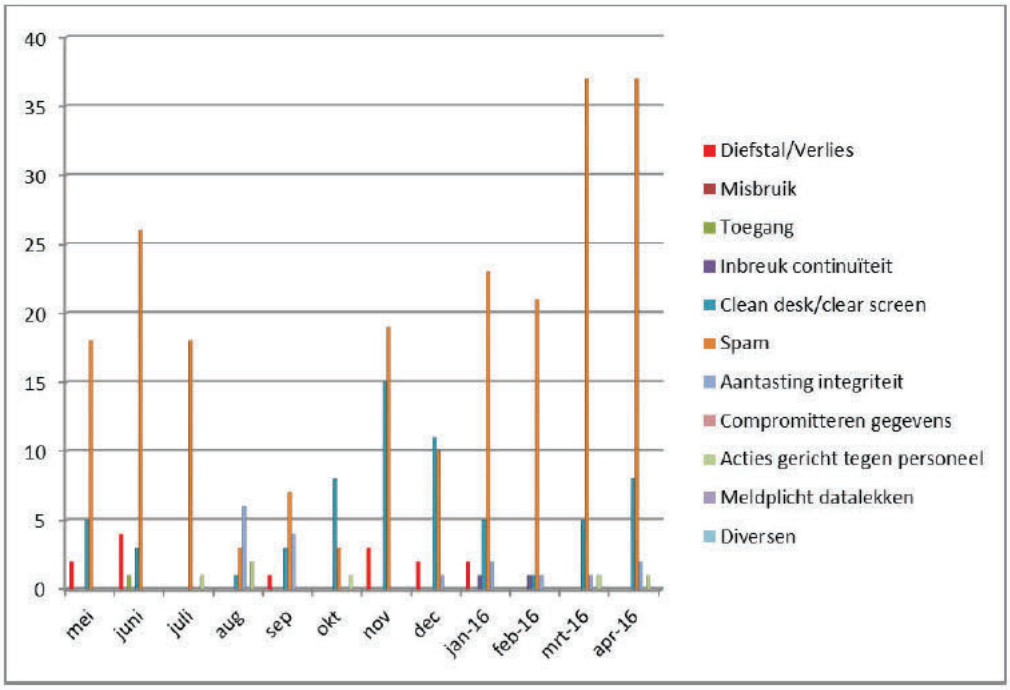
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten april



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Cleandesk/clear screen
Er zijn 6 [redacted] en één harde schijf onbeheerd aangetroffen op werkplekken tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers. Tevens is bij [redacted] een openstaande kluis aangetroffen tijdens de cleandeskronde. De kluis is door de beveiligingsmedewerkers gesloten.

SPAM/Phising mail
Er zijn 26 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] Er zijn mails van [redacted] onderschept waarin de ontvanger wordt verzocht op een link te klikken omdat een factuur niet betaald kon worden. Op intranet is een waarschuwing geplaatst.

De afgelopen maand zijn er 11 meldingen binnengekomen van medewerkers die door een onbekend buitenlands nummer zijn gebeld. Op 24 april is er in de media gemeld dat [redacted] haar particuliere klanten die door deze bellers financieel benadeeld zijn, zal compenseren. Voor als nog lijkt het er niet op dat de NCTV financieel is benadeeld.

Aantasting Integriteit
Op de website www.zuinigopuwdigid.nl staat een artikel waarin het probleem van typosquatting onder de aandacht wordt gebracht. [redacted]

Het reisbureau van VenJ heeft reis en persoonsgegevens van gedeeld via een G-mail account. Er is melding van gemaakt bij . Het onderzoek loopt nog.

Acties gericht tegen personeel
Er is door een stalker een dreigmail gestuurd naar diverse medewerkers die werkzaam zijn bij VenJ waaronder ook NCTV medewerkers. In overleg met onze juristen hebben wij de afhandeling van het incident belegd bij . Het incident is nog in behandeling.

Meldplicht Datalekken
In een persoonlijk e-mailbericht van de afdeling aan 105 medewerkers en hun 53 leidinggevenden van het bestuursdepartement is op 5 april abusievelijk een bijlage meegestuurd met de gegevens van 32.000 medewerkers van VenJ. De ontvangers van het bericht is gevraagd de bijlage te vernietigen. In de lijst stonden geen persoonsgegevens van . De lijst betrof namen van medewerkers die een kaart hebben. Het incident is niet aan de Autoriteit Persoonsgegevens (AP) gemeld omdat het bericht alleen binnen VenJ is verzonden en dit dan niet als datalek wordt aangemerkt.

Overige

Websites NCTV
In april is de update van getest door de ADR. De kwetsbaarheden zijn op één na hersteld en akkoord bevonden. De laatste kwetsbaarheid wordt in mei hersteld.

Veerkrachtmeting
Bij de veerkrachtmeting werd de uitnodiging door het onderzoeksbureau om hieraan deel te nemen tevens naar een gmail-account gestuurd. Dit was niet de bedoeling. Diverse medewerkers hebben het bericht van de veerkrachtmeting aangemerkt als phising mail en hiervan melding gemaakt.

Uitfaseren websites met Flash
In 2015 heeft de ADR in het kader van verbetering van de beveiliging van de NCTV onderzocht. De geconstateerde kwetsbaarheden zijn verholpen, met uitzondering van het gebruik van Flash.
Beveiligingsexperts zoals de ADR en , raden het gebruik van Flash af omdat kwetsbaarheden in Flash player op grote schaal worden misbruikt. Daarnaast kunnen systemen met iOS en Linux deze niet gebruiken omdat deze systemen geen Flash ondersteunen.

Een aantal [redacted] blijkt ook verouderd te zijn, trekt weinig bezoekers en voldoet niet meer aan de huisstijl van de NCTV. De afdeling [redacted] heeft in overleg met [redacted] de betreffende systeemeigenaren geadviseerd deze websites op te heffen en te archiveren.

De volgende websites zullen worden opgeheven en gearchiveerd:

[redacted]

[redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~Dep. VERTROUWELIJK~~
MT NCTV

Stafafdeling
Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

nota

Managementrapportage mei 2016
Programma Integrale Beveiliging

Datum
15 juni 2016

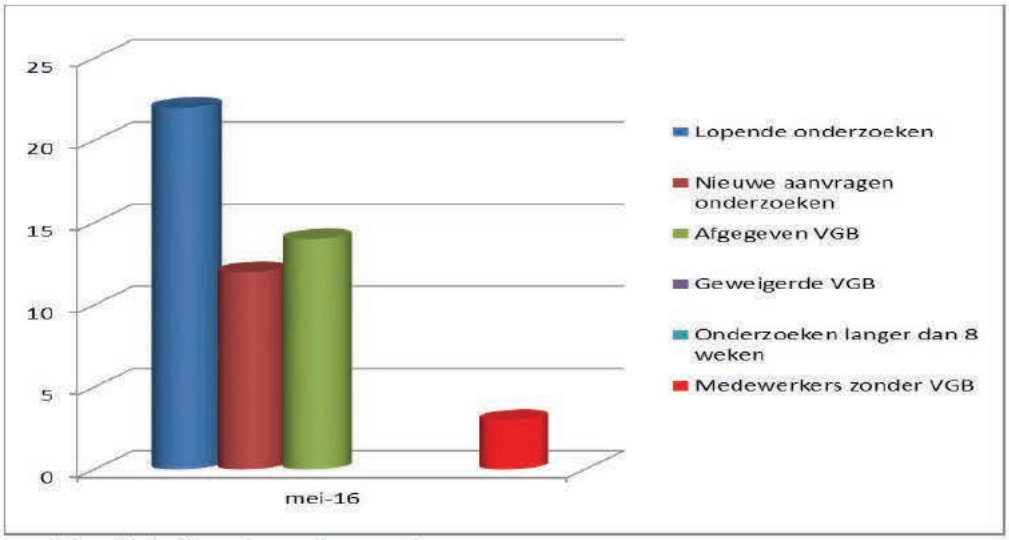
Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisneming.

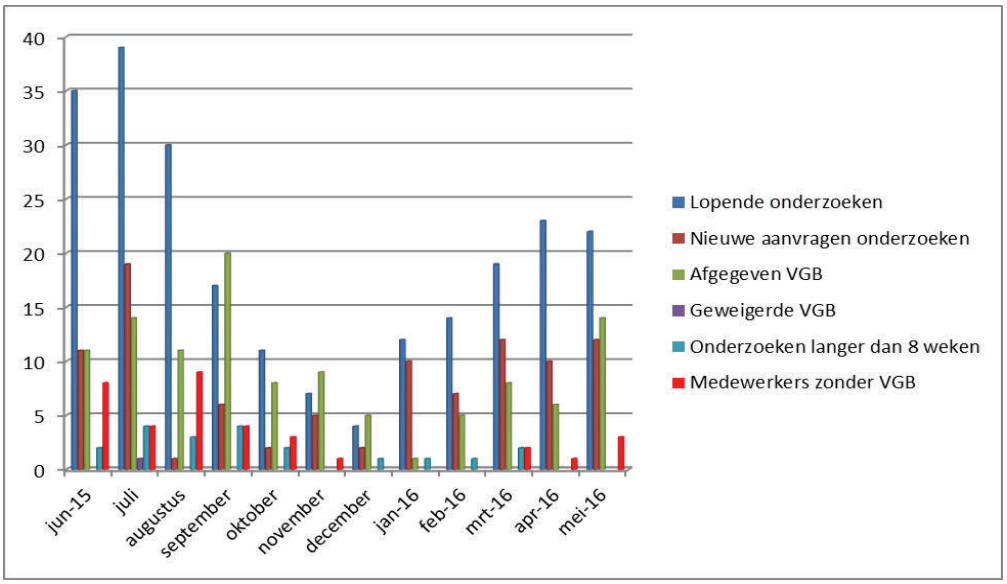
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In mei waren er drie uitzonderingen op het tijdelijk werken zonder VGB bij de NCTV (1 bij [redacted] en 2 bij [redacted]). Eén kandidaat voor een functie bij het projectteam [redacted] heeft zich teruggetrokken nadat de AIVD aanvullende onderzoeksvragen had gesteld. De beschikbare informatie zou mogelijk hebben geleid tot een weigering van de VGB.

Zie onderstaand beeld.



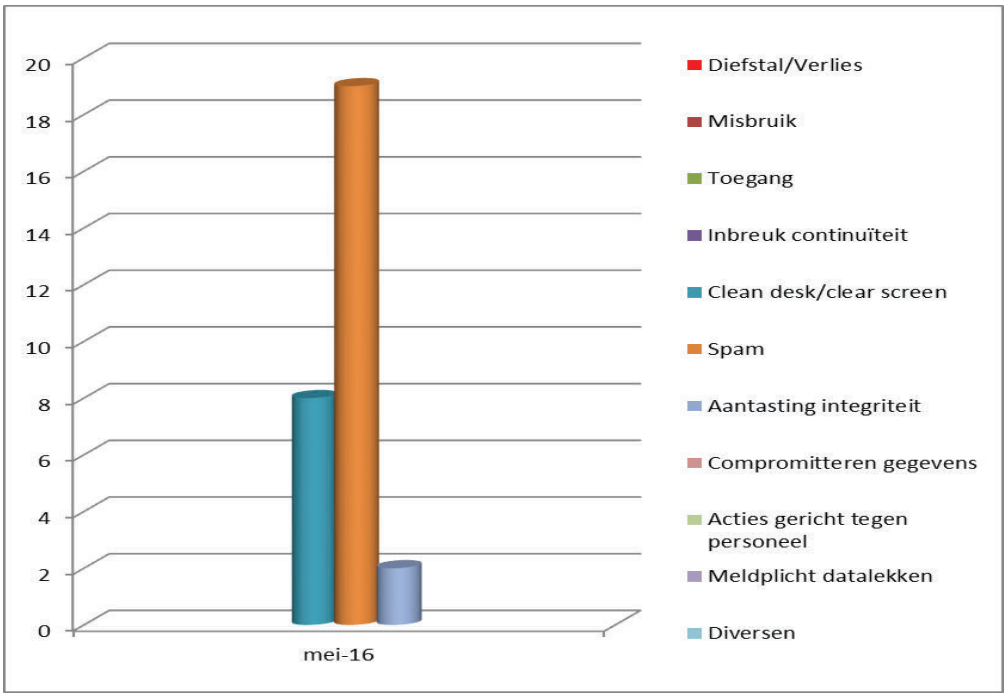
Beeld veiligheidsonderzoeken mei



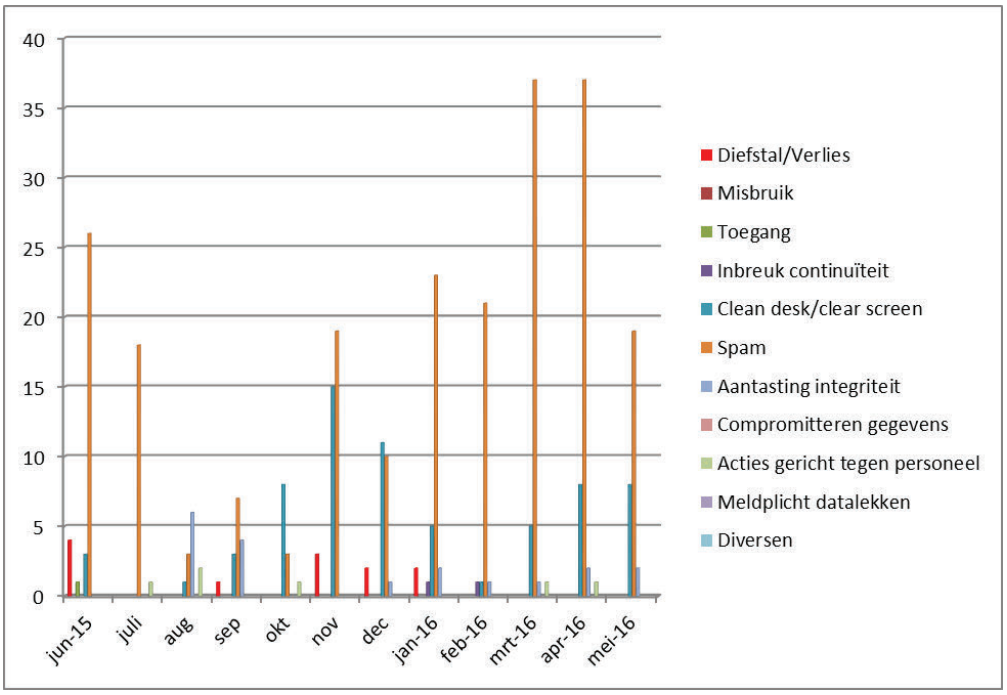
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten mei



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Cleandesk/clear screen
Er zijn 6 onbeheerd aangetroffen op werkplekken (1x op de 4e etage, 1x , 2x , 2x) tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers. Tevens is bij een openstaande kast met 4 laptops aangetroffen tijdens de cleandeskronde. De kast is door de beveiligingsmedewerkers afgesloten. Bij werd een sleutelkluis open aangetroffen tijdens de cleandeskronde. De beveiligingsmedewerkers hebben de sleutelkluis afgesloten.

SPAM/Phising mail
Er zijn 18 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar . Er is een toename zichtbaar in het aantal valse mailberichten van bedrijven.
De afgelopen maand is er 1 melding binnengekomen van een medewerker die door een onbekend buitenlands nummer was gebeld.

Aantasting Integriteit
Een medewerker heeft een notitieboekje verloren binnen de organisatie. Het bevat persoonlijke aantekeningen en geen gerubriceerde informatie.
Een projectmedewerker maakte gebruik van om zakelijke informatie te delen. De medewerker is gewezen op de afspraken binnen de NCTV.

Meldplicht Datalekken
Er hebben zich geen bijzondere meldingen in het kader van de meldplicht datalekken voorgedaan binnen de NCTV.

De afgelopen weken hebben we gezien dat er datalekken hebben plaatsgevonden bij [redacted] en [redacted]. Daarom hebben we een bericht op intranet geplaatst dat medewerkers die van deze social media gebruik maken hun wachtwoord wijzigen. Belangrijk is dat wachtwoorden sterk worden aangemaakt en periodiek worden aangepast.

Overige

Uitwijktest [redacted]
In mei zijn de testen van de uitwijkomgeving voor het [redacted] succesvol afgerond. Hiermee is aangetoond dat indien het [redacted] uitvalt de belangrijkste applicaties die benodigd zijn voor het primaire proces van het [redacted] binnen [redacted] weer beschikbaar zijn [redacted]

[redacted]
Eind mei heeft de Stafafdeling [redacted] met succes aangetoond dat het mogelijk is om [redacted] beschikbaar te hebben op [redacted]. Hiermee kan het primaire proces van de [redacted] weer gebruik maken van [redacted].

Kwetsbaarheidsanalyse Spionage
Vanuit interdepartementale afspraken moet er iedere twee jaar binnen een organisatie een inventarisatie van de [redacted]
Via de mail hebben de leidinggevenden een verzoek ontvangen of zij, in Q3, medewerking kunnen verlenen aan het houden van de interviews. De uiteindelijke selectie van medewerkers vindt plaats in overleg met de leidinggevenden.
Alle te interviewen personen krijgen vooraf een aantal vragen en het huidige overzicht van de Cruciale Belangen en Te Beschermen Belangen.

Smartphone lockers
Begin mei heeft de stafafdeling [redacted] op de [redacted] smartphonelockers geplaatst. In deze lockers kunnen deelnemers van een vergadering waarin vertrouwelijke onderwerpen worden besproken hun mobiele devices (laptops, tablets, smartphone EN smartwatches) veilig opbergen.
De voorzitter kan de deelnemers aan een vergadering verzoeken om hun mobiele devices op te bergen in deze lockers.

Gmail
Naar aanleiding van de berichten in de media dat minister Kamp voor zakelijke informatie van zijn departement zijn g-mailaccount heeft gebruikt, is een bericht op intranet geplaatst waarin de medewerker er op wordt gewezen om voor het verzenden van zakelijke informatie alleen gebruik te maken van het NCTV-mailaccount.

[redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

~~Dep. VERTROUWELIJK~~
MT NCTV

Directie Strategie en Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
7 juli 2016

Ons kenmerk
123456

nota

Managementrapportage juli/augustus 2015
Programma Integrale Beveiliging

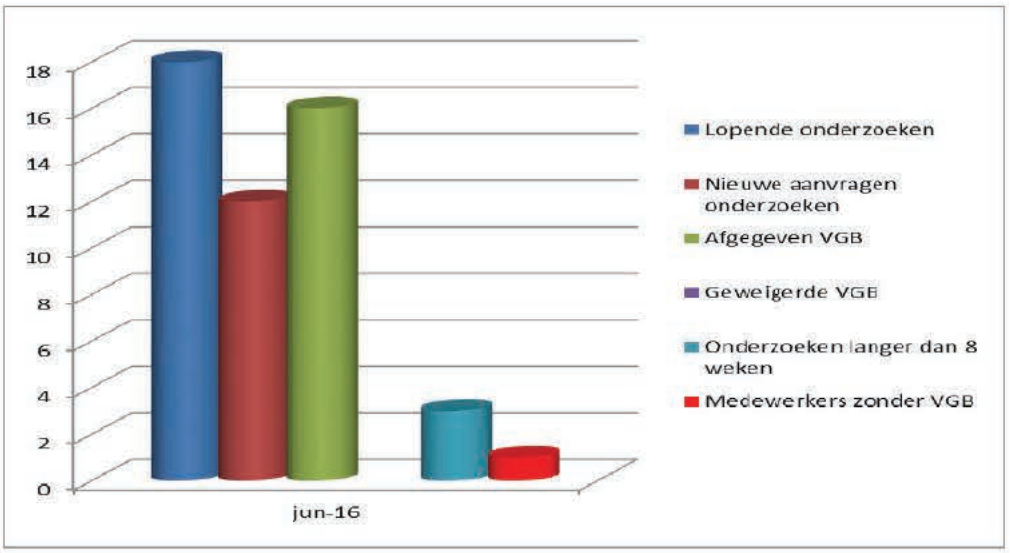
Van
[redacted]
Datum/eindparaaf

Advies
Ter kennisneming.

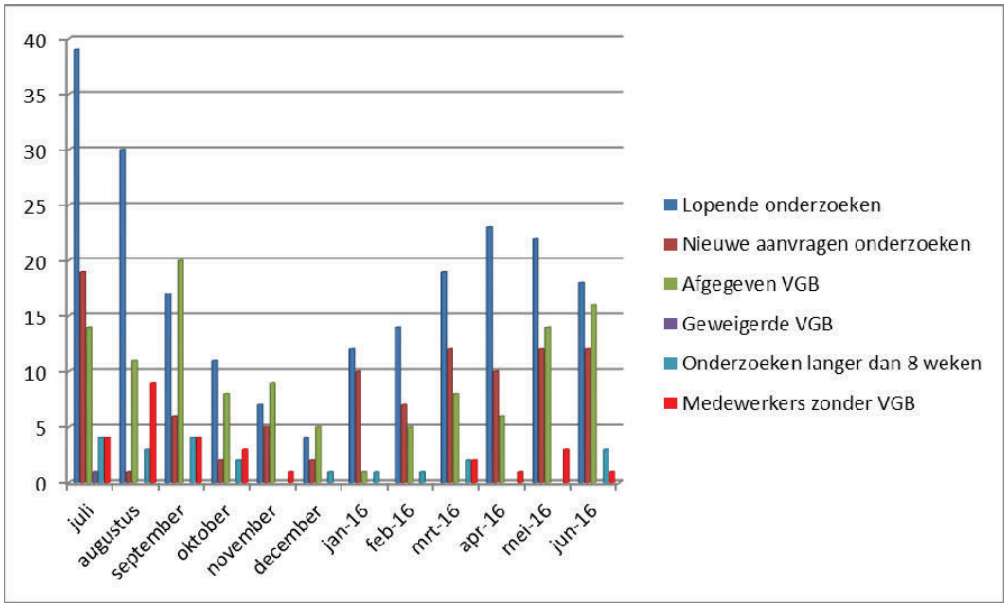
Toelichting

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In juni was er één uitzondering op het tijdelijk werken zonder VGB bij de NCTV (1 bij [redacted]).

Zie onderstaand beeld.



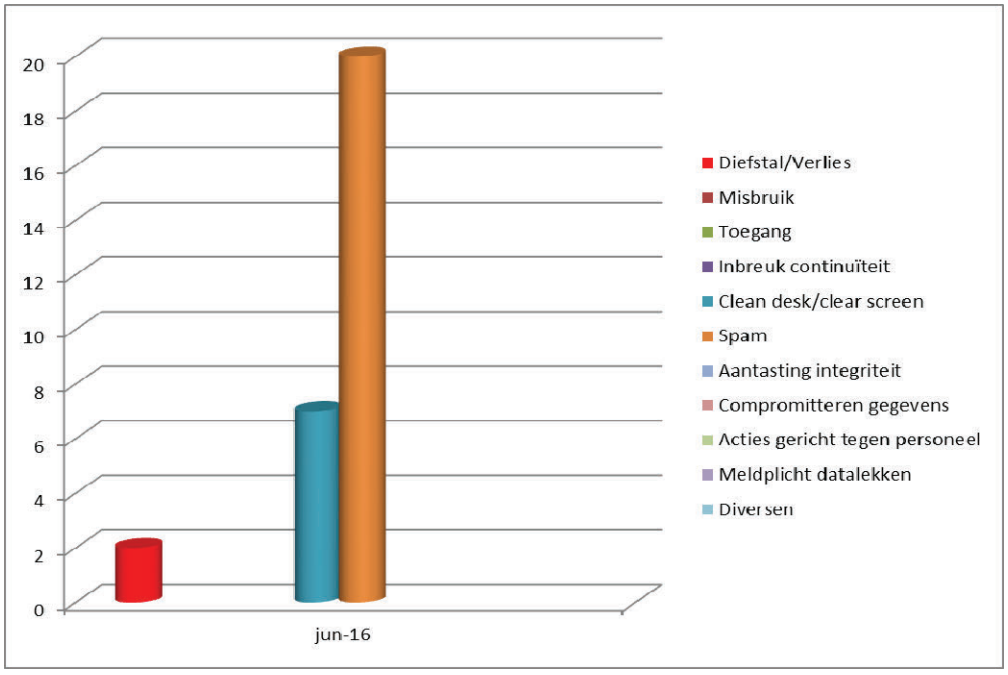
Beeld veiligheidsonderzoeken mei



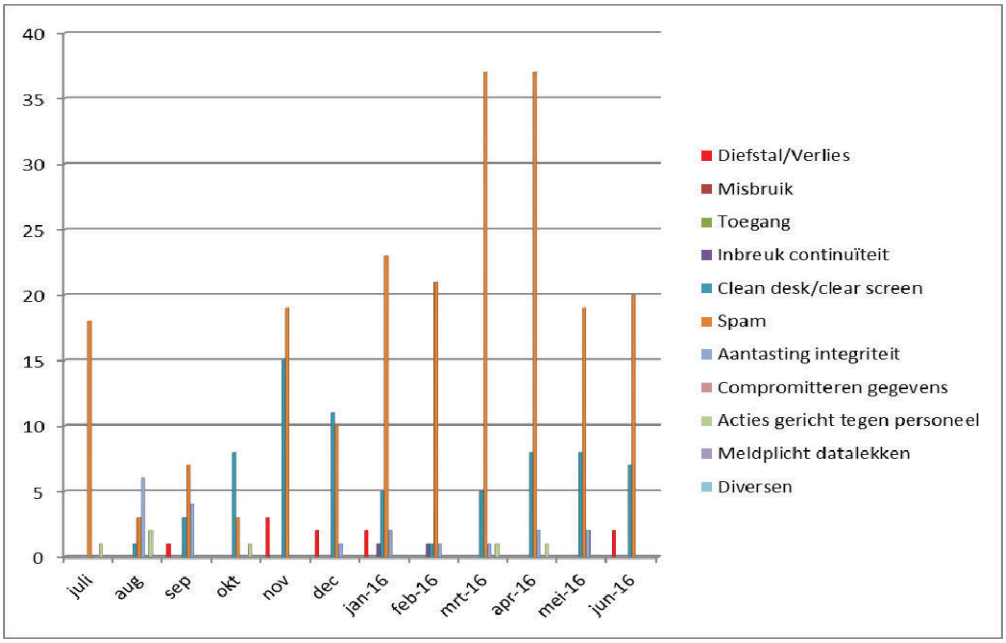
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten juni



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Cleandesk/clear screen
Er zijn 6 [redacted] onbeheerd aangetroffen op werkplekken [redacted] tijdens de cleandeskrondes en veilig gesteld door de beveiligingsmedewerkers.
Een laptop was na intern gebruik vergeten in de vergaderzaal. De laptop is door de beveiligingsmedewerkers veilig gesteld en in de kluis opgeborgen.

SPAM/Phising mail
Er zijn 18 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]. Er is een toename zichtbaar in het aantal valse mailberichten van bedrijven. Voorbeelden: rekeningen voor privé-telefonie of aanmaning van een incassobureau op het zakelijke mailadres van een medewerker.
De afgelopen maand is er 1 melding binnengekomen van een medewerker die door een onbekend buitenlands nummer was gebeld.

Meldplicht Datalekken
Er hebben zich geen meldingen in het kader van de meldplicht datalekken voorgedaan binnen de NCTV.

De afgelopen weken hebben we gezien dat er datalekken hebben plaatsgevonden bij [redacted] en [redacted]. Het betrof hier data met informatie over [redacted]. Er zijn geen indicaties vrijgekomen over het gebruik door NCTV.

Overige

[redacted]
Het [redacted] heeft in samenwerking met [redacted] een nieuw product geïntroduceerd voor het flexibel werken. Er waren veel vragen over of dit veilig is. De voorziening voldoet aan de gestelde eisen. Wij hebben een artikel geplaatst op intranet voor alle NCTV medewerkers.

Autorisaties
Afgelopen maand is er aan alle leidinggevenden een verzoek gedaan om de autorisaties voor de toegang tot ICT mappen op het VenJ netwerk te controleren. Inmiddels zijn de meeste reacties binnen en zijn ze verwerkt.
Ook de autorisaties voor alle rijkspassen zijn gecontroleerd en daar waar nodig aangepast.

Voortgang BIR
Begin 2016 is een ICV (In Control Verklaring) BIR van de NCTV opgesteld en naar de CISO VenJ gestuurd. Hierin zijn explains opgenomen met een planning voor uitvoering van verbeteracties.
In april heeft de ADR een eindrapport over de BIR-onderzoeken 2015 gepubliceerd. Ook de ARK heeft onderzoek gedaan naar de status van informatiebeveiliging bij VenJ. De bevindingen uit deze rapporten hebben er toe geleid dat binnen VenJ extra verbeteracties zijn benoemd.

Onderstaande rapportage geeft een beeld van de voortgang van bovenstaande verbeteracties binnen de NCTV. Hierbij is de NCTV op de goede weg, maar nog niet alle maatregelen zijn volgens planning gerealiseerd. Dit blijft aandacht vergen in de tweede helft van 2016.

Explains ICV BIR 2015 (zie ICV BIR NCTV 2015 d.d. 21 januari 2016)
De volgende maatregelen uit de ICV zijn volgens planning gereed gemeld in Q2 2016:

[redacted]

De volgende maatregelen zijn in de planning doorgeschoven van Q2 naar Q3 2016:

Maatregelen uit de risicoanalyse
In 2015 is een risicoanalyse op het uitgevoerd, deze risicoanalyse is voor akkoord getekend door hoofd M&R.
De afdeling M&R heeft naar aanleiding van deze risicoanalyse een concept plan van aanpak opgesteld voor het invoeren van aanvullende beveiligings-maatregelen.
De volgende maatregelen zijn volgens planning gereed gemeld in Q2 2016:

- Test van de (zie managementrapportage van mei).
- Trainen van de nieuwe medewerkers.

De volgende maatregelen worden in de tweede helft van 2016 ingevoerd:

- Implementatie van het SIEM met .
- Het koppelen van de aan de centrale gebruikersdatabase.
- Het trainen van de bestaande gebruikers van het .
- Een studie naar aanvullende DDoS maatregelen voor het .

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage juli en augustus 2016
Programma Integrale Beveiliging

Datum
13 september 2016

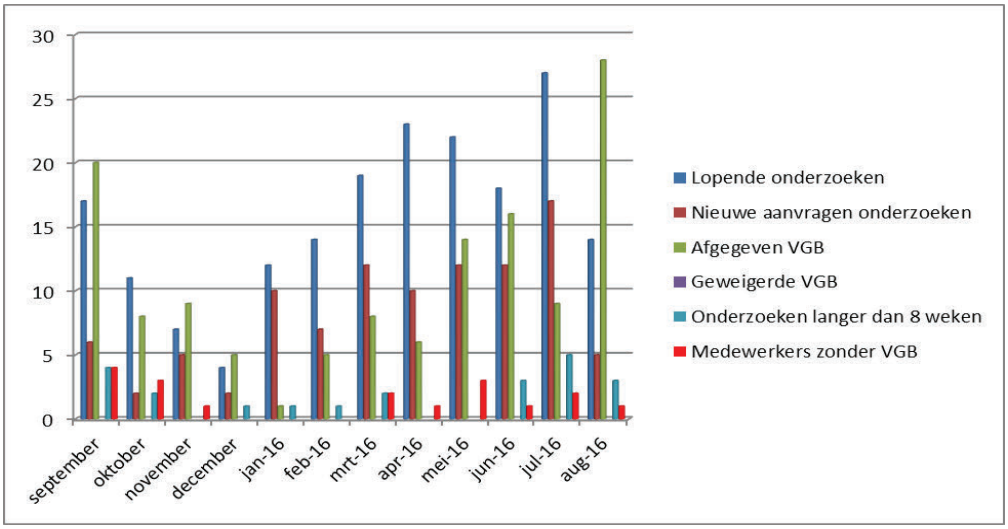
Van

Datum/eindparaaf

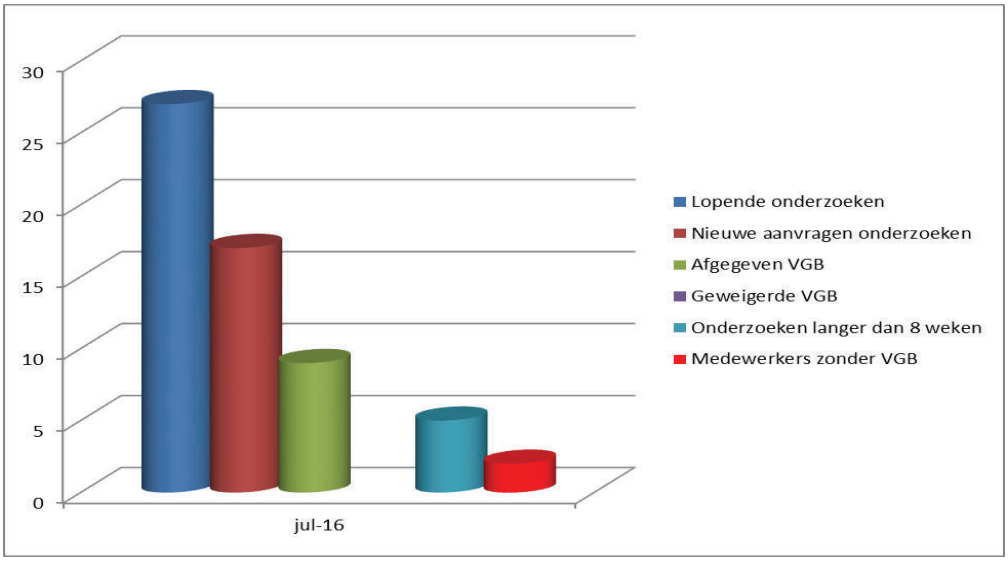
Advies
Ter kennisneming.
Uitnodiging om de werkgroepleden beveiliging in het afdelingsoverleg een presentatie te laten geven over ransomware.

Toelichting
Het betreft de rapportage over de (zomer)maanden juli en augustus.

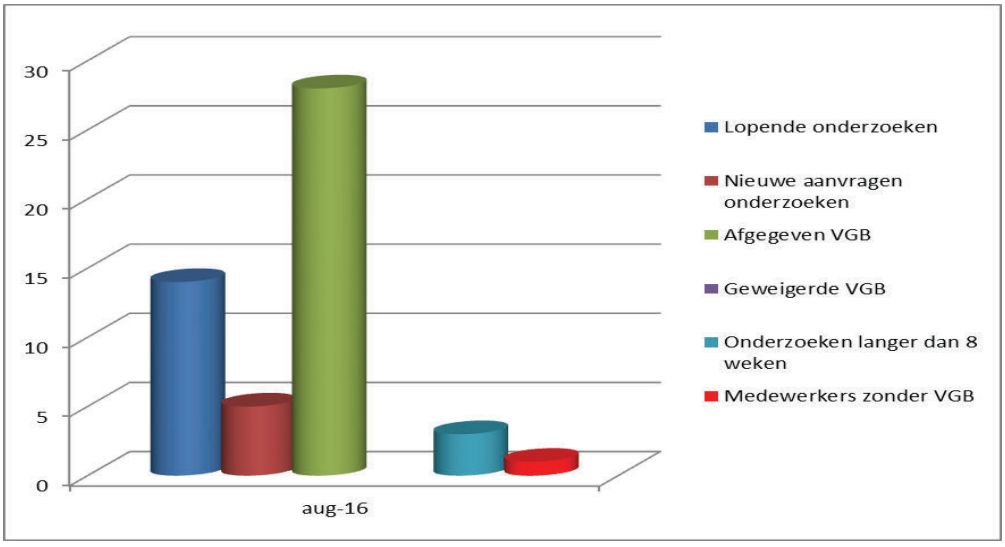
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In juli waren er twee uitzonderingen op het tijdelijk werken zonder VGB bij de NCTV (1 en 1). In augustus was er nog één uitzondering op het tijdelijk werken zonder VGB bij de NCTV (1 bij).



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



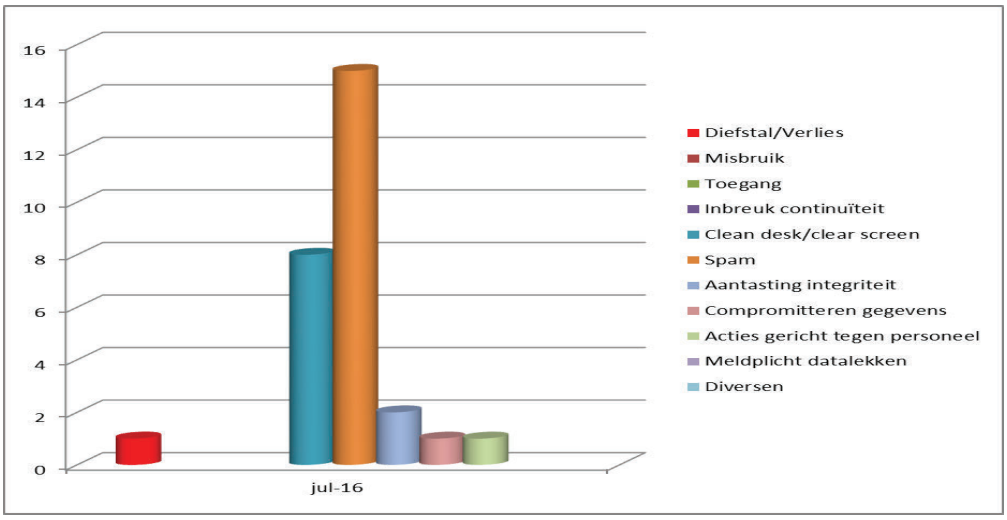
Beeld veiligheidsonderzoeken juli



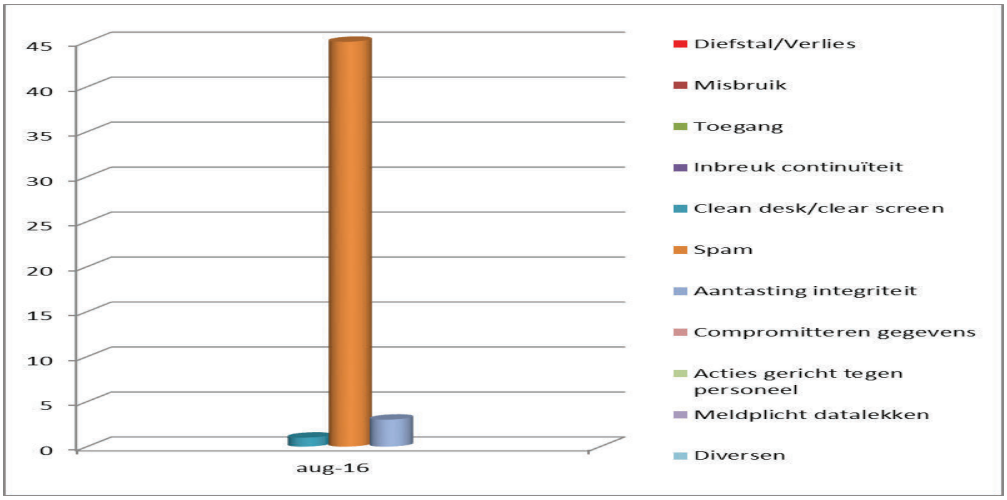
Beeld veiligheidsonderzoeken augustus

Incidentenregistratie

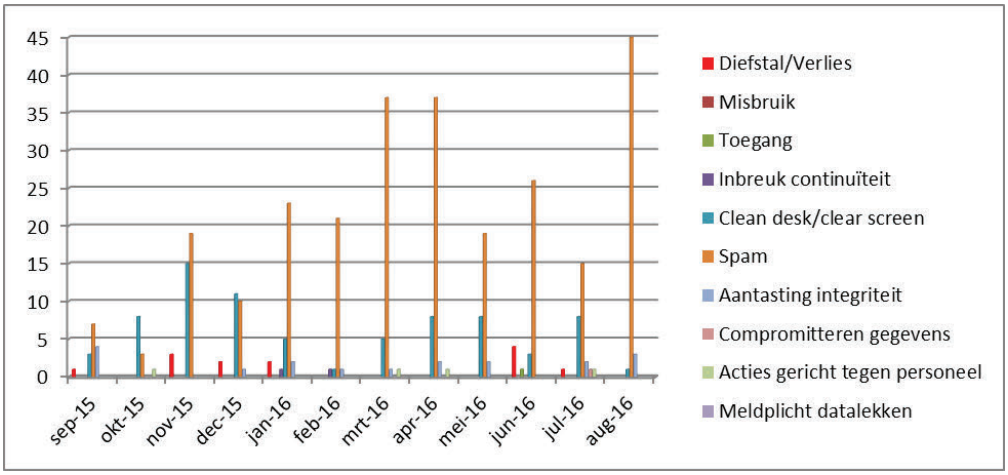
Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Beeld beveiligingsincidenten juli



Beeld beveiligingsincidenten augustus



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting tabellen

Diefstal/verlies
- Een medewerker heeft zijn rijkspas verloren. Na de melding is de rijkspas geblokkeerd.

Cleandesk/clear screen
- In een prullenbak van een medewerker zijn [redacted] stukken aangetroffen. De documenten zijn opgeborgen in de kluis bij de receptie en de medewerker is er op aangesproken.

De beveiligingsmedewerkers hebben tijdens cleandeskrondes;
- een open kluis bij [redacted] aangetroffen en alsnog afgesloten. Een melding is gemaakt voor de leidinggevende die het besproken heeft met de medewerkers.
- 6 [redacted] onbeheerd aangetroffen op werkplekken [redacted] en veilig gesteld.
- een onbeheerde IPad aangetroffen en veilig opgeborgen in de kluis.

SPAM/Phising mail
- *Mail.* In juli en augustus zijn 60 meldingen van spam en phising mail binnengekomen waaronder berichten van mailadressen die de uitstraling hadden van [redacted].
- *Mobiel.* De afgelopen maand zijn er 38 meldingen binnengekomen van medewerkers die spam op hun telefoon hebben ontvangen als SMS. Een groot deel van de meldingen betrof meldingen over de [redacted] heeft de medewerkers hierover geïnformeerd via een interne mail.
- *Vaste telefonie.* In augustus hebben we diverse telefoontjes binnen gekregen op het vaste telefoonnet van personen die zich voor deden als medewerker van [redacted]. De bedoeling was om in te loggen en zo malware te installeren. De pogingen zijn mislukt. Er is melding gemaakt bij [redacted] die verantwoordelijk is voor het telefoonnet.

Aantasting integriteit
- Een medewerker heeft de inloggegevens gebruikt van een collega (afwezig i.v.m. vakantie). De betreffende medewerker is aangesproken en gewezen op de mogelijkheid van het opslaan van informatie op gezamenlijke mappen.
- Een deelnemer aan een bijeenkomst met een [redacted] heeft zonder overleg een bericht getwitterd met een foto van deelnemers. Hierbij was de [redacted] zichtbaar. Van belang is dat NCTV medewerkers zich hiervan bewust zijn en dat vooraf met de aanwezigen afspraken worden gemaakt.
- [redacted] Het gedrag is waargenomen door monitoring en logging van de systemen. In dit geval betrof het een actie op het anonieme [redacted] waardoor een risico bestaat dat de integriteit van dit net wordt aangetast. De leidinggevende heeft de medewerker aangesproken op zijn gedrag.
- Bij de postkamer is per ongeluk een enveloppe geopend die [redacted] informatie bevatte. De leidinggevende van de postkamer heeft de medewerkers aangesproken en het proces opnieuw geëvalueerd.

- Een medewerker heeft mogelijk te hoge declaraties ingediend. Het onderzoek loopt nog. De medewerker is inmiddels niet meer werkzaam voor de NCTV.

Compromitteren gegevens

- [redacted]

Acties gericht tegen personeel

- Er is een mail ontvangen van een stalker die contact blijft zoeken met de NCTV. Het betreft hier een [redacted] die regelmatig deze acties uitvoert. In dit geval is de melding ook doorgezonden naar [redacted].

Overige

[redacted]
Vanuit de NCTV is melding gemaakt bij het Dienstencentrum en [redacted] over de kwetsbaarheden die aanwezig zijn in het [redacted]. Het betreft voor namelijk patchmanagement en software updates. Beide partijen erkennen de noodzaak om de kwetsbaarheden te beperken maar door de vele onderlinge (keten)afhankelijkheden in de systemen, is een snelle patching niet altijd mogelijk is. Inmiddels is melding gemaakt bij [redacted] om deze zaak te behandelen.

Kwetsbaarheden netwerken en systemen
Door de recentelijke digitale inbraak bij de NSA in de Verenigde Staten zijn kwetsbaarheden beschikbaar gekomen van diverse netwerken en applicaties.
[redacted]
Diverse kwetsbaarheden hebben zich voorgedaan in het besturingssysteem van [redacted]. [redacted] heeft voor het mitigeren van de gevolgen een upgrade beschikbaar gesteld. De medewerkers van de NCTV zijn via een bericht op intranet gewezen op de upgrade en kwetsbaarheden.
[redacted]
In een artikel op intranet zijn de medewerkers gewezen op de mogelijke risico's van het gebruik van [redacted] en een optie om veiliger gebruik te maken van [redacted]
De afgelopen maand zijn diverse kwetsbaarheden van het besturingssysteem [redacted] bekend gemaakt. Onder andere het meekijken en meeluisteren op afstand [redacted] wordt weer gemeld als mogelijk risico. Bij de NCTV hebben we hier al eerder lockers voor aangeschaft.
<u>Websites:</u>
Er zijn kwetsbaarheden gevonden in 'https' verbindingen. De kwetsbaarheden zijn gemeld aan de website beheerders van de NCTV.

Stafafdeling
Bedrijfsvoering

Datum
13 september 2016

Ransomware
De afgelopen tijd is ransomware veel in het nieuws.
Aangezien we deel uitmaken van een netwerkorganisatie met veel externe contacten bestaat de kans dat we het slachtoffer worden van ransomware doordat medewerkers bijvoorbeeld een bijlage in een mail openen die toch niet van een bekende en vertrouwde relatie kwam. De werkgroepleden beveiliging kunnen een presentatie over het onderwerp geven tijdens bijvoorbeeld een afdelingsoverleg.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage september 2016
Programma Integrale Beveiliging

Datum
12 oktober 2016

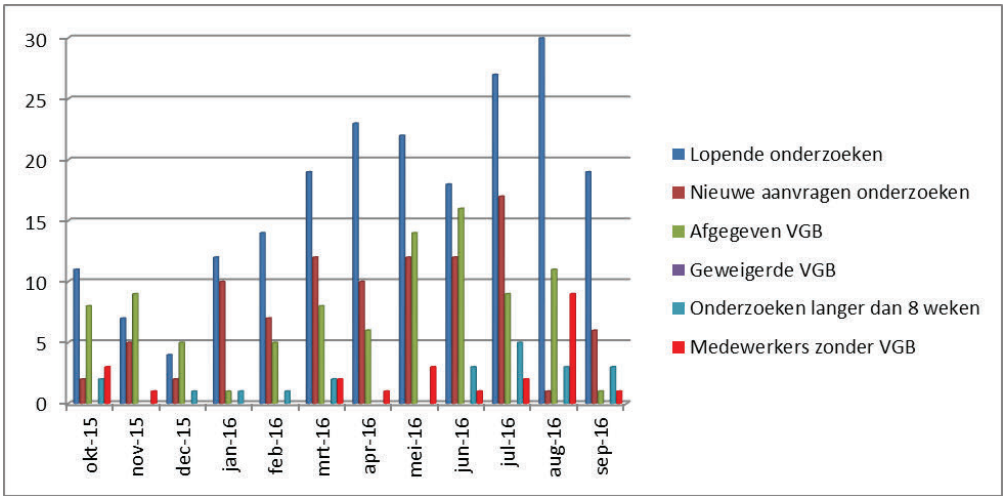
Van

Datum/eindparaaf

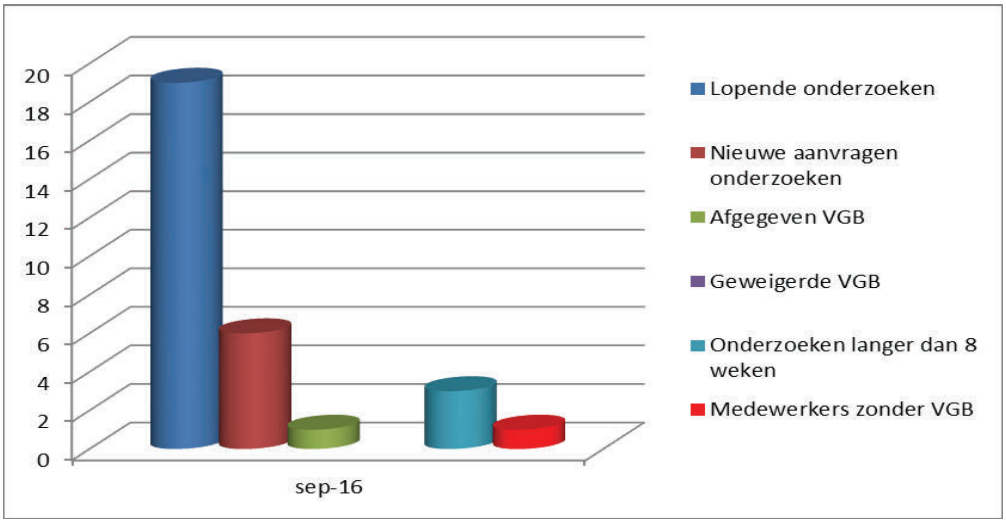
Advies
Ter kennisneming.

Toelichting
Het betreft de rapportage over de maand september.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In september was er één uitzondering op het tijdelijk werken zonder VGB bij de NCTV



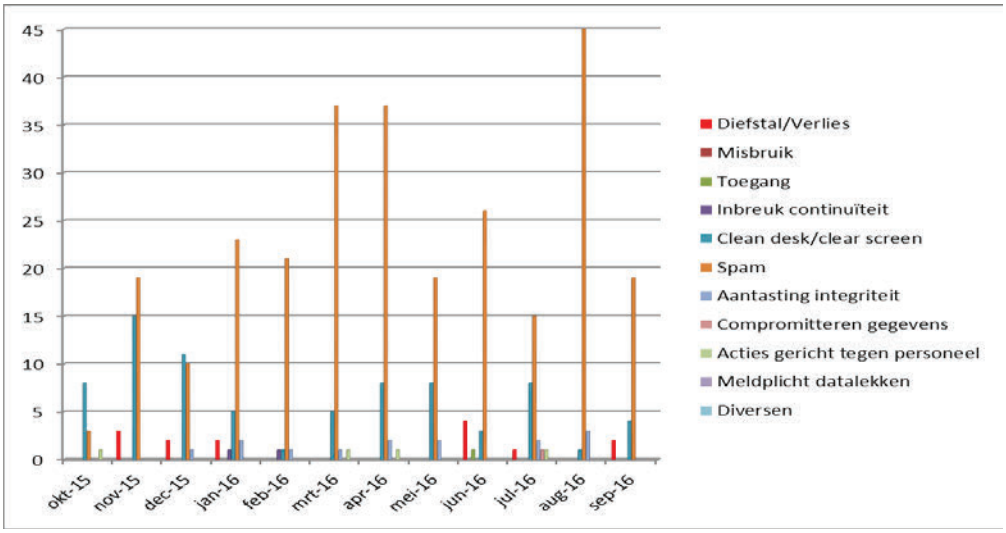
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



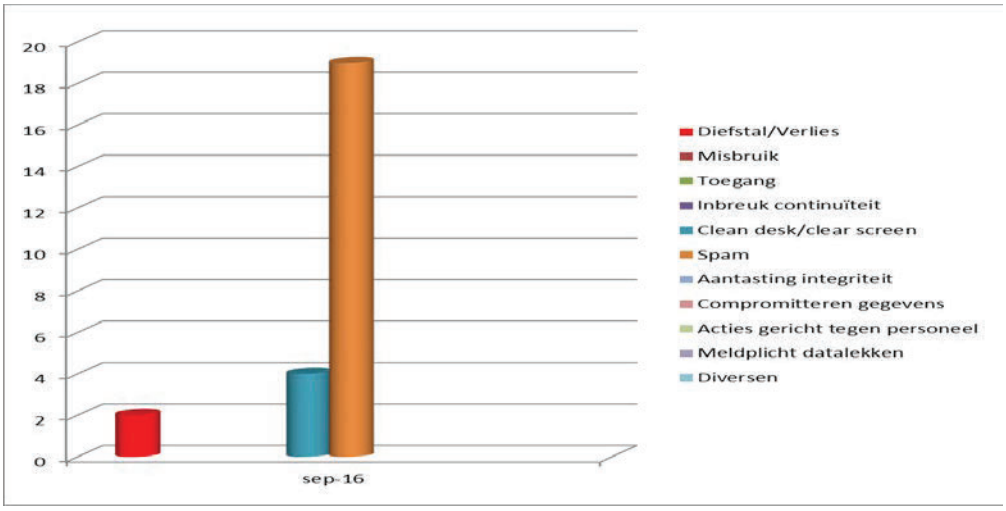
Beeld veiligheidsonderzoeken september

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten september

Toelichting tabellen

Diefstal/verlies

- Een medewerker heeft zijn [redacted] intern verloren. Er is geen misbruik gemaakt van [redacted]. [redacted] is inmiddels geblokkeerd.
- Van een medewerker is de toilettas gestolen uit de kleedkamer [redacted]. Er is melding gemaakt bij [redacted].

Cleandesk

Na afloop van vergaderingen hebben (beveiligings)medewerkers 4 keer melding gemaakt van documenten die op de vergadertafels en in de prullenbakken waren achtergelaten. Het verzoek aan de leidinggevenden om dit te bespreken binnen de afdelingsoverleggen.

SPAM/Phising mail

- *Mail.* In september zijn 11 meldingen van spam en phising mail binnengekomen waaronder berichten van mailadressen die de uitstraling hadden van [redacted]
- *Mobiel.* De afgelopen maand zijn er 8 meldingen binnengekomen van medewerkers die spam op hun telefoon hebben ontvangen als SMS. Een groot deel van de meldingen betrof meldingen over de [redacted]. [redacted] heeft de NCTV medewerkers hierover geïnformeerd via een interne mail.
- *Laptop.* Op een [redacted] van [redacted] is malware ontdekt. [redacted]

Overige

Ransomware
De afgelopen tijd is ransomware veel in het nieuws.
Aangezien we deel uitmaken van een netwerkorganisatie met veel externe contacten bestaat de kans dat we het slachtoffer worden van ransomware doordat medewerkers bijvoorbeeld een bijlage in een mail openen die toch niet van een bekende en vertrouwde relatie kwam. De werkgroepleden beveiliging kunnen een presentatie over het onderwerp geven tijdens bijvoorbeeld een afdelingsoverleg.
Inmiddels zijn er presentaties gegeven bij .

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

nota

Managementrapportage oktober 2016
Programma Integrale Beveiliging

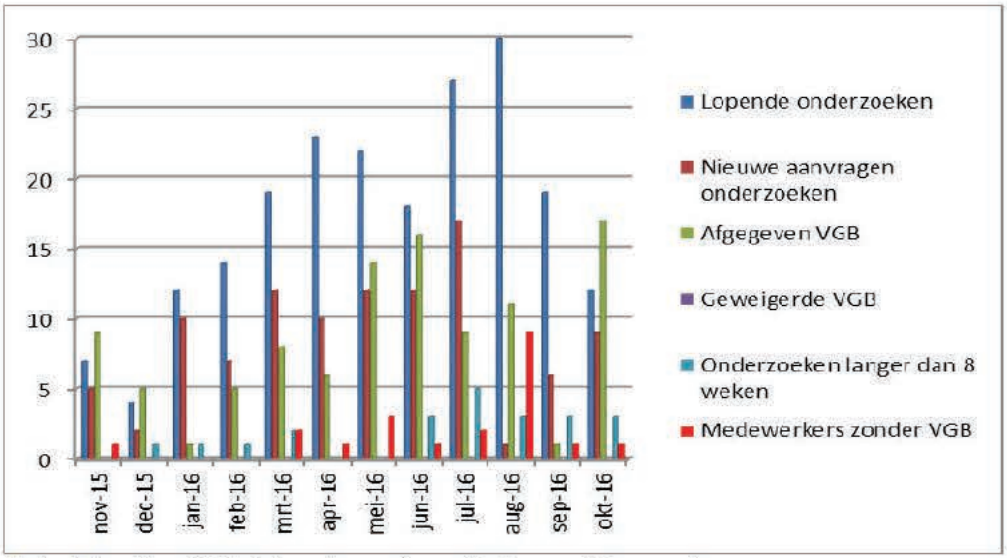
Datum
12 november 2016

Van
[redacted]
Datum/eindparaaf

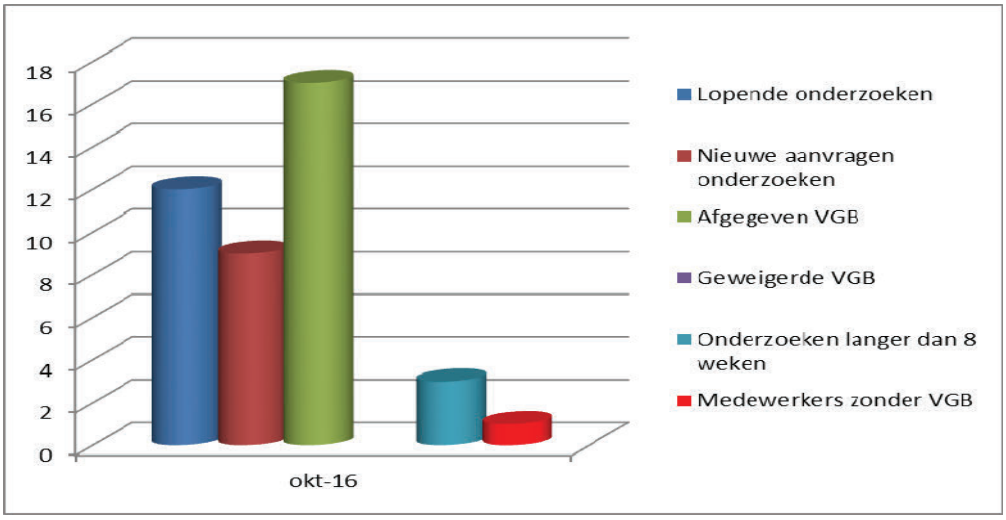
Advies
Ter kennisneming.

Toelichting
Het betreft de rapportage over de maand oktober.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In oktober was er één uitzondering op het tijdelijk werken zonder VGB bij de NCTV ([redacted]).



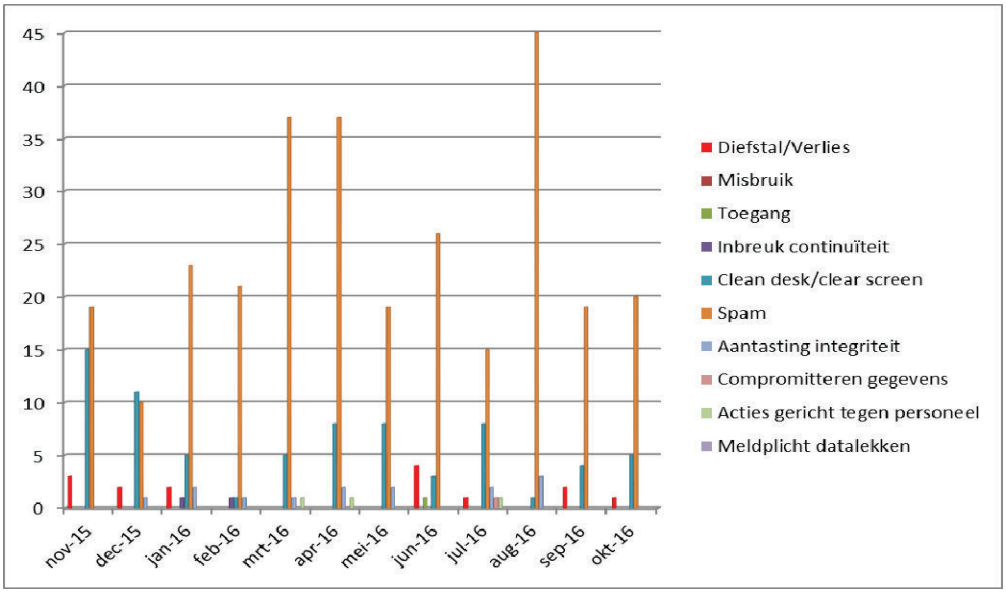
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



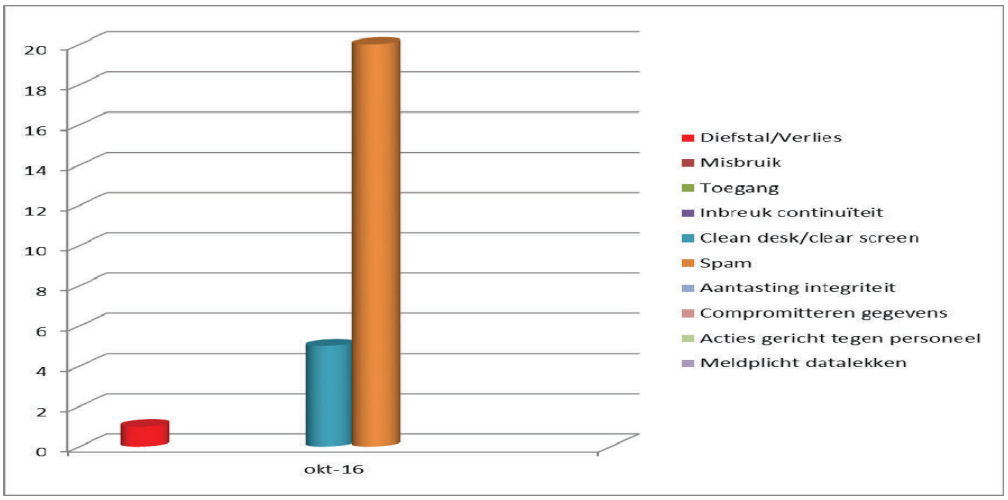
Beeld veiligheidsonderzoeken oktober

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten oktober

Toelichting tabellen

Diefstal/verlies

- Een medewerker heeft een Ipad verloren. Er is aangifte gedaan en de Ipad is op afstand geblokkeerd. Er zijn nog geen goede afspraken over het proces van melden buiten kantooruren. zal in overleg met het proces afstemmen.

Cleandesk

- De beveiligingsmedewerkers hebben tijdens cleandeskrondes onbeheerd aangetroffen op werkplekken en veilig gesteld.

SPAM/Phising mail

- *Mail.* In oktober zijn 20 meldingen van spam en phising mail binnengekomen waaronder 11 berichten van met een nepfactuur. De meldingen zijn doorgestuurd naar en besproken met .

Overige

Rijkspassen

Begin november zijn de autorisaties voor de rijkspassen gecontroleerd en daar waar nodig aangepast. De aanpassingen waren nodig omdat het vertrek van de bewuste medewerkers niet op tijd is gemeld (14x) bij .

Alert Online

Begin oktober zijn in het kader van Alert Online presentaties gegeven in 2 afdelingsoverleggen over ransomware. Tevens zijn uitgedeeld. Als laatste zijn binnen de afdelingen posters opgehangen om het beveiligingsbewustzijn bij de medewerkers te verbeteren.

SIEM
In 2016 heeft [redacted] een Security Information en Event Management (SIEM) tool ingericht op het [redacted]. Dit SIEM verzamelt log-informatie van alle aangesloten ICT-systemen, bewaakt de correcte werking daarvan en correleert gebeurtenissen in het netwerk bijv. als gevolg van een hack of een virusinfectie. Indien het SIEM verdachte activiteiten ontdekt in een netwerk, geeft het een alarm. Ook controleert het SIEM of de software van alle systemen actueel is en of de software correct is geconfigureerd.

Elke maand levert het SIEM een rapportage op. [redacted] is nog zoekende naar een juiste vorm van rapportage. Bijgaand een samenvatting van deze rapportage over oktober.

[redacted]
[redacted] heeft in oktober 4 alarmen met laag risico gegenereerd.

[redacted]
In het [redacted] is door het Siem een besmet werkstation gedetecteerd. Het werkstation is uit [redacted] gehaald en overgedragen aan het [redacted] voor forensisch onderzoek. Het resultaat van dit onderzoek is nog niet bekend.

[redacted])
In het [redacted] heeft het SIEM een geïnfecteerd werkstation van een gast gedetecteerd. Dit is [redacted] waarbij de eigenaar verantwoordelijk is voor de [redacted]. Een besmet [redacted] kan andere [redacted] besmetten. Ook heeft het SIEM een [redacted]. Tevens is vanuit dit netwerk een [redacted] met een werkstation buiten de NCTV opgezet.
Deze besmettingen hebben geen andere infecties veroorzaakt.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage november 2016
Programma Integrale Beveiliging

Datum
12 december 2016

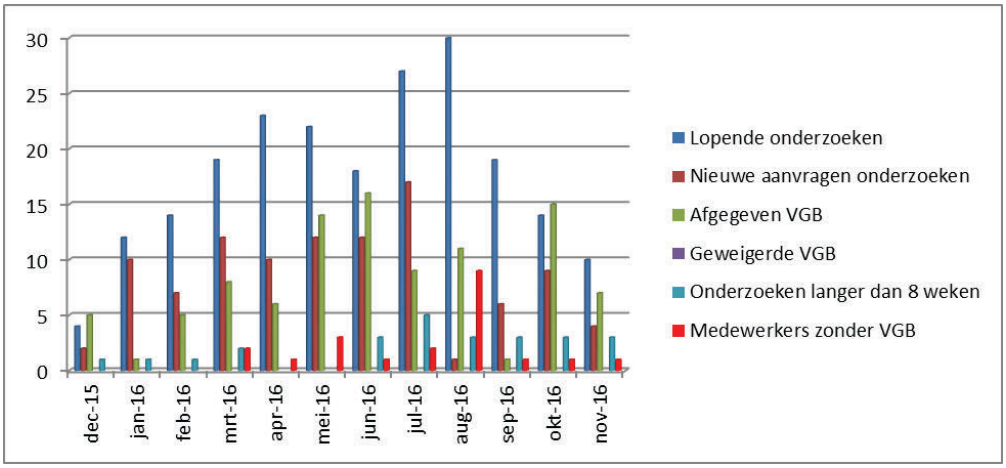
Van

Datum/eindparaaf

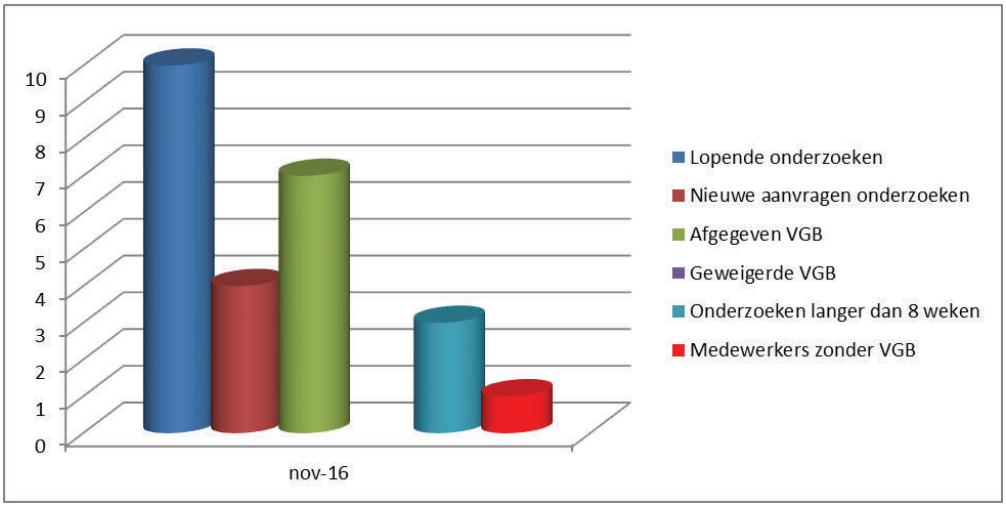
Advies
Ter kennisneming.

Toelichting
Het betreft de rapportage over de maand november.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In november was er één uitzondering op het tijdelijk werken zonder VGB bij de NCTV (



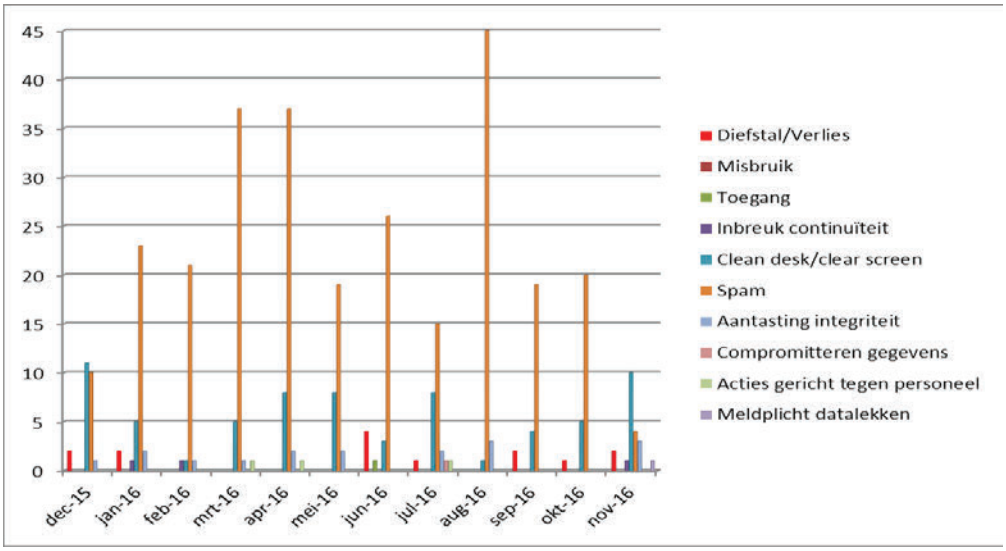
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



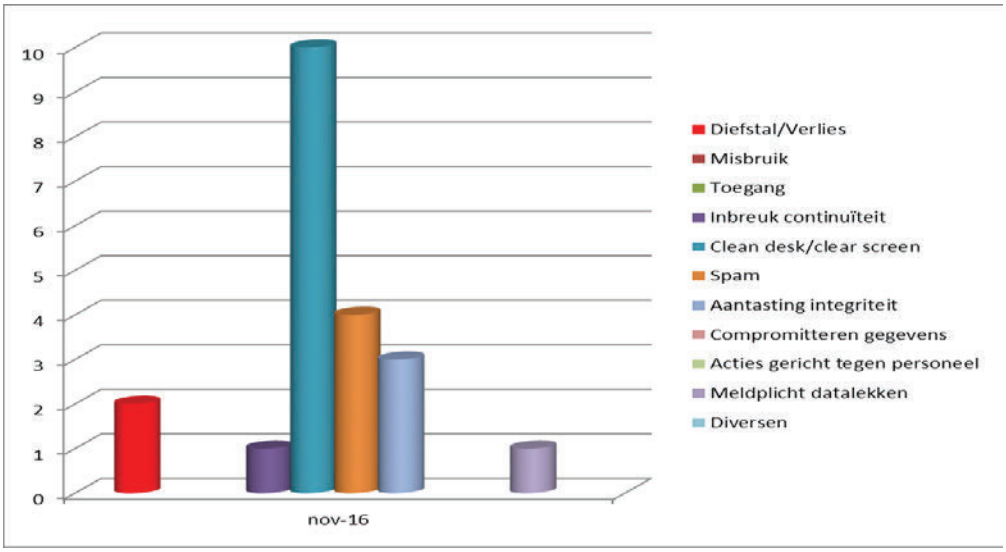
Beeld veiligheidsonderzoeken november

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten november

Toelichting tabellen

Diefstal/verlies

- Twee medewerkers hebben hun smartphone verloren. Er is melding gemaakt en de smartphones zijn op afstand geblokkeerd.

- *Inbreuk continuïteit*
  In november heeft er een DDOS aanval plaatsgevonden op de website van het [redacted]. De website is kort niet bereikbaar geweest. Er zijn tegenmaatregelen getroffen en er is aangifte gedaan van de aanval.

Cleandesk

- De beveiligingsmedewerkers hebben tijdens cleandeskrondes [redacted] onbeheerd aangetroffen op werkplekken [redacted] en veilig gesteld. Op de afdeling [redacted] is een open kluis aangetroffen tijdens de cleandeskronde. De kluis is afgesloten en er is een melding gestuurd naar de leidinggevende.

SPAM/Phising mail

- *Mail.* In november zijn 4 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted].

Aantasting Integriteit

- In november is een beveiligingslek geconstateerd op de applicatie van een nieuwe tool bij [redacted]. Het betrof nog een tool die in ontwikkeling is. De database was niet gevuld. De leverancier heeft het probleem opgelost en er zijn geen data gecompromitteerd.
- Op het [redacted] is een mail geopend door een medewerker met malware. Om verdere besmetting te voorkomen is de PC ontkoppeld en zijn verdere maatregelen getroffen om de malware te verwijderen.

- Op [redacted] hebben we een [redacted] die gebruikt wordt door [redacted] om alle zaken te archiveren en af te handelen. In [redacted] werd vastgesteld dat er dossiers waren verwijderd. Na onderzoek is vastgesteld door wie ze, per ongeluk, waren verwijderd. De leidinggevende heeft een gesprek gehad met de medewerker. Om soortgelijke incidenten voor de toekomst te voorkomen wordt er met de ontwikkelaars van [redacted] gezocht naar een structurele oplossing.

Meldplicht datalekken
Eind november hebben we als NCTV onze eerste datalek gehad. Tijdens een teamuitje heeft men een lijst laten liggen met namen en mailadressen. De Functionaris Gegevensbescherming (FG) VenJ heeft ons opgedragen om melding te maken van het incident bij de AP (Autoriteit Persoonsgegevens). De leidinggevende heeft de medewerkers geïnformeerd. De lijst is waarschijnlijk weggegooid met het afval.

Overige

Autorisatie netwerk VenJ, [redacted]
Eind november zijn de autorisatie overzichten voorgelegd aan de leidinggevenden voor controle. De aanpassingen zijn reeds uitgevoerd.

SIEM
In 2016 heeft [redacted] een Security Information en Event Management (SIEM) tool ingericht op het [redacted] en het [redacted]. Dit SIEM verzamelt log-informatie van alle aangesloten ICT-systemen, bewaakt de correcte werking daarvan en correleert gebeurtenissen in het netwerk bijv. als gevolg van een hack of een virusinfectie.

[redacted]
[redacted] heeft in november geen alarmen gegenereerd.

[redacted]
[redacted] is op een werkstation met succes malware gedetecteerd en verwijderd door de virusscanner.

Gastennetwerk (onderdeel van niet [redacted])
In het gastennetwerk heeft het SIEM [redacted] gedetecteerd met kwetsbare [redacted]. De kwetsbaarheid heeft geen infectie veroorzaakt.
Een andere bevinding is dat vanuit het gasten netwerk een [redacted] verbinding met een werkstation buiten de NCTV is opgezet. Er is nu geen gedragscode waarin beschreven is wat nu wel of niet mag. In het project voor de komst van het nieuwe [redacted] zal meegenomen worden dat een gedragscode opgesteld moet worden voor het gebruik van de diverse netwerken van de NCTV.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage februari 2017
Programma Integrale Beveiliging

Datum
14 maart 2017

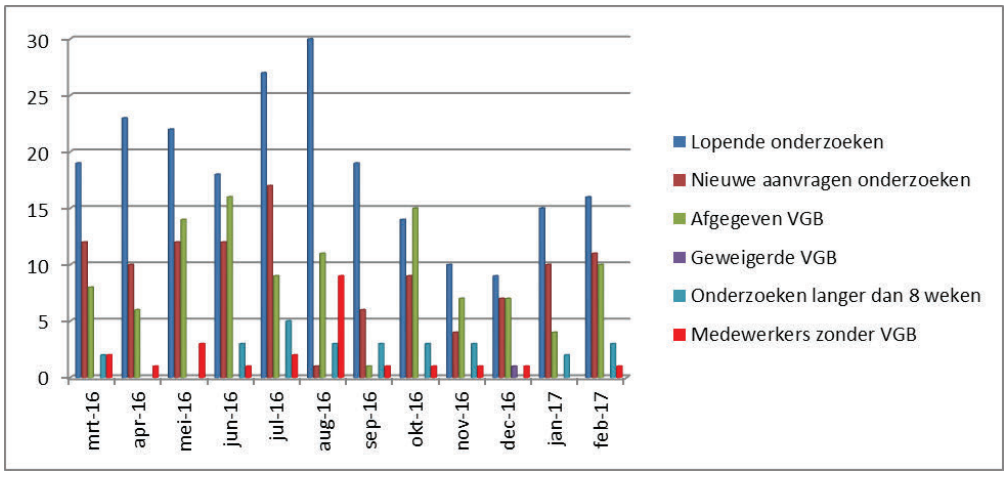
Van

Datum/eindparaaf

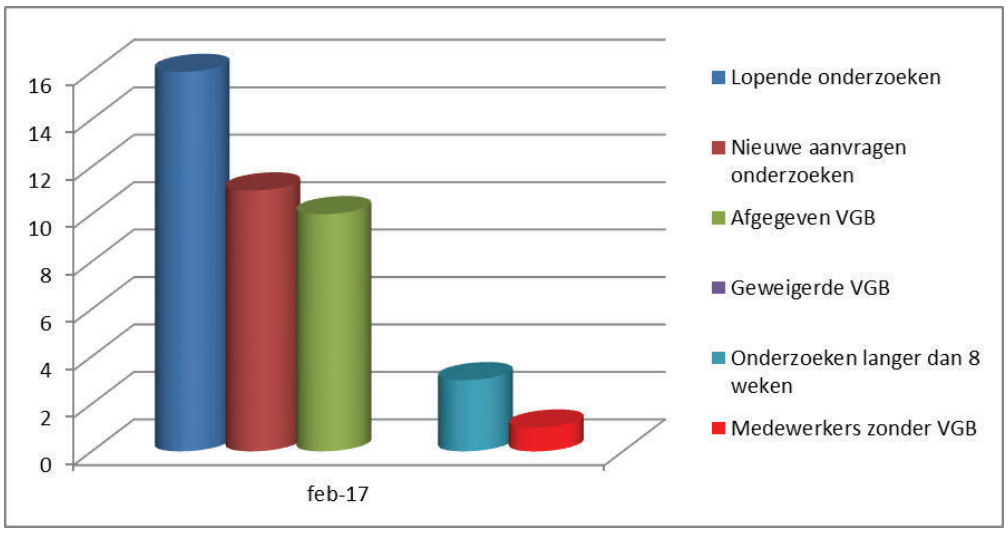
Advies
Ter kennisneming.

Toelichting
Het betreft de rapportage over de maand februari.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In februari was er één uitzondering) op het tijdelijk werken zonder VGB bij de NCTV.



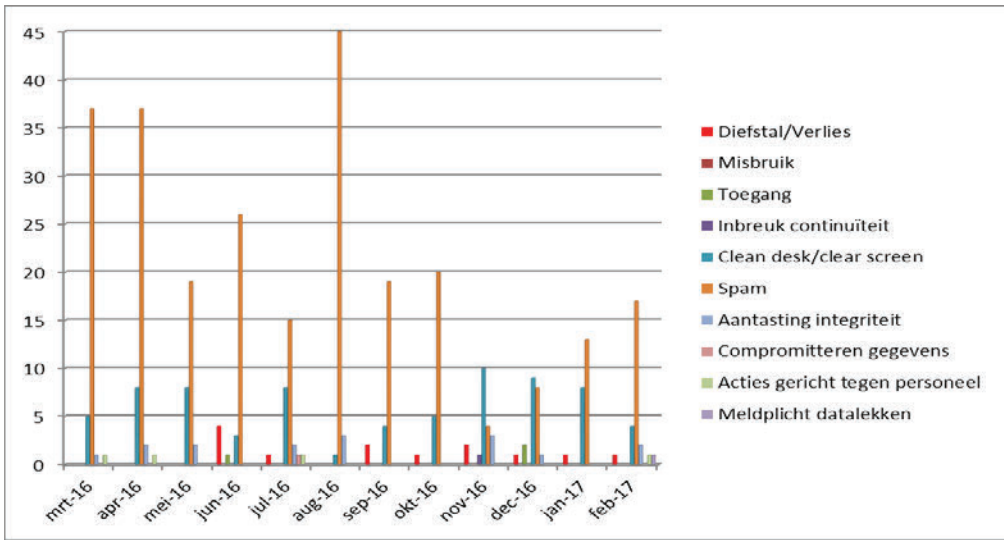
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



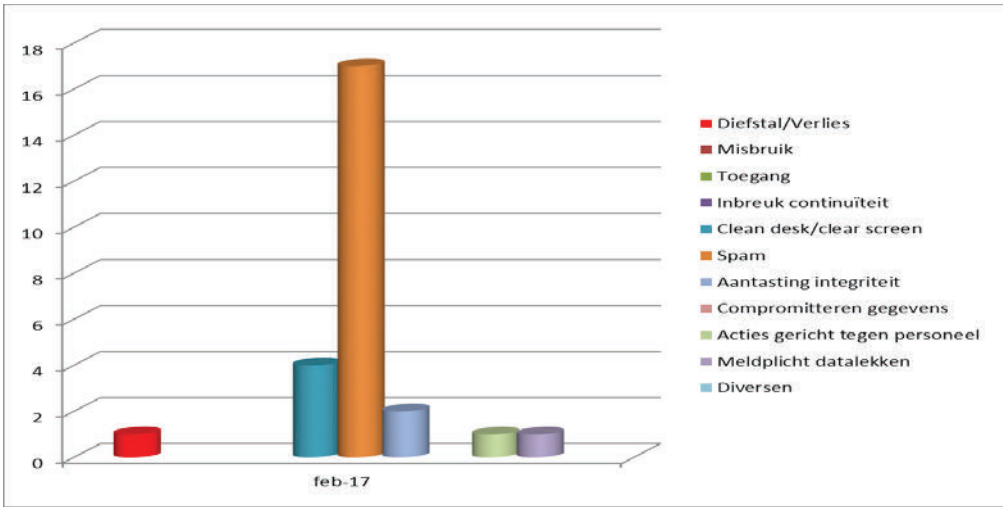
Beeld veiligheidsonderzoeken februari

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen, om herhaling in de toekomst te voorkomen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten februari

Toelichting tabellen

Diefstal/verlies

- Een medewerker heeft een rijkspas verloren. Na de melding is de rijkspas geblokkeerd. Het risico op misbruik is laag omdat de rijkspas alleen binnen de NCTV zone gebruikt kan worden met een handscan.

Cleandesk

- De beveiligingsmedewerkers hebben tijdens cleandeskrondes 4 [redacted] onbeheerd aangetroffen op werkplekken (4x [redacted]) en veilig gesteld.

SPAM/Phising mail

- In februari zijn 17 meldingen van spam en phising mail binnengekomen. Acht meldingen zijn doorgestuurd naar [redacted]. De overige 11 zijn geregistreerd op het [redacted] en door de beheerders afgehandeld. Na een waarschuwing van het [redacted] dat er ransomware in omloop was, hebben drie NCTV-medewerkers gemeld dat ze een e-mail met ransomware hadden ontvangen. De medewerkers hadden de bijlagen met ransomware niet geopend waardoor de ransomware niet is geactiveerd.

Aantasting Integriteit

- Een burger had een bericht ontvangen van het [redacted] over een juridisch onderzoek. Het mailbericht bleek vervalst en niet afkomstig van [redacted]. De burger is geadviseerd aangifte te doen.
- Door een DDOS aanval op de [redacted] bij VenJ was de beschikbaarheid van websites, die bij [redacted] worden gehost, beperkt. Voor de NCTV had dat gevolgen voor [redacted]. De aanval is door het [redacted] en SOC VenJ tijdig gedetecteerd. Er zijn tegenmaatregelen getroffen. De beperkte beschikbaarheid heeft een paar uur geduurd.

Acties gericht tegen personeel

- Een verwarde persoon belde regelmatig met [redacted] en uitte lichte bedreigingen. Onderzoek loopt nog en is bekend bij [redacted].

Meldplicht datalekken
In februari en maart 2017 zijn 3 datalekken opgetreden.

- In februari hadden we een datalek doordat bij de afhandeling van een WOB verzoek vergeten was de persoonsgegevens van medewerkers te verwijderen. De WOB aanvraag was op internet geplaatst met de namen van de medewerkers. Inmiddels zijn de persoonsgegevens verwijderd.
- Begin maart heeft een medewerker een schrift, met
-

In alle gevallen is melding gemaakt bij de AP (Autoriteit Persoonsgegevens) en zijn de betrokken personen ingelicht. Om alle collega's te waarschuwen om zorgvuldig om te gaan met persoonsgegevens is op het intranet NCTV een artikel geplaatst.

Overige

Wijzigingsbeheer
In december 2016 had de NCTV bij het een verzoek gedaan om het patchmanagement bij te verbeteren. De NCTV had vastgesteld dat ernstige kwetsbaarheden vertoonde door verouderde software. Inmiddels hebben toegezegd om verbeteringen door te voeren.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage maart 2017
Programma Integrale Beveiliging

Datum
11 april 2017

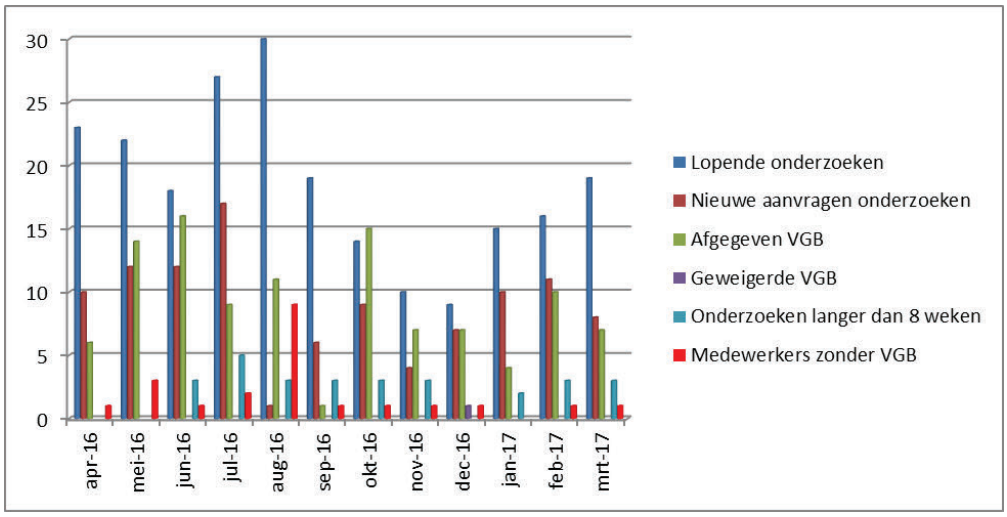
Van

Datum/eindparaaf

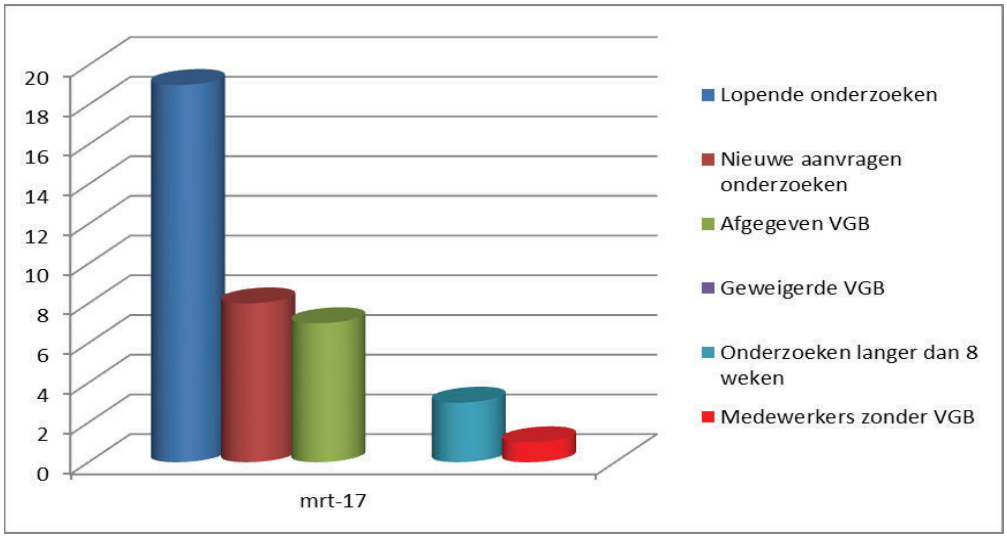
Advies
Ter kennisneming.

Toelichting
Het betreft de rapportage over de maand maart.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In maart was er één uitzondering (bij op het tijdelijk werken zonder VGB bij de NCTV.



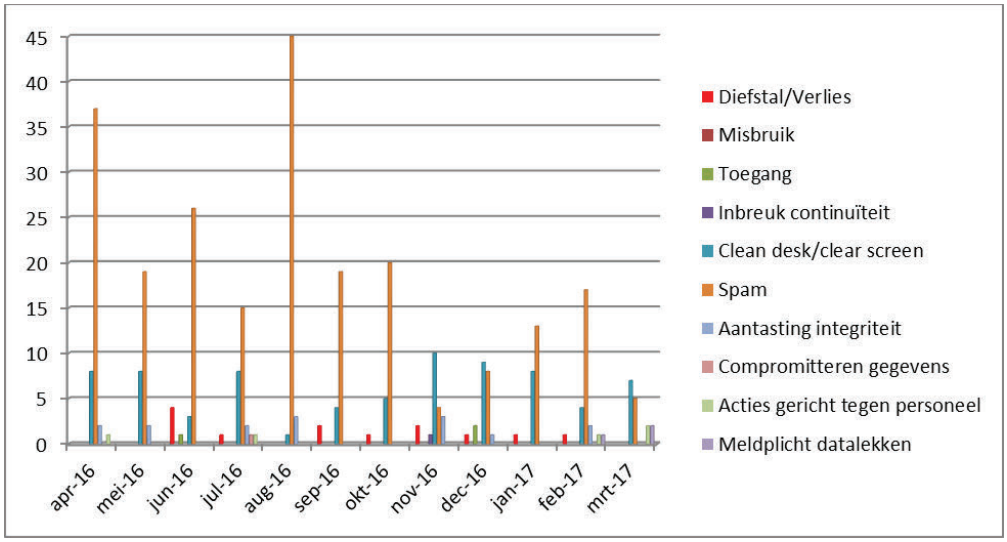
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



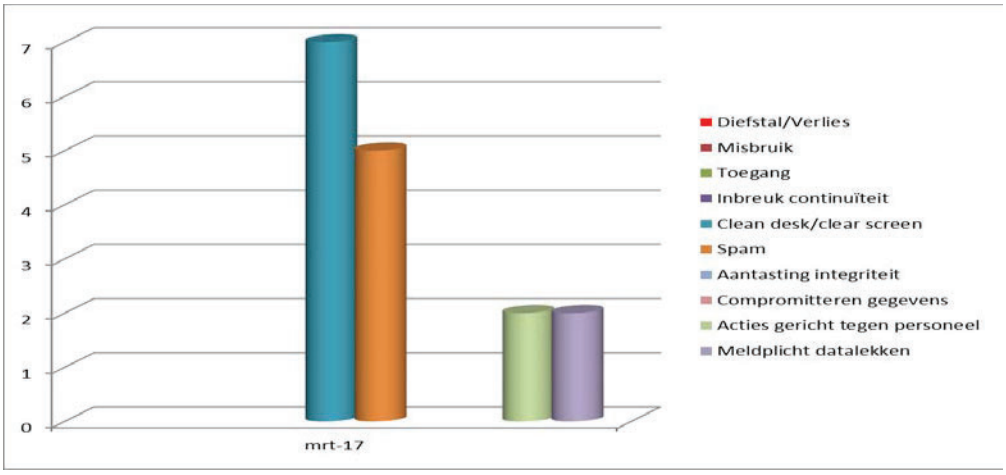
Beeld veiligheidsonderzoeken maart

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen, om herhaling in de toekomst te voorkomen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten maart

Toelichting tabellen

Cleandesk

- *Open kluis.* De beveiligingsmedewerkers hebben tijdens een cleandeskronde een open kluis aangetroffen in een ruimte van . De kluis is afgesloten en de melding is doorgestuurd naar de leidinggevenden om het incident te bespreken met de medewerkers.
- *Stg informatie.* Na een overleg van de afdeling is een document achtergelaten in de vergaderzaal. Dit incident is besproken met de leidinggevenden en de medewerkers.
- *Tokens.* De beveiligingsmedewerkers hebben tijdens cleandeskrondes onbeheerd aangetroffen op werkplekken) en veilig gesteld.

SPAM/Phising mail

- In maart zijn 5 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar .

Acties gericht tegen personeel

- Een had via de mail twee berichten gestuurd aan Er was geen sprake van een directe dreiging. De informatie is doorgestuurd naar .

Meldplicht datalekken

In maart 2017 heeft de NCTV 2 datalekken moeten melden bij de Autoriteit Persoonsgegevens.

- Begin maart heeft een medewerker een schrift, met Staatsgeheime aantekeningen en persoonsgegevens van onze netwerkpartners met organisatienamen, verloren. Het schrift is tot op heden nog niet gevonden.
- Begin maart is een gevonden op een treinstation. De vinder had toegang tot de opgeslagen informatie omdat het wachtwoord op de was geplakt. De bevatte veel persoonsgegevens. De betrokken medewerkers van de NCTV zijn ingelicht. De externe organisaties zijn op de

hoogte gebracht van de persoonsgegeven van hun medewerkers. De afhandeling loopt nog. De vinder is beloond met een cadeaubon.
Om alle collega's te waarschuwen om zorgvuldig om te gaan met persoonsgegevens is op het intranet NCTV een artikel geplaatst (zie: . Tevens is het proces van registratie en uitgifte verbeterd en zijn actieve gebruikers van een gewezen op de mogelijke risico's.

Overige

Autorisatie rijkspassen
In april zijn de autorisaties voor toegang tot de door gecontroleerd en daar waar nodig aangepast.

Kwetsbaarheid
In maart is een kwetsbaarheid gemeld voor het gebruik van De kwetsbaarheid had met name invloed op het Aanvullende maatregelen zijn getroffen en de gebruikers zijn geïnformeerd.

Malware op laptop
Op een laptop die aangesloten was op het was malware gedetecteerd. Deze laptop is uit gehaald en de malware is verwijderd.

Externe laptop aangesloten
Het SIEM (interne detectie applicatie) heeft een externe laptop gedetecteerd op het . Deze laptop is verwijderd omdat op het alleen door de NCTV beheerde laptops mogen worden aangesloten. Externe laptops kunnen worden aangesloten op het gastennetwerk.

Kwetsbare laptops
Het SIEM heeft op 3 werkstations van het gevonden. Deze software is voorzien van een update.

In maart is een kwetsbaarheid gemeld in de . Uit voorzorg is de offline gezet wegens een technische storing. De kwetsbaarheid is verholpen en de is weer online.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage mei en juni 2017
Programma Integrale Beveiliging

Datum
11-07-2017

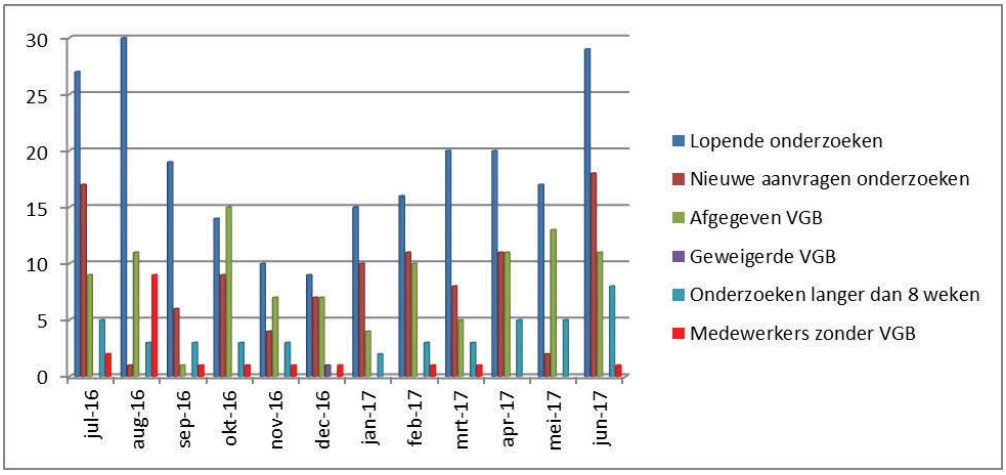
Van

Datum/eindparaaf

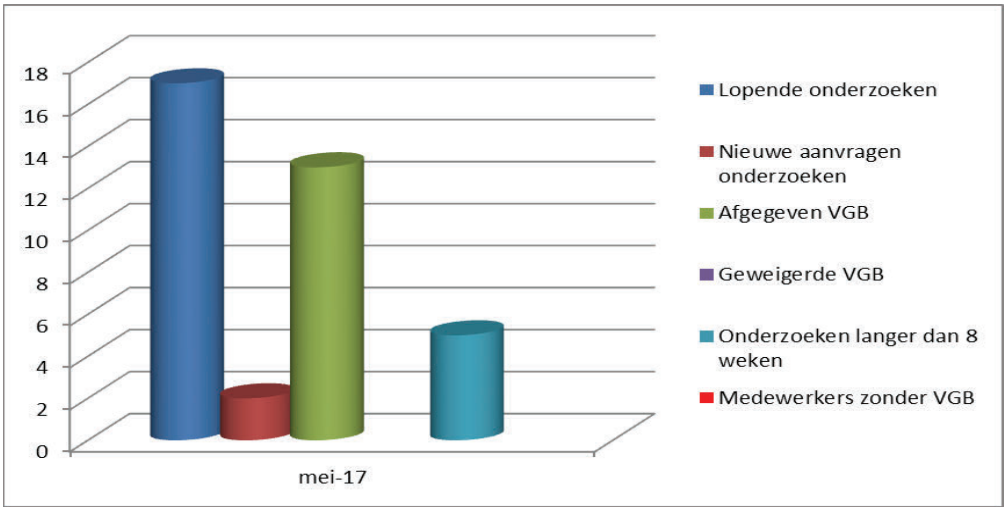
Advies
Ter kennisneming.

Toelichting
Het betreft de rapportages over de maanden mei en juni.

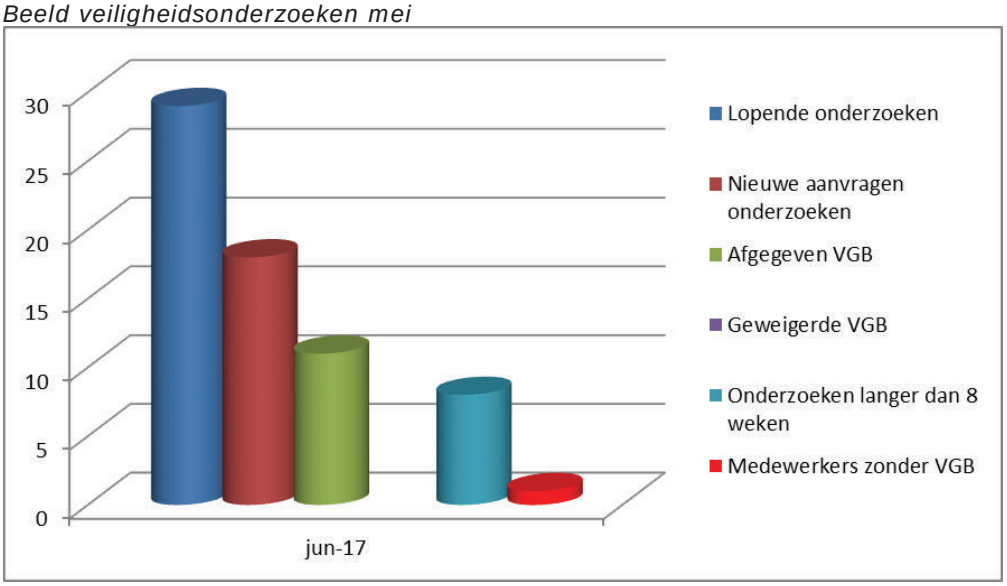
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In mei was er géén uitzondering op het tijdelijk werken zonder VGB en in juni was er 1 uitzondering op het tijdelijk werken zonder VGB bij de NCTV.



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



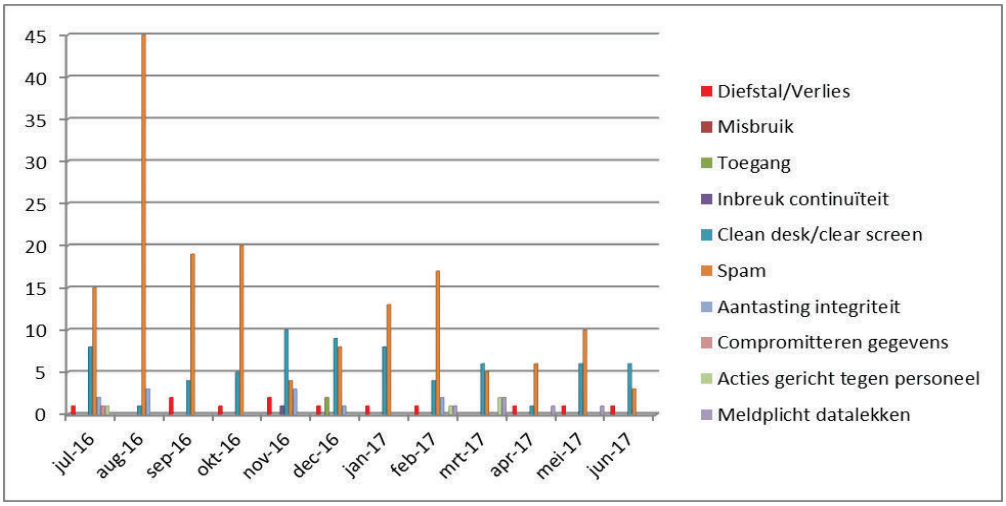
Beeld veiligheidsonderzoeken mei



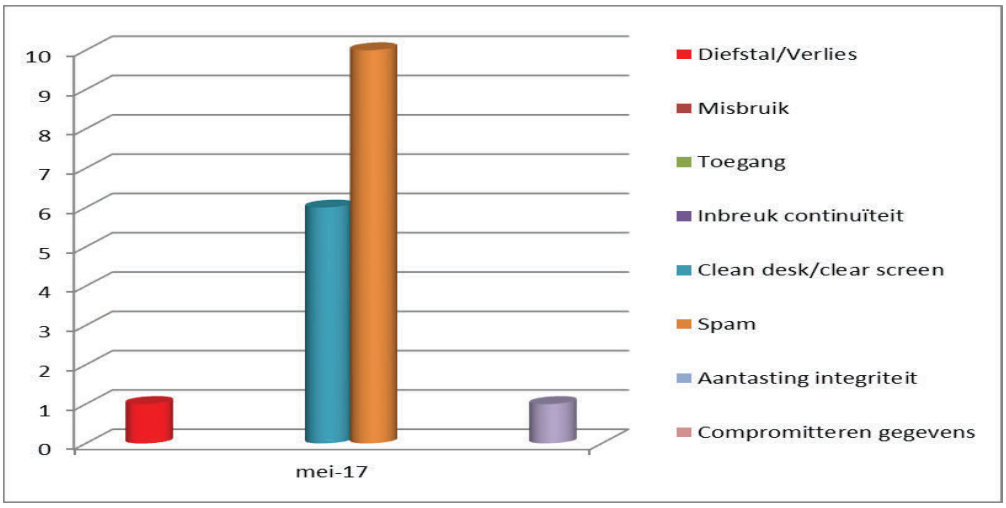
Beeld veiligheidsonderzoeken juni

Incidentenregistratie

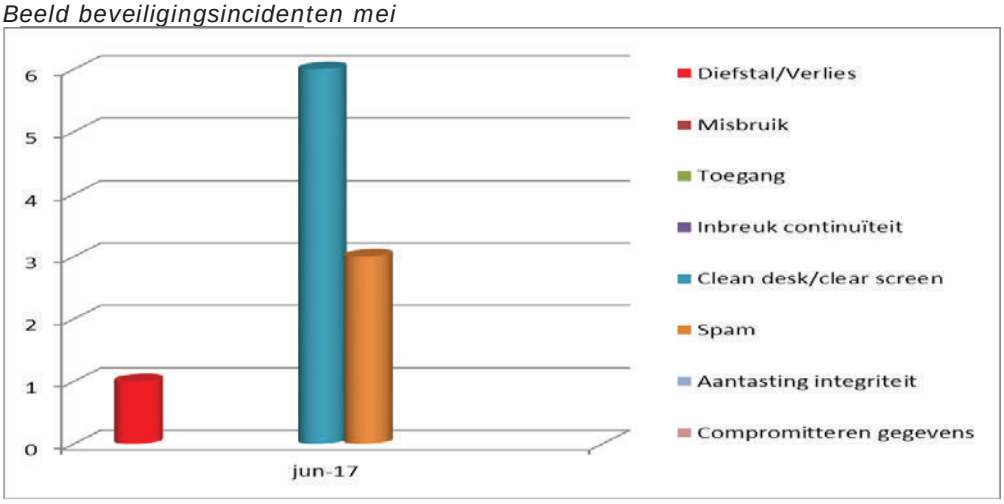
Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt. Het is de verantwoordelijkheid van de lijnmanager om hierop te sturen, om herhaling in de toekomst te voorkomen of extra maatregelen te laten treffen.
Ernstige incidenten worden direct aan de lijnmanager gemeld.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten mei



Beeld beveiligingsincidenten juni

Toelichting tabellen

Diefstal/verlies

- Eén medewerker had zijn [redacted] intern verloren. Het risico op misbruik is laag omdat tevens een wachtwoord is vereist. De [redacted] is na de melding geblokkeerd. Eén medewerker had zijn OV kaart verloren. De kaart is na verlies geblokkeerd om misbruik te voorkomen.

Cleandesk

- [redacted] De beveiligingsmedewerkers hebben tijdens de cleandeskrondes in mei en juni [redacted] onbeheerd aangetroffen op een werkplek ([redacted]) en veilig gesteld.

SPAM/Phising mail

- In mei en juni zijn 13 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] .

Meldplicht datalekken
In mei is er door een secretariaat vanuit de mailbox van de leidinggevende een uitnodiging voor een bijeenkomst verstuurd naar 69 externe personen. Daarbij waren per abuis de geadresseerden voor elkaar zichtbaar. Volgens de meldplicht datalekken is er dan sprake van een incident en is er melding gemaakt bij de Autoriteit Persoonsgegevens. Een aantal ontvangers heeft ook een reactie gestuurd. Het incident is besproken binnen de directie en er is een bericht op intranet geplaatst.

[redacted]

Overige

Veiligheidsbewustzijn
Het [redacted] VenJ is in april gestart met een voorlichtingscampagne over phising-mails. De NCTV doet daar ook aan mee. De medewerkers hebben inmiddels diverse mailberichten ontvangen. Na afloop van de campagne volgt een rapportage.

Integriteit

[redacted]

Digitale kwetsbaarheid
heeft in samenwerking met de een aantal workshops tijdens de afdelingsoverleggen georganiseerd over kwetsbaarheden die zich voor kunnen doen bij de NCTV en haar medewerkers. In deze workshops kwamen ook integriteitsvraagstukken aan de orde.

Siem
De SIEM-systemen (interne detectie applicaties) hebben in mei en juni geen alarmen gedetecteerd op het . De SIEM bij het NCSC voor is vanaf april opgenomen in het regulier, dagelijks beheerproces.

Ransomware
In mei en juni zijn wereldwijd grote ransomware aanvallen uitgevoerd waarbij veel bedrijven zijn getroffen.
Het en het NCSC hebben alle partijen binnen VenJ op de hoogte gehouden van de ontwikkelingen en tevens maatregelen aanbevolen.
Vanuit het zijn enkele maatregelen genomen of gecontroleerd die besmetting en verspreiding van deze Ransomware tegen moeten gaan. Zo worden de Phishing mailtjes met bewuste malware tegengehouden op de centrale mailserver en worden enkele poorten op de interne firewalls geblokkeerd om verspreiding te voorkomen.
Binnen de NCTV is onderzocht of alle systemen voorzien waren van de laatste patches (updates). De medewerkers zijn via de mail en intranet gewaarschuwd. Het Dienstencentrum VenJ heeft ook een bericht verstuurd naar alle medewerkers. De NCTV of haar medewerkers hebben geen schade opgelopen.

Tijdens de conferentie kwamen ‘dreigmails’ van een verwarde persoon binnen. De berichten zijn gedeeld met de politie en de beveiligers van de conferentie.
Aan de balie bij de conferentie meldde zich een persoon (stalker) die in contact wilde komen met de minister Kamp. De persoon is door de beveiligers overgedragen aan de politie en uit het onderzoek bleek dat hij al meerdere pogingen had ondernomen om de minister te benaderen.

Periodieke EU inspectie
De NSA (National Security Authority Netherlands) heeft gecontroleerd of de NCTV, EU en NATO informatie op de juiste wijze verwerkt. De NCTV voldoet aan alle eisen. Aandachtspunt blijft wel op nationaal niveau de wijze van digitale registratie. Vanuit Brussel zijn wel regels opgesteld over de registratie van fysieke documenten maar nog niet over documenten die in de digitale informatiestroom worden verwerkt.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
04-09-2017

nota

Managementrapportage juli en augustus 2017
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

Advies

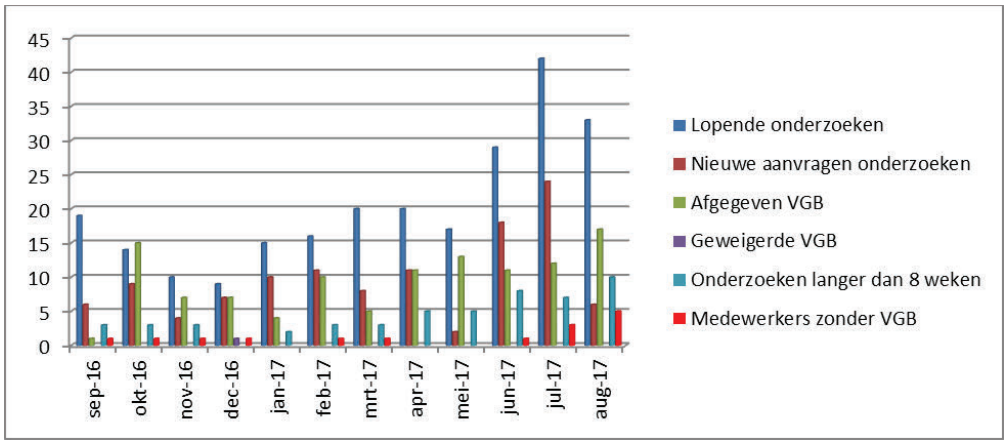
Bespreek tijdens de afdelingsoverleggen het belang van het afsluiten van kluizen met informatie als de medewerkers naar huis gaan. (Er zijn 7 meldingen ([redacted] van niet afgesloten kluizen binnengekomen).

Toelichting

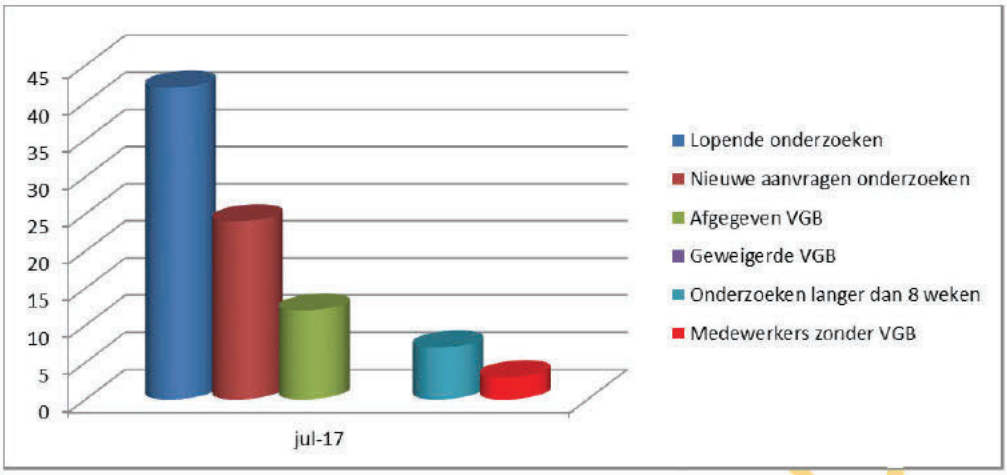
Bijgaand ontvangt u de rapportages over de maanden juli en augustus.

Veiligheidsonderzoeken

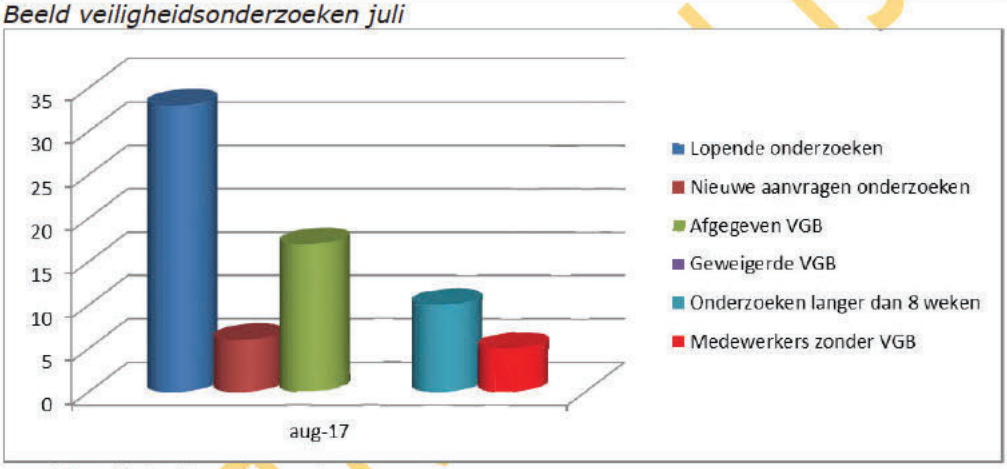
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In juli waren er drie tijdelijke medewerkers aan het werk met een waiver (bij [redacted]) zonder VGB en in augustus waren er 5 tijdelijke medewerkers met een waiver aan het werk(bij [redacted] zonder VGB.



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



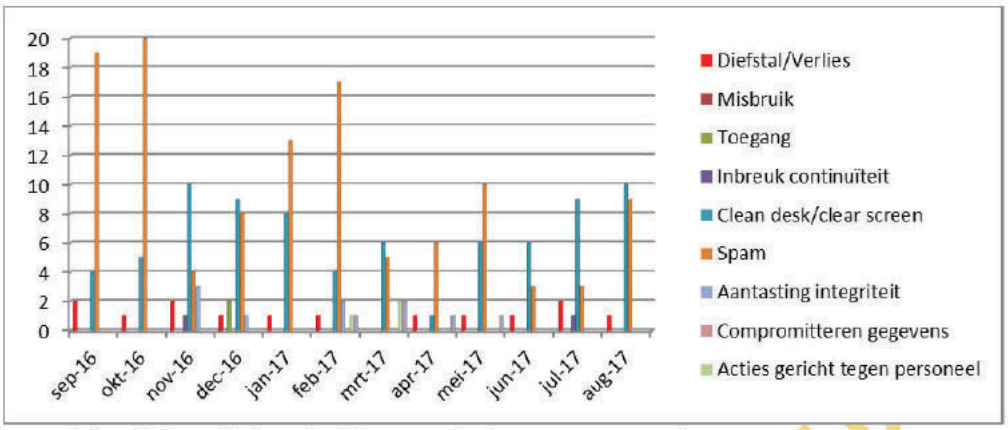
Beeld veiligheidsonderzoeken juli



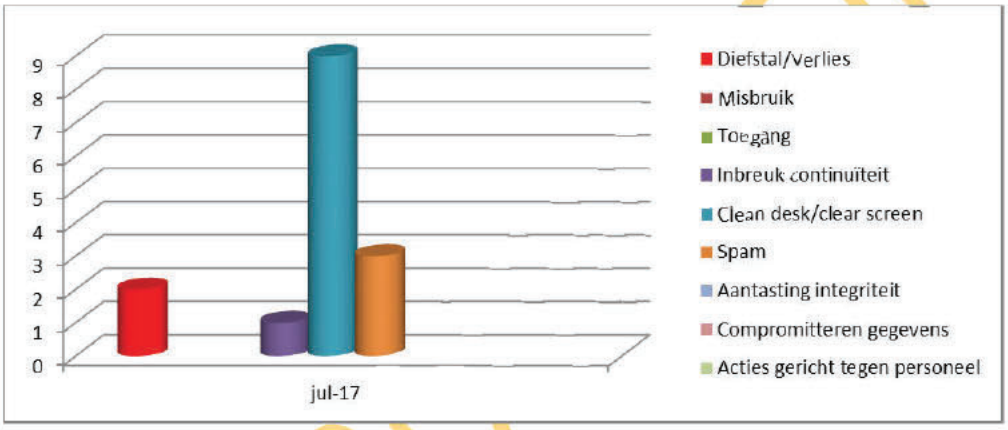
Beeld veiligheidsonderzoeken augustus

Incidentenregistratie

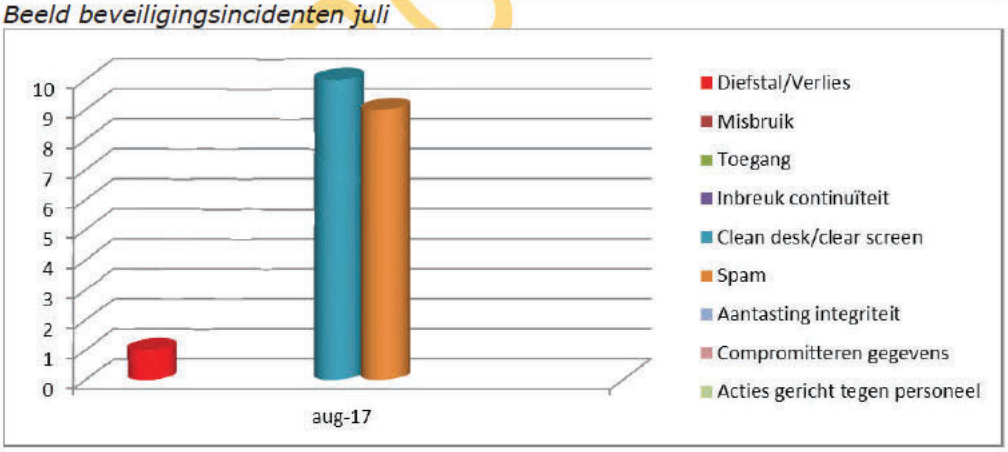
Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten juli



Beeld beveiligingsincidenten augustus

Toelichting tabellen

Diefstal/verlies

- Eén medewerker had zijn Iphone verloren deze is direct op afstand gewist. Eén medewerker had zijn [redacted] intern verloren. Het risico is laag omdat een wachtwoord is vereist. En één medewerker had zijn OV kaart verloren. De OV kaart is geblokkeerd.

Inbreuk continuïteit

- Op 10 juli deed zich een storing voor op de Haagse Ring. Er bleek sprake van een kabelbreuk waardoor het VenJ netwerk niet beschikbaar was. NCTV heeft verzocht om een nader onderzoek omdat de Haagse Ring redundant uitgevoerd zou moeten zijn. Onderzoek loopt nog door het Dienstencentrum.

Cleandesk

- [redacted] De beveiligingsmedewerkers hebben tijdens de cleandeskrondes in juli en augustus 12 [redacted] onbeheerd aangetroffen op een werkplek ([redacted]) en veilig gesteld.
- *Kluizen.* In juli en augustus zijn 7 meldingen ([redacted]) binnengekomen van niet afgesloten kluizen. De kluizen zijn als nog gesloten door de beveiligingsmedewerkers.

SPAM/Phising mail

- In juli en augustus zijn 12 meldingen van spam en phising mail binnengekomen waarvan het 2 meldingen betreffen van spam op de smartphones. De meldingen zijn doorgestuurd naar [redacted]

Meldplicht datalekken

Tijdens een periodieke controle van de [redacted] bleken externe personen gedurende maximaal 3 jaar dezelfde rechten gehad te hebben als [redacted].
Hierdoor konden externe personen mogelijk de lijst met geregistreerde accounts op [redacted] inzien. Deze lijst bevat namen, organisaties, emailadressen en telefoonnummers van de geregistreerde accounts. Het is niet uit te sluiten dat mensen deze lijst ook daadwerkelijk bekeken hebben.
Hier is wel sprake van een datalek maar zijn we niet melding plichtig naar de Autoriteit Persoonsgegevens (AP). Er is namelijk geen aanzienlijke kans op ernstige nadelige gevolgen voor de persoonsgegevens. Het betreft een beperkte groep die elkaar al kent. De impact is laag.
De procedure voor het aanmaken van accounts is aangepast en de rechten zijn gecorrigeerd.

Overige

AVG

Begin juni is [redacted] gestart als tijdelijke [redacted] om de AVG (Algemene Verordening Gegevensbescherming) bij de NCTV in te voeren. [redacted] zal gesprekken voeren met de leidinggevenden om de verwerking van persoonsgegevens in werkprocessen in kaart te brengen. De informatie van de leidinggevenden is essentieel om de werkprocessen door te lichten op privacy zaken en aan te passen. Tevens is de informatie van belang voor het inrichten van het documentmanagement, het inrichten van de archieffunctie in [redacted] en

[redacted] project. In mei 2018 moet de NCTV voldoen aan de nieuwe wetgeving ten aanzien van de AVG en moet er een voorstel liggen hoe de functie van privacy officer geborgd zal worden binnen de NCTV.
[redacted] is ook de contactpersoon voor het verplicht uitvoeren van een Privacy Impact Analyse (PIA) voor nieuwe informatievoorzieningen waarin persoonsgegevens worden verwerkt. In juli is de PIA uitgevoerd op het [redacted].

RD-meldingen
Eind juli zijn 2 responsible disclosure meldingen ontvangen. De NCTV krijgt 60 dagen de tijd om een gemelde kwetsbaarheid te verhelpen, indien dat niet gebeurt heeft de melder het recht om deze kwetsbaarheid te publiceren (zie https://www.ncsc.nl/incident-response/responsible-disclosure-melding.html).

[redacted]
Van deze site kan het wachtwoord achterhaald worden. Tot op heden is deze kwetsbaarheid nog niet verholpen.

[redacted]
Door een verkeerde configuratie van enkele pagina's had gevoelige informatie gelekt kunnen worden. Deze kwetsbaarheid is op 16 augustus verholpen.

Audit ICV BIR 2016
Op 21 augustus heeft de ADR in het kader van de goedkeuring van de jaarrekening een audit uitgevoerd op de ICV BIR 2016 (In Control Verklaring Baseline Informatiebeveiliging Rijksdienst) van de NCTV.
Er zijn geen tekortkomingen geconstateerd door de ADR.

Pentesten websites NCTV
In augustus heeft de ADR de rapportages opgeleverd van de pentesten op NCTV.nl en cybersecurityraad.nl.
Er zijn geen kwetsbaarheden met een hoog risico geconstateerd. Wel doet de ADR enkele aanbevelingen om de beveiliging van deze websites te verbeteren. De betreffende website eigenaar is verantwoordelijk voor opvolging van deze aanbevelingen.

Siem
De SIEM-systemen (interne detectie applicaties) hebben in juli en augustus geen alarmen gedetecteerd op het [redacted].

Ontruimingsoefening (BHV)
Op 13 juli heeft een ontruimingsoefening plaatsgevonden. De oefening is goed verlopen. De medewerkers zijn allen (en ook individueel) geïnformeerd over de aandachtspunten via intranet.

Mailboxen
Uit een onderzoek van [redacted] was gebleken dat bij een aantal functionele postbussen in Outlook de machtiging-instellingen niet goed stonden. Hierdoor waren deze functionele postbussen ook toegankelijk voor niet-geautoriseerden.
[redacted] De laatste is opgeheven en bij de andere twee zijn de instellingen aangepast waardoor de kwetsbaarheid is weggenomen.

Stafafdeling
Bedrijfsvoering

Datum
4-9-2017

De [redacted] is een applicatie die met name door [redacted] wordt gebruikt op het internet. De NCTV was gewezen op het feit dat de database met abonneegegevens was gehackt. Medewerkers die gebruik maken van de applicatie zijn gewezen op de risico's, wachtwoorden en userid's zijn aangepast.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage september 2017
Programma Integrale Beveiliging

Datum
10-10-2017

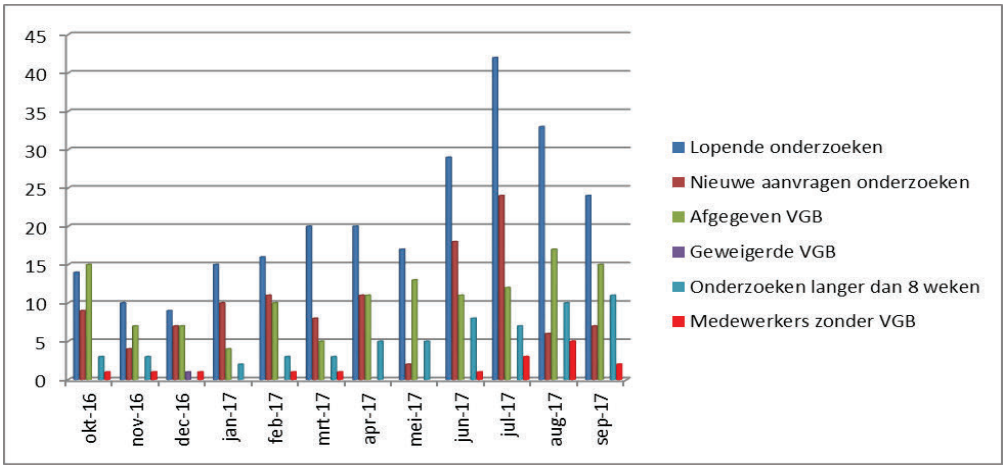
Van

Datum/eindparaaf

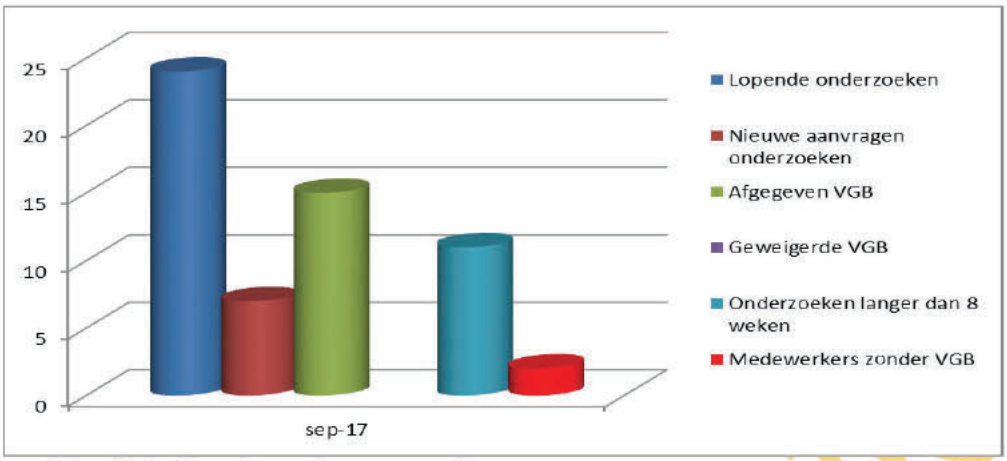
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand september.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In september waren er twee tijdelijke medewerkers aan het werk met een waiver ( ) zonder VGB.



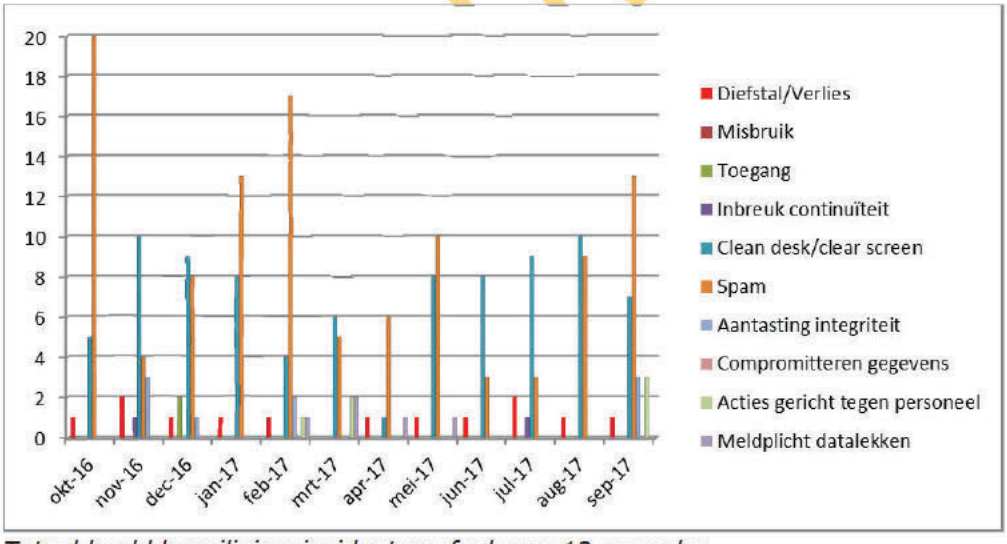
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



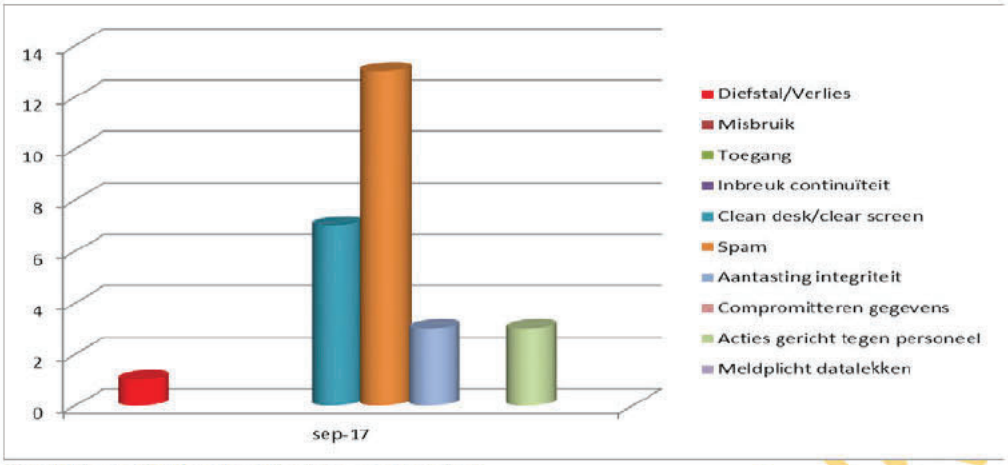
Beeld veiligheidsonderzoeken september

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten september

Toelichting tabellen

Diefstal/verlies

- Eén medewerker had zijn [redacted] verloren deze is direct geblokkeerd. Het risico is laag omdat toegang tot de NCTV zone nodig is voor gebruik.

Cleandesk

- In september is driemaal een kluissleutel veiliggesteld door de beveiligingsmedewerkers bij de directie [redacted] op de [redacted].
  Bij [redacted] zijn eenmaal gerubriceerde stukken, na sluitingstijd, op het bureau gevonden. Deze zijn door de beveiligingsmedewerkers meegenomen en opgeborgen in de kluis.
  De beveiligingsmedewerkers hebben tijdens de cleandeskrondes tweemaal [redacted] onbeheerd aangetroffen op een werkplek bij [redacted] en veilig gesteld.
  Opvallend is dat we nog steeds documenten vinden in prullenbakken in plaats van dat ze versnipperd worden. In de week van de veiligheid zal hier meer aandacht aan geschonken worden.

SPAM/Phising mail

- In september zijn 13 meldingen van spam en phising mail binnengekomen waarvan het 7 meldingen betreffen van spam op de smartphones. De meldingen zijn doorgestuurd naar [redacted] Daarnaast was er een phising-mail ontvangen van [redacted]. Deze is gemeld bij de contactpersoon van [redacted].

Aantasting integriteit

- In september zijn er twee meldingen geweest over het feit dat de beheerder [redacted] de [redacted] van personen die uit dienst waren, niet had verwijderd. De meldingen zijn doorgestuurd naar [redacted]. Er loopt een verbetertraject waar de NCTV ook bij betrokken is. Dit zal daar ook in meegenomen worden.

Overige

RD-meldingen
In september is een [redacted] ontvangen van het [redacted]. Er blijkt een kwetsbaarheid te bestaan voor de [redacted]. De NCTV heeft melding gedaan bij [redacted] en bij de leverancier. [redacted] heeft de maatregel ingevoerd dat sloten niet meer weggegooid mogen worden.
[redacted] meldingen voor de k[redacted] zijn binnen de gestelde tijd afgehandeld.

Autorisatie rijkspassen
In september zijn de autorisaties voor toegang tot de [redacted] door [redacted] gecontroleerd en daar waar nodig aangepast.

Autorisatie netwerk VenJ
Eind september zijn de autorisatie overzichten voorgelegd aan de leidinggevenden voor controle. De aanpassingen zijn reeds uitgevoerd.

Siem
De SIEM-systemen (interne detectie applicaties) hebben in juli en augustus geen alarmen gedetecteerd op het [redacted].

Pentesten websites NCTV
De ADR heeft de rapportages van de pentesten van de volgende domeinen opgeleverd:
[redacted]

Beide websites bevatten geen kwetsbaarheden met risico hoog. [redacted]
De betreffende systeemeigenaren zijn op de hoogte gesteld van de bevindingen van de ADR en zij worden geacht te bezien of de risico's aanvaardbaar zijn of dat mitigerende maatregelen moeten worden getroffen.

Het team [redacted] gepentest. De website van [redacted] bevat geen kwetsbaarheden met hoog of midden risico's.

Inbreuk continuïteit
Op 10 juli deed zich een storing voor [redacted]. Nader onderzoek heeft uitgewezen dat er sprake was van gepland onderhoud maar dat dat niet was gemeld aan alle gebruikers. [redacted] is geïnformeerd. Het Dienstencentrum en [redacted] hebben beterschap beloofd.

Stafafdeling
Bedrijfsvoering

Datum
10-10-2017

Week van de veiligheid
Uit recente rapportages, zoals de KWAS, blijkt dat het veiligheidsbewustzijn bij de NCTV continu aandacht vergt, daarom willen we het veilig werken weer eens onder de aandacht te brengen. Tevens is vanuit het MT het verzoek gekomen om meer aandacht aan veiligheidsbewustzijn te besteden. [redacted] de werkgroep beveiliging van 6 tot 9 november de 'Week van de veiligheid' met als motto: 'samen maken we het veilig'.

De week van het veilig werken kent elke dag een ander thema. Per thema worden managers en/of medewerkers voorzien van informatie. Leidinggevenden wordt gevraagd hun medewerkers te stimuleren om hier aandacht aan te schenken. De week wordt afgesloten met een veiligheidsmarkt met als doel om het de medewerkers gemakkelijker te maken veilig te werken.

De volgende thema's staan op het programma
- Leidinggevenden overleg 30 oktober aandacht vragen voor het onderwerp veiligheid.
- Maandag 6 november: clean desk.
- Dinsdag 7 november: privacy (AVG).
- Woensdag 8 november: hoe om te gaan met gerubriceerde informatie.
- Donderdag 9 november: veiligheidsmarkt op [redacted] met factsheets en informatie voor veilig werken.
- Op intranet zullen ook artikelen geplaatst worden.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
06-11-2017

nota

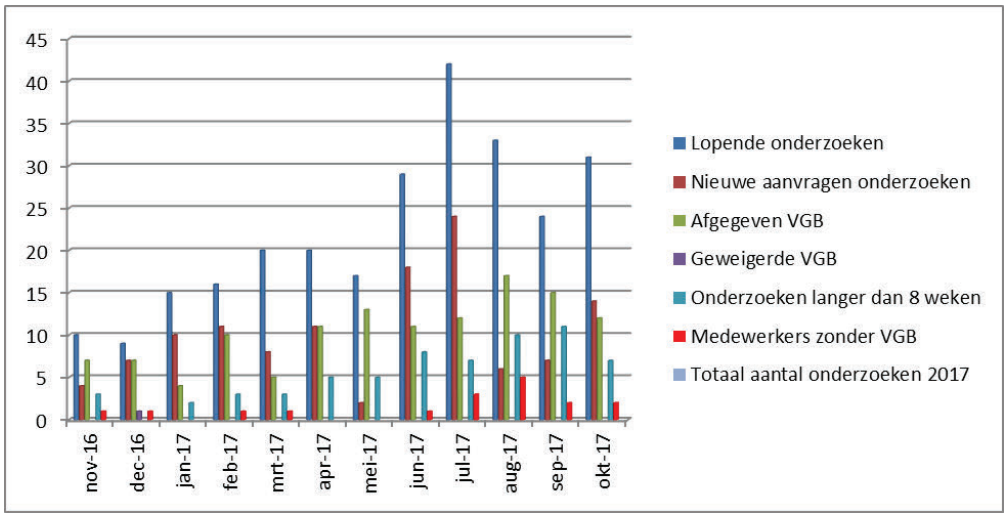
Managementrapportage oktober 2017
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

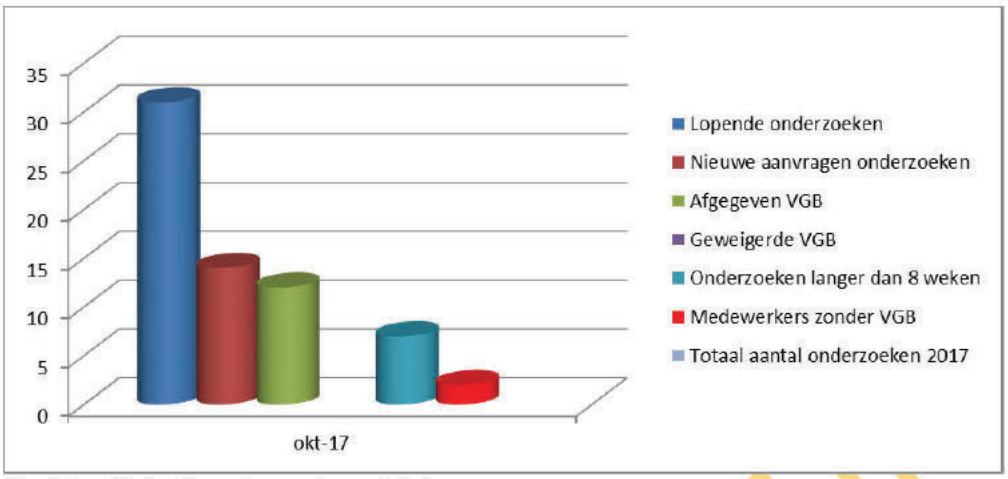
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand oktober.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In oktober waren er twee tijdelijke medewerkers aan het werk met een waiver [redacted] zonder VGB.



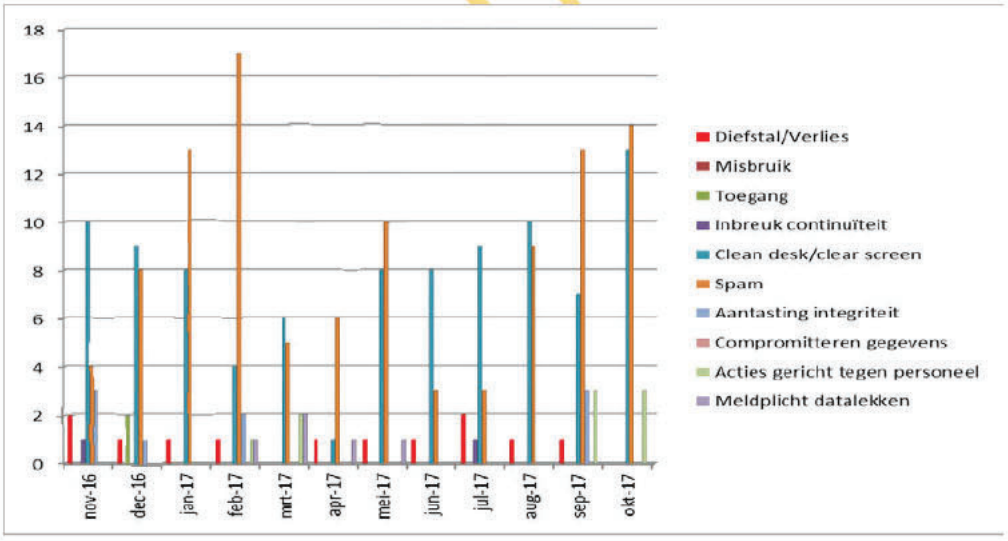
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



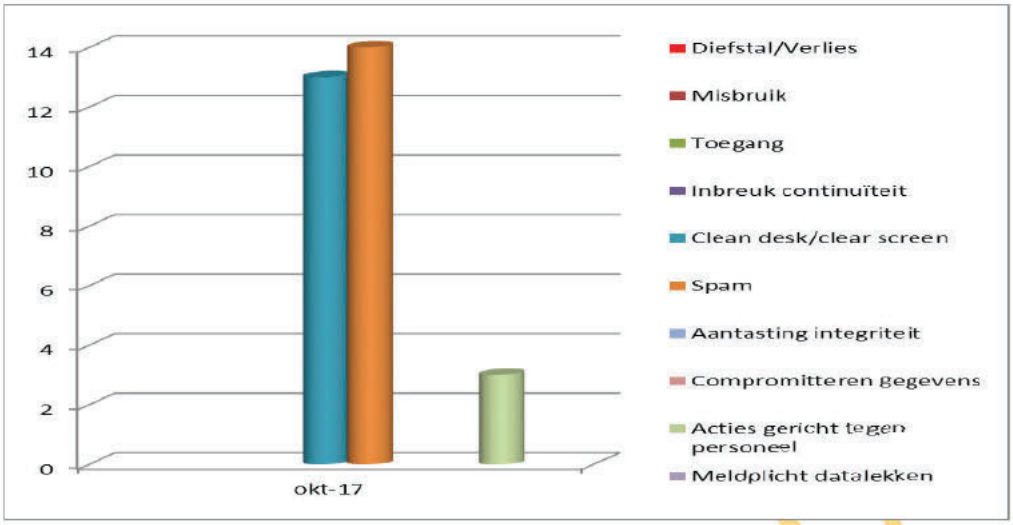
Beeld veiligheidsonderzoeken oktober

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten wordt een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten oktober

Toelichting tabellen

Cleandesk

- In oktober is driemaal een kluissleutel veiliggesteld door de beveiligingsmedewerkers bij de [redacted] De kluizen zaten wel vergrendeld met de pincode.
  Op een kopieerapparaat had een medewerker zijn paspoort achtergelaten. Deze is veiliggesteld en in de kluis opgeborgen.
  De beveiligingsmedewerkers hebben tijdens de cleandeskrondes [redacted] onbeheerd aangetroffen op een werkplek (bij [redacted]) en veilig gesteld.
  Opvallend is dat we nog steeds documenten vinden in prullenbakken in plaats van dat ze versnipperd worden. In de week van de veiligheid zal hier meer aandacht aan geschonken worden.

SPAM/Phising mail

- In oktober zijn 14 meldingen van spam en phising mail binnengekomen waarvan het 1 melding betrof van spam op de smartphones. De meldingen zijn doorgestuurd naar [redacted]

Acties gericht tegen personeel

- In oktober zijn er drie meldingen geweest van berichten van [redacted] die een bericht hadden gestuurd naar de [redacted]. [redacted].

Overige

RD-meldingen

Er is een melding binnengekomen dat er een tekortkoming bestaat in het [redacted]. Dit protocol was op dit moment het veiligste protocol waarmee een [redacted] kon worden opgezet. Deze kwetsbaarheid heeft de naam [redacted] meegekregen. Omdat de kwetsbaarheid in het protocol zit, zijn waarschijnlijk alle systemen die de [redacted] standaard gebruiken kwetsbaar.

De medewerkers bij [redacted] maken gebruik van [redacted]) en kunnen gebruik maken van [redacted] Na overleg met de leverancier is gebleken dat er een extra beveiligde verbinding wordt opgezet [redacted]. Hierdoor is het risico laag dat misbruik wordt gemaakt van de verbinding. Medewerkers zijn gewezen op de kwetsbaarheid.

Ook [redacted] heeft een RD-melding ontvangen over het ontbreken van [redacted] Dit issue was bekend bij de NCTV en er worden acties ondernomen om dit issue op te lossen. Men verwacht dat deze werkzaamheden voor het eind van het jaar zijn afgerond.

Siem
De SIEM-systemen (Security Incidente & Event Management systeem waarmee security incidenten gedetecteerd worden) hebben in oktober geen alarmen gedetecteerd op het [redacted].

Pentesten [redacted]
In oktober is door DJI een pentest uitgevoerd op [redacted] De meeste kwetsbaarheden zijn verholpen. De eigenaar is geïnformeerd.

Verlies [redacted]
Vorige maand had een medewerker een melding gemaakt van het verlies van een [redacted]. Nu is gebleken dat de 'onrechtmatige eigenaar' de kaart vóór blokkering heeft gebruikt om een fiets te 'lenen'. De kosten van de fiets worden door [redacted] verhaald op de NCTV.

'e-mail spoofing'
Deze maand is er veel aandacht geweest voor het al veel langer bekende fenomeen 'e-mail spoofing'. Spoofing gebeurt als iemand een e-mail verstuurt op naam van iemand anders. Onderzoekers hebben laten zien hoe mensen mail kunnen versturen die afkomstig lijkt te zijn [redacted] Ook blijken andere domeinen kwetsbaar te zijn voor dergelijke misbruik, z[redacted] l. Een medewerker van de NCTV heeft een soortgelijk bericht ontvangen [redacted] werd gebruikt en de persoon zich voor deed als medewerker van een ambassade.
Ook het e-mail-domein [redacted] is kwetsbaar voor dit type spoofing. Daarom is een wijzigingsverzoek naar [redacted] gestuurd om de daarvoor noodzakelijke wijzigingen door te laten voeren.

Herhaalonderzoeken
Tot voor kort werden herhaalonderzoeken alleen uitgevoerd als er sprake was van een wijziging in de persoonlijke levenssfeer of een wijziging van functie, feiten of omstandigheden die een verzoek rechtvaardigen. In juni 2017 heeft de Bestuursraad, mede gezien de veranderingen in de maatschappij, besloten dat herhaalonderzoeken iedere 5 jaar zullen plaatsvinden na de datum van afgifte van de laatste VGB (Verklaring van Geen Bezwaar). De SG ziet toe op een tijdig uitvoering van het besluit. In samenspraak met de betrokken leidinggevenden zijn we per 1 november gestart met de uitvoering van de herhaalonderzoeken. Het verloop zal zichtbaar gemaakt worden met een grafiek in de maandrapportage. Op dit moment zijn er 152 medewerkers die een VGB ouder hebben dan 5 jaar.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

nota

Managementrapportage november 2017
Programma Integrale Beveiliging

Datum
07-12-2017

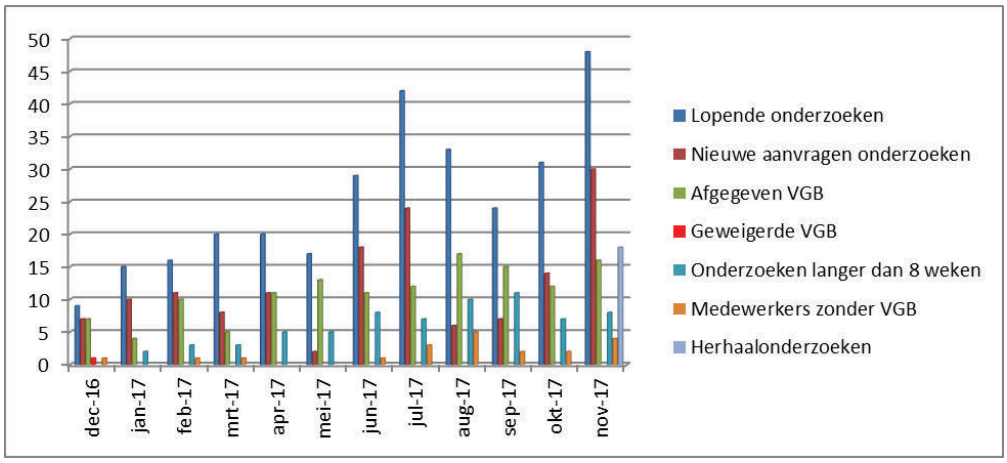
Van

Datum/eindparaaf

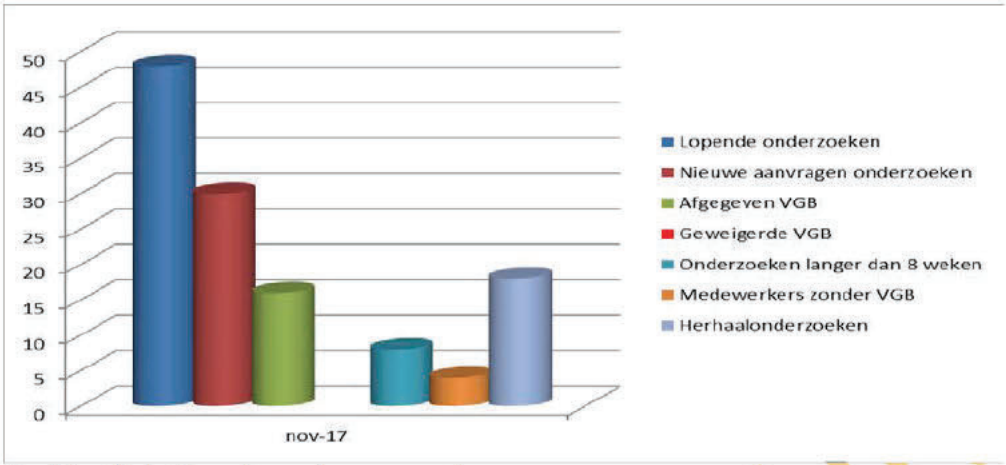
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand november.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In november waren er vier tijdelijke medewerkers aan het werk met een waiver (bij) zonder VGB.



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



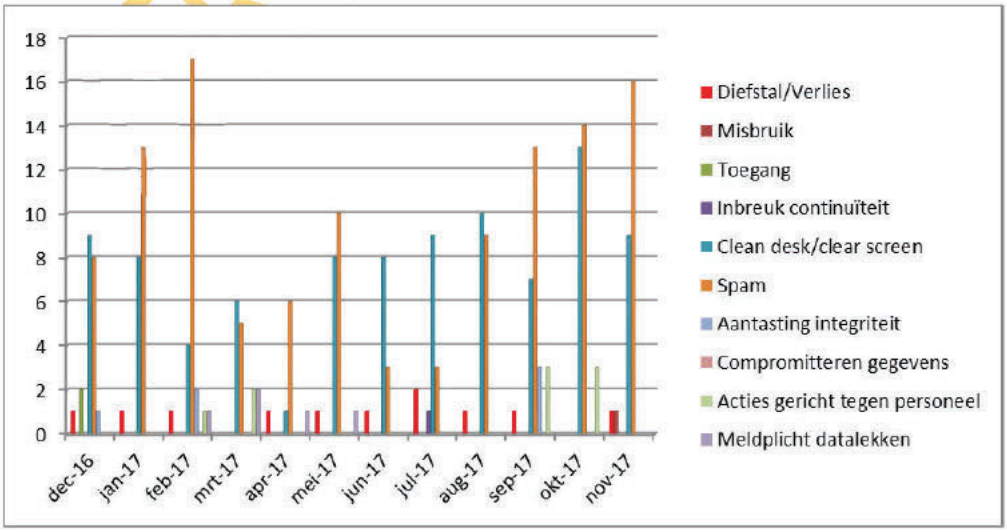
Beeld veiligheidsonderzoeken november

Herhaalonderzoeken

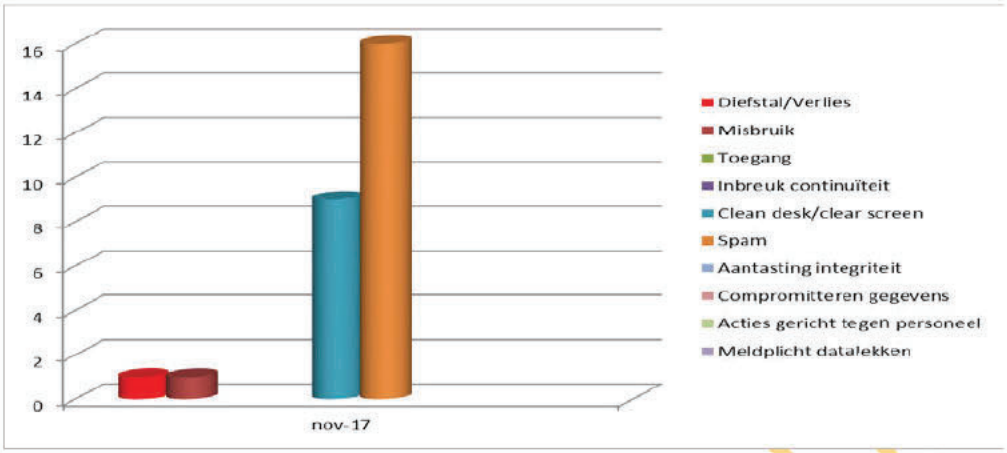
Deze maand is gestart met herhaalonderzoeken. Er zijn nu binnen de NCTV 126 medewerkers werkzaam met een VGB ouder dan 5 jaar. [redacted] heeft een voorstel uitgewerkt om de herhaalonderzoeken uit te voeren. In overleg met de leidinggevenden worden medewerkers gevraagd om een aanvraag voor een nieuwe veiligheidsonderzoek in te dienen voor de huidige functie. In november 2017 zijn er 18 aanvragen ingediend. Binnen 5 jaar verwachten we dat iedere medewerker beschikt over een VGB niet ouder dan 5 jaar.

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten november

Toelichting tabellen

Diefstal/verlies
- Een medewerker heeft de mobiliteitskaart verloren. Na de melding is de kaart direct geblokkeerd.

Misbruik
- Een medewerker ( ) had zijn rijkspas uitgeleend aan een andere medewerker omdat die nog geen rijkspas had. Beiden zijn aangesproken door op hun gedrag.

Cleandesk
- In november is tweemaal een kluissleutel veiliggesteld door de beveiligingsmedewerkers bij de directie De kluizen zaten wel vergrendeld met de pincode.
  De beveiligingsmedewerkers hebben tijdens de cleandeskrondes 6 onbeheerd aangetroffen op een werkplek (bij en veilig gesteld.

SPAM/Phising mail
- In november zijn 16 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar

Overige

Week van de veiligheid
Van 6 tot 9 november is de week van de veiligheid georganiseerd.
In die week is aandacht gevraagd voor de volgende thema's:
- clean desk
- privacy
- omgaan met gerubriceerde informatie

Deze week is afgesloten met een veiligheidsmarkt .

SIEM
De SIEM-systemen (Security Incidente & Event Management systeem waarmee security incidenten gedetecteerd worden) hebben in november de volgende meldingen gegenereerd.

In het is één werkstation mogelijk besmet geraakt met malware. Dit werkstation is tijdelijk van het netwerk verwijderd en zal opnieuw van software worden voorzien (het werkstation wordt opnieuw ingespoeld).
Verder blijkt dat er in de maand november 2 besmette werkstations op het zijn aangesloten. De gebruikers zijn geïnformeerd.

Op het zijn geen SIEM alarmen opgetreden in de maand november.
Niet alle systemen in het zijn voorzien van de laatste software updates of een nieuwe virusscanner omdat de werkstations niet altijd zijn ingeschakeld. Dit geeft voor ICT als aandachtspunt om de werkstations via aan te zetten om software updates te kunnen installeren en ten aanzien van beheer om nog een aantal werkstations te voorzien van de nieuwe virusscanner. Hier is geen sprake van een groot risico omdat de werkstations niet verbonden zijn met het internet.

De beschikbaarheid van de was 100% in de maand november.

Pentesten websites NCTV
Voor de website crisis.nl ontbrak nog een actueel goedgekeurd certificaat. In november is die geïnstalleerd waardoor de website nu voldoet aan alle actuele eisen.

De ADR heeft nog een aantal onvolkomenheden ontdekt bij de website, . De webbeheerder heeft de onvolkomenheden nog niet opgelost.

Responsible Disclosure meldingen
In november is een RD (Responsible Disclosure) melding ontvangen over een kwetsbaarheid op de website . De kwetsbaarheid is inmiddels opgelost.
Tevens is een RD-melding ontvangen over een . Deze melding is in behandeling bij

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
5 februari 2018

Ons kenmerk
123456

nota

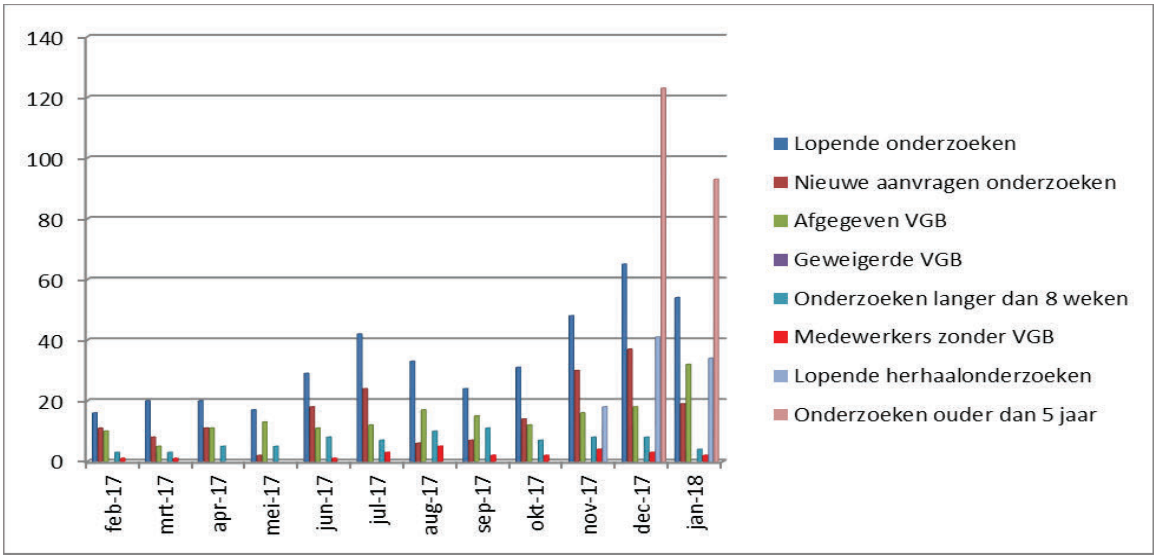
Managementrapportage januari 2018
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

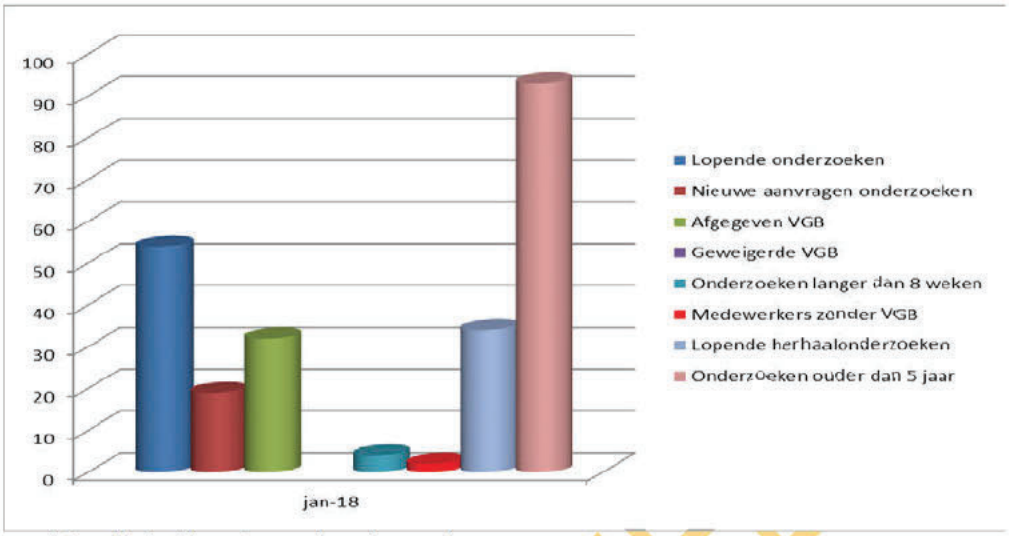
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand januari.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In januari waren er twee tijdelijke medewerkers aan het werk met een waiver [redacted]) zonder VGB.
Er zijn nu binnen de NCTV 93 medewerkers werkzaam met een VGB ouder dan 5 jaar. In januari zijn er 13 herhaalonderzoeken aangevraagd. De NCTV ligt hier mee op koers voor het behalen van de beoogde doelstellingen van de SG JenV.



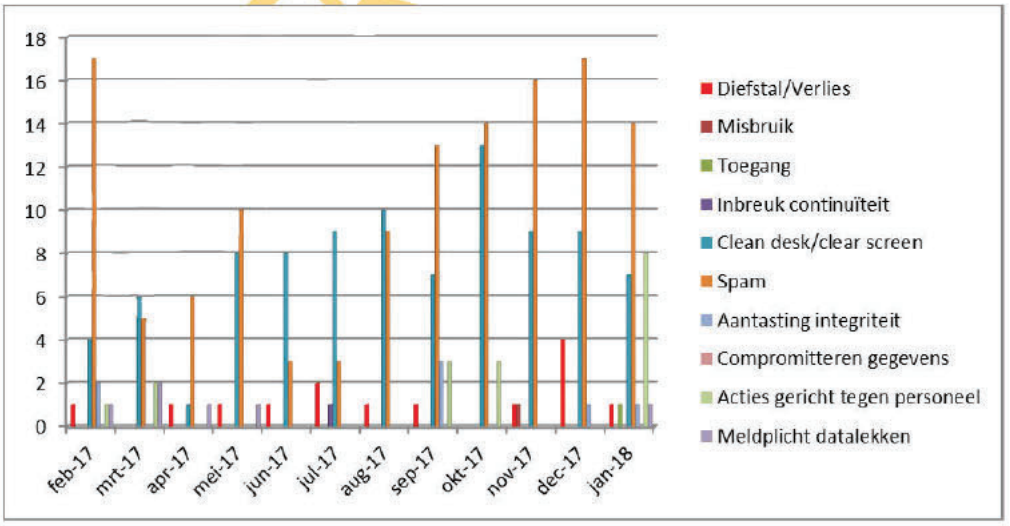
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



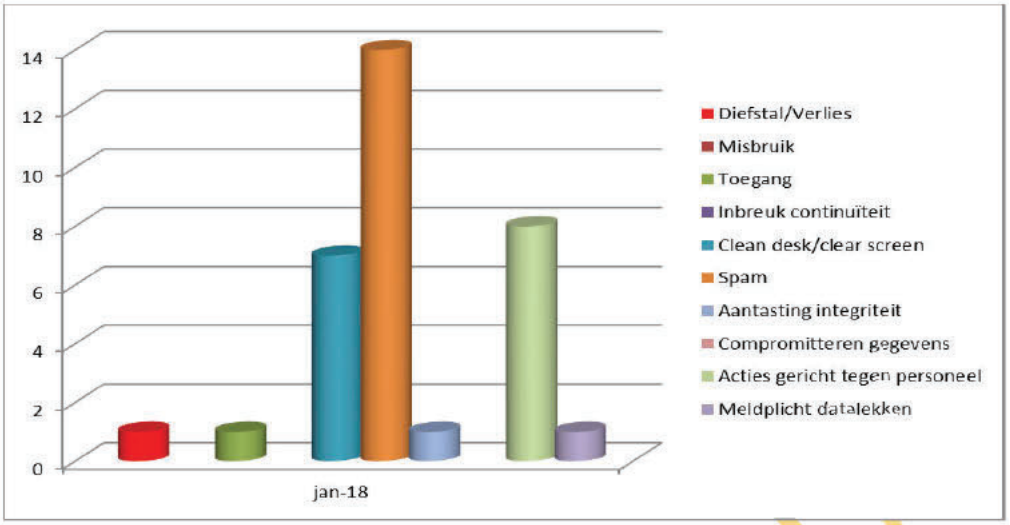
Beeld veiligheidsonderzoeken januari

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten januari

Toelichting tabellen

Diefstal/verlies
- Een medewerker heeft zijn smartphone verloren. Na de melding is de smartphone op afstand gewist.

Toegang
- Een medewerker heeft per ongeluk een verkeerde [redacted] verzonden. Na de melding is het proces aangepast om herhaling te voorkomen.

Cleandesk
- In januari driemaal een kluissleutel veiliggesteld door de beveiligingsmedewerkers bij de directie [redacted]). De kluizen zaten wel vergrendeld [redacted].
  De beveiligingsmedewerkers hebben tijdens de cleandeskrondes [redacted] onbeheerd aangetroffen op een werkplek ([redacted] en veilig gesteld.

SPAM/Phising mail
- In januari zijn 14 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Aantasting Integriteit
- Op een [redacted] PC is mogelijk malware ontdekt. Het onderzoek loopt nog. De PC wordt voorlopig niet meer gebruikt.

Acties gericht tegen medewerkers
- Er zijn een 8-tal mailberichten binnengekomen bij de NCTV en pNCTV waarin onder andere wantoestanden bij de overheid worden gemeld. De berichten lijken afkomstig van [redacted] en zijn toegevoegd aan de dossiers [redacted].

Meldplicht Datalekken

- In de openbare rapportage van min JenV over integriteitsmeldingen 2017 aan de Tweede Kamer worden de namen van de vertrouwenspersonen [redacted] en organisaties genoemd zonder dat ze daar mee hadden ingestemd. De zaak is besproken met de betreffende personen.

Overige

Meltdown en Spectre
Begin januari werden kwetsbaarheden gemeld over chips die zich bevinden in o.a. computers, smartphones, laptops en servers. (MELTDOWN en SPECTRE). Deze kwetsbaarheden hebben ook grote gevolgen voor zakelijke systemen.
Het Security Operation Centre (SOC) JenV en de NCSC hebben de situatie gemonitord en waar nodig adviezen gegeven. Bedrijfsvoering heeft er op toegezien dat de patches, die beschikbaar kwamen, snel werden geïmplementeerd op onze eigen netwerken.

DDOS-aanvallen
Eind januari deden zich meerdere DDOS-aanvallen voor op diverse instellingen. Bedrijfsvoering heeft de berichtgeving en opvolgingen nauwlettend gevolgd. Er hebben zich op onze netwerken en websites geen bijzondere situaties voorgedaan.

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hebben in januari de volgende meldingen gegenereerd.

[redacted]
In het [redacted] is één werkstation mogelijk besmet geraakt met malware. Dit werkstation is tijdelijk van het netwerk verwijderd en zal opnieuw van software worden voorzien (het werkstation wordt opnieuw ingespoeld).
De verschillende netwerken binnen [redacted] zijn zodanig geconfigureerd dat een besmetting van een werkstation op het netwerk niet kan leiden tot een besmetting van de andere werkstations op [redacted].

[redacted] zijn geen SIEM alarmen opgetreden in de maand januari.
Niet alle systemen in het [redacted] zijn voorzien van de laatste software updates of een nieuwe virusscanner omdat de werkstations niet altijd zijn ingeschakeld. Dit geeft voor ICT als aandachtspunt om de werkstations [redacted] aan te zetten om software updates te kunnen installeren en ten aanzien van beheer om nog een aantal werkstations ([redacted]) te voorzien van de nieuwe virusscanner. Hier is geen sprake van een groot risico omdat de werkstations niet verbonden zijn met het internet.

De beschikbaarheid van de kritieke informatiesystemen [redacted] was 99,9 % in de maand januari.

Stafafdeling
Bedrijfsvoering

Datum
7-12-2017

Pentesten websites NCTV
Voor het portaal 'Informatievoorziening capaciteitsmanagement' (IVCM) is een pentest uitgevoerd in januari. De aangetroffen kwetsbaarheden zijn gemeld aan de eigenaar en de hosting partij met het verzoek deze nog op te lossen voordat het portaal beschikbaar is.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~Dep. VERTROUWELIJK~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon

Datum
12 maart 2018

Ons kenmerk
123456

nota

Managementrapportage februari 2018
Programma Integrale Beveiliging

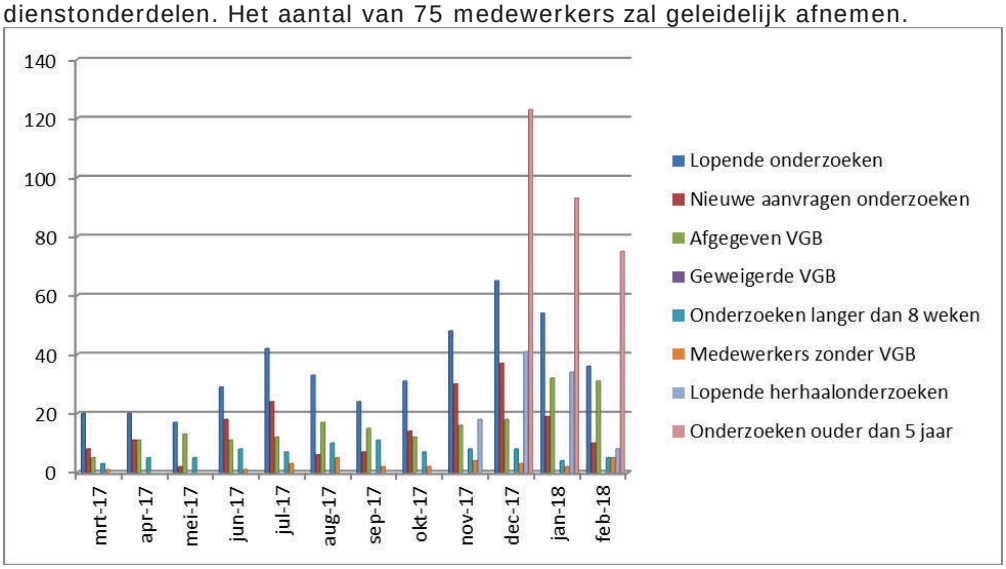
Van

Datum/eindparaaf

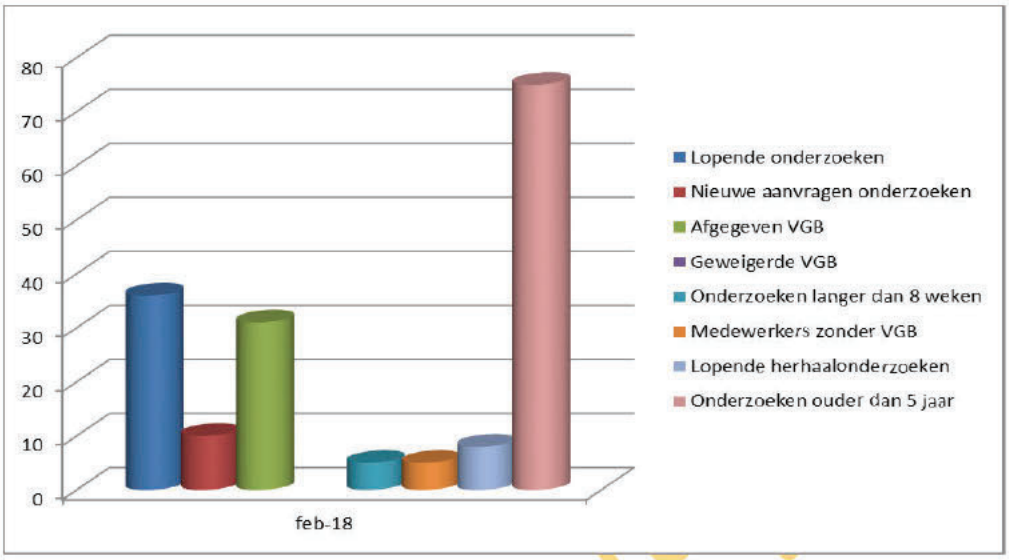
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand februari.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In februari waren er vijf tijdelijke medewerkers aan het werk met een waiver (bij) zonder VGB.
Er zijn nu binnen de NCTV 75 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 75 medewerkers zal geleidelijk afnemen.



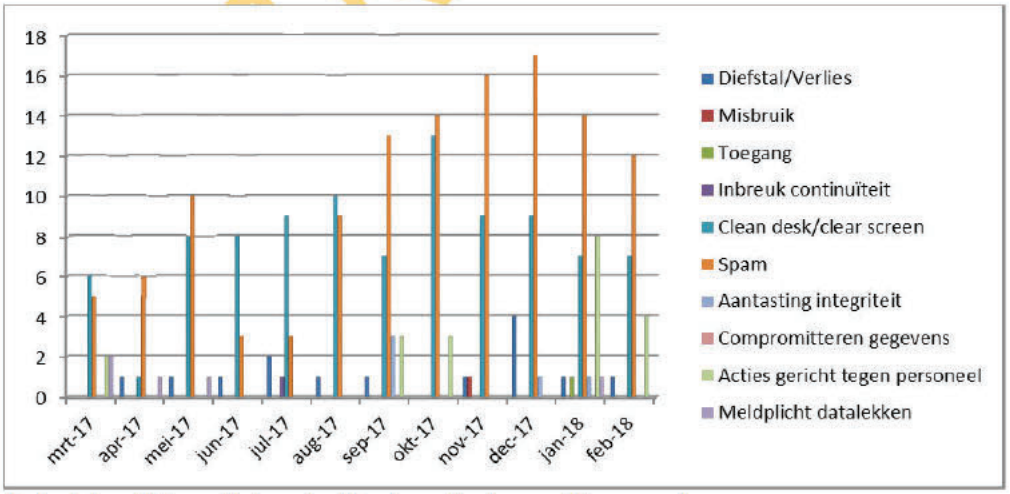
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



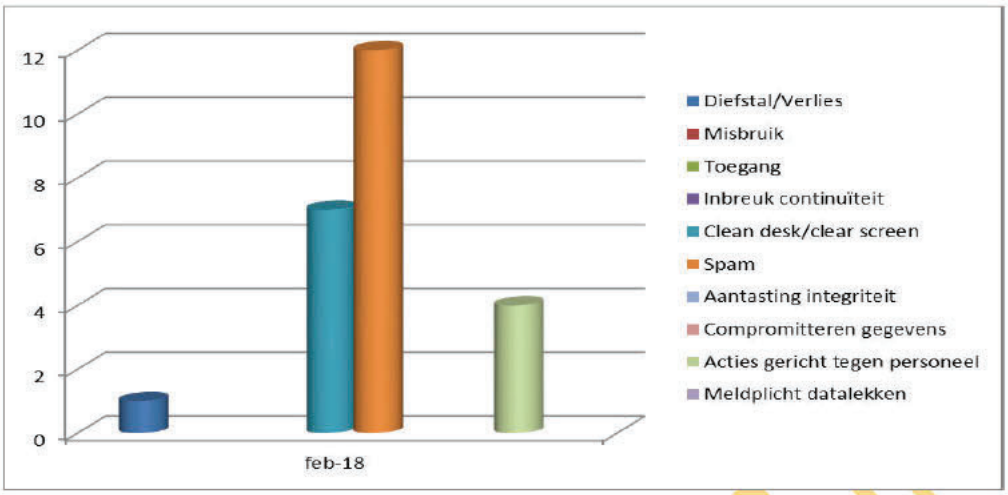
Beeld veiligheidsonderzoeken februari

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten februari

Toelichting tabellen

Diefstal/verlies

- Een medewerker heeft zijn OV kaart verloren. Na de melding is de OV kaart geblokkeerd.

Cleandesk

- In februari is driemaal een kluissleutel veiliggesteld door de beveiligingsmedewerkers bij de directie [redacted] x). De kluizen zaten wel vergrendeld met [redacted].
  De beveiligingsmedewerkers hebben tijdens de cleandeskrondes 4 [redacted] onbeheerd aangetroffen op een werkplek ([redacted]) en veilig gesteld.

SPAM/Phising mail

- In februari zijn 12 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] Twee meldingen betroffen telefoontjes van [redacted] om fouten in het systeem op te lossen. De medewerkers hebben de gesprekken afgebroken.

Acties gericht tegen medewerkers

- Er zijn een 4-tal mailberichten binnengekomen bij de [redacted] waarin onder andere wantoestanden bij de overheid worden gemeld. De berichten lijken afkomstig van [redacted] en zijn toegevoegd aan de dossiers [redacted].

Overige

Stg Documenten

Tijdens een overleg met externe partners zijn Stg documenten gedeeld met de aanwezigen. Per abuis zijn de documenten mee gegeven aan de aanwezigen. De documenten bevatten [redacted] en mochten niet meegegeven worden omdat de personen geen

screening hadden en geen middelen om het veilig op te bergen. Tevens waren de documenten niet voorzien van [redacted]. De documenten zijn teruggehaald en vernietigd. Het incident is besproken met [redacted] en binnen de afdeling is het proces besproken in het kader van de verhoging van het veiligheidsbewustzijn.

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hebben in februari de volgende meldingen gegenereerd.

[redacted]
Er hebben zich geen bijzondere meldingen voor gedaan op het [redacted] de afgelopen maand.

De beschikbaarheid van de kritieke informatiesystemen [redacted] was 99,9 % in de maand januari.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
12 april 2018

Ons kenmerk
123456

nota

Managementrapportage maart 2018
Programma Integrale Beveiliging

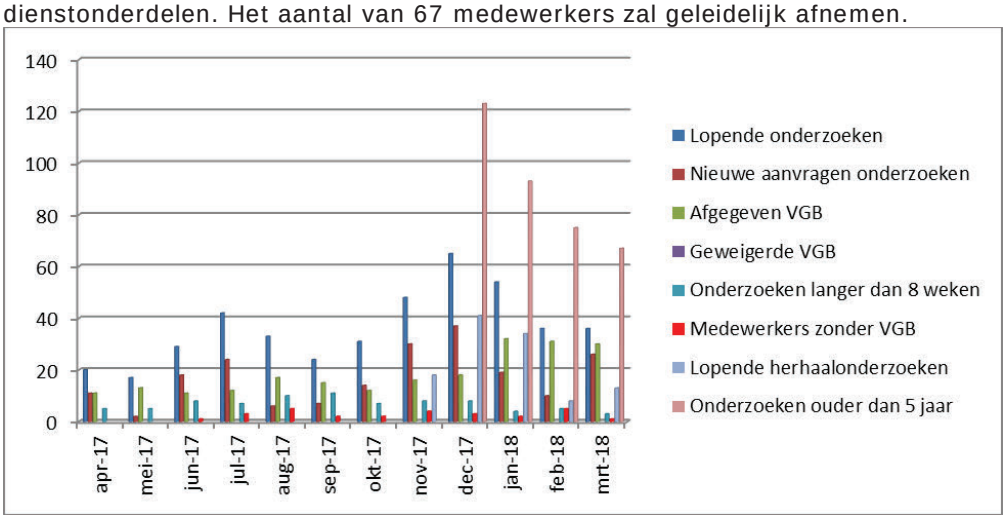
Van

Datum/eindparaaf

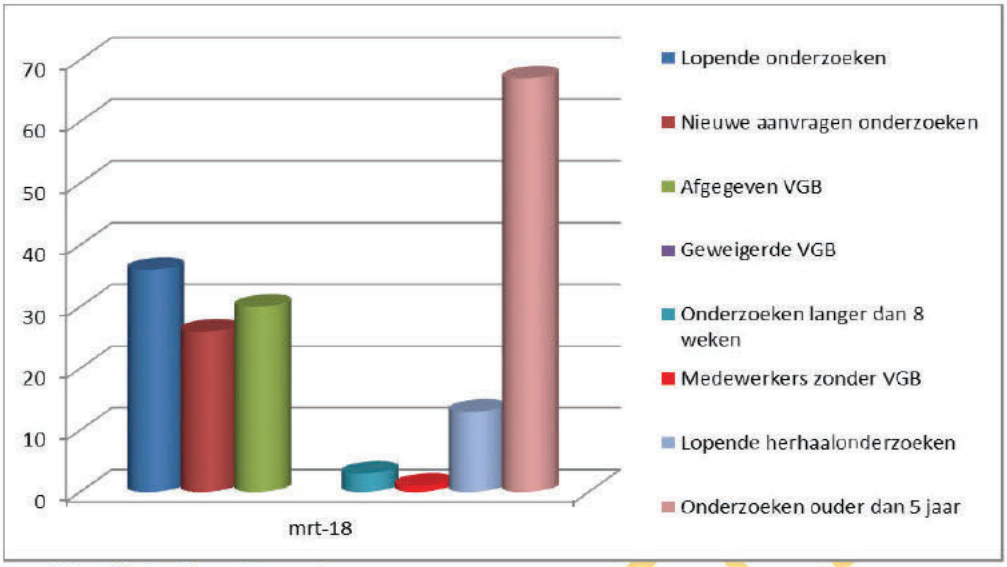
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand maart.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In maart was er één tijdelijke medewerker aan het werk met een waiver bij zonder VGB.
Er zijn nu binnen de NCTV 67 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 67 medewerkers zal geleidelijk afnemen.



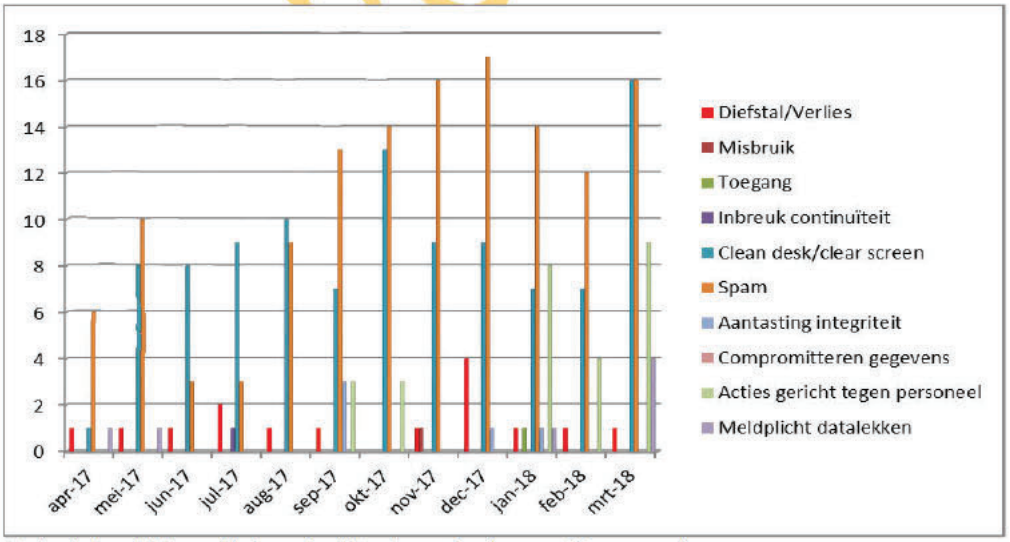
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



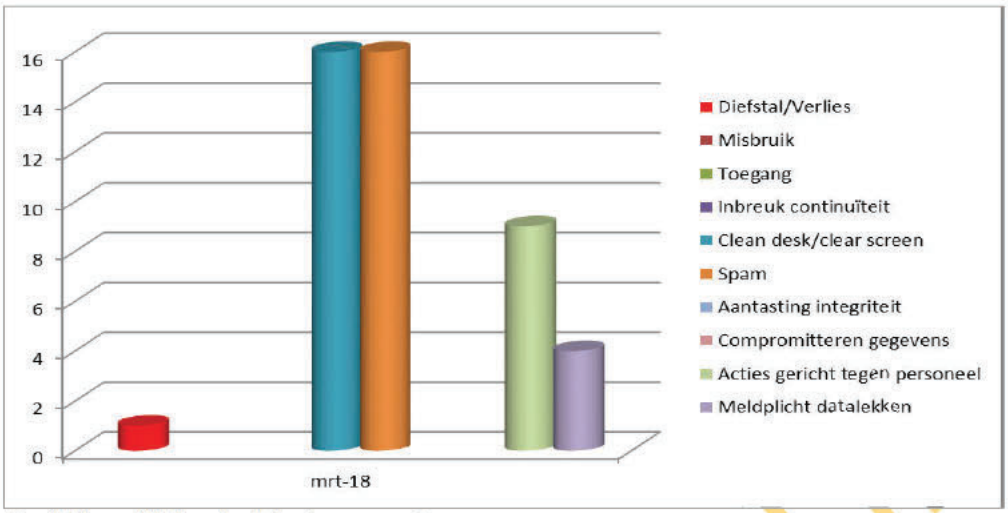
Beeld veiligheidsonderzoeken maart

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten maart

Toelichting tabellen

Diefstal/verlies

- Een medewerker heeft zijn smartphone verloren. Na de melding is de telefoon geblokkeerd.

Cleandesk

- In maart zijn bij [redacted] twee kluizen open aangetroffen en is tweemaal een kluissleutel veiliggesteld door de beveiligingsmedewerkers bij de directie [redacted]. Beide, laatst genoemde, kluizen waren wel vergrendeld met [redacted].
  De beveiligingsmedewerkers hebben tijdens de cleandeskrondes 12 [redacted] onbeheerd aangetroffen op een werkplek (bij [redacted] en veilig gesteld.
  Bij [redacted] zijn [redacted] documenten aangetroffen bij de [redacted] (printer). De documenten zijn veiliggesteld.

SPAM/Phising mail

- In maart zijn 16 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Acties gericht tegen medewerkers

- Er zijn een 8-tal mailberichten binnengekomen bij de [redacted] waarin onder andere wantoestanden bij de overheid worden gemeld. De berichten lijken afkomstig van [redacted] en zijn toegevoegd aan de dossiers [redacted].
- [redacted]

Meldplicht datalekken

- Bij een externe partij van [redacted] zijn persoonsgegevens van medewerkers van [redacted] gelekt. De externe partner heeft onze medewerkers geïnformeerd. De leidinggevende heeft de melding verder afgehandeld.
- [redacted].
- Bij [redacted] heeft een medewerker een mailbericht met een bestand geüpload naar een portaal voor onderzoek. Hierbij is de naam van de melder zichtbaar geworden. Het incident is met de leidinggevende en de tijdelijk privacy coördinator besproken. De impact en ernst waren laag waardoor de afweging is gemaakt om geen melding te maken.
- Naar aanleiding van diverse vragen van medewerkers over het gebruik en verwerken van persoonsgegevens voor de oude [redacted] is er aan de medewerkers aanvullende informatie ter beschikking gesteld via intranet en zijn persoonlijke vragen beantwoord.

Datalek wachtwoorden

Begin april is er in de media veel aandacht geweest voor een datalek met 3,3 miljoen wachtwoorden. Het blijkt dat veel van de informatie al bekend was. Toch is nu ook zichtbaar geworden dat er [redacted] gecompromitteerd zijn. De gegevens zijn mogelijk gebruikt door medewerkers om zich ergens voor te registreren dat kan bijvoorbeeld een congres, bijeenkomst of nieuwsbrief zijn. De gegevens kunnen niet direct gebruikt worden om toegang te krijgen tot accounts van medewerkers in de [redacted]. Het is wel zo dat de [redacted].
Tevens kunnen de mailadressen gebruikt worden om gericht phisingmails te sturen. Het risico [redacted] is beperkt maar er is wel sprake van een zekere imagoschade. Het incident zal gebruikt worden voor introductiebijeenkomsten met nieuwe medewerkers om bewuste keuzes te maken bij externe aanmeldingen.

Overige

SIEM

De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hebben in maart de volgende meldingen gegenereerd.

[redacted]

Er hebben zich geen bijzondere meldingen voor gedaan op het [redacted] de afgelopen maand.

De beschikbaarheid van de kritieke informatiesystemen [redacted] was 99,9 % in de maand maart.

Er hebben zich geen bijzondere meldingen voor gedaan. Wel is zichtbaar dat het aantal kwetsbaarheidsmeldingen toeneemt.

ADR pentesten
De ADR heeft de nieuwe website van onderzocht. De geconstateerde aandachtspunten worden inmiddels door de leverancier verwerkt.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
23 mei 2018

Ons kenmerk
123456

nota

Managementrapportage april 2018
Programma Integrale Beveiliging

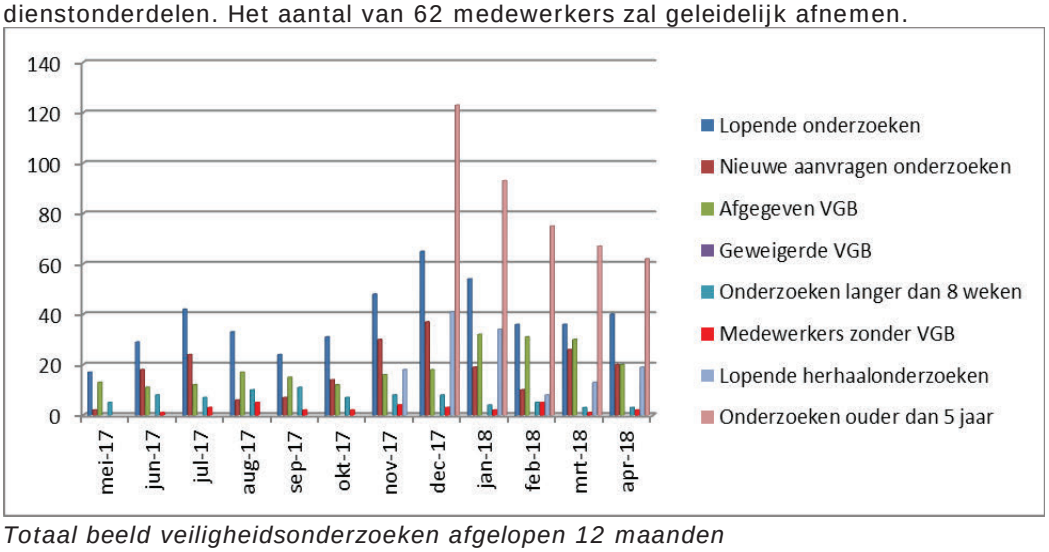
Van

Datum/eindparaaf

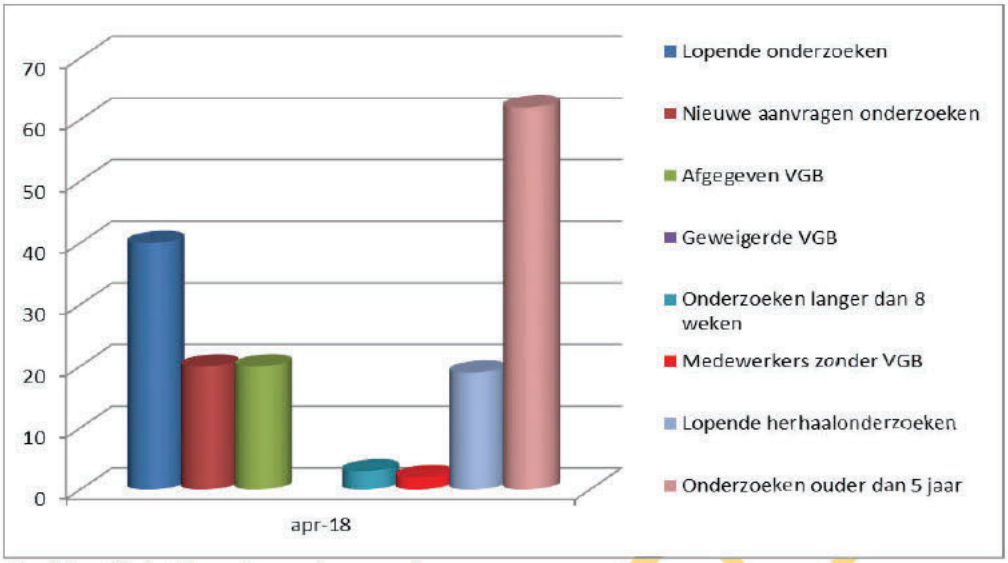
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand april.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In april waren er twee tijdelijke medewerkers aan het werk met een waiver bij zonder VGB.
Er zijn nu binnen de NCTV 62 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 62 medewerkers zal geleidelijk afnemen.



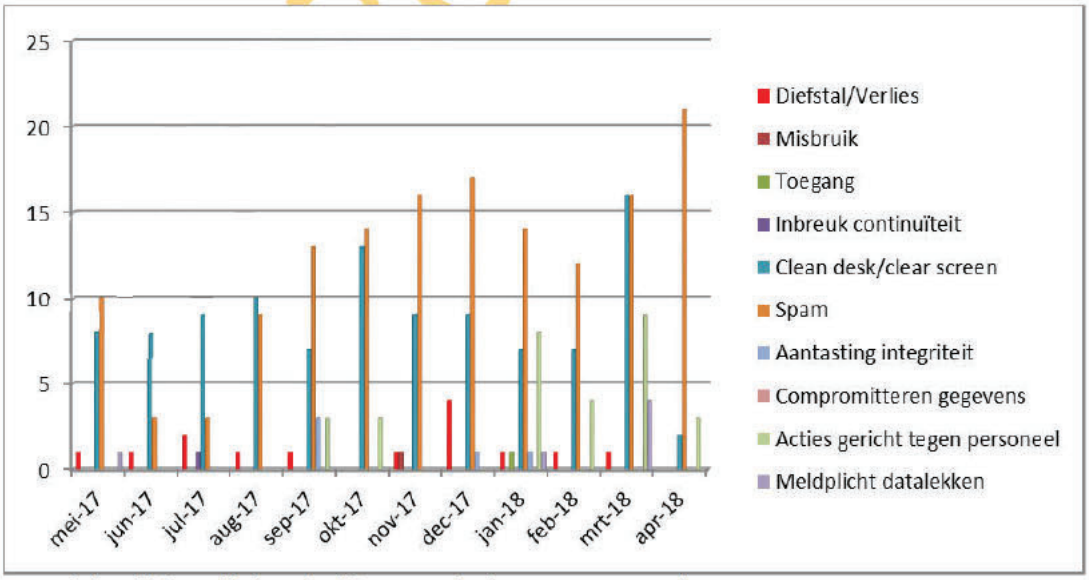
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



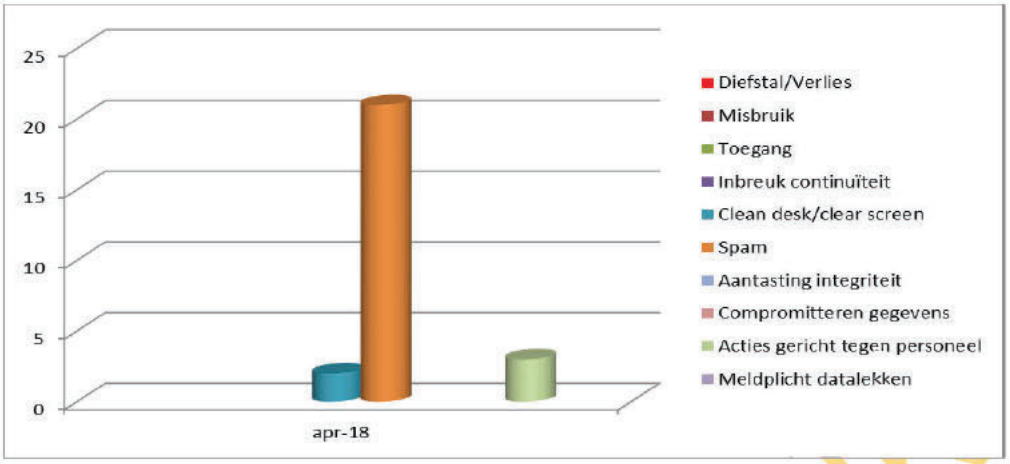
Beeld veiligheidsonderzoeken april

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten april

Toelichting tabellen

Cleandesk

- In april zijn bij [redacted] tweemaal de kluissleutels aangetroffen in de kluizen. De kluissleutels zijn veiliggesteld door de beveiligingsmedewerkers.

SPAM/Phising mail

- In april zijn 21 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] Overigens zien we wel een stijging van het aantal meldingen en het bewustzijn bij medewerkers is duidelijk aanwezig. Vreemde mailberichten worden gemeld.

Acties gericht tegen medewerkers

- Er zijn een 3-tal mailberichten binnengekomen bij de [redacted] waarin onder andere wantoestanden bij de overheid worden gemeld. De berichten lijken afkomstig van [redacted] en zijn toegevoegd aan de dossiers van [redacted].

Overige

SIEM

De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hebben in april de volgende meldingen gegenereerd.

[redacted]

Er heeft zich één bijzondere melding voor gedaan op het [redacted]. De melding betrof malware. Het station is direct uitgeschakeld en de malware is verwijderd.

Door een verbetering van de software zijn er meer kwetsbaarheden waargenomen. De beschikbaarheid van de kritieke informatiesystemen [redacted] was 98,785 % in de maand april.

Er hebben zich geen bijzondere meldingen voor gedaan. Wel is zichtbaar dat het aantal kwetsbaarheidsmeldingen toeneemt.

Vernietiging hardware
Op 11 april zijn er laptops en harde schijven vernietigd . Ook nu was er weer de gelegenheid voor medewerkers om apparatuur in te leveren voor een zorgvuldige afvoer en vernietiging.

Reizen naar het buitenland
Naar aanleiding van berichten in de media is een artikel voor de medewerkers geplaatst waarin de risico's worden geschetst van het reizen met apparatuur en wordt verwezen naar het bestaande document (advies) 'Reizen naar het buitenland' van de NCTV.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
12 juni 2018

Ons kenmerk
123456

nota

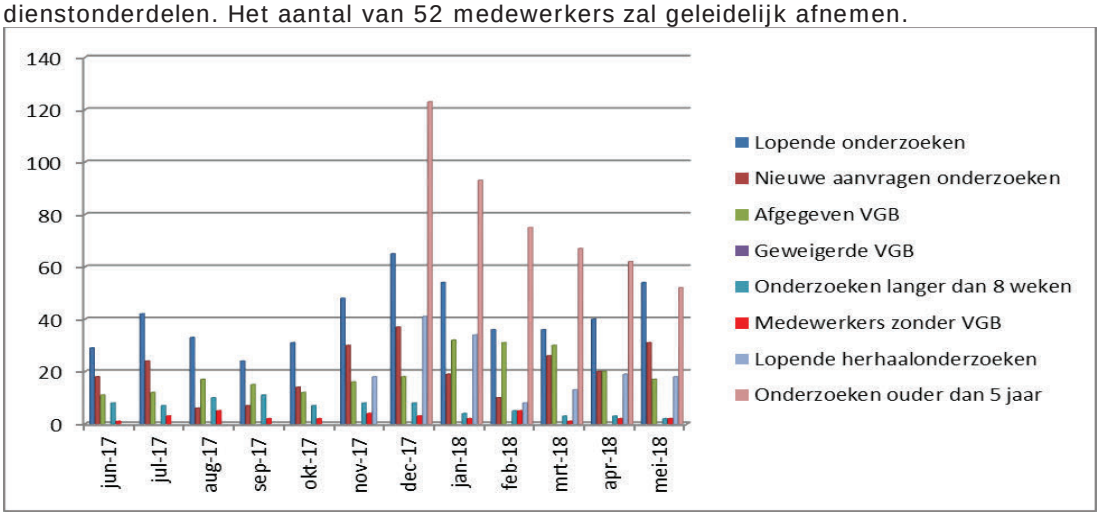
Managementrapportage mei 2018
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

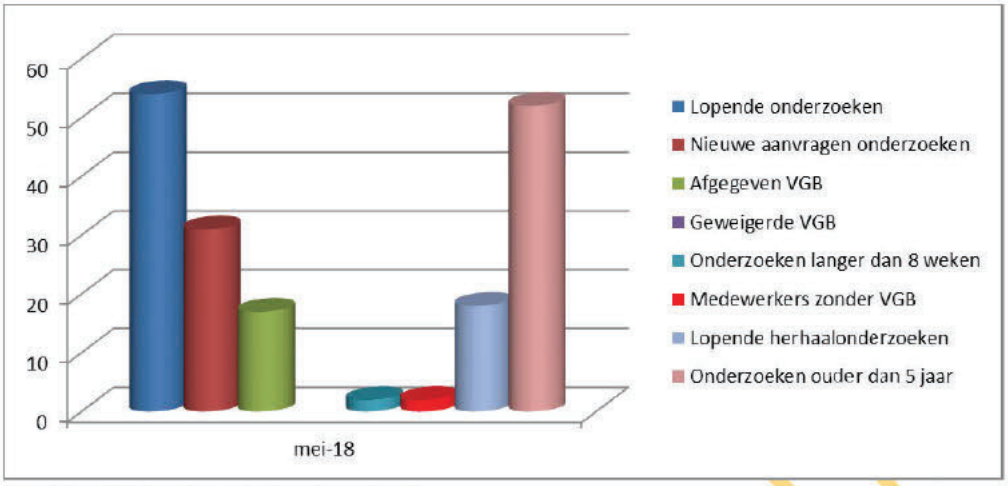
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand april.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In mei waren er twee tijdelijke medewerkers aan het werk met een waiver bij [redacted] zonder VGB.
Er zijn nu binnen de NCTV 52 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 52 medewerkers zal geleidelijk afnemen.



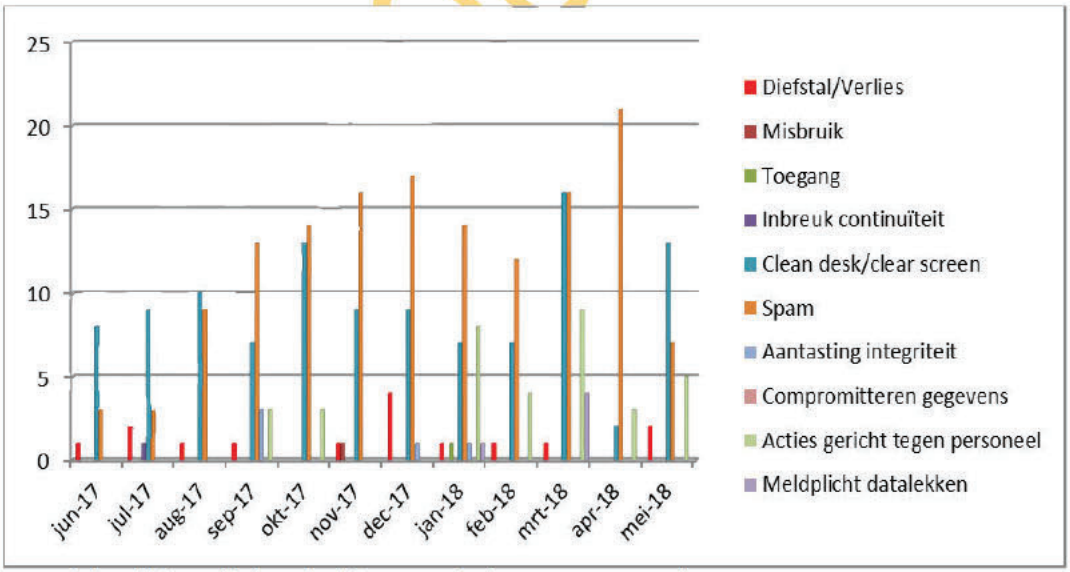
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



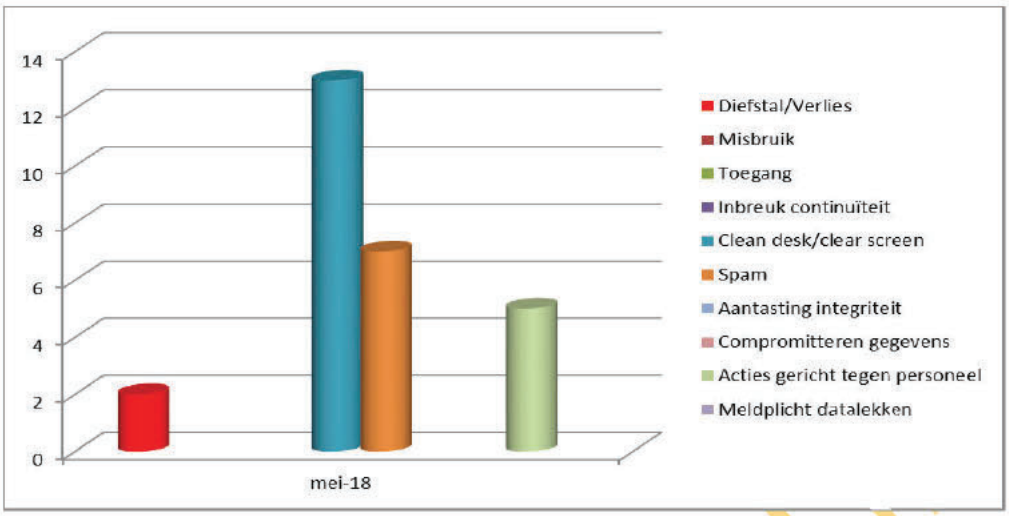
Beeld veiligheidsonderzoeken mei

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten mei

Toelichting tabellen

Diefstal/Verlies

- In mei zijn door medewerkers één iPhone en één [redacted] verloren. De devices zijn op afstand gewist.

Cleandesk

- In mei zijn bij [redacted] (2x) de kluissleutels aangetroffen in de kluizen. In het geval van [redacted] stonden de kluizen nog open. De kluissleutels zijn veiliggesteld door de beveiligingsmedewerkers. Tevens is er een laptop onbeheerd aangetroffen bij [redacted]. De leidinggevenden zijn geïnformeerd en hebben het besproken met de medewerkers. Er zijn ook 6 [redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In mei zijn 7 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] Overigens zien we wel een stijging van het aantal meldingen en het bewustzijn bij medewerkers is duidelijk aanwezig. Vreemde mailberichten worden gemeld.

Acties gericht tegen medewerkers

- Er zijn een 5-tal mailberichten binnengekomen bij de [redacted] waarin onder andere wantoestanden bij de overheid en bezorgdheid door familie over kinderen in IS-gebied worden gemeld. De eerste berichten lijken afkomstig van [redacted] en zijn toegevoegd aan de dossiers [redacted]. De berichten over families van IS leden zijn doorgezet naar [redacted] voor verdere afhandeling.

Datalekken

Vanaf 25 mei is de registratie en meldplicht voor datalekken verscherpt. Het verlies van de iPhone eerder in mei is niet gemeld als datalek maar zou volgens de nieuwe AVG wel in het vervolg gemeld moeten worden omdat de iPhone persoonsgegevens bevatte.

Overige

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hebben in mei geen kwetsbare meldingen gegenereerd.

Door een verbetering van de software zijn er meer kwetsbaarheden waargenomen. De beschikbaarheid van de kritieke informatiesystemen was 94% in de maand mei als gevolg van een update in mei.

Er hebben zich geen bijzondere meldingen voor gedaan.

Websites
Via de procedure 'responsible disclosure meldingen' van , kregen we een melding dat de website een kwetsbaarheid bevatte. De melding is doorgegeven aan de functioneel beheerder. De leverancier heeft de kwetsbaarheid nog niet opgelost.

Kaspersky
Maandag 14 mei heeft de minister van Justitie en Veiligheid de Tweede Kamer met een brief geïnformeerd over de voorzorgsmaatregel van het kabinet om antivirussoftware van Kaspersky Lab bij de Rijksoverheid uit te faseren. De NCTV maakt geen gebruik van Kaspersky producten.

DDoS-aanvallen
Rond 25 mei werd er gewaarschuwd voor mogelijk meerdere DDoS aanvallen op financiële instellingen en rijksoverheid. De Frontoffice is hierover geïnformeerd om de continuïteit en beschikbaarheid van de NCTV websites te monitoren. Er hebben zich tot op heden nog geen incidenten voor gedaan.

Het heeft kennis genomen van de berichtgeving over een kwetsbaarheid in het gebruik van voor e-mailverkeer. Het houdt deze ontwikkeling nauwlettend in de gaten. Het is alleen mogelijk om van de kwetsbaarheid misbruik te maken door een Het risico is dan ook op dit moment laag.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
11 juli 2018

Ons kenmerk
123456

nota

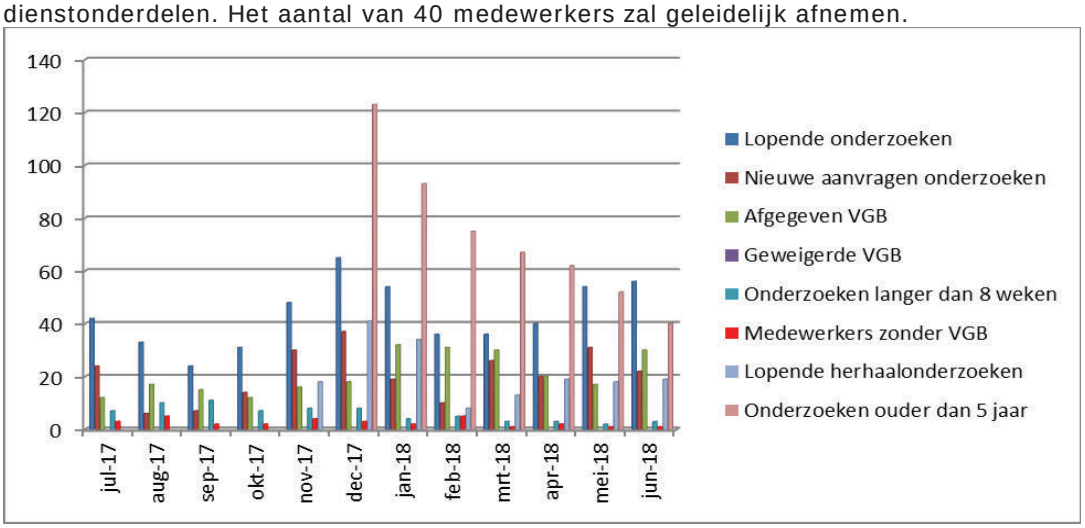
Managementrapportage juni 2018
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

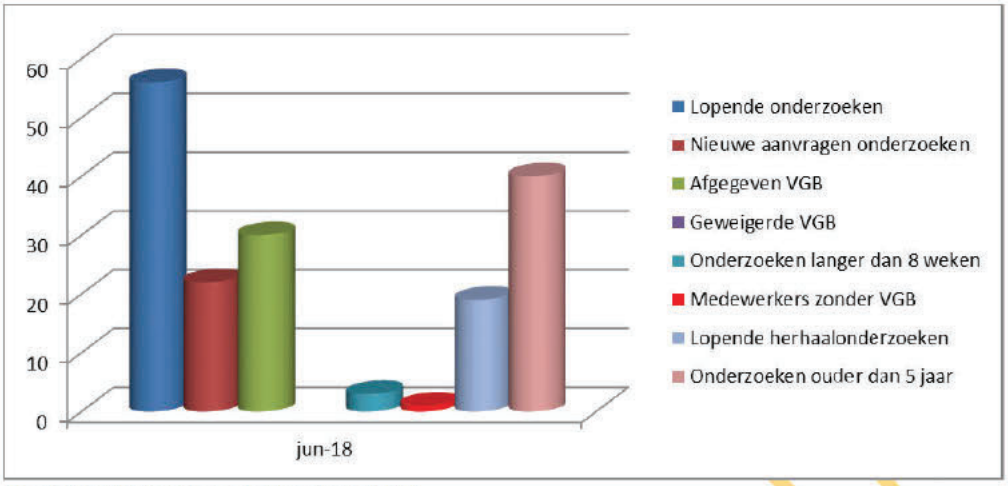
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand juni.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In juni was er één tijdelijke medewerker aan het werk met een waiver bij [redacted] zonder VGB.
Er zijn nu binnen de NCTV 40 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 40 medewerkers zal geleidelijk afnemen.



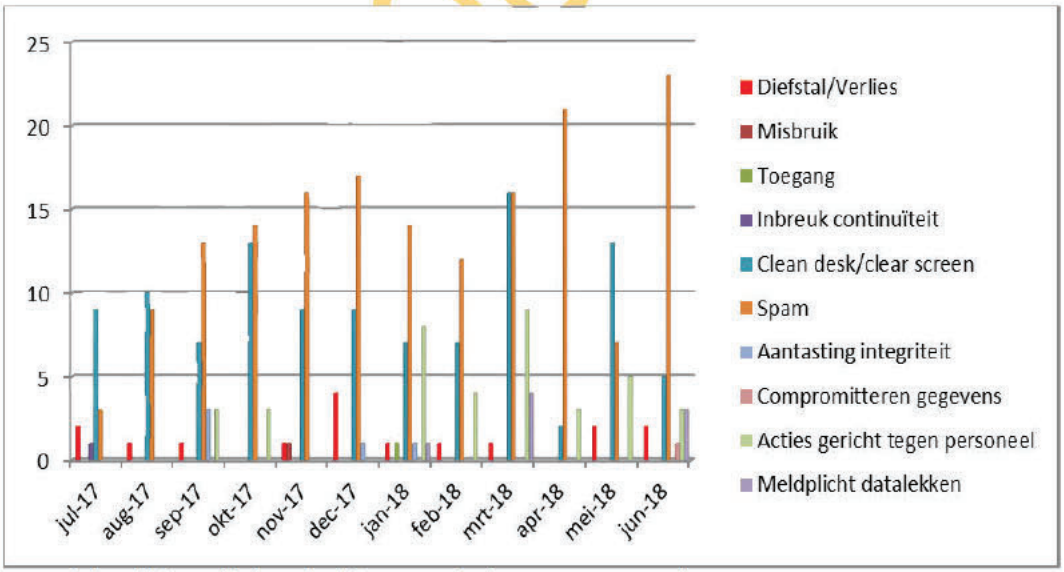
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



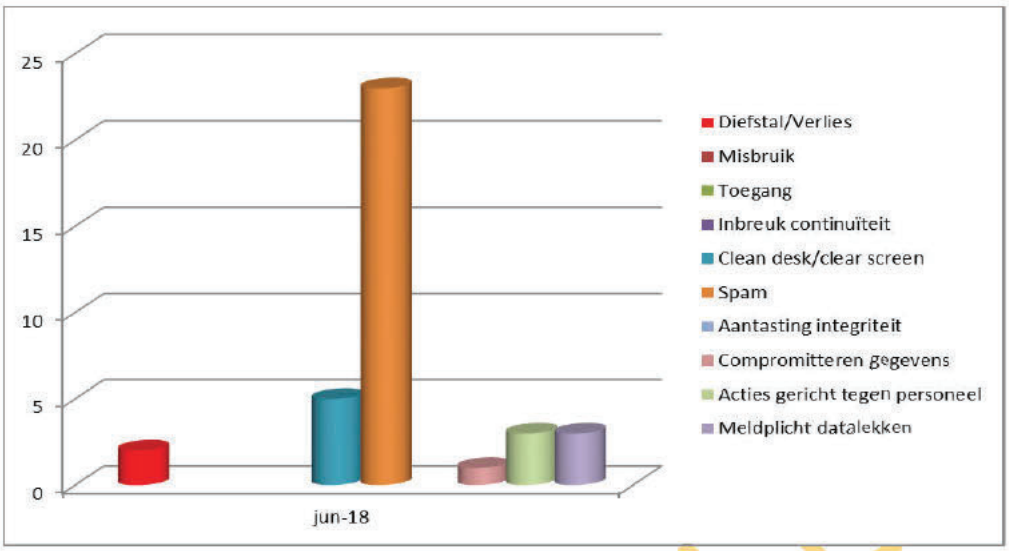
Beeld veiligheidsonderzoeken juni

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten juni

Toelichting tabellen

Diefstal/Verlies

- In juni is er van een medewerker tijdens een dienstreis een IPad en rijkspas gestolen. Er is aangifte gedaan en de IPad is direct geblokkeerd op afstand.

Cleandesk

- In juni zijn bij [redacted] (1x) en [redacted] (1x) de kluissleutels aangetroffen in de kluizen. De kluissleutels zijn veiliggesteld door de beveiligingsmedewerkers. De leidinggevenden zijn geïnformeerd en hebben het besproken met de medewerkers. Er zijn ook 3 [redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In juni zijn 15 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] Er zijn 11 meldingen gedaan door medewerkers van bellers uit het buitenland. Hier gaat het om buitenlandse telefoniefraudeurs. Hier is vrij weinig tegen te doen. De meeste medewerkers zijn zich wel bewust van deze mogelijke fraudeurs en nemen niet op. Overigens worden nummers ad random gebeld en zijn ze niet gericht op NCTV medewerkers.

- *Compromitteren gegevens*
  In juni is een Staatsgeheim stuk ([redacted]) volgens de juiste procedure afgeleverd bij [redacted]. Er is voor ontvangst getekend maar de beoogde geadresseerde geeft aan dat hij het niet heeft ontvangen. Het onderzoek loopt nog. Overigens gaat het om een stuk met lage impact bij compromittering.

Acties gericht tegen medewerkers

- Er is een 3-tal mailberichten binnengekomen bij de [redacted] waarin onder andere wantoestanden bij de overheid en bezorgdheid door familie over

kinderen in IS-gebied worden gemeld. De eerste berichten lijken afkomstig van [redacted] en zijn toegevoegd aan de dossiers [redacted]. De berichten over families van IS leden zijn doorgezet naar [redacted] voor verdere afhandeling.

Datalekken

- In het kader van het open data beleid van J&V heeft het NCSC haar beveiligingsadviezen als open data beschikbaar gesteld op de website data.overheid.nl maar was men vergeten [redacted]. Het datalek is volgens de nieuwe procedure afgehandeld. Na onderzoek is gebleken dat de informatie nog niet geraadpleegd of ingezien was door derden. Hierdoor is er geen melding naar de AP gedaan.
- Bij [redacted] had men een mail gestuurd naar externe contacten met een overzichtsdocument met [redacted]. De melding is onderzocht door de privacycoördinator. Het bleek dat medewerkers mondeling hadden ingestemd waardoor er geen direct sprake was van een datalek. Wel waren er wat aandachtspunten en die zijn in een voorlichtingsbijeenkomst aan de betreffende afdeling voorgelegd.
- Bij de diefstal van de iPad en de tas waarin onder andere visitekaartjes zaten was er ook sprake van een datalek omdat er persoonsgegevens op stonden. Ondanks het feit dat de IPad beveiligd was en op afstand is gewist en geblokkeerd bestaat er de meldplicht bij de AP. Er is dan ook melding van gemaakt.

Overige

SIEM

De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hadden in juni een verdachte situatie van mogelijke malware op het [redacted] gedetecteerd. Nader onderzoek heeft uitgewezen dat er sprake was van malware of besmetting.

Door een verbetering van de software zijn er meer kwetsbaarheden waargenomen. De beschikbaarheid van de kritieke informatiesystemen [redacted] was 97,4 % in de maand juni.

[redacted]

Er hebben zich geen bijzondere meldingen voor gedaan.

Websites

Via de procedure 'responsible disclosure meldingen' van [redacted], kregen we een melding dat de website [redacted] een kwetsbaarheid bevatte. De melding is doorgegeven aan de functioneel beheerder. De leverancier heeft de kwetsbaarheid direct opgelost.

CSBN

Het CSBN 2018 is uitgegeven. De werkgroep Beveiliging betrekt de aanbevelingen en bevindingen bij de analyse van de [redacted]. Het CSBN onderschrijft de digitale dreigingen zoals de werkgroep die al eerder signaleerde ten aanzien van informatiebeveiliging.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
28-08-2018

Ons kenmerk
123456

nota

Managementrapportage juli en augustus 2018
Programma Integrale Beveiliging

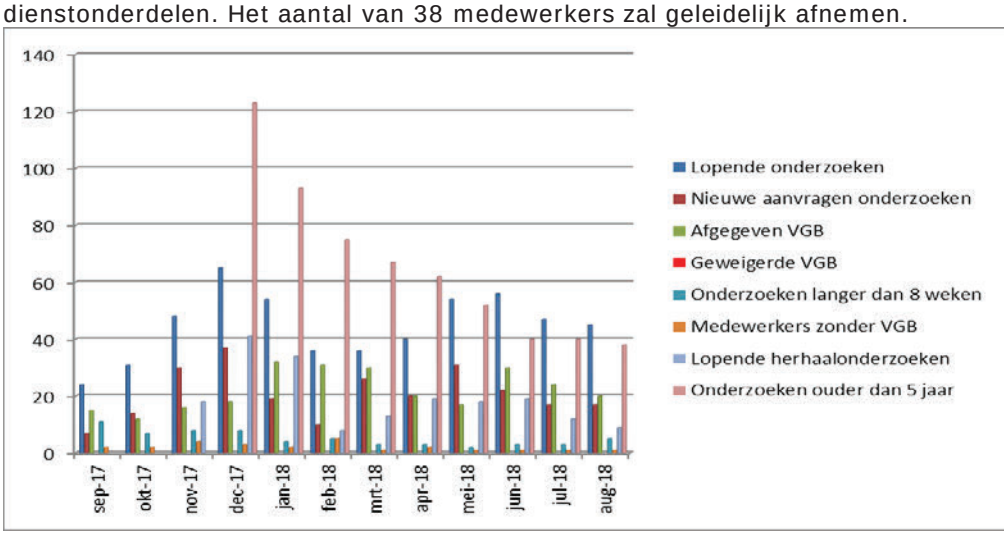
Van

Datum/eindparaaf

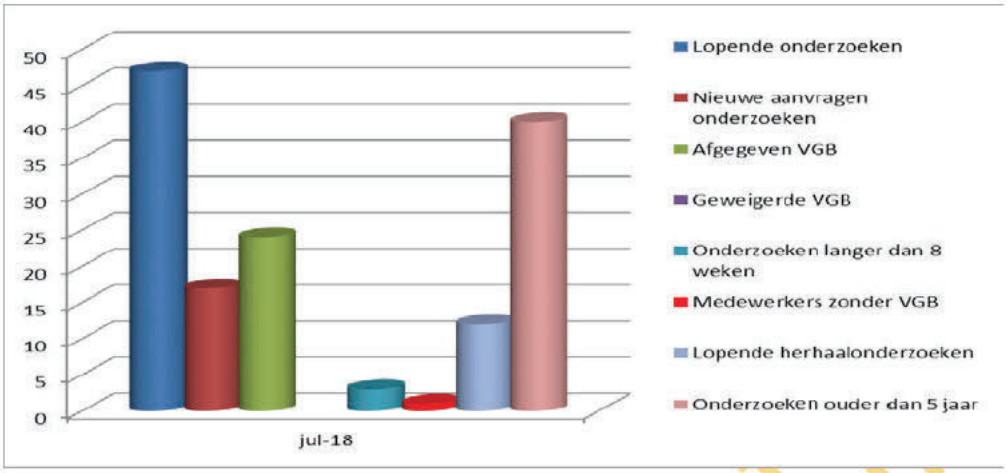
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maanden juli en augustus.

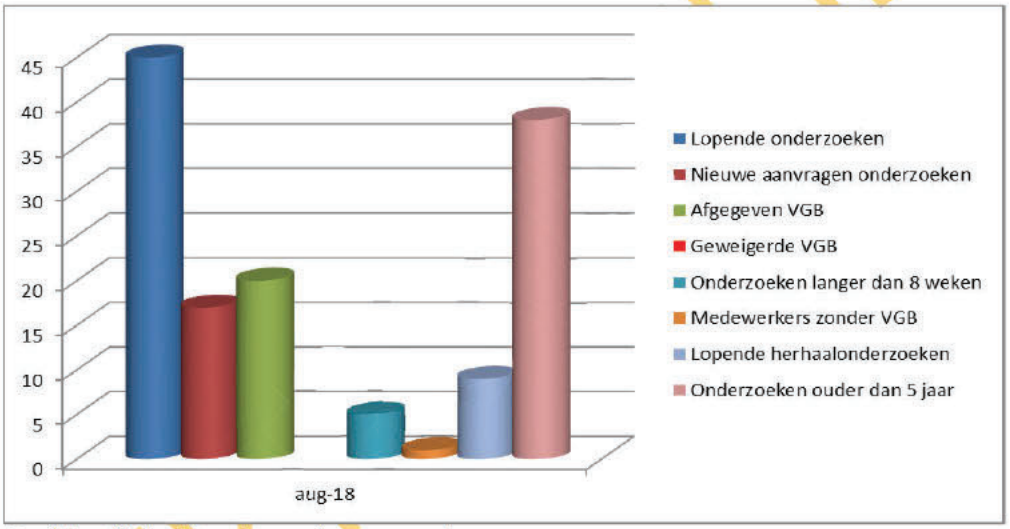
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In juli en augustus was er één tijdelijke medewerker aan het werk met een waiver bij zonder VGB.
Er zijn nu binnen de NCTV 38 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 38 medewerkers zal geleidelijk afnemen.



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



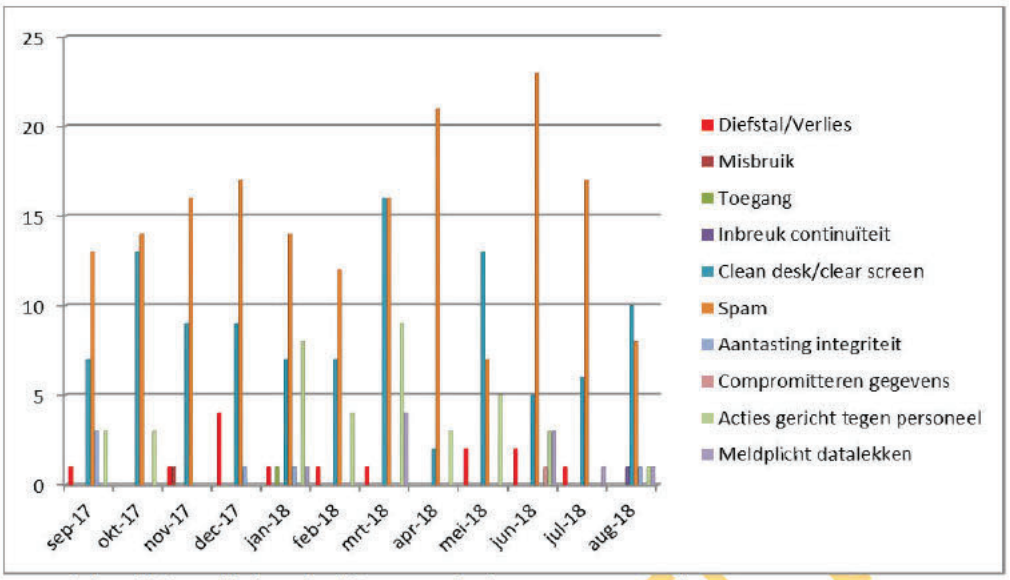
Beeld veiligheidsonderzoeken juli



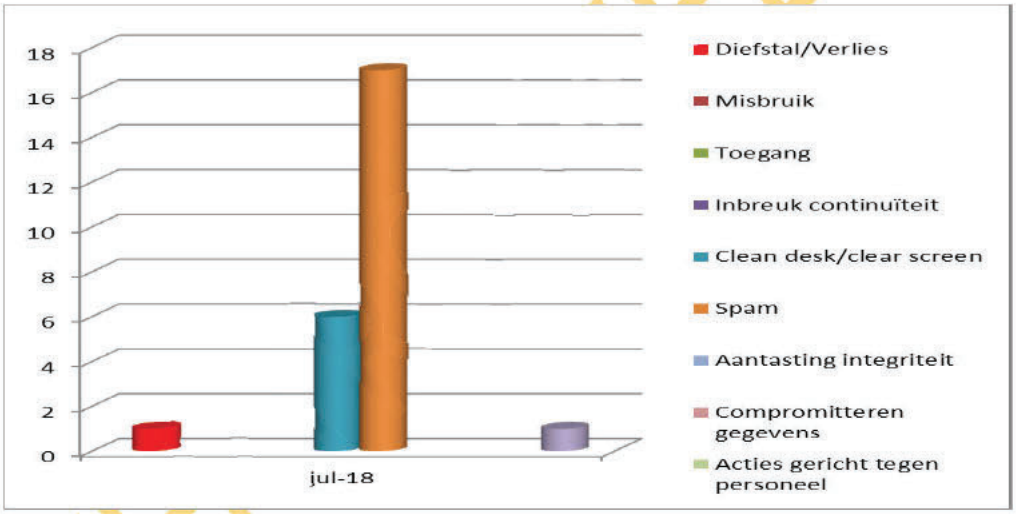
Beeld veiligheidsonderzoeken augustus

Incidentenregistratie

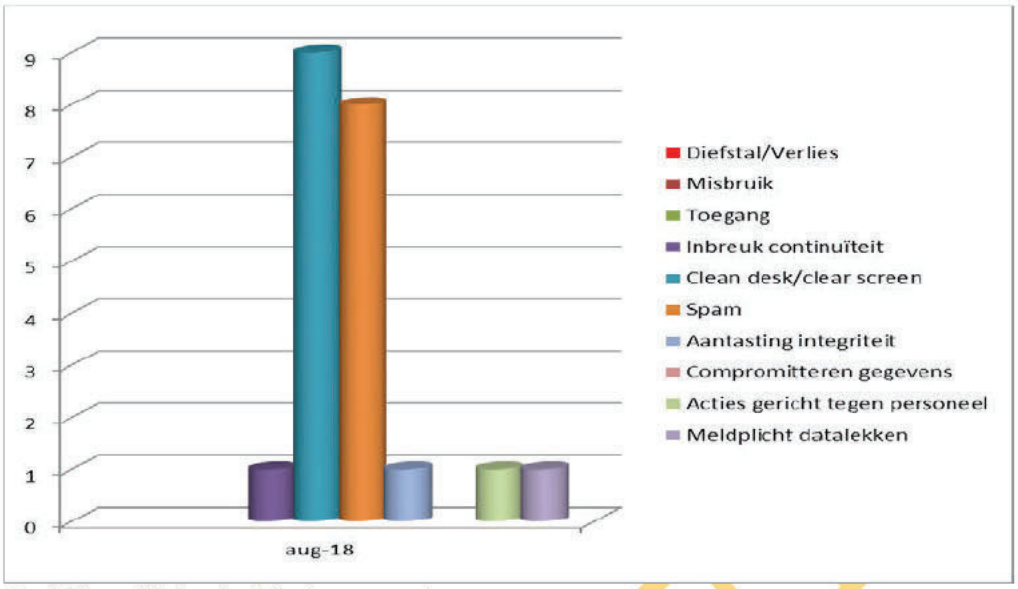
Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten juli



Beeld beveiligingsincidenten augustus

Toelichting tabellen

Diefstal/Verlies

- In juli heeft een medewerker binnen de zone zijn [redacted] verloren. Risico op misbruik is beperkt omdat je ook nog een [redacted] nodig hebt.

Cleandesk

- In juli en augustus zijn bij [redacted] (2x) en bij [redacted] (1x) de kluissleutels aangetroffen in de kluizen of stonden de kluizen zelfs open. De kluissleutels zijn veiliggesteld door de beveiligingsmedewerkers. De leidinggevenden zijn geïnformeerd en hebben het besproken met de medewerkers. Er zijn ook 12 [redacted]) aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers. Bij [redacted] is tijdens de cleandeskronde een [redacted] document op een bureau aangetroffen. Het document is meegenomen en opgeslagen in de kluis.

SPAM/Phising mail

- In juli en augustus zijn 21 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted] Er zijn 4 meldingen gedaan door medewerkers van bellers uit het buitenland. Hier gaat het om buitenlandse telefoniefraudeurs. Hier is vrij weinig tegen te doen. De meeste medewerkers zijn zich wel bewust van deze mogelijke fraudeurs en nemen niet op. Overigens worden nummers ad random gebeld en zijn ze niet gericht op NCTV medewerkers.

Continuïteit

- In augustus is het mobiele netwerk uitgevallen dat heeft niet geleid tot grote verstoringen van de werkprocessen. De oorzaak is nog niet bekend.

Aantasting integriteit

- Door [redacted] is bij het installeren van de [redacted] op een mobiel device van een gebruiker het verkeerde userid van een NCTV medewerker gebruikt. De medewerker had hierdoor tijdelijk toegang tot de mailbox van de NCTV medewerker. De fout is na een paar dagen opgelost en de [redacted] is geïnformeerd.

Acties gericht tegen personeel

- [redacted]

Datalekken

- Er is een poststuk met personeelsvertrouwelijk informatie door de postkamer geopend en naar een verkeerde organisatie gestuurd. Het poststuk is uiteindelijk bij de juiste persoon terecht gekomen. Er is geen melding gemaakt bij de Autoriteit Persoonsgegevens. Het incident is wel gemeld bij de [redacted] voor verdere afhandeling.
- Een mail met (gevoelige) persoonsgegevens werd per abuis aan een verkeerde ontvanger geadresseerd binnen de rijksoverheid. Deze persoon had dezelfde achternaam als degene naar wie de mail had moeten gaan, maar is werkzaam bij een ander dienstonderdeel van JenV (IND te Zwolle). Gezien de gevoeligheid van de gegevens hebben wij besloten dit toch te melden bij de AP. De impact voor betrokkene is echter als 'beperkt' ingeschat aangezien de foutieve ontvanger de mail heeft verwijderd en, zoals gezegd, werkzaam is voor JenV.

Overige

SIEM

De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hadden in juli en augustus geen verdachte situatie van mogelijke malware op het [redacted] gedetecteerd.

Door een verbetering van de software zijn er meer kwetsbaarheden waargenomen. De beschikbaarheid van de kritieke informatiesystemen [redacted] was 99,9 % in de maanden juli en augustus.

[redacted]

Er hebben zich geen bijzondere meldingen voor gedaan.

[redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT/Programmaraad NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
10 oktober 2018

Ons kenmerk
123456

nota

Managementrapportage september 2018
Programma Integrale Beveiliging

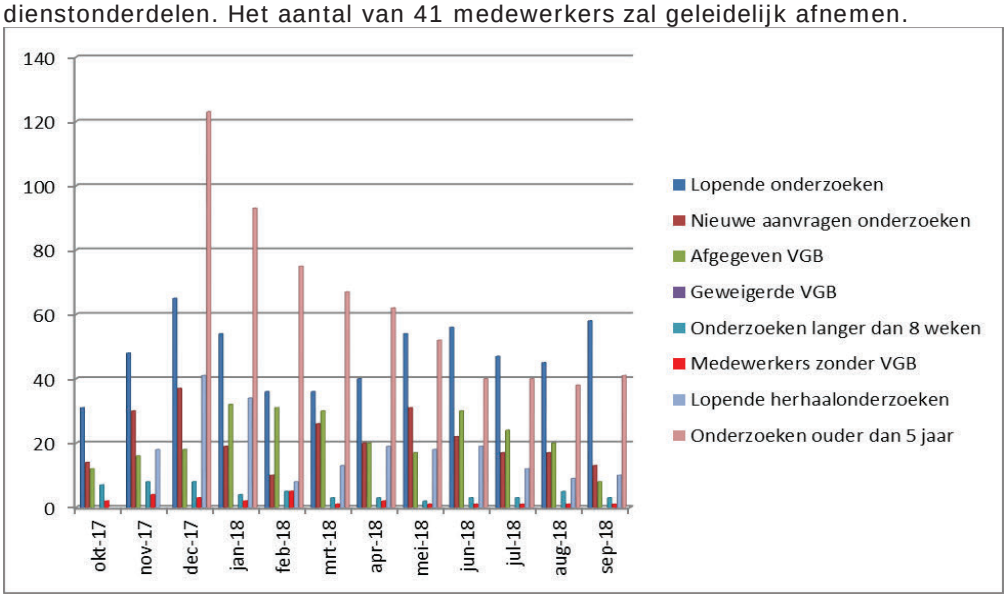
Van

Datum/eindparaaf

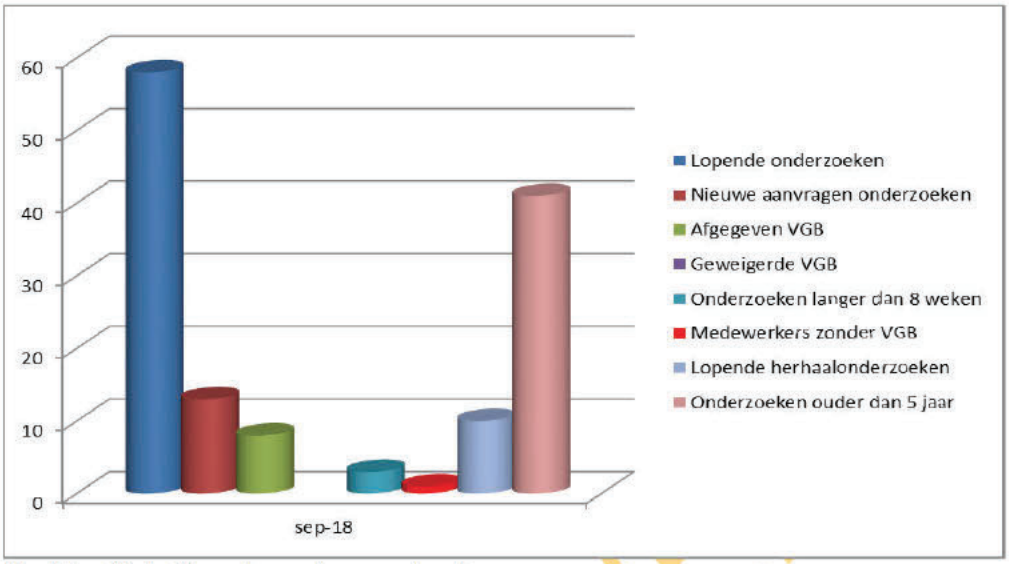
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand september.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In september was er één tijdelijke medewerker aan het werk met een waiver bij zonder VGB.
Er zijn nu binnen de NCTV 41 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 41 medewerkers zal geleidelijk afnemen.



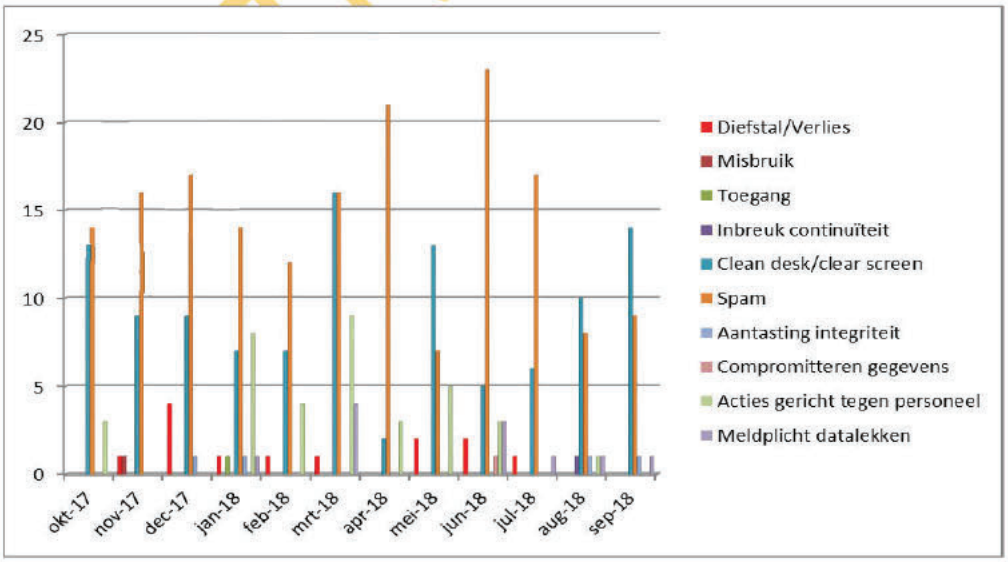
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



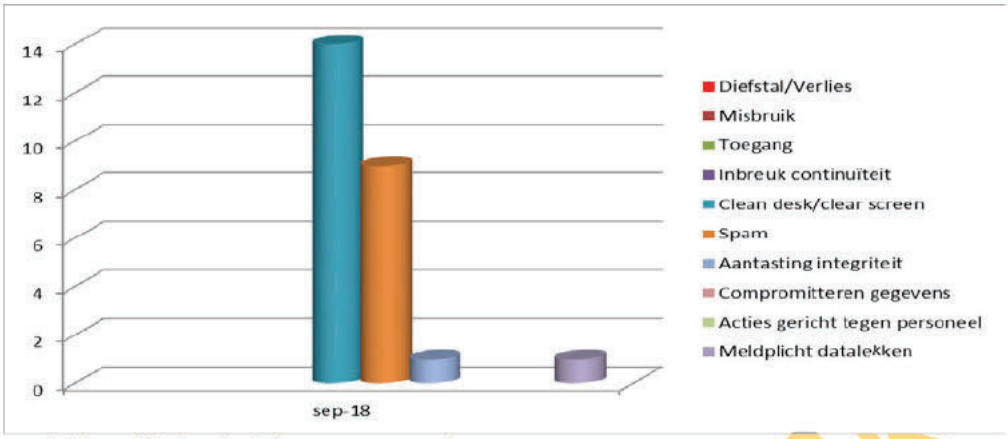
Beeld veiligheidsonderzoeken september

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten september

Toelichting tabellen

Diefstal/Verlies

- In september heeft een medewerker binnen de zone zijn [redacted] verloren en een medewerker heeft een [redacted] verloren. Beide [redacted] zijn na melding geblokkeerd. Risico op misbruik is beperkt omdat je ook nog een [redacted] nodig hebt.

Cleandesk

- In september zijn bij [redacted] (2x) en bij [redacted] (5x) de kluissleutels aangetroffen in de kluizen of stonden de kluizen zelfs open. De kluissleutels zijn veiliggesteld door de beveiligingsmedewerkers. De leidinggevenden zijn geïnformeerd en hebben het besproken met de medewerkers. Er zijn ook 7 [redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In juli en augustus zijn 9 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Aantasting integriteit

- Een medewerker, die zijn eigen rijkspas kwijt was, heeft een rijkspas gebruikt van een collega om zich binnen het gebouw te verplaatsen. De leidinggevende is hierover geïnformeerd.

Datalekken

- [redacted]
  Er heeft een datalek plaatsgevonden bij het [redacted] bedrijf [redacted]. Dit bedrijf, gespecialiseerd in [redacted], heeft door een verkeerd geconfigureerde server mogelijk [redacted]. Hierdoor was het mogelijk dat ongeveer 445 miljoen records, waaronder namen, IP adressen en email adressen beschikbaar waren voor mogelijke kwaadwillende.
  [redacted] staat ook in het adressenbestand van [redacted]. In de week na de datalek [redacted] van mogelijke hackers die

gebruik hebben gemaakt van contactgegevens die gestolen waren. Op de berichten is niet gereageerd.

Overige

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden, had in september geen verdachte situatie van mogelijke malware op het [redacted] gedetecteerd.
De beschikbaarheid van de kritieke informatiesystemen [redacted] was 100 % in de maand september.

[redacted]
Er hebben zich geen bijzondere meldingen voor gedaan.

Websites
Via het [redacted] is een responsible disclosure melding binnengekomen over de website [redacted]
Het gaat om een kwetsbaarheid op een onderdeel van de genoemde website. De kwetsbaarheid is nog niet opgelost. Het proces is gestart om de website offline te halen.

[redacted]

Veel [redacted] zijn vaak kwetsbaar omdat basismaatregelen nog niet voldoende op orde zijn. Dit varieert van [redacted]

[redacted]
Het NCSC heeft melding gemaakt van een internationaal grootschalige [redacted] phishing-campagne, ook gericht op Nederlandse gebruikers. Binnen JenV lopen we geen risico's. Mogelijk dat medewerkers wel thuis problemen kunnen ondervinden.

Week van de Veiligheid
In samenwerking met de [redacted] en de werkgroep beveiliging NCTV zullen we in november weer de 'Week van de Veiligheid' organiseren.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
5 november 2018

Ons kenmerk
123456

nota

Managementrapportage oktober 2018
Programma Integrale Beveiliging

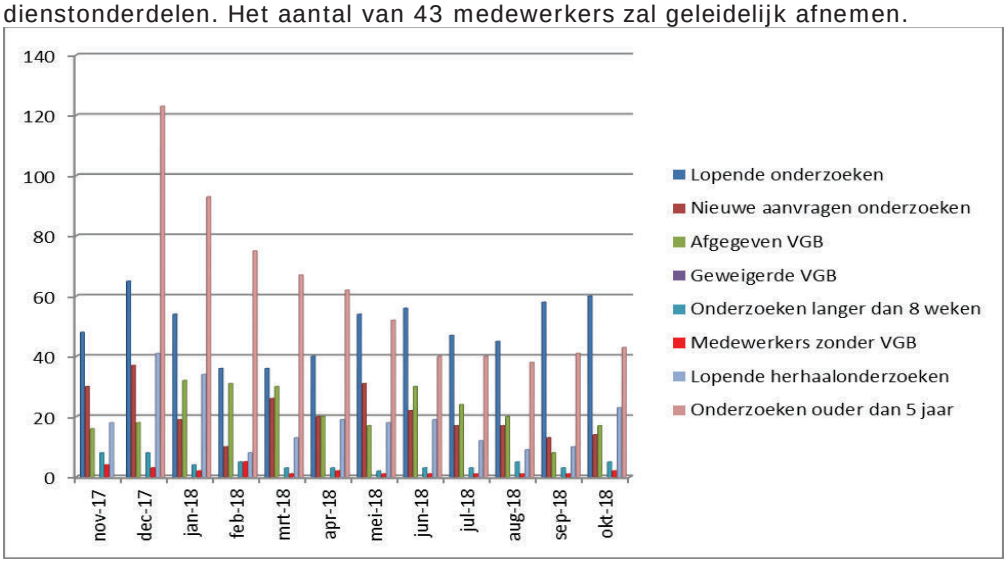
Van

Datum/eindparaaf

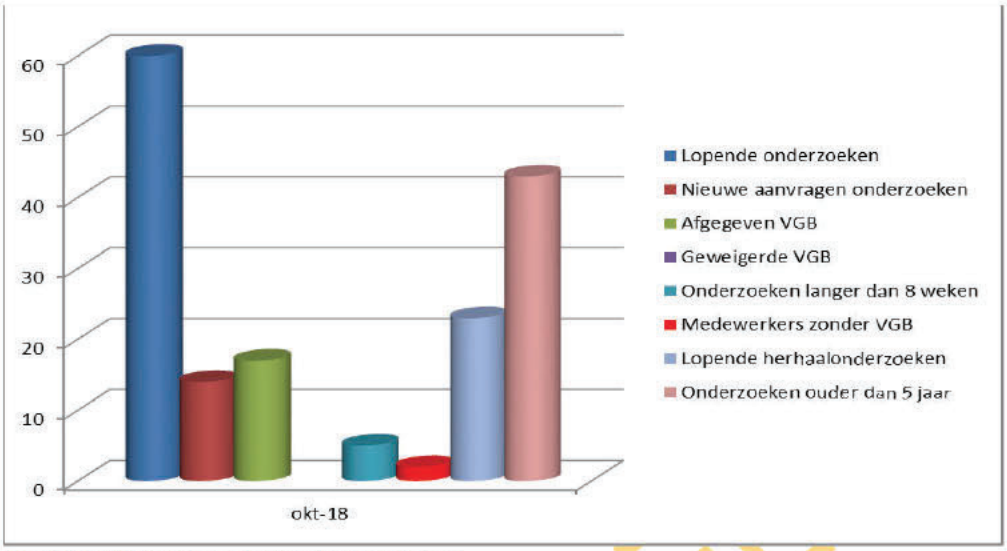
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand oktober.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In oktober waren er twee tijdelijke medewerkers aan het werk met een waiver bij zonder VGB.
Er zijn nu binnen de NCTV 43 medewerkers werkzaam met een VGB ouder dan 5 jaar. Vanaf 1 januari 2018 is het maandelijks quotum voor aan te leveren herhaalonderzoeken aangepast in verband met de aanlevering door andere dienstonderdelen. Het aantal van 43 medewerkers zal geleidelijk afnemen.



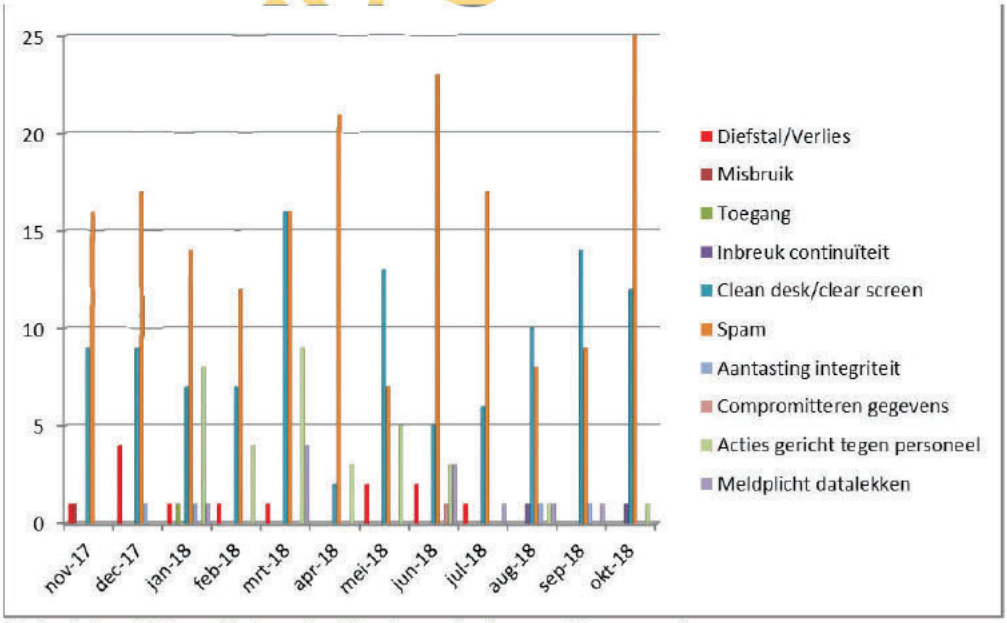
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



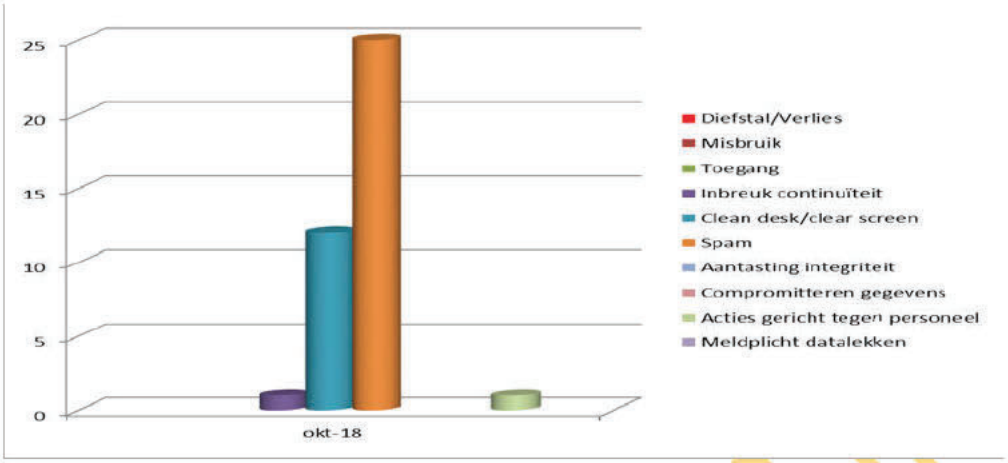
Beeld veiligheidsonderzoeken oktober

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten oktober

Toelichting tabellen

Cleandesk

- In oktober zijn bij [redacted] (1x) en bij [redacted] (2x) de kluissleutels aangetroffen in een kluis. De kluissleutels zijn veiliggesteld door de beveiligingsmedewerkers. De leidinggevenden zijn geïnformeerd en hebben het besproken met de medewerkers. Er zijn 9 [redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In oktober zijn 23 meldingen van spam en phising mail binnengekomen en 2 meldingen van spam via sms-berichten. De meldingen zijn doorgestuurd naar [redacted]

Acties gericht tegen personeel

[redacted]

Overige

SIEM

De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden, had in oktober geen verdachte situatie van mogelijke malware op het [redacted] gedetecteerd.
De beschikbaarheid van de kritieke informatiesystemen [redacted] was 100 % in de maand september.

[redacted]

Er hebben zich geen bijzondere meldingen voor gedaan.

Alertonline
In oktober vond de Alertonline bewustzijnscampagne plaats. Op intranet zijn artikelen geplaatst. Op het plein zijn voorlichtingsfilmpje afgespeeld. Posters zijn binnen de NCTV opgehangen.

Advies
Het NCSC heeft een algemeen advies gegeven naar aanleiding van de kwetsbaarheden in de . De NCTV heeft onderzoek gedaan naar de risico's voor zijn eigen netwerk. De risico's doen zich met name voor op het . In het huidige PvA voor de wordt de kwetsbaarheid onderkend en aangepast. Voor oplevering zal de ADR het systeem toetsen en ook beoordelen of deze kwetsbaarheid is uitgesloten.

In de media kwam het bericht naar buiten dat bij een dienstonderdeel van de onzorgvuldig omgegaan wordt met informatie. Hierdoor is mogelijk een risico ontstaan voor de integriteit van zijn hierover geïnformeerd en zij gaan in gesprek met de afdeling.

Storingen
De afgelopen tijd hebben zich meerdere storingen voor gedaan bij de telecom provider . Door de storingen was de bereikbaarheid van medewerkers beperkt en de continuïteit niet geborgd. Via kunnen vervangende telefoons met simkaarten tijdelijk ter beschikking worden gesteld.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Kern Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
27 februari 2019

Ons kenmerk
123456

nota

Managementrapportage januari 2019
Programma Integrale Beveiliging

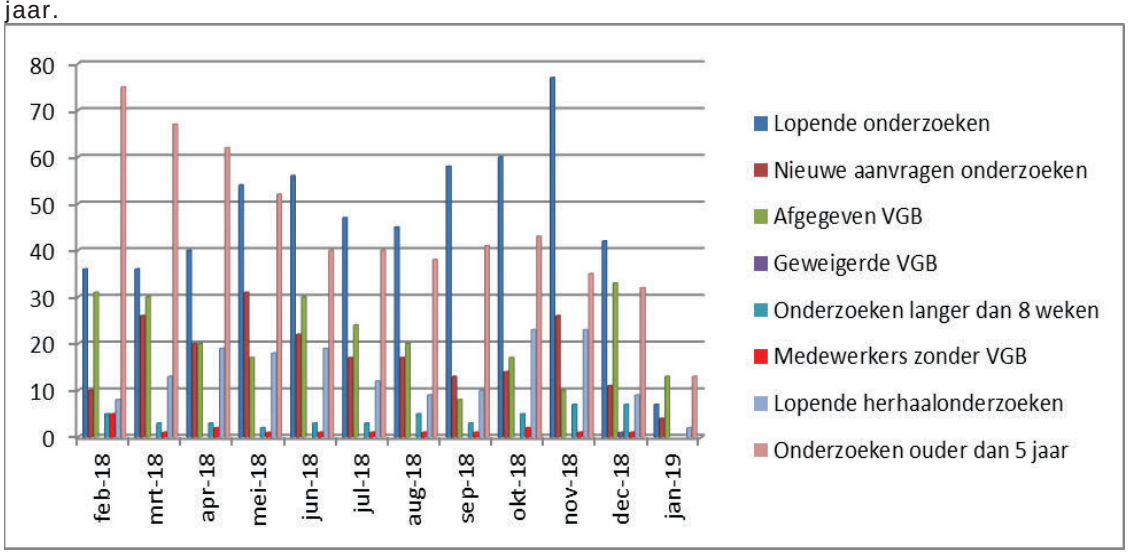
Van

Datum/eindparaaf

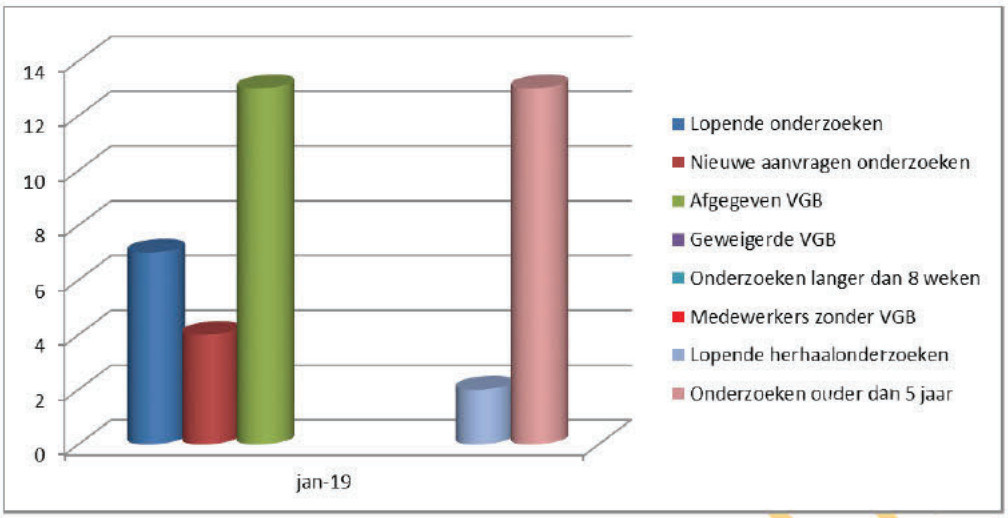
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand januari.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In januari waren er geen tijdelijke medewerkers aan het werk met een waiver zonder VGB.
Er zijn nu binnen de NCTV 13 medewerkers werkzaam met een VGB ouder dan 5 jaar.



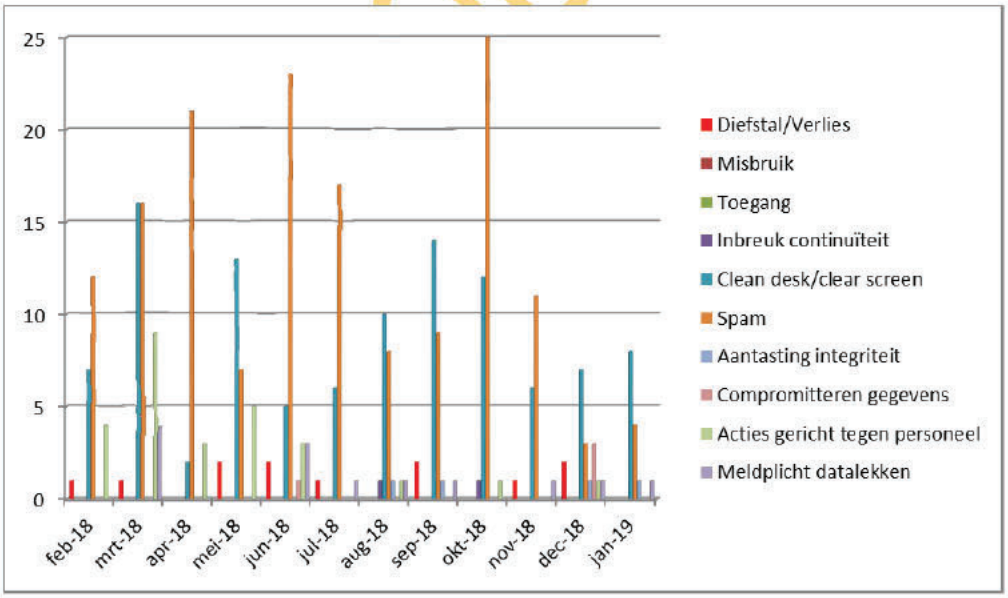
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



Beeld veiligheidsonderzoeken januari

Incidentenregistratie

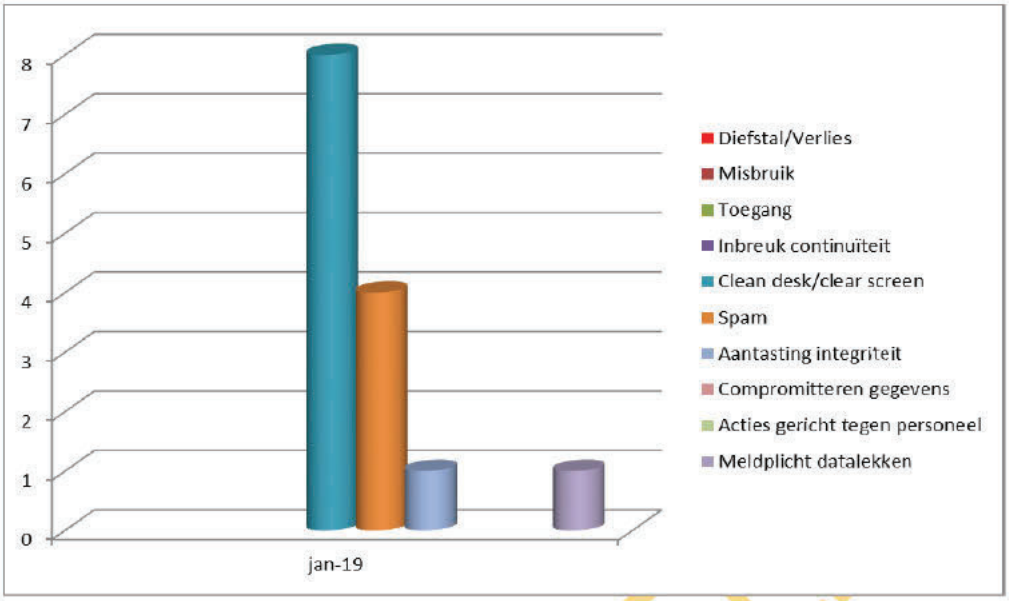
Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
27-02-2019



Beeld beveiligingsincidenten januari

Toelichting tabellen

Cleandesk

- In januari is bij [redacted] (1x) de kluissleutel aangetroffen in een kluis. De kluissleutel is veiliggesteld door de beveiligingsmedewerkers. De leidinggevende is geïnformeerd en heeft het besproken met de medewerkers. Er zijn 7 [redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In januari zijn 4 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Aantasting Integriteit

- In januari is een melding gedaan van niet afgeschermde zaken van de NCTV in [redacted]. Het [redacted] team heeft dit opgepakt en zal meer communiceren naar medewerkers. De problemen binnen [redacted] zijn bekend en worden niet gezien als een meldingsplichtige melding datalekken.

Datalekken

- Er is melding gedaan door een medewerker over een datalek bij [redacted]. De medewerker had tijdens een dienstreis een verblijf in het hotel. Bij de hack van data zijn gegevens van de medewerker buitgemaakt. Het betreft paspoortgegevens en het zakelijk mailadres. De medewerker heeft zich gemeld bij het meldpunt en daar waar mogelijk zelf maatregelen getroffen.

Overige

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
27-02-2019

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden, had in januari één verdachte situatie gedetecteerd op het . Het betrof een Dos attack via een IP adres. De poging is door de filters gestopt.
De beschikbaarheid van de kritieke informatiesystemen was 99.99 % in de maand januari.

Veiligheidsbewustzijn
De campagne van de voor veiligheidsbewustzijn is begonnen. De campagne duurt een aantal maanden, "Ook jouw informatie is interessant genoeg voor spionage". De NCTV maakt gebruik van de middelen en volgt de campagne. In samenspraak met wordt informatie op intranet geplaatst.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
Programmaraad NCTV
MT NCTV

Kern Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
13 maart 2019

Ons kenmerk
123456

nota

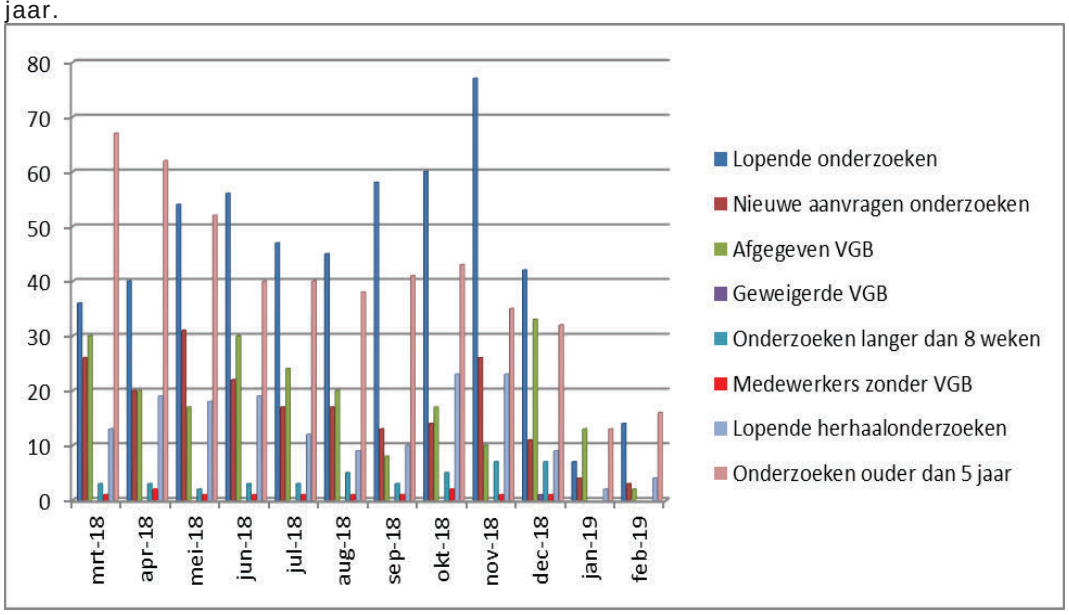
Managementrapportage februari 2019
Programma Integrale Beveiliging

Van
Hoofd[redacted]
Datum/eindparaaf

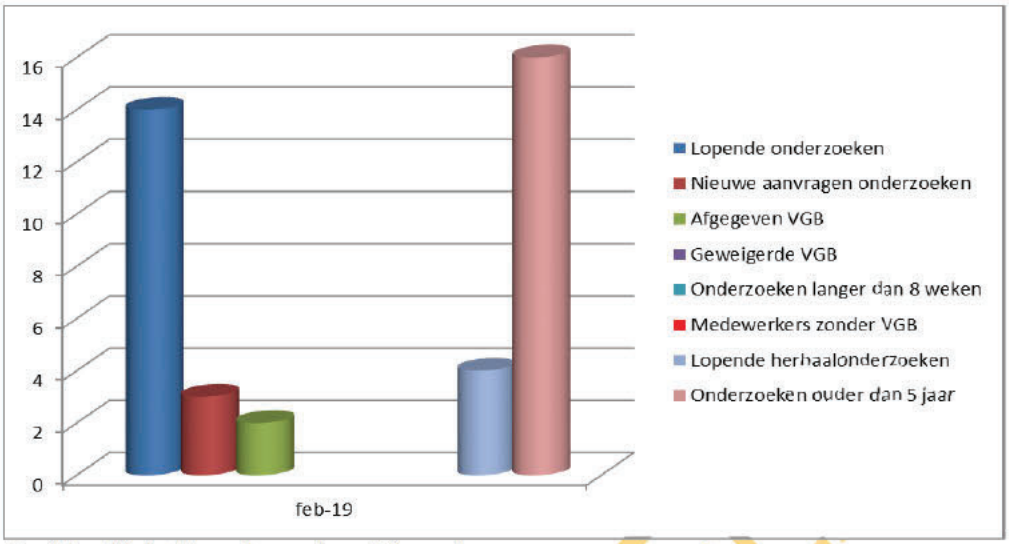
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand februari.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In februari waren er geen tijdelijke medewerkers aan het werk met een waiver zonder VGB.
Er zijn nu binnen de NCTV 16 medewerkers werkzaam met een VGB ouder dan 5 jaar.



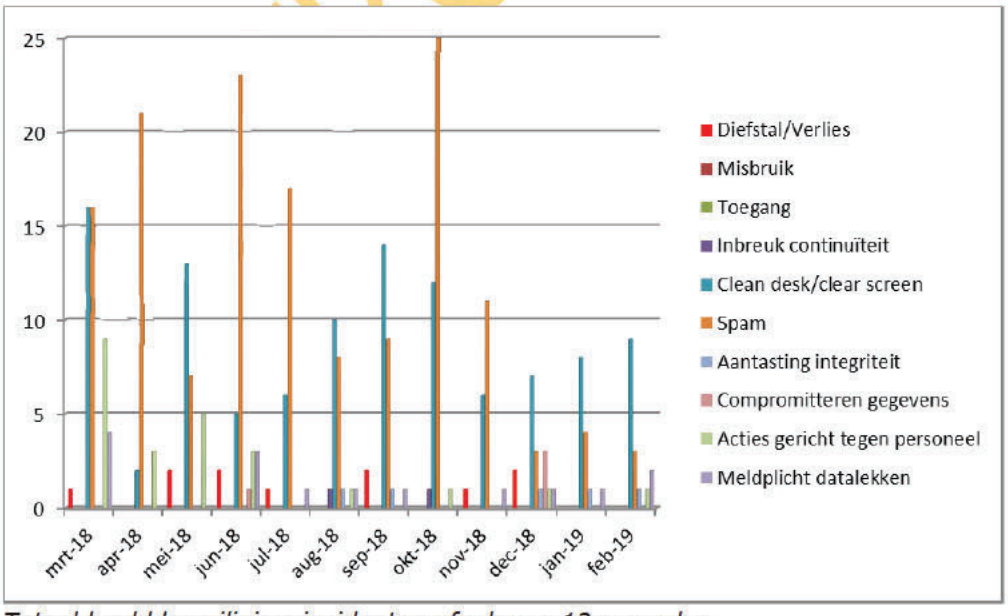
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



Beeld veiligheidsonderzoeken februari

Incidentenregistratie

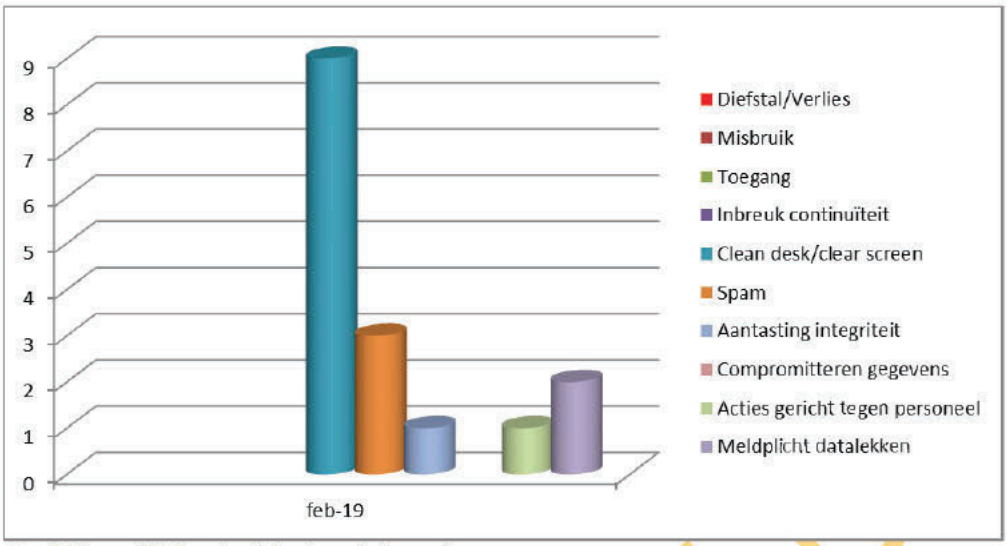
Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
13-03-2019



Beeld beveiligingsincidenten februari

Toelichting tabellen

Cleandesk

- In februari is bij [redacted] (1x) de kluissleutel aangetroffen in een kluis. De kluissleutel is veiliggesteld door de beveiligingsmedewerkers. De leidinggevende is geïnformeerd en heeft het besproken met de medewerkers. Bij het [redacted] (1x) is de sleutelkluis open aangetroffen. Er zijn 7 [redacted]-sticks [redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In februari zijn 3 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Aantasting Integriteit

- In februari is in een zaak de naam van een ambtenaar naar voren gekomen. De NCTV heeft hiervan melding gemaakt bij de leiding van de andere organisatie.

Actie gericht tegen personeel

- [redacted]

Datalekken

- Er zijn twee meldingen gedaan over kwetsbaarheden in zaken die in [redacted] stonden. In beide gevallen is er een melding gedaan bij de beheerder en zijn zaken aangepast. Het projectteam [redacted] neemt het ook mee in de communicatie naar gebruikers.

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
13-03-2019

Overige

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden, had in februari geen verdachte situaties gedetecteerd op het [redacted].
De beschikbaarheid van de kritieke informatiesystemen [redacted] was 100 % in de maand februari.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
Programmaraad NCTV
MT NCTV

Kern Bedrijfsvoering
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T

Datum
3 april 2019

Ons kenmerk
123456

nota

Managementrapportage maart 2019
Programma Integrale Beveiliging

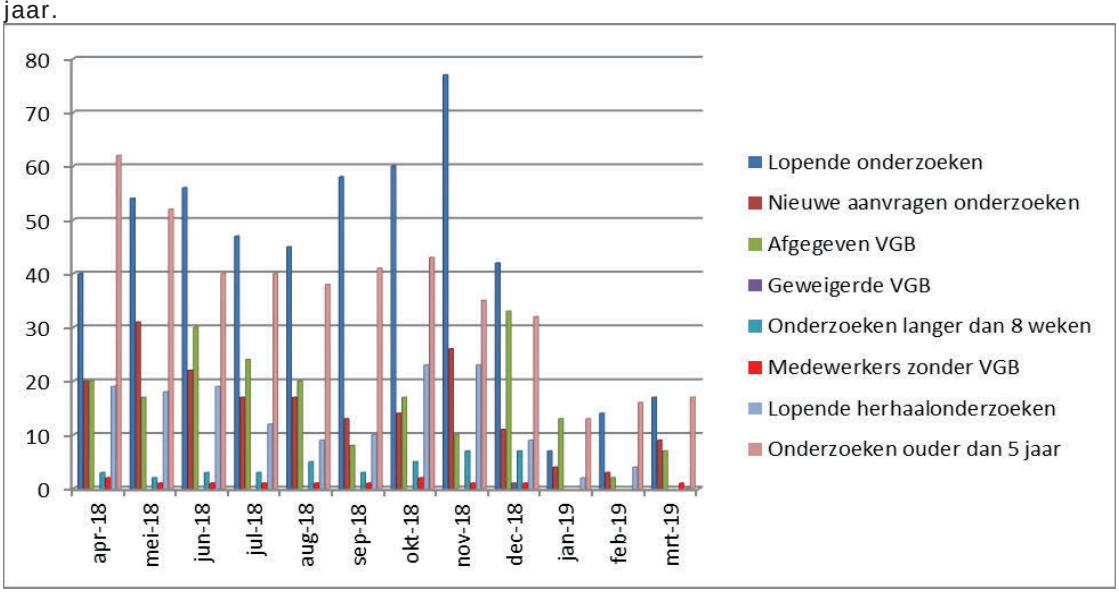
Van

Datum/eindparaaf

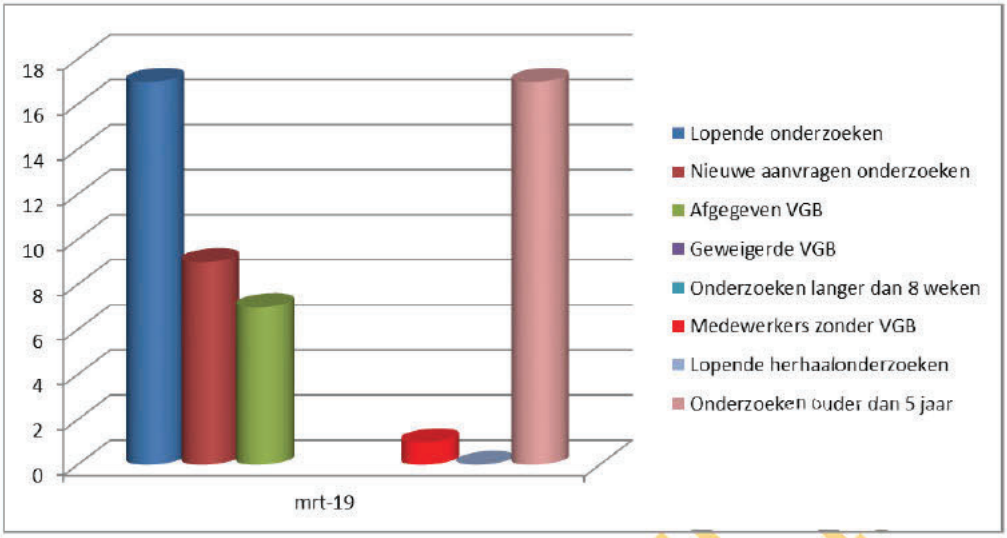
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand maart.

Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In maart was er één tijdelijke medewerker aan het werk met een waiver zonder VGB (bij NCTV).
Er zijn nu binnen de NCTV 17 medewerkers werkzaam met een VGB ouder dan 5 jaar.



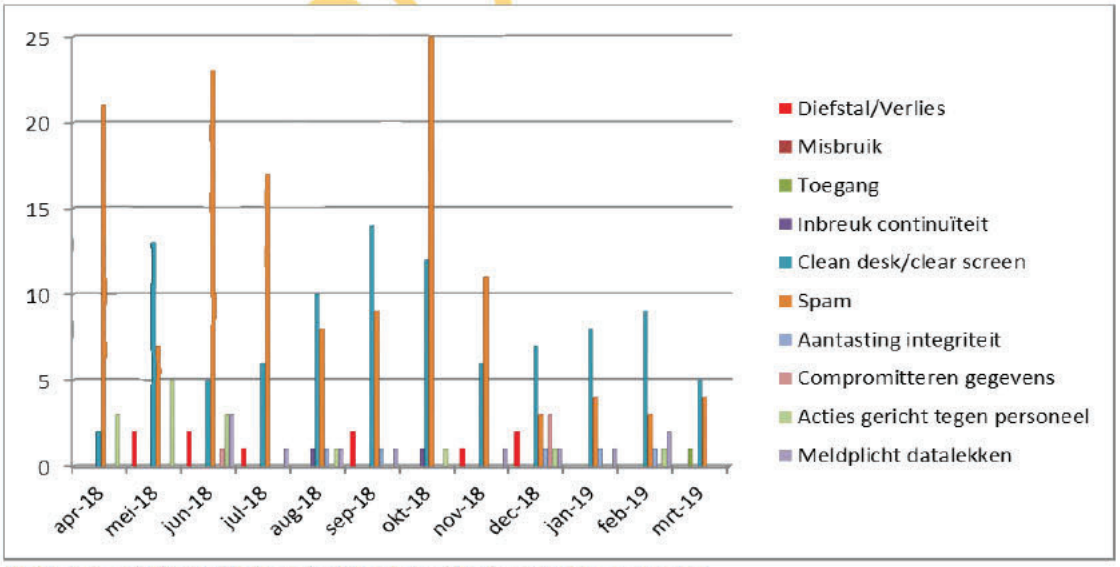
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



Beeld veiligheidsonderzoeken maart

Incidentenregistratie

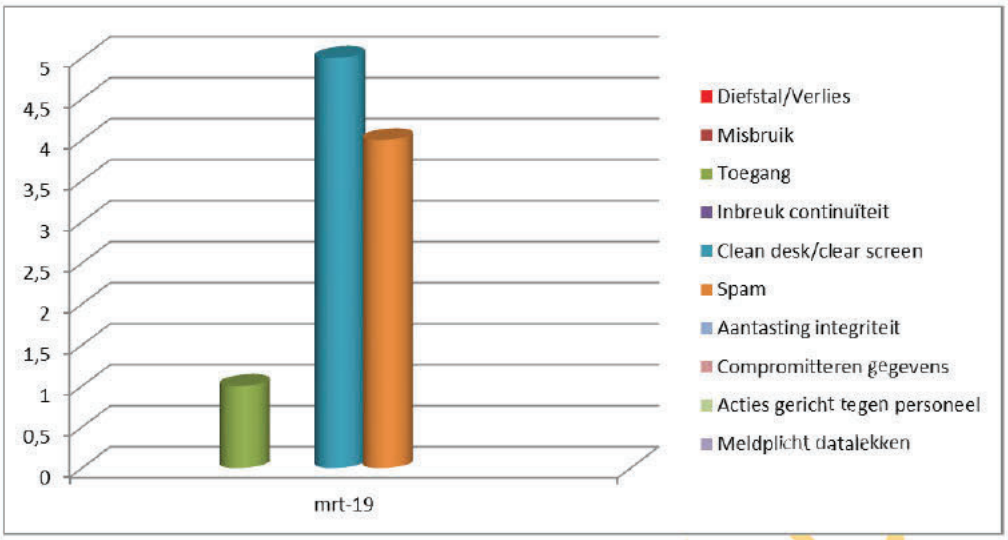
Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
03-04-2019



Beeld beveiligingsincidenten maart

Toelichting tabellen

Toegang

- Een bezoeker van [redacted] is meegelopen met een schoonmaakster door een goederensluis op de 7e etage. [redacted] gaat een gesprek aan met de bezoeker. De zaak is nog niet afgerond.

Cleandesk

- In maart is bij [redacted] (1) en [redacted] (1x) de kluissleutel aangetroffen in een kluis. De kluissleutel is veiliggesteld door de beveiligingsmedewerkers. Er zijn 2 tokens/USB-sticks (1 x [redacted]) aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers.

SPAM/Phising mail

- In maart zijn 4 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Overige

[redacted]

Het bedrijf [redacted] was slachtoffer geworden van een hack. Het bedrijf [redacted] heeft bekend gemaakt dat hun interne bedrijfsnetwerk gehackt is door een criminele actor. Het is vooralsnog onbekend welke informatie daarbij gestolen is. [redacted] geeft aan dat er op dit moment geen aanwijzingen zijn dat de beveiliging van producten en diensten van [redacted] zijn getroffen door deze hack. De hack is nog in onderzoek. [redacted] is één van de grootste aanbieders van virtuele private netwerken (VPN) en telewerkvoorzieningen ter wereld. [redacted]

[redacted] *certificaten*

[redacted] heeft gemeld dat zij hebben geconstateerd dat een deel van de [redacted]-overheidscertificaten niet voldoen aan de eisen zoals gesteld voor certificaten. In

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
03-04-2019

Nederland raakt dit ongeveer 22.000 overheid-certificaten. Deze certificaten zijn uitgegeven in de periode van 30 september 2016 t/m 5 maart 2019. heeft de uitgevende certificaatautoriteit opgedragen de betreffende certificaten binnen 30 dagen in te trekken en te vervangen. Op dit moment heeft dit nog geen gevolgen voor de certificaten die door de NCTV worden gebruikt in systemen.

Integriteit
Een medewerker heeft in een artikel op internet zijn mening gegeven over de mogelijke schending van persoonsgegevens bij de aanbesteding en keuze van voor de levering van kaarten.
De medewerker was op internet herleidbaar naar zijn werkgever ( ). Hierdoor bestond de mogelijkheid dat de mening van de medewerker gelezen kon worden als de visie van de werkgever. Tevens was de met persoonsgegevens in het artikel toegevoegd. De medewerker is door de leidinggevende op het voorval aangesproken en aan BZK is als documenteigenaar voorgelegd of ze een datalek melding willen doen. De MT leden NCTV zijn over de casus geïnformeerd.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~**Dep. VERTROUWELIJK**~~
Programmaraad NCTV
MT NCTV

Kern Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
T [redacted]

Datum
27 mei 2019

Ons kenmerk
123456

nota

Bedrijfsvoeringsrapportage april 2019
Programma Integrale Beveiliging

Van
[redacted]
Datum/eindparaaf

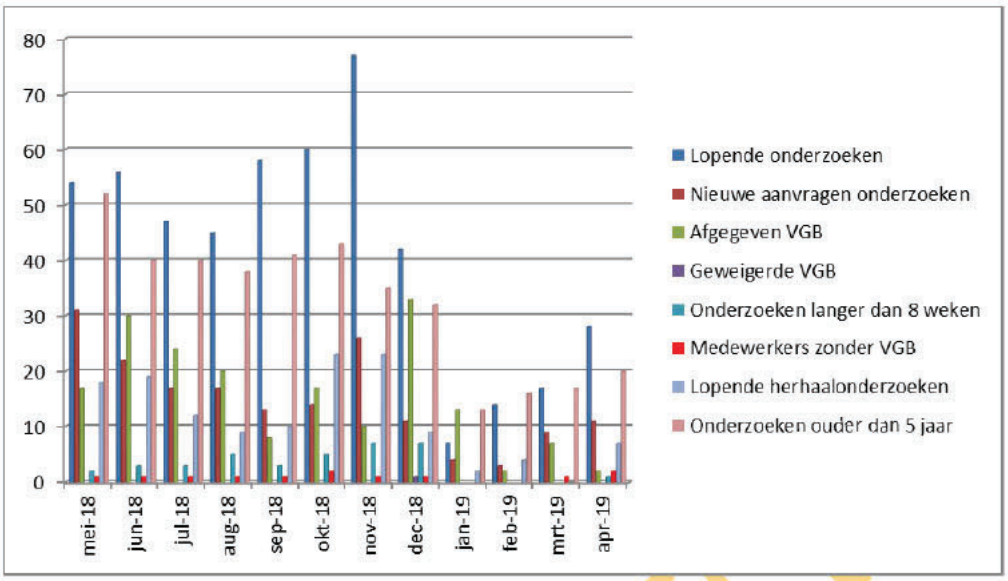
Advies
Ter kennisneming.

Toelichting
Bijgaand ontvangt u de rapportage over de maand april.
De maandrapportage van het Programma Integrale Beveiliging is onderdeel van de bredere Bedrijfsvoeringsrapportage. De komende maanden zal een verdere integratie van de rapportages plaats vinden.

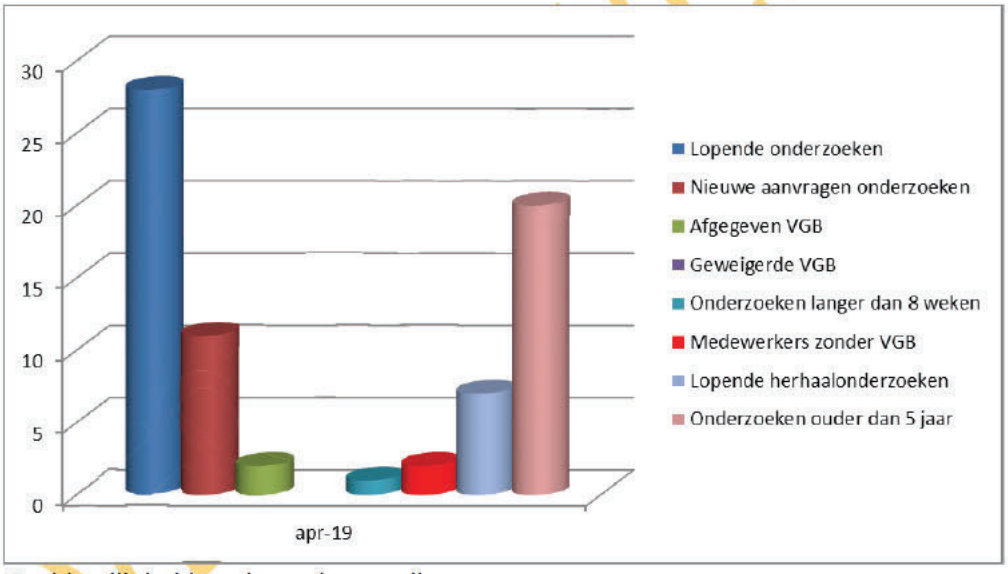
Veiligheidsonderzoeken
Een veiligheidsonderzoek is een (wettelijke) vereiste om te kunnen werken binnen de NCTV op een vertrouwensfunctie. In april waren er [redacted] tijdelijke medewerkers aan het werk met een waiver zonder VGB ([redacted]).
Er zijn nu binnen de NCTV 20 medewerkers werkzaam met een VGB ouder dan 5 jaar.
Overzicht herhaalonderzoeken;
Uitzondering ivm vertrek; [redacted].
Lopende onderzoeken; [redacted]
Verzoek verzonden voor een herhaalonderzoek; [redacted]
Rappels voor het aanleveren van aanvragen;, [redacted]

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
03-04-2019



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden



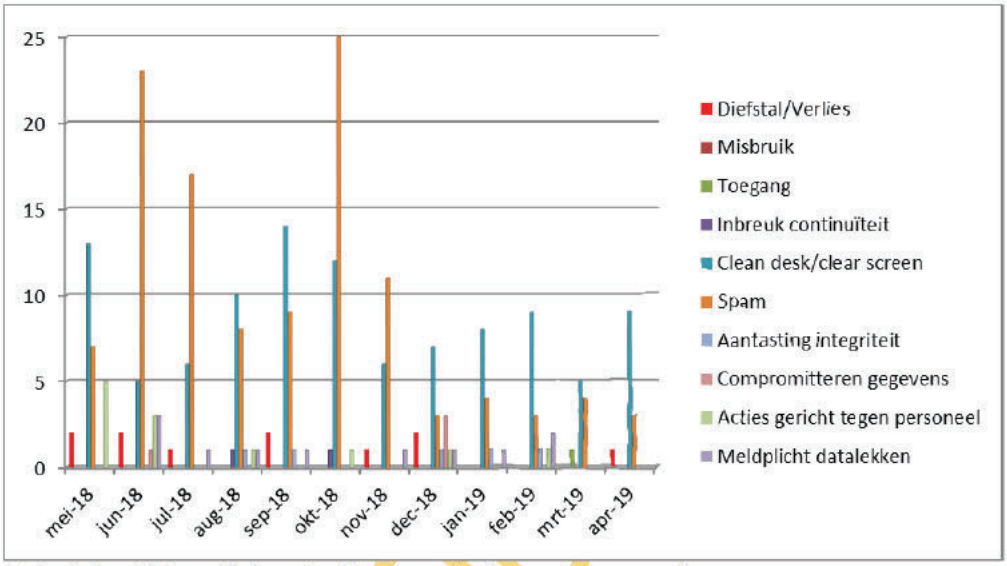
Beeld veiligheidsonderzoeken april

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

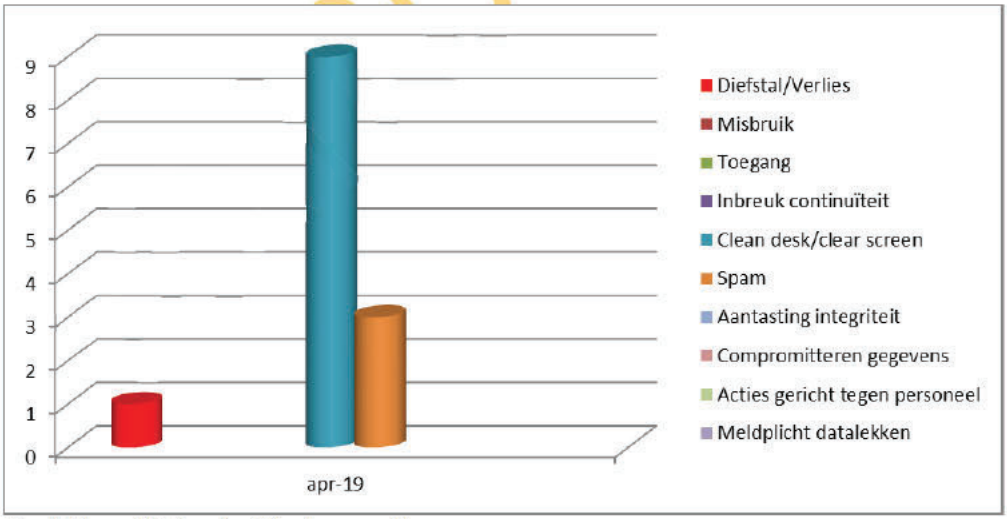
Datum
03-04-2019

Incidentenregistratie

Om een beeld te geven over de aard van de incidenten is een maandoverzicht van de beveiligingsincidenten gemaakt.
Ernstige incidenten worden direct aan de lijnmanager gemeld.
Het is de verantwoordelijkheid van de leidinggevende om beveiligingsincidenten (incl. datalekken) af te handelen en maatregelen te treffen om de schade van een incident te beperken en om herhaling in de toekomst te voorkomen.



Totaal beeld beveiligingsincidenten afgelopen 12 maanden



Beeld beveiligingsincidenten april

Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Datum
03-04-2019

Toelichting tabellen

Toegang
- Een medewerker is een token van het [redacted] verloren. Het token is geblokkeerd. Het risico is laag omdat het [redacted] bevat over het netwerk en alleen intern gebruikt kan worden.

Cleandesk
- In april is bij [redacted] (2x) de kluissleutel aangetroffen in een kluis. De kluissleutel is veiliggesteld door de beveiligingsmedewerkers. Bij [redacted] is (1x) de sleutelkluis open aangetroffen. Er zijn 4 tokens/USB-sticks ([redacted] aangetroffen en opgeborgen in de kluis door de beveiligingsmedewerkers. Bij [redacted] een laptop aangetroffen en deze is veiliggesteld. Bij een [redacted] is een [redacted] document aangetroffen van [redacted].

SPAM/Phising mail
- In april zijn 3 meldingen van spam en phising mail binnengekomen. De meldingen zijn doorgestuurd naar [redacted]

Overige

Beschikbaarheid internet
Een aantal malen was internet niet beschikbaar in de avonduren bij de FrontOffice NCC. Hiervan is melding gemaakt bij [redacted] omdat het invloed had op de beschikbaarheid en bereikbaarheid. Het onderzoek loopt nog.

Onbevoegd toegang
Op een applicatie [redacted] bij een externe leverancier werd ontdekt dat iemand rechten had gekregen zonder toestemming. De leverancier heeft het onderzocht en er bleek sprake van een menselijk fout dat iemand rechten had gekregen tot de verkeerde groep. Er zijn aanvullende afspraken gemaakt.

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden, had in april een DDOS aanval vanaf [redacted] IP adressen gedetecteerd en tegen gehouden op het [redacted]
De beschikbaarheid van de kritieke informatiesystemen [redacted] was 100 % in de maand april.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon

Datum
05-02-2018

Ons kenmerk
-

nota

Rapportage Integrale Beveiliging 2017

Van
Hoofd
Datum/eindparaaf

Inleiding

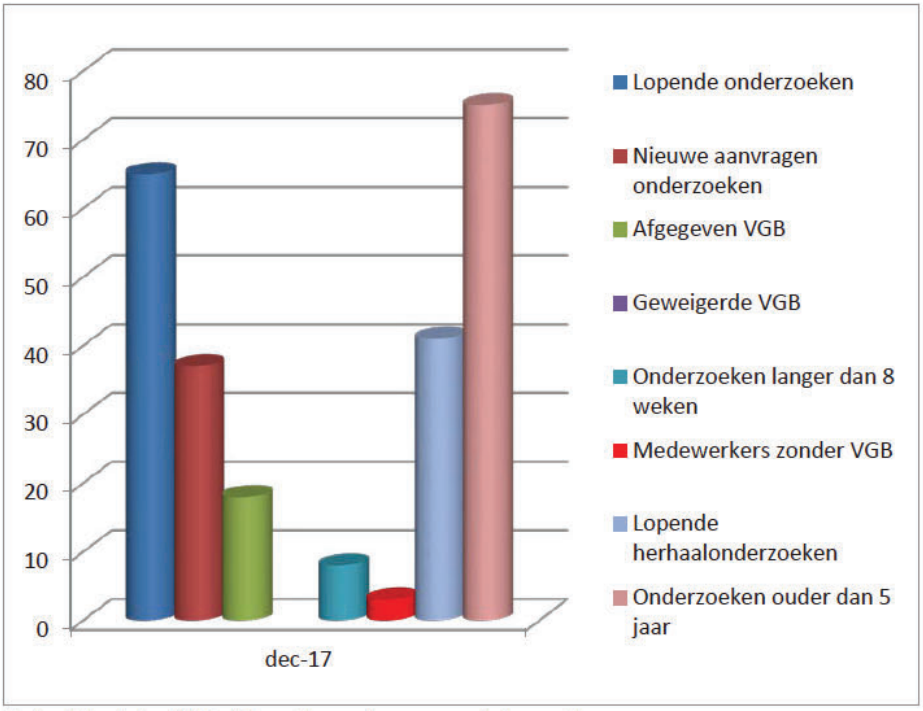
Bijgaand ontvangt u de jaarrapportage integrale beveiliging over 2017. De jaarrapportage geeft een beeld van de activiteiten die in samenwerking met de werkgroep beveiliging in 2017 zijn uitgevoerd, zijn beschreven in het Plan van Aanpak Interne Controle Risicobeheersing NCTV d.d. 13-02-2017 en het jaarplan 2017 .

Advies

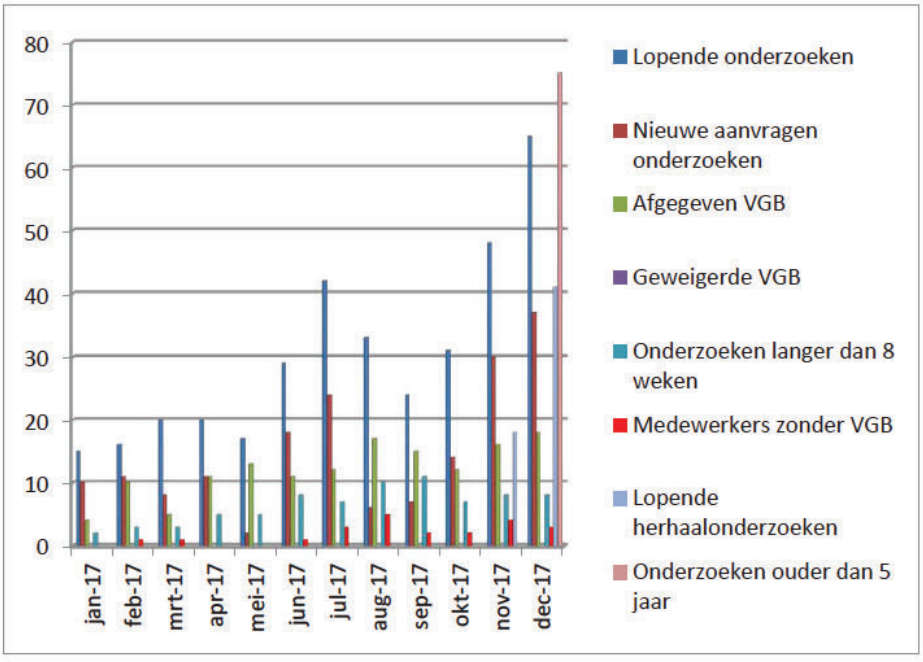
Zie oplegnota.

Veiligheidsonderzoeken

In 2017 is voor J&V besloten dat er een inhaalslag wordt gemaakt om herhaalonderzoeken uit te voeren bij medewerkers met een VGB ouder dan 5 jaar. Eind 2017 waren er binnen de NCTV 123 medewerkers werkzaam met een VGB ouder dan 5 jaar. In 2017 zijn er 44 aanvragen voor herhaalonderzoeken ingediend. Successievelijk worden medewerkers uitgenodigd om een aanvraag te doen. De SG JenV heeft alle dienstonderdelen de plicht op gelegd om binnen 5 jaar te zorgen dat alle medewerkers beschikken over een VGB niet ouder dan 5 jaar. Het proces binnen de NCTV verloopt naar tevredenheid.



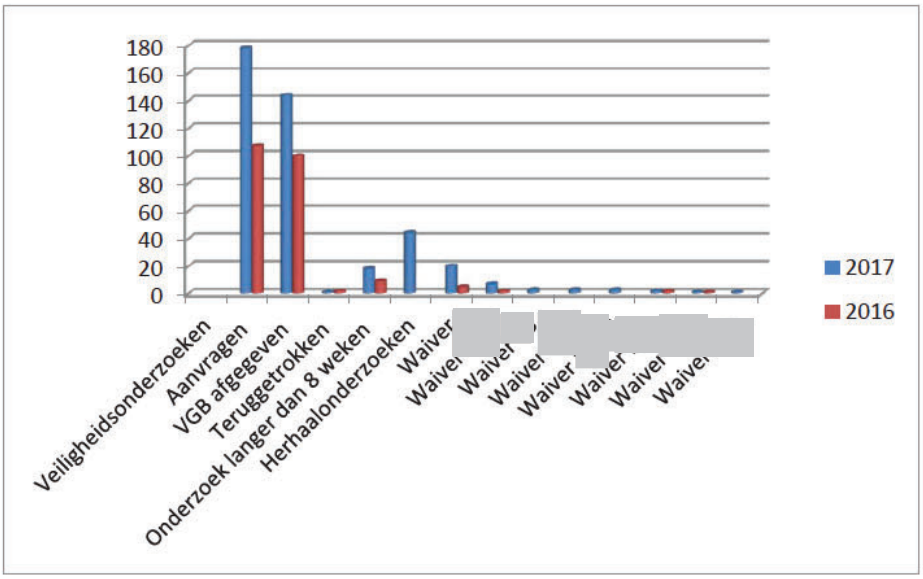
Totaal beeld veiligheidsonderzoeken maand december



Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Terugkijkend op 2017 zien we dat:

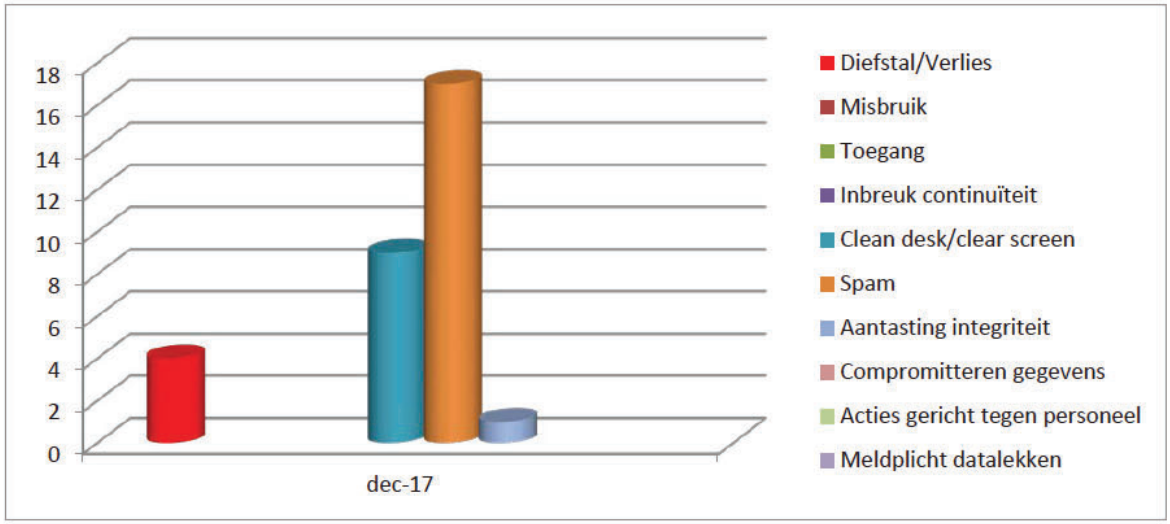
- In totaal 178 veiligheidsonderzoeken zijn aangevraagd (2016: 107).
- In totaal 144 VGB's zijn afgegeven (2016: 100).
- Eén kandidaat zich heeft teruggetrokken tijdens het lopende onderzoek (2016: 2x).
- 18 onderzoeken langer dan 8 weken hebben geduurd. Dit werd meestal veroorzaakt doordat de kandidaat langere tijd in het buitenland had gewoond en de AIVD aanvullende informatie op moest vragen bij een buitenlandse dienst (2016: 9).
- Er in 2017 20 medewerkers eerder zijn gestart met de uitvoering van hun werkzaamheden dan dat het veiligheidsonderzoek was afgerond. In al deze gevallen is een waiver met beperking van de autorisaties afgegeven door de NCTV.
  (2016: 5 medewerkers,)
- In 2017 zijn 44 verzoeken voor een herhaalonderzoek gedaan.



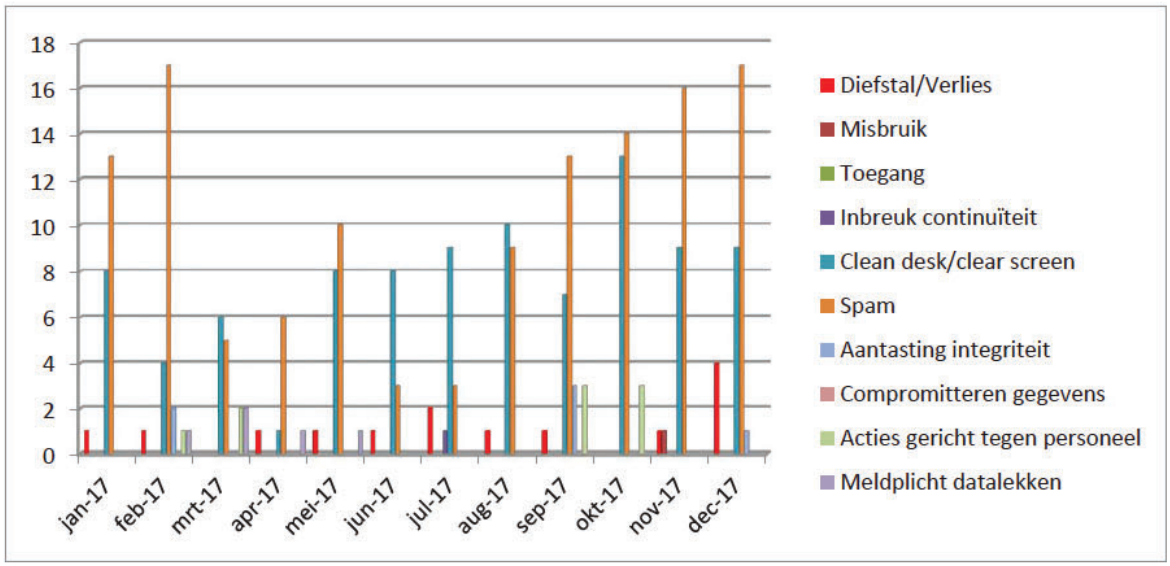
Conclusie;
Mede als gevolg van de invoer van de herhaalonderzoeken is het aantal aanvragen voor veiligheidsonderzoeken gestegen ten opzichte van 2016. Er is ook een duidelijke toename zichtbaar in het aantal verzoeken met een waiver van 5 in 2016 naar 20 in 2017. Verder zien we dat steeds meer onderzoeken langer duren dan de gebruikelijke verwachte termijn van 8 weken. Waarschijnlijk doordat jonge ambtenaren eerder werkzaamheden hebben verricht in het buitenland.

Beveiligingsincidenten

Datum
05-02-2018

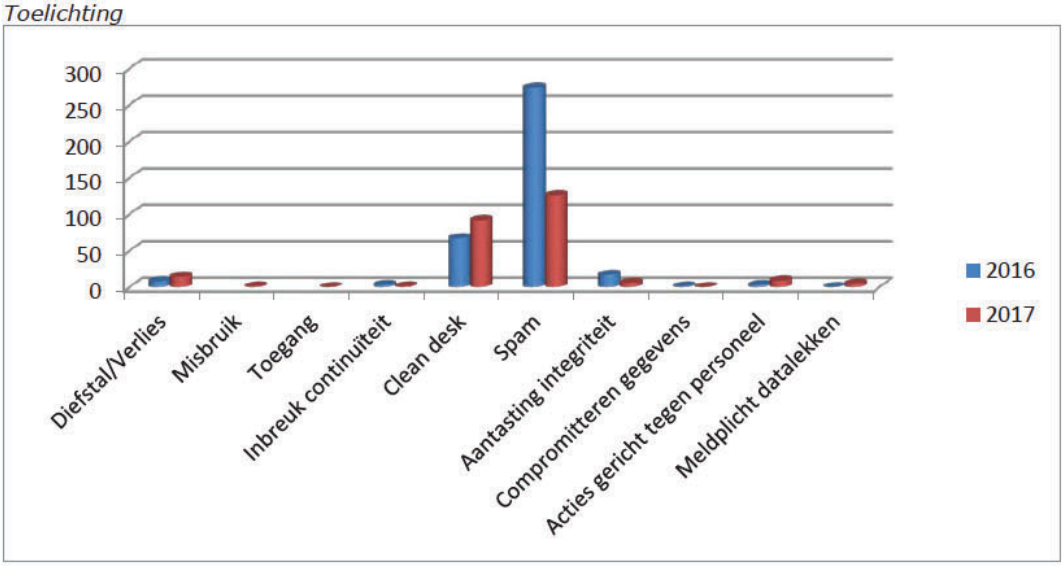


Beeld veiligheidsonderzoeken december



Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting



Terugkijkend op 2017 zien we dat:

- Medewerkers in 2017 1x Iphone, 3x rijkspas, 5x OV-kaart, [redacted] en 1x een [redacted] hebben verloren. (2016; 3 iPhones, 1 iPad, [redacted] en 1 rijkspas).
- Medewerkers 58 x zijn vergeten hun [redacted] veilig op te bergen. (2016: 51x)
- Medewerkers 19 X zijn vergeten een kluis af te sluiten. (2016: 4x)
- We 5x een datalek hebben moeten melden bij de Autoriteit Persoonsgegevens. (2016: 1x).

Controle autorisaties

We controleren in samenwerking met leidinggevenden de autorisaties op het [redacted] en voor de rijkspassen. Het is belangrijk dat bedrijfsvoering tijdig op de hoogte is van een verandering van functie of het vertrek van een medewerker en dat autorisaties op tijd kunnen worden ingetrokken.

Kwetsbaarheden websites

Om na te gaan of websites, voorzien zijn van een update, of kwetsbaarheden vertonen heeft de Audit Dienst Rijk (ADR) pentesten uitgevoerd op 9 websites. De door de ADR geconstateerde kwetsbaarheden in de geteste websites zijn verholpen.
De NCTV heeft meldingen van kwetsbaarheden (responsible disclosures) ontvangen van 3 websites. De kwetsbaarheden zijn opgelost. In 2017 zijn 19 websites opgeheven.

Periodieke testen

In 2017 heeft de [redacted] maandelijks testen uitgevoerd op de actieve inbraak/bewegingsdetectoren in de beveiligingsinstallatie. Deze detectoren geven in normale omstandigheden geen alarm en moeten daarom apart worden getest om na te gaan of ze niet defect zijn. Onvolkomenheden zijn aan [redacted] gemeld voor reparatie.

Elektronische veiligheidsonderzoeken

[redacted]

In 2017 zijn er geen verdachte omstandigheden of voorzieningen aangetroffen.

Te Beschermen Belangen/Kwetsbaarheidsanalyse Spionage (KWAS)

In 2017 is een zelfanalyse KWAS uitgevoerd. Hiervan is een aparte rapportage opgesteld voor het MT.

Baseline Informatiebeveiliging Rijksdienst

De ICV (in control verklaring) BIR (Baseline Informatiebeveiliging Rijksdienst) voor 2017 is opgesteld. Daarin wordt de status vermeld van nog te nemen- en reeds genomen maatregelen in het kader van de BIR. De ICV is een jaarlijkse verplichte rapportage die onder andere naar de SG JenV en BZK wordt gezonden. De ADR voert steekproeven uit bij organisaties om te controleren of de grondslag voor de ICV wel op de juiste feiten is gebaseerd. In 2017 heeft de ADR een steekproef uitgevoerd bij de NCTV. De steekproef heeft geen tekortkomingen opgeleverd.
In samenwerking met de NCTV heeft [redacted] een projectleider aangesteld die de ICV BIR en AVG verplichting voor de [redacted] gaat uitvoeren. De verantwoordelijkheid ligt hier bij [redacted] maar de NCTV moet ook aantonen dat zij ‘in control’ is voor het beheer van de toegangscontrole ten aanzien van rijkspas autorisaties en opslag van biometrische gegevens van haar medewerkers.

Algemene Verordening Gegevensbescherming

In samenspraak met het juridisch cluster is er een projectleider aangetrokken voor de implementatie van de AVG (Algemene verordening gegevensbescherming). Doel van het project is dat de NCTV aan alle verplichtingen van de AVG voldoet op 28 mei 2018 (eis vanuit de EU).

Integriteit

In 2017 zijn de Gedragscode voor de Digitale werkomgeving en de Gedragscode Integriteit Rijk geïmplementeerd binnen JenV en de NCTV. In samenwerking met de Integriteitcoördinator JenV en Vertrouwenspersonen NCTV zijn de diverse documenten onder de aandacht gebracht bij de leidinggevenden en de medewerkers.

Update beleidsdocumenten
De NCTV heeft in 2017 enkele documenten van het Programma Integrale Beveiliging, in het kader van voortschrijdend inzicht en ontwikkelingen, geactualiseerd. Dit betreft:
- Omgaan met Vertrouwensfuncties;
- Rubriceringsmethodiek;
- Fysieke Beveiliging NCTV;
- Cryptobeleid;
- Patchmanagement.

Veiligheidsbewustzijn
- Het afgelopen jaar zijn er diverse initiatieven geweest om het veiligheidsbewustzijn onder de medewerkers van de NCTV te vergroten. In samenwerking met de werkgroep beveiliging is de 'week van de veiligheid' gehouden. Tijdens deze week hebben diverse onderwerpen zoals cleandesk, rubriceren en privacy extra aandacht gekregen.
- In samenwerking [redacted] zijn er voorlichtingssessies gehouden bij alle directies over digitale kwetsbaarheden.
- Er zijn factsheets (met tips en handelingsperspectieven) gemaakt over diverse onderwerpen zoals; gebruik smartphone, gebruik social media, gebruik facebook en gebruik [redacted].
- Een rubriceringskaart is gemaakt voor alle medewerkers die hen kan helpen bij het verwerken van gerubriceerde informatie. De factsheets zijn uitgereikt en op het intranet voor de medewerkers beschikbaar.
- Alertonline is onder de aandacht gebracht bij de medewerkers.
- Tenslotte heeft de NCTV deelgenomen aan de awareness campagne van JenV over phishing-mails. Medewerkers hebben diverse berichten ontvangen en voorlichting met handelingsperspectieven gekregen.

[redacted]

[redacted]
Binnen de organisatie bestond de behoefte om op een veiligere manier informatie te delen [redacted]. In samenwerking met [redacted] is het product [redacted] aangeschaft en na een risico-analyse in beheer genomen bij [redacted].
Het product is beschikbaar voor alle medewerkers en tijdelijk voor onze partners tijdens een opschaling, crisis of calamiteit.

Toezicht [redacted]
De [redacted] houdt toezicht op de uitvoering van (inter)departementale regelgeving en beleidskaders bij de diverse dienstonderdelen. De toetsing vindt jaarlijks plaats. De NCTV had geen tekortkomingen het afgelopen jaar. Het enige aandachtspunt is het vastleggen van afspraken met de concerndienstverleners.

Afvoer hardware

Er is een inzamelingsactie gehouden voor het veilig afvoeren van hardware voor zowel oude producten van de NCTV als oude producten van medewerkers. De producten waarop mogelijk nog informatie aanwezig was, zijn versnipperd en de overige producten zijn afgevoerd via de Domeinen.

Peer review

In het kader van de collegiale toetsing heeft de de processen onderzocht en aanbevelingen gedaan. Alle aanbevelingen zijn overgenomen. In Q1 2018 verwachten we de laatste aandachtspunten te hebben overgenomen.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
Programmaraad

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Kern Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon

oplegnota

Jaarrapportage 2018 en jaarplan 2019
Programma Integrale Beveiliging

Datum
13 februari 2019

Ons kenmerk

Van
Hoofd
Datum/eindparaaf

Advies

Instemmen met de volgende adviezen.

Zie bijlage, 'Jaarrapportage 2018 Integrale Beveiliging';

- In 2018 is er 54 maal een melding gemaakt van kluissleutels die werden aangetroffen in kluizen. In 2017 was dat 19 maal.
- In 2018 is er 13 maal melding gemaakt van een datalek. In 2017 was dat 5 maal.

We zien, in 2018, een toename op beveiligingsissues die zich voor doen binnen de organisatie. Gesteld mag worden dat veiligheidsbewustzijn continue aandacht en sturing behoeft van het management.

- Het advies is dan ook om in afdelingsoverleggen hier blijvend aandacht aan te besteden en eventuele lacunes in informatie of behoeften te melden zodat de het management nog beter kan faciliteren.

Zie bijlage, 'Interne controle risicobeheersing 2019' ter kennisneming;

- De zal de aanvragen voor pentesten van websites coördineren maar heeft daarbij wel de instemming nodig van de eigenaren. Tevens vragen wij de eigenaren kritisch te zijn over het voortbestaan van de websites.
- Voor de implementatie van de BIR2017 hebben we ondersteuning nodig van de eigenaren van kritieke systemen
- Voor de doorontwikkeling van het en hebben we voldoende capaciteit nodig en informatie over de werkprocessen. Bij een veranderende organisatie is het belangrijk om de behoeften van de projecten en programma's tijdig kenbaar te maken bij de (bijvoorbeeld tijdens de accountgesprekken).
- Alle verwerkingen van persoonsgegevens waarop de AVG van toepassing is dienen geheel op orde te zijn. De verwacht dan ook een actieve houding en betrokkenheid van de managers om te voldoen aan onze plicht.

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Kern Bedrijfsvoering

Datum
13 februari 2019

Ons kenmerk

- De NCTV is gestart met de uitvoering van de herhaalonderzoeken voor alle medewerkers die een VGB hebben die ouder is dan 5 jaar. De verantwoordelijkheid voor de uitvoering van deze herhaalonderzoeken ligt bij de leidinggevenden waarbij de [redacted] ondersteunt, coördineert, faciliteert en rapporteert.
- Maak ook in 2019 incidenten bespreekbaar binnen de afdelingen. Het bespreekbaar maken versterkt het veiligheidsbewustzijn.
- Periodiek worden overzichten met autorisaties voorgelegd aan de leidinggevenden. De verantwoordelijkheid voor het toekennen van autorisaties ligt bij de leidinggevenden, de uitvoering hiervan ligt bij de [redacted]. Indien de [redacted] niet tijdig op de hoogte wordt gesteld van een interne overplaatsing of het beëindigen van een dienstverband dan kan een medewerker ongeautoriseerd toegang houden tot (gerubriceerde) informatie.
- Wees kritisch vanuit het principe ‘need to know’ bij het toekennen van autorisaties. Het risico op interne dreigingen (Insider Threats) neemt toe.
- In het kader van de informatieveiligheid is het belangrijk dat de manager en de medewerker voldoende kennis hebben om informatie op een juiste en veilige wijze te verwerken in een Document Management Systeem [redacted]). De [redacted] zal ondersteuning bieden vanuit het [redacted] en [redacted] project. De managers dienen voldoende zicht te hebben op de werkprocessen.
- De controle op de beschikbaarheid van voorzieningen door [redacted] en [redacted] op de [redacted] kan verbeterd worden.

Toelichting
In het kader van de ‘Plan Do Check Act’ (PDCA) cyclus stellen we jaarlijks een rapportage op over de resultaten, bevindingen en gebeurtenissen die zich in dat jaar hebben voorgedaan en die extra aandacht behoefden vanuit het Programma Integrale Beveiliging. Vervolgens beschrijven we in het jaarplan ‘Interne controle risicobeheersing’ de nieuwe trends of ontwikkelingen die zich mogelijk zullen voordoen en de wijze waarop we de reeds bekende risico’s en maatregelen controleren op hun effectiviteit. Via de managementrapportages informeren wij u periodiek over de genoemde ontwikkelingen en nieuwe incidenten die zich hebben voorgedaan.

Bijlages;
‘Jaarrapportage 2018 integrale beveiliging’
‘Interne controle risicobeheersing 2019’

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~

Programmaraad

Kern Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
[redacted]

Datum
28 februari 2019

Ons kenmerk
-

nota

Rapportage Integrale Beveiliging 2018

Van
Hoofd [redacted]
Datum/eindparaaf

Inleiding

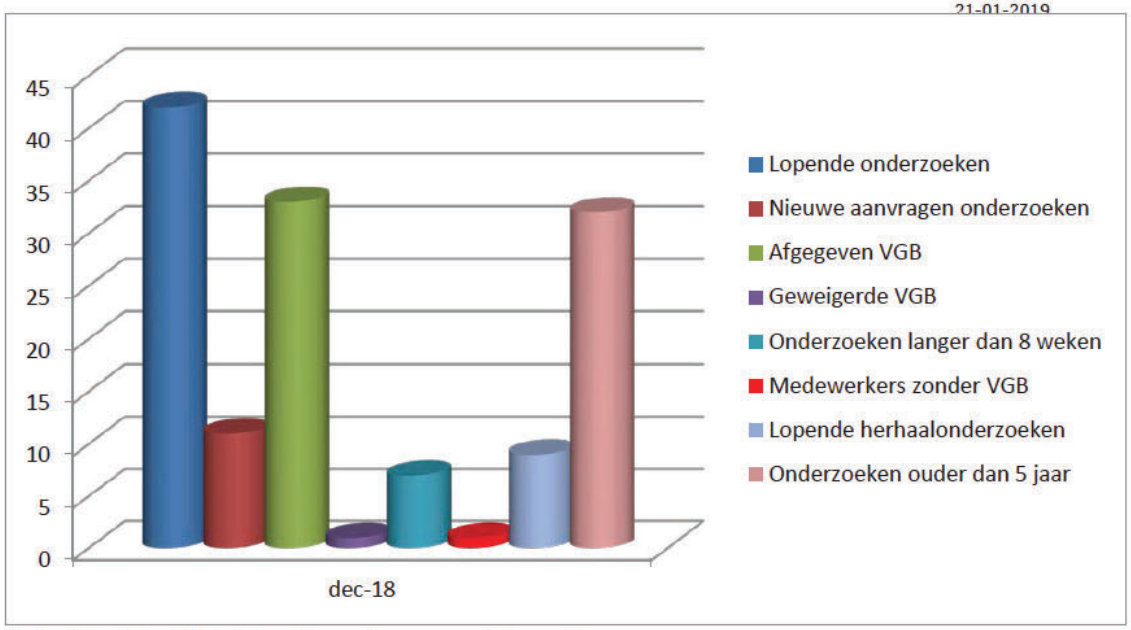
Bijgaand ontvangt u de jaarrapportage integrale beveiliging over 2018. De jaarrapportage geeft een beeld van de activiteiten die in samenwerking met de werkgroep beveiliging in 2018 zijn uitgevoerd, zijn beschreven in het Plan van Aanpak Interne Controle Risicobeheersing NCTV d.d. 17-01-2018 en het jaarplan 2018 van [redacted].

Advies

Zie oplegnota.

Veiligheidsonderzoeken

In 2017 is voor J&V besloten dat er een inhaalslag wordt gemaakt om herhaalonderzoeken uit te voeren bij medewerkers met een VGB ouder dan 5 jaar. Eind 2018 waren er binnen de NCTV 32 medewerkers werkzaam met een VGB ouder dan 5 jaar. Overigens is dat aantal op 1 januari 2019 door de transitie van NCSC gedaald naar 18 medewerkers. Op 1 november 2017 was dat aantal 126 medewerkers.
In 2018 zijn er 72 aanvragen voor herhaalonderzoeken ingediend. Successievelijk worden medewerkers uitgenodigd om een aanvraag te doen. De SG JenV heeft alle dienstonderdelen de plicht op gelegd om binnen 5 jaar te zorgen dat alle medewerkers beschikken over een VGB niet ouder dan 5 jaar. Het proces binnen de NCTV verloopt naar tevredenheid.



Totaal beeld veiligheidsonderzoeken maand december

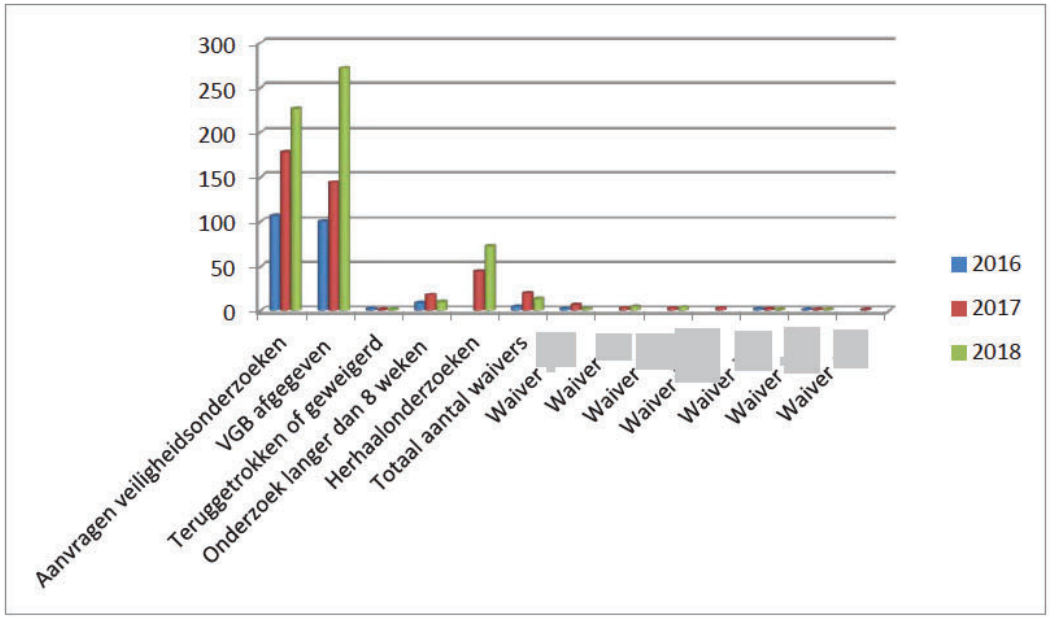
Totaal beeld veiligheidsonderzoeken afgelopen 12 maanden

Stafafdeling Bedrijfsvoering
Kern Bedrijfsvoering

Datum
21-01-2019

Terugkijkend op 2018 zien we dat:

- In totaal 226 veiligheidsonderzoeken (inclusief herhaalonderzoeken) zijn aangevraagd (2016: 107, 2017: 178).
- In totaal 272 VGB's zijn afgegeven (2016: 100, 2017: 144).
- [redacted]
- 10 onderzoeken langer dan 8 weken hebben geduurd. Dit werd meestal veroorzaakt doordat de kandidaat langere tijd in het buitenland had gewoond en de AIVD aanvullende informatie op moest vragen bij een buitenlandse dienst (2016: 9, 2017:18).
- Er in 2018 13 medewerkers [redacted] eerder zijn gestart met de uitvoering van hun werkzaamheden dan dat het veiligheidsonderzoek was afgerond. In al deze gevallen is een waiver met beperking van de autorisaties afgegeven door de NCTV. (2016: 5 medewerkers, [redacted] en (2017: 20 medewerkers [redacted]
- In 2018 zijn 72 verzoeken voor een herhaalonderzoek gedaan. (2017: 44)

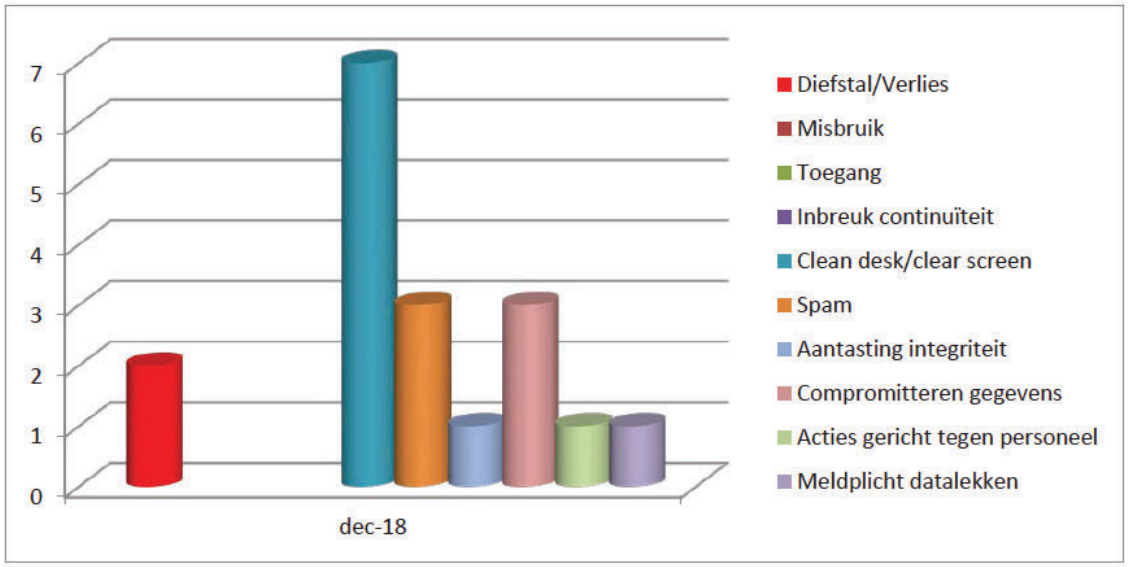


Conclusie;
Mede als gevolg van de invoer van de herhaalonderzoeken is het aantal aanvragen voor veiligheidsonderzoeken gestegen. Het aantal verzoeken om medewerkers met een waiver te laten starten is afgenomen. Verder zien we een afname van het aantal onderzoeken dat langer duurt dan de gebruikelijke verwachte termijn van 8 weken.

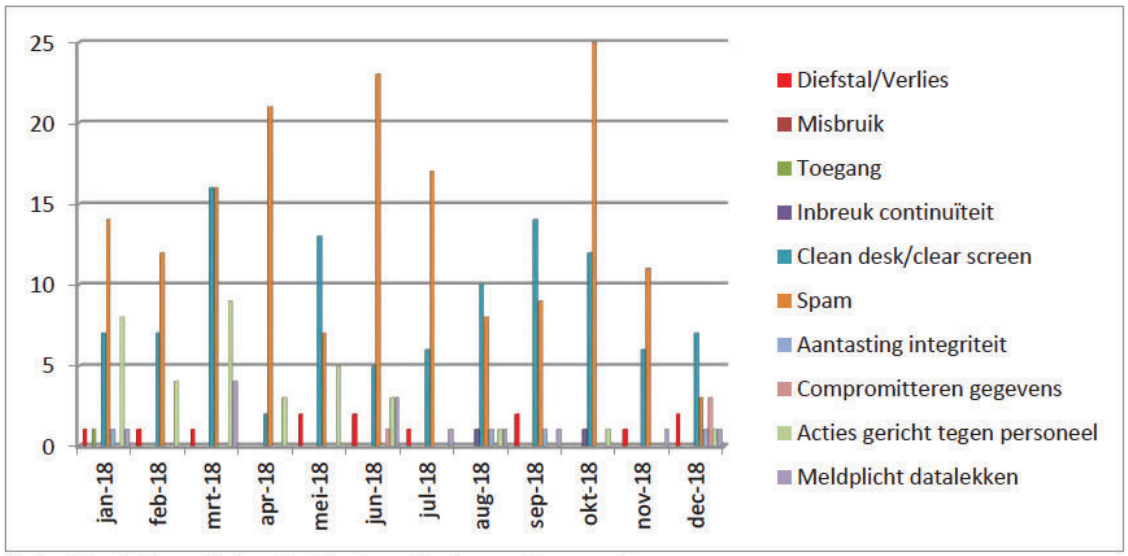
Stafafdeling
Bedrijfsvoering
Kern Bedrijfsvoering

Beveiligingsincidenten

Datum
21-01-2019



Totaal beeld beveiligingsincidenten december 2018

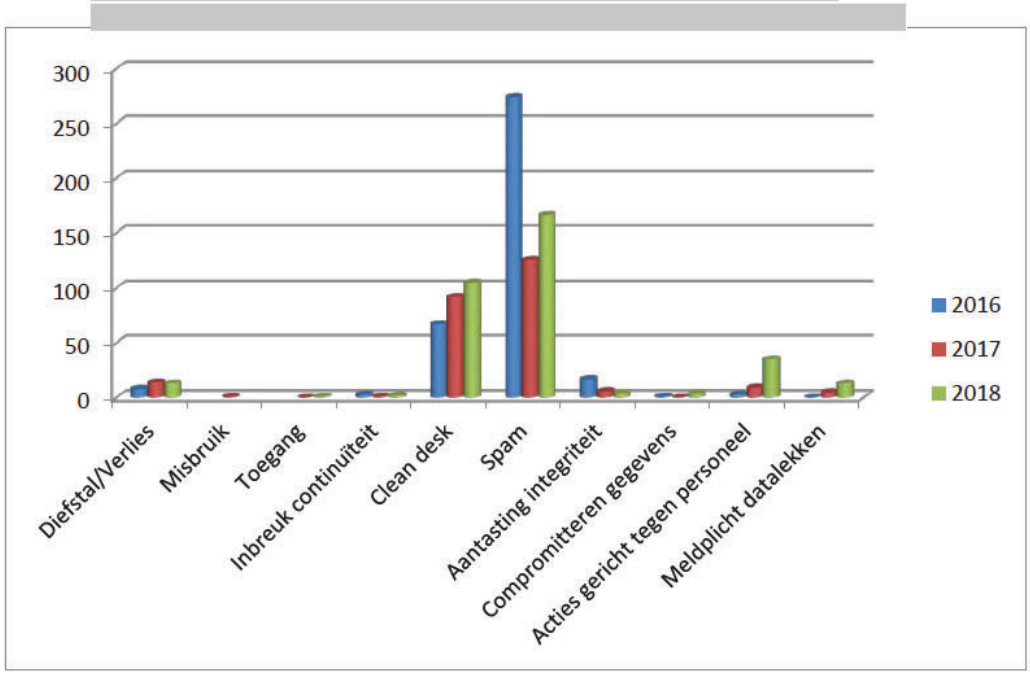


Totaal beeld beveiligingsincidenten afgelopen 12 maanden

Toelichting

Terugkijkend op 2018 zien we dat:

- Medewerkers in 2018 5x mobiele devices, 1x rijkspas, 1x OV-kaart, 6x [redacted] hebben verloren. (2016; 3 iPhones, 1 iPad, 3 tokens en 1 rijkspas; 2017 1x IPhone, 3x rijkspas, 5x OV-kaart, 4x [redacted] en 1x een [redacted]
- Medewerkers 54 x zijn vergeten hun [redacted] veilig op te bergen. (2016: 51x; 2017: 58)
- Medewerkers zijn 36x vergeten een kluis af te sluiten. (2016: 4x; 2017:19)
- We 13x een datalek hebben gehad en we hebben 2x de melding gemaakt bij de Autoriteit Persoonsgegevens. (2016: 1x; 2017: 5).
- We 35 meldingen hebben betreffende acties gericht tegen personeel. Een groot deel betreft mailberichten van verwarde personen aan de bestuurder. [redacted]



Controle autorisaties

We controleren in samenwerking met leidinggevenden de autorisaties op het [redacted] en voor de rijkspassen. Het is belangrijk dat bedrijfsvoering tijdig op de hoogte is van een verandering van functie of het

vertrek van een medewerker en dat autorisaties op tijd kunnen worden ingetrokken.

Kwetsbaarheden websites/applicaties
Om na te gaan of websites en applicaties, voorzien zijn van een update, of kwetsbaarheden vertonen heeft de Audit Dienst Rijk (ADR) pentesten uitgevoerd op 2 websites, 2 applicaties en het [redacted]. De door de ADR geconstateerde kwetsbaarheden zijn verholpen.

Periodieke testen
In 2018 heeft de Rijksbeveiligingsorganisatie (RBO) maandelijks testen uitgevoerd op de actieve inbraak/bewegingsdetectoren in de beveiligingsinstallatie. Deze detectoren geven in normale omstandigheden geen alarm en moeten daarom apart worden getest om na te gaan of ze niet defect zijn. Onvolkomenheden zijn aan [redacted] gemeld voor reparatie.

Elektronische veiligheidsonderzoeken
[redacted]
In 2018 zijn er geen verdachte omstandigheden of voorzieningen aangetroffen.

Baseline Informatiebeveiliging Rijksdienst
De ICV (in control verklaring) BIR (Baseline Informatiebeveiliging Rijksdienst) voor 2018 is opgesteld. Daarin wordt de status vermeld van nog te nemen- en reeds genomen maatregelen in het kader van de BIR. De ICV is een jaarlijkse verplichte rapportage die onder andere naar de SG JenV en BZK wordt gezonden. De ADR voert steekproeven uit bij organisaties om te controleren of de grondslag voor de ICV wel op de juiste feiten is gebaseerd.
In samenwerking met de NCTV heeft [redacted] een projectleider aangesteld die de ICV BIR en AVG verplichting voor de [redacted] gaat uitvoeren. De verantwoordelijkheid ligt hier bij [redacted] maar de NCTV moet ook aantonen dat zij ‘in control’ is voor het beheer van de toegangscontrole ten aanzien van rijkspas autorisaties en opslag van biometrische gegevens van haar medewerkers.

Algemene Verordening Gegevensbescherming
In samenspraak met het juridisch cluster had Bedrijfsvoering een projectleider aangetrokken voor de implementatie van de AVG (Algemene verordening gegevensbescherming). Op 28 mei 2018 voldeed de NCTV aan de AVG verplichtingen. Het verwerkingsregister is opgesteld. In 2018 is het proces tot werving van een Privacycoördinator gestart en dat heeft geresulteerd tot een aanstelling per 1 januari 2019.

Integriteit
In 2018 heeft integriteit meer aandacht gekregen en zijn er diverse sessies gehouden voor medewerkers en leidinggevenden. Er is een brede werkgroep Integriteit geformeerd. Er is extra aandacht geschonken aan data gebruik op mobiele devices (in het buitenland).

Update beleidsdocumenten
De NCTV heeft in 2018 enkele documenten van het Programma Integrale Beveiliging en BIR verplichtingen, in het kader van voortschrijdend inzicht en ontwikkelingen, geactualiseerd. Dit betreft:
- Leidraad exitgesprekken;
- Aanwijzing Vertrouwensfuncties;
- Beleid mobiele devices.

Veiligheidsbewustzijn
- Het afgelopen jaar zijn er diverse initiatieven geweest om het veiligheidsbewustzijn onder de medewerkers van de NCTV te vergroten.
- Er zijn factsheets (met tips en handelingsperspectieven) gemaakt over diverse onderwerpen zoals; gebruik smartphone, gebruik social media, gebruik facebook en gebruik [redacted].
- Incidenteel zijn er artikelen geplaatst op intranet over gebeurtenissen met een advies voor een handelingsperspectief voor de medewerkers [redacted]).
- Alertonline is onder de aandacht gebracht bij de medewerkers.
- De NCTV heeft zich aangesloten bij de awareness campagne van het IBR (Integraal Beveiligingsberaad Rijksoverheid) die in 2019 doorloopt en diverse onderwerpen onder de aandacht brengt.
- De NCTV is betrokken geweest bij de voorbereidingen van de awareness campagne van JenV, Weerbaar JenV. In 2019 zullen de eerste producten worden opgeleverd.

[redacted]

Toezicht Beveiligingsautoriteit JenV
De BVA JenV houdt toezicht op de uitvoering van (inter)departementale regelgeving en beleidskaders bij de diverse dienstonderdelen. De toetsing vindt jaarlijks plaats. De NCTV had geen tekortkomingen het afgelopen jaar.

Afvoer hardware
Er is een inzamelingsactie gehouden voor het veilig afvoeren van hardware voor zowel oude producten van de NCTV als oude producten van medewerkers. De producten waarop mogelijk nog informatie aanwezig was, zijn versnipperd en de overige producten zijn afgevoerd via de Domeinen.

SIEM
De SIEM-systemen (Security Incident & Event Management systeem) waarmee security incidenten of kwetsbaarheden gedetecteerd worden hebben in 2018 goed gewerkt. Er hebben zich geen bijzondere gebeurtenissen voor gedaan.

In het is in 2018 één werkstation besmet geraakt met malware. Dit werkstation is uit het netwerk verwijderd en opnieuw van software voorzien. De verschillende netwerken binnen zijn zodanig geconfigureerd dat een besmetting van een werkstation op het netwerk niet kan leiden tot een besmetting van de andere werkstations op

zijn geen SIEM alarmen opgetreden in 2018.

Er hebben zich geen bijzondere meldingen voor gedaan in 2018 op het netwerk.

Datalekken
We zien een toename van datalekken waarna persoonsgegevens worden gepubliceerd. Bij een aantal datalekken zijn ook persoonsgegevens van medewerkers openbaar geworden. Er is extra aandacht geschonken aan het gebruik van app's zoals de sportapp waarmee andere personen en organisaties de gebruiker kunnen volgen.

DDOS aanvallen en verstoringen
In 2018 hebben diverse DDOS aanvallen plaatsgevonden, ook op websites van de NCTV. Dit heeft niet geleid tot uitval of beschikbaarheid van de websites. De uitval van stroom en netwerken (heeft wel geleid tot tijdelijk uitval of verstoring. De onderzoeken naar oorzaken lopen nog bij de Concerndienstverlener. In 2019 verdient dit extra aandacht.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT

Kern Bedrijfsvoering
KBV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon

Datum
28 januari 2020

Ons kenmerk

nota

Jaarrapportage 2019 Programma Integrale Beveiliging

Door tussenkomst van

Datum/eindparaaf

Inleiding

Bijgaand ontvangt u de jaarrapportage integrale beveiliging over 2019. De jaarrapportage geeft een beeld van de activiteiten die in samenwerking met de werkgroep beveiliging in 2019 zijn uitgevoerd. Deze activiteiten staan ook beschreven in het Plan van Aanpak Interne Controle Risicobeheersing NCTV d.d. 4-3-2019 en het jaarplan 2019 van .

Veiligheidsonderzoeken

In 2017 is voor J&V besloten dat er een inhaalslag wordt gemaakt om herhaalonderzoeken uit te voeren bij medewerkers met een VGB ouder dan 5 jaar. Ieder dienstonderdeel heeft de plicht om binnen 5 jaar de herhaalonderzoeken op orde te hebben.

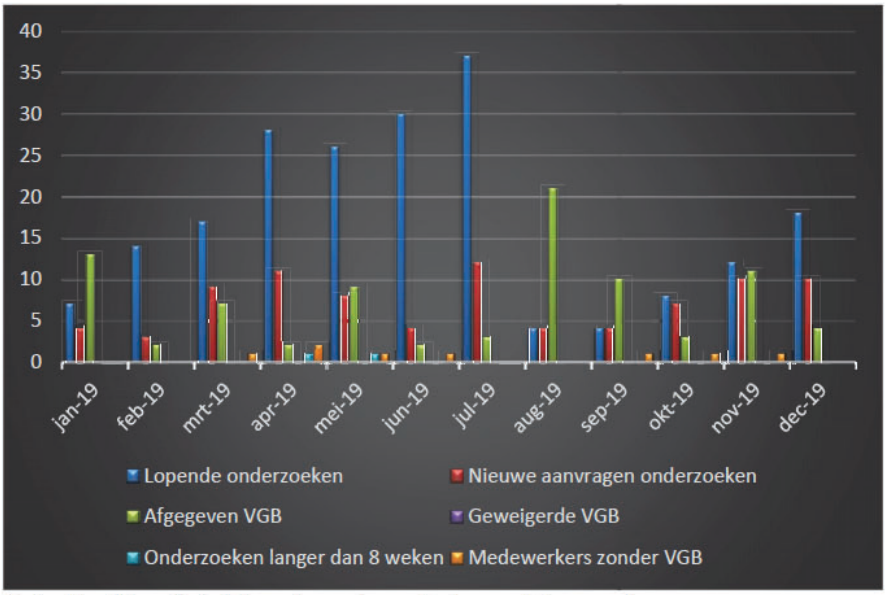
De trend die we zien is dat het aantal aanvragen voor veiligheidsonderzoeken en herhaalonderzoeken afneemt tot een stabiel en beheersbaar niveau dat past bij de omvang van de organisatie. Er worden bewustere keuzes gemaakt voor eventuele uitzonderingen zoals het werken zonder VGB met een waiver.

De NCTV heeft eind 2019 de inhaalslag voltooid, 126 herhaalonderzoeken. Er zijn geen medewerkers binnen de NCTV werkzaam die een VGB hebben ouder dan 5 jaar. Dat betekent dat er alleen nog reguliere herhaalonderzoeken plaatsvinden voor medewerkers van wie de afgifte datum na 5 jaar verstrijkt.

Kern Bedrijfsvoering
KBV

Datum
28 januari 2020

Ons kenmerk



Totaalbeeld veiligheidsonderzoeken afgelopen 12 maanden

Toelichting
Terugkijkend op 2019 zien we dat:

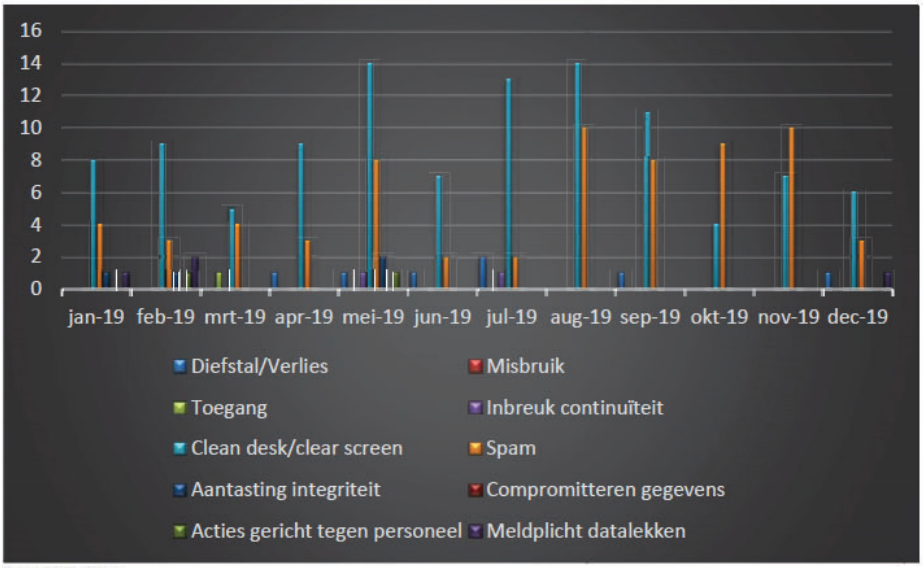
- In totaal 86 veiligheidsonderzoeken (inclusief herhaalonderzoeken) zijn aangevraagd (2016: 107, 2017: 178, 2018: 226).
- In totaal 87 VGB's zijn afgegeven (2016: 100, 2017: 144, 2018: 272).
- In twee gevallen duurde het onderzoek langer dan de vastgestelde termijn van 8 weken. In veel gevallen ontstaat dit door navraag in het buitenland.
- In 2019 zijn geen aanvragen geweigerd of afgewezen.
- Er in 2019 8 medewerkers eerder zijn gestart met de uitvoering van hun werkzaamheden dan dat het veiligheidsonderzoek was afgerond. In al deze gevallen is een waiver met beperking van de autorisaties afgegeven door de NCTV.
  (2016: 5 medewerkers, 2017: 20 medewerkers, 2018: 13 medewerkers)

Kern Bedrijfsvoering
KBV

Datum
28 januari 2020

Ons kenmerk
[redacted]

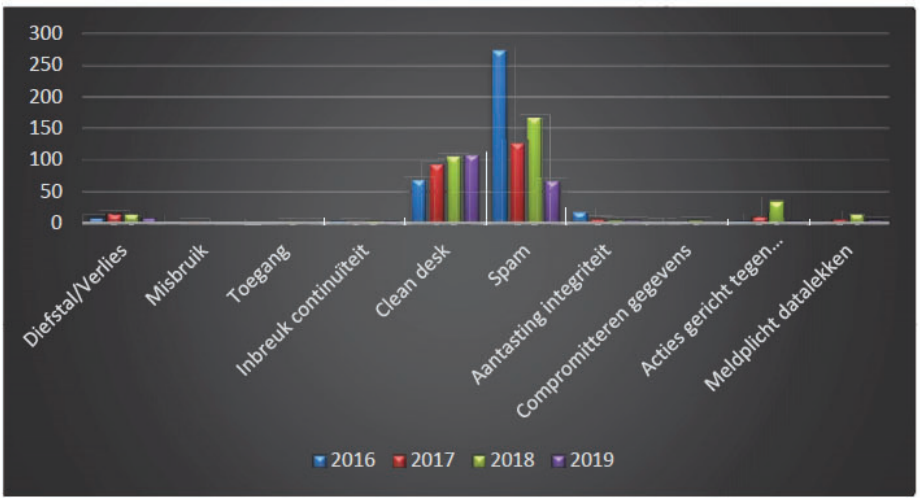
Beveiligingsincidenten



Toelichting

Terugkijkend op 2019 zien we dat:

- Medewerkers hebben in 2019 7 items verloren. (2016; 8 items; 2017 14 items, 2018 13 items).
- Medewerkers 68x zijn vergeten hun [redacted] veilig op te bergen. (2016: 51x; 2017: 58; 2018: 54)
- Medewerkers zijn 9x vergeten een kluis af te sluiten. (2016: 4x; 2017:19; 2018: 36)
- We 1x een datalek hebben gehad en we hebben 1x de melding gemaakt bij de Autoriteit Persoonsgegevens. (2016: 1x; 2017: 5; 2018: 13).



Controle autorisaties

We hebben in samenwerking met leidinggevenden de autorisaties op het en voor de rijkspassen periodiek gecontroleerd. Regelmatig is geconstateerd dat bedrijfsvoering niet geïnformeerd was over de vertrekkende medewerker of een verandering van functie. Hierdoor werden autorisaties pas later aangepast.

Kwetsbaarheden websites/applicaties

Om na te gaan of websites en applicaties, voorzien zijn van een update, of kwetsbaarheden vertonen heeft de Audit Dienst Rijk (ADR) pentesten uitgevoerd op 4 websites en 2 applicaties. De door de ADR geconstateerde kwetsbaarheden zijn verholpen in overleg met de functioneel beheerders en systeemeigenaren. In overleg met een systeemeigenaar zijn 5 websites offline gehaald en is het archiveringsproces in gang gezet. In de planning stond een technische toets door de ADR van onderdelen van het . Deze is verplaatst naar 2020.

Periodieke testen

In 2019 heeft de Rijksbeveiligingsorganisatie (RBO) maandelijks testen uitgevoerd op de actieve inbraak/bewegingsdetectoren in de beveiligingsinstallatie. Deze detectoren geven in normale omstandigheden geen alarm en moeten daarom apart worden getest om na te gaan of ze niet defect zijn. Onvolkomenheden zijn aan FMH Gebouwbeheer gemeld voor reparatie.

Elektronische veiligheidsonderzoeken

In 2019 zijn er geen verdachte omstandigheden of voorzieningen aangetroffen.

Baseline Informatiebeveiliging Rijksdienst

De ICV (in control verklaring) BIR (Baseline Informatiebeveiliging Rijksdienst) voor 2019 is opgesteld. Daarin wordt de status vermeld van nog te nemen- en reeds genomen maatregelen in het kader van de BIR2017. De ICV is een jaarlijkse verplichte rapportage die onder andere naar de SG JenV en BZK wordt gezonden. De status per 31 december 2019 van de invoer van de BIR2017 is gerapporteerd aan het management.

.

In 2019 zijn de risicoanalyses voor de kritische systemen; uitgevoerd. De actiepunten zijn gerealiseerd of opgenomen in de ICT-planning

Algemene Verordening Gegevensbescherming

In de AVG worden eisen gesteld aan de bescherming van persoonsgegevens, inclusief de informatiebeveiliging. De NCTV is in control voor wat betreft de AVG,

maar had een aantal restpunten die in 2019 uitgewerkt moesten worden. Per 1 januari 2019 is de nieuwe Privacycoördinator begonnen.
Door de complexiteit van diverse vraagstukken en het ontbreken van grondslagen zijn niet alle doelen gehaald in 2019. De privacycoördinator heeft dit opgenomen in het jaarplan 2020.

Datalekken
In 2019 hebben we extra aandacht besteed aan het voorkomen van datalekken en medewerkers handelingsperspectieven geboden. Er heeft zich 1 datalek voor gedaan die ook is gemeld bij de Autoriteit Persoonsgegevens. Het voorval van het datalek is anoniem beschreven op het intranet om alle medewerkers te wijzen op de risico's.

[redacted] is de centrale beveiligingsinstallatie en het centrale toegangscontrolesysteem waar van de NCTV gebruik maakt. In [redacted] worden persoonsgegevens van onder andere NCTV medewerkers verwerkt en het systeem wordt gebruikt voor autorisatie van personen tot de NCTV zone. [redacted]

Integriteit
In 2019 heeft de werkgroep Integriteit aandacht gevraagd voor diverse vraagstukken. De NCTV is aangesloten bij het project van JenV voor de bevordering van bewustzijn bij medewerkers. In september is de week van het 'onbesproken gedrag' georganiseerd.

EU inspectie
In oktober heeft er bij de NCTV een EU inspectie plaatsgevonden. In overleg met een team van de [redacted] hebben de inspecteurs beoordeeld hoe de NCTV omgaat met EU informatie. Een van de bevindingen is dat de wijze van registratie in Nederland verbeterd moet worden. Aangetoond moet kunnen worden wie op welk moment inzage had in de informatie. De EU regelgeving verschilt hierin ten op zichten van onze nationale regelgeving. In samenwerking met [redacted] zullen de nationale actiepunten worden opgepakt. Het rapport wordt later in 2020 verwacht.

Actualiseren beleidsdocumenten
De NCTV heeft in 2019 documenten van het Programma Integrale Beveiliging in het kader van voortschrijdend inzicht en ontwikkelingen en de BIR2017 verplichtingen geactualiseerd. Dit betrof:
- EU procesbeschrijving;
- Beleid Informatiebeveiliging;
- Tactisch kader Integrale beveiliging;
- Eigenaarschap;
- Beleid Interne risicobeheersing NCTV;
- Toegangscontrole tot netwerken en elektronische informatie;
- Bijlage afspraken BHV-ontruimingsplan.

Kern Bedrijfsvoering
KBV

Datum
28 januari 2020

Ons kenmerk
[redacted]

Veiligheidsbewustzijn

- Het afgelopen jaar zijn er diverse initiatieven geweest om het veiligheidsbewustzijn onder de medewerkers van de NCTV te vergroten.
- In mei is de 'week van de veiligheid' georganiseerd.
- Er zijn factsheets (met tips en handelingsperspectieven) gemaakt over diverse onderwerpen zoals; rubriceringskaart, gebruik smartphone, gebruik social media, gebruik facebook en gebruik [redacted].
- Incidenteel zijn er artikelen geplaatst op intranet over gebeurtenissen met een advies voor een handelingsperspectief voor de medewerkers.
- De NCTV doet mee aan de volgende campagnes: Alertonline, awareness campagne van het Integraal Beveiligingsberaad Rijksoverheid en van de awareness campagne het programma Weerbaar JenV (o.a. phising mail0.

[redacted]

Toezicht [redacted]

De [redacted] houdt toezicht op de uitvoering van (inter)departementale regelgeving en beleidskaders bij de diverse dienstonderdelen. De toetsing vindt jaarlijks plaats. De NCTV had geen tekortkomingen het afgelopen jaar.

Vlekkenplan herhuisvesting NCTV

Voor het uitvoeren van werkprocessen met gerubriceerde informatie is informatiebeveiliging van groot belang. Om werkprocessen zo efficiënt en veilig mogelijk uit te kunnen voeren is een risicoafweging gemaakt met voorstellen om aanvullende maatregelen te treffen in een aantal ruimten.

[redacted]

Continuïteit

In verband met de ontwikkelingen en latere oplevering [redacted] hebben we een aantal aanpassingen in het continuïteitsplan nog niet uitgevoerd.
Het afgelopen jaar hebben zich meerdere incidenten voor gedaan ten aanzien van uitval c.q. beschikbaarheid van voorzieningen bij de NCTV. In de meeste gevallen betrof het diensten die we van andere partijen of concerndienstverleners afnamen (uitval en beperkte beschikbaarheid van de telecomprovider, stroomstoringen op de Turfmarkt en beperkte beschikbaarheid [redacted]

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT/PR

Kern Bedrijfsvoering
KBV

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon
[redacted]

Datum
29 maart 2022

Ons kenmerk
...

nota

Jaarrapportage 2021 Integrale Beveiliging

Inleiding

Bijgaand ontvangt u de jaarrapportage integrale beveiliging over 2021. De jaarrapportage geeft een beeld van de activiteiten die in samenwerking met de werkgroep beveiliging in 2021 zijn uitgevoerd. Deze activiteiten staan ook beschreven in het Plan van Aanpak Interne Controle Risicobeheersing NCTV.

Veiligheidsonderzoeken

Eerder is binnen J&V besloten dat veiligheidsonderzoeken niet ouder mogen zijn dan 5 jaar. Ieder dienstonderdeel heeft de plicht om de administratie op orde te hebben.

In 2021 hebben er 15 herhaalonderzoeken en 68 nieuwe veiligheidsonderzoeken plaatsgevonden. In 10 gevallen is een eerder afgegeven VGB van een andere organisatie geaccepteerd. In 2021 zijn 2 VGB's geweigerd. Deze cijfers komen over een met eerdere jaren.

Beveiligingsincidenten

- [redacted]
- Verder hebben zich nog een aantal andere incidenten voorgedaan waarbij informatie is gelekt naar de media.
- [redacted]
- Meerdere oud-medewerkers hebben zich uitgelaten naar de media over interne zaken van de NCTV. In 2021 is dit een opvallend verschijnsel omdat dit niet eerder heeft plaatsgevonden in deze omvang.
- [redacted]
- [redacted]

- We hebben een toename gezien van spamberichten, sms en telefoontjes waarbij het telefoonnummer is gespoofd.

Controle autorisaties
We hebben in samenwerking met leidinggevenden de autorisaties op [redacted] en voor de rijkspassen periodiek gecontroleerd. Regelmatig is geconstateerd dat bedrijfsvoering niet geïnformeerd was over de vertrekkende medewerker of een verandering van functie. Hierdoor werden autorisaties pas later aangepast.

Kwetsbaarheden websites / applicaties
Om na te gaan of websites en applicaties, voorzien zijn van een update, of kwetsbaarheden vertonen heeft de Audit Dienst Rijk (ADR) pentesten uitgevoerd op 3 websites. De door de ADR geconstateerde kwetsbaarheden zijn verholpen in overleg met de functioneel beheerders en systeemeigenaren.

Periodieke testen
In 2021 heeft de Rijksbeveiligingsorganisatie (RBO) maandelijks testen uitgevoerd op de actieve inbraak/bewegingsdetectoren in de beveiligingsinstallatie. Deze detectoren geven in normale omstandigheden geen alarm en moeten daarom apart worden getest om na te gaan of ze niet defect zijn. Onvolkomenheden zijn aan [redacted] gemeld voor reparatie.

Elektronische veiligheidsonderzoeken
[redacted]
In 2021 zijn er geen verdachte omstandigheden of voorzieningen aangetroffen.
[redacted]

Baseline Informatiebeveiliging Overheid
De ICV (in control verklaring) BIO (Baseline Informatiebeveiliging Overheid) voor 2021 is opgesteld. Daarin wordt de status vermeld van nog te nemen en reeds genomen maatregelen in het kader van de BIO. De ICV is een jaarlijkse verplichte rapportage die onder andere naar de SG JenV en BZK wordt gezonden. De status per 31 december 2021 van de invoer van de BIO is gerapporteerd aan het management. [redacted]
In 2021 zijn de risicoanalyses voor de kritische systemen; [redacted] uitgevoerd. De actiepunten zijn gerealiseerd of opgenomen in de ICT-planning [redacted] voor 2022.

Datalekken
In 2021 hebben we extra aandacht besteed aan het voorkomen van datalekken en medewerkers handelingsperspectieven geboden. Er hebben zich 4 datalekken voor gedaan die ook zijn gemeld bij de Autoriteit Persoonsgegevens. De overige 16 datalekken zijn niet gemeld aan de AP. De meldingen zijn opgenomen in de rapportage voor DFEZ. [redacted]. Een

deel van de bezorgdheid is weggenomen door gesprekken in de afdelingen, intranet en de interne nieuwsbrief.

[redacted] is de centrale beveiligingsinstallatie en het centrale toegangscontrolesysteem waar van de NCTV gebruik maakt. In [redacted] worden persoonsgegevens van onder andere NCTV medewerkers verwerkt en het systeem wordt gebruikt voor autorisatie van personen tot de NCTV zone. [redacted]

Handreiking persoonlijke veiligheid
In 2021 hebben we een handreiking opgesteld voor eigen medewerkers die op een kwetsbare functie werkzaam zijn. In dit geval gaat het met name om medewerkers die op het dossier [redacted] werkzaam zijn. Onderdeel van de handreiking is een intakeformulier en risicomatrix. In de praktijk zijn die nu toegepast en dat heeft geleid tot aanpassingen aan de eigen woning van medewerkers. Tevens zijn twee lease voertuigen aangeschaft ten behoeve van werkbezoeken aan locaties. De handreiking is opgesteld in samenwerking met het OM, NP en BVA JenV.

ISMS
De NCTV beschikt over een nieuw [redacted] dat in samenwerking met [redacted] is geïmplementeerd [redacted]. In de [redacted] worden de BIO maatregelen ingevoerd en beoordeeld waarop via een rapportage een actueel beeld gerealiseerd kan worden. Door technisch problemen is de [redacted] eind 2021 nog niet operationeel.

SOC NCTV
Het Security Operation Center beheerd de digitale veiligheid met een applicatie die de systemen controleert op afwijkend gedrag of gebeurtenissen. Er is een verplichting om samen te werken met het SOC JenV. In 2020 is daarvoor een proces ingericht en in 2021 heeft de evaluatie van het proces plaatsgevonden. In 2021 is het proces van kwetsbaarheidsmeldingen intern NCTV ook opnieuw ingericht. In 2021 is gestart met de verkenning van de aanschaf van een nieuwe Siem in overleg met SOC JenV.

Red Teaming
In maart 2021 heeft een RT plaatsgevonden op de DWR omgeving met de applicaties [redacted] die de NCTV gebruikt. [redacted]

Kern Bedrijfsvoering
KBV

Datum
29 maart 2022

Ons kenmerk
...

Afvoer Stg producten
Door de aanschaf van nieuwe computers, toetsenborden en beeldschermen zijn de oude apparaten via het bestaande proces afgevoerd. Tegelijk is het proces aangepast op de actuele situatie.

Actualiseren beleidsdocumenten
De NCTV heeft in 2021 documenten van het Programma Integrale Beveiliging in het kader van voortschrijdend inzicht en ontwikkelingen en de BIO verplichtingen geactualiseerd. Dit betrof:

- Beleid Interne risicobeheersing NCTV;
- Toegangscontrole tot netwerken en elektronische informatie;
- Bijlage afspraken BHV-ontruimingsplan [redacted]

Veiligheidsbewustzijn

- Het afgelopen jaar zijn er diverse initiatieven geweest om het veiligheidsbewustzijn onder de medewerkers van de NCTV te vergroten.
- In juni is de 'week van de veiligheid' georganiseerd.
- Er zijn factsheets (met tips en handelingsperspectieven) gemaakt over diverse onderwerpen zoals; hybride (thuis)werken, rubriceringskaart, gebruik smartphone, gebruik social media, gebruik facebook en gebruik [redacted].
- Incidenteel zijn er artikelen geplaatst op intranet over gebeurtenissen met een advies voor een handelingsperspectief voor de medewerkers.
- Teksten op intranet voor veiligheidsbewustzijn en het werken met staatsgeheimen zijn geactualiseerd.
- [redacted]
- De NCTV heeft nog niet een LMS (LeerManagementSysteem) om medewerkers een e-learning aan te bieden. Door omstandigheden is er geen projectleider gevonden om het project vorm te geven.
- [redacted]

[redacted]

[redacted]

[redacted]

Toezicht JenV
De houdt toezicht op de uitvoering van (inter)departementale regelgeving en beleidskaders bij de diverse dienstonderdelen. De toetsing vindt jaarlijks plaats. De NCTV had geen tekortkomingen het afgelopen jaar.

SRA
Met een Security Risk Assessment (SRA) worden dreigingen en kwetsbaarheden op een systematische en transparante wijze in kaart gebracht en de risico's bepaalt zodat deze gecontroleerd beheerd kunnen worden. Risico's kunnen vaak voor een groot deel niet opgelost worden, maar zijn dan tot op zekere hoogte wel beheersbaar te maken. De SRA methodiek is onder andere toegepast bij de Handreiking voor persoonlijke veiligheid van medewerkers. De beoogde herziening van het SRA beleid en de inventarisatie van TBB (Te Beschermen Belangen) heeft door de COVID maatregelen niet kunnen plaatsvinden in 2021.

Hybride werken NCTV
Er is een projectleider aangesteld om het Hybride werken voor de NCTV verder uit te werken. Het Hybride werken wordt verder via de managers geïmplementeerd. De geeft advies over de beveiligingsrisico's en te nemen maatregelen.

Continuïteit
In verband met de ontwikkelingen en latere oplevering hebben we een aantal aanpassingen in het continuïteitsplan nog niet uitgevoerd.
Het afgelopen jaar hebben zich meerdere incidenten voor gedaan ten aanzien van uitval c.q. beschikbaarheid van voorzieningen bij de NCTV. In de meeste gevallen betrof het diensten die we van andere partijen of concerndienstverleners afnamen (uitval en beperkte beschikbaarheid van de telecomprovider, stroomstoringen op de Turfmarkt en beperkte beschikbaarheid

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon

Datum
15 november 2017

Ons kenmerk
123456

nota

Zelfanalyse KWAS 2017

Van
Hoofd
Datum/eindparaaf

Aanleiding

In 2016 is de volledige Kwetsbaarheidsanalyse Spionage (KWAS) uitgevoerd. In 2017 heeft er een zelfanalyse plaatsgevonden. Tijdens de zelfanalyse zijn de kwetsbaarheden opnieuw met de leden van de werkgroep beveiliging beoordeeld en is bekeken of de actiepunten van 2016 al zijn geïmplementeerd of wat de status daarvan is.

De ontwikkelingen op het gebied van cyber security en de ontwikkelingen in de buitenwereld leiden jaarlijks tot nieuwe inzichten, andere risico's en een mogelijke actualisering van de genomen maatregelen.

Advies

Wij vragen u actie te nemen op de 'nog te realiseren acties 2017/2018' op pagina 3.

Samenvatting KWAS zelfanalyse

Externe ontwikkelingen

In 2017 zien we het risico op het gebruik van digitale apparaten voor spionage toenemen. Daarnaast zien we een toename van pogingen om het digitale verkeer te beïnvloeden (verkiezingen en nepnieuws). Dit jaar zet de stijgende lijn zich voort van het aantal incidenten, op digitaal gebied, door criminelen en statelijke actoren. Zie ook het CSBN 2017. Steeds meer data en netwerken van overheden worden gecompromitteerd of worden verstoord. Verder dragen de veranderingen in de maatschappij zoals de behoefte aan 'open data' van de overheid en het gebruik van de 'cloud' bij tot mogelijk nieuwe kwetsbaarheden en risico's.
Binnen de diverse diensten ontstaat nu meer aandacht voor de 'interne dader' (Inside threat).

Interne ontwikkelingen

In 2017 hebben wij investeringen gedaan om het veiligheidsbewustzijn omtrent spionage te verbeteren. De aangeboden workshops 'Digitale Kwetsbaarheden", in samenwerking met de , hebben daaraan een positieve bijdrage geleverd.

Stafafdeling Bedrijfsvoering

Datum
15 november 2017

Ons kenmerk
123456

We zien dat beveiligingsonderwerpen bespreekbaar worden gemaakt en de medewerkers worden gestimuleerd om bewust na te denken over de consequenties van het gebruik van social media en het internet.
De netwerken [redacted] zijn voorzien van een applicatie (SIEM) waarmee door middel van monitoring en logging afwijkende gebeurtenissen op het netwerk achteraf kunnen worden vastgesteld. In 2017 heeft de ADR (Auditdienst Rijk) pentesten (onderzoeken op kwetsbaarheden) van diverse NCTV websites uitgevoerd.

Toelichting uitvoering KWAS zelfanalyse

KWAS NCTV 2017
Ten aanzien van de benoemde 'Te Beschermen belangen' (TBB) en de mogelijke 'Dreigers' hebben zich in 2017 geen veranderingen voorgedaan.

Te Beschermen Belangen
De TBB zijn de kernbelangen van de NCTV die interessant zijn voor 'dreigers'. Alle factoren die aantasting van de kernbelangen, onder andere door spionage mogelijk maken, hangen samen met mens en techniek. De NCTV heeft de volgende belangen als TBB benoemd.

[redacted]

Dreigers
De bovengenoemde belangen zijn mogelijk interessant voor andere inlichtingendiensten (statelijke actoren), extremistische groeperingen, terroristen, solistische dreigers, journalisten, activisten, bedrijfsspionage, scriptkiddies, cybercriminelen, hacktivisten, cyberactivisten.

Kwetsbaarheden
In 2017 zijn er diverse acties ondernomen om de mogelijke kwetsbaarheden binnen de NCTV te beperken.

A. Gerealiseerde acties 2017;

A.1. Tijdens de week van de veiligheid is aandacht besteed aan 'cleandesk'. In 2018 zal dit een vervolg krijgen.

A.2. Medewerkers zijn tijdens de week van de veiligheid gewezen op de risico's van het gebruik van mobiele apparaten. Tevens is de informatie op intranet geplaatst.

A.3. Nieuwe medewerkers worden tijdens de introductiebijeenkomst gewezen op de risico's van zichtbaarheid op internet en social media.

A.4. Tijdens de week van de veiligheid hebben medewerkers extra informatie ontvangen over de wijze van rubriceren en is de documentatie geactualiseerd en op intranet beschikbaar gemaakt.

A.5. In samenwerking met de zijn bijeenkomsten gehouden voor de afdelingen over 'Digitale kwetsbaarheden'.

A.6. In juni 2017 is een tijdelijke privacy-officer aangesteld om de NCTV voor te bereiden op de verplichtingen van de Algemene Verordening Gegevensbescherming (AVG), mei 2018.

A.7. Monitoring en logging van systemen zijn voor de NCTV netwerken gerealiseerd maar de handzame en minder technische rapportagevormen behoeven nog de aandacht.

B. Nog te realiseren acties 2017/2018;

B.1. Houd met iedere medewerker die (tijdelijk) vertrekt een exit-gesprek en leg eventuele afspraken schriftelijk vast. **Actie leidinggevenden**.

B.2. Bespreek periodiek tijdens afdelingsoverleggen onderwerpen als cleandesk, rubriceren en het gebruik van social media. **Actie leidinggevenden**.

B.3. Voor het gebruik van anoniem dient een handleiding voor (nieuwe) medewerkers beschikbaar te zijn. **Actie eigenaar en .**

B.4. Maak de Gedragsregels voor de Digitale werkomgeving bekend aan de medewerkers. **Actie**

B.5. Het testen van continuïteitsmaatregelen zoals de logistiek naar en het werken op de uitwijk en het werken op de applicatie dient meer aandacht krijgen. Niet alle medewerkers hebben de omgeving geactiveerd. **Actie leidinggevenden**.

B.6. De zal voor mei 2018 een voorstel doen om de functie van privacy-officer te beleggen binnen de NCTV. **Actie**

B.7. De processen voor verwerking van persoonsgegevens bij de Concern Dienstverleners zijn nog onvoldoende geborgd. De NCTV werkt met de samen aan een verbetering van deze verwerking. **Actie**

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT

Stafafdeling
Bedrijfsvoering

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl
Contactpersoon

Datum
20 november 2017

Ons kenmerk
123456

oplegnota

Herziening regeling
'Omgaan met Vertrouwensfuncties'

Van
Hoofd
Datum/eindparaaf

Advies

Ter kennisgeving
- Lijst met geclusterde vertrouwensfuncties NCTV.

Akkoord te gaan met
- Aanpassing regeling 'Omgaan met Vertrouwensfunctie'.
- Vanaf 1-11-2017 zijn we gestart met de uitvoering van de herhaalonderzoeken.

Deze regeling versturen naar de OR ter informatie.
- Na kennisname door het MT zal de aangepaste regeling ter informatie naar de OR worden gezonden.

Toelichting

De regeling 'Omgaan met Vertrouwensfuncties' is gebaseerd op de 'Leidraad aanwijzing vertrouwensfunctie' onder de Wet Veiligheidsonderzoeken (Wvo 2014). Voor de administratieve uitvoering van veiligheidsonderzoeken worden functieprofielen beschreven. Die functieprofielen hebben een waardering voor de hoogte van het uit te voeren veiligheidsonderzoek A, B of C. Een functieprofiel voor een veiligheidsonderzoek staat los van de functie van de medewerker en heeft meer betrekking op de taken die de medewerker uitvoert.

Oude situatie
In 2012 heeft – bij de vorming van de NCTV - een inventarisatie plaats gevonden van alle vertrouwensfuncties binnen de NCTV. In de gesprekken met de leidinggevenden zijn de functies (Functiegebouw Rijk) beoordeeld op de inhoud van de taken van de functionaris. Deze beoordelingen hebben toen geleid tot een keuze van een bijpassend functieprofiel voor het veiligheidsonderzoek op niveau A, B of C. Dat was toen het meest passend. Later ontstond hierdoor wel het beeld dat een adviseur bij één afdeling een A onderzoek moest hebben en bij een andere afdeling een B onderzoek. Tevens waren er meerdere functies van gelijk niveau van onderzoek maar bij verschillende afdelingen met verschillende taken. In deze situatie had iedere afdeling dus een eigen lijst met functieprofielen en onderzoek niveaus. Deze lijst is toen vastgesteld door de SG JenV.

Stafafdeling Bedrijfsvoering

Datum
20 november 2017

Ons kenmerk
123456

Alle medewerkers van de NCTV hebben destijds een brief ontvangen waarin hun functie wordt genoemd en welk niveau van veiligheidsonderzoek daaraan is toegewezen.
In 2013 heeft de Bestuursraad JenV besloten om geen herhaalonderzoeken voor alle vertrouwensfuncties bij JenV uit te voeren tenzij hier nadrukkelijk een noodzaak toe was.

NCTV Ontwikkelt
Inmiddels leidt een aantal ontwikkelingen tot een nieuwe lijst en aanpassing van de regeling uit 2012. Alle NCTV medewerkers hebben een NCTV-brede aanstelling en niet meer bij een afdeling. Om medewerkers flexibeler in te kunnen zetten, het harmoniseren van werkzaamheden te bevorderen en aan te kunnen sluiten bij de ontwikkelingen voor de keuze van het matchingsproces is er voor gekozen dit door te trekken naar de vertrouwensfuncties (VF) om deze minder afdeling- en taakafhankelijk te maken.
Zo zijn de functieprofielen van alle afdelingen samengevoegd op een nieuwe lijst van vertrouwensfuncties. Deze clustering heeft tot gevolg dat bijvoorbeeld een ‘adviseur’ van afdeling [redacted] qua vertrouwensfunctie hetzelfde profiel heeft gekregen als de ‘adviseur’ bij afdeling [redacted]. Er is nog wel onderscheid in de categorien, A, B of C, dus een afhankelijkheid van welke taken je uitvoert. Er heeft geen herbeoordeling van functieprofielen plaats gevonden. Bijkomend voordeel is dat de administratieve verwerking bij de afdeling [redacted] minder tijd in beslag neemt nu functies zijn samengevoegd.
Voor de medewerker verandert er niets bij de aanvraag van een (herhaal) onderzoek. Onlangs heeft de SG JenV de nieuwe lijst vertrouwensfuncties NCTV vastgesteld.

Naar aanleiding van bovenstaande wijzigingen is onze interne regeling ‘Omgaan met Vertrouwensfunctie’ aangepast. De belangrijkste wijzigingen zijn:

- Werken zonder VGB (met waiver):
    - Er was een oude visie op het werken zonder VGB. In 2013 was besloten dat er geen uitzonderingen (waivers) toegestaan waren voor het verrichten van werkzaamheden in afwachting van de afgifte van een VGB. Inmiddels is dit besluit door het MT NCTV herzien en kunnen onderbouwde uitzonderingen, door middel van een waiver, toegekend worden.
- Herhaalonderzoeken
    - In juni 2017 is het besluit tot het uitvoeren van herhaalonderzoeken door de BR JenV herzien en dienen alle personen die een VF bekleden in het bezit te zijn van een VGB niet ouder dan 5 jaar.

Inmiddels zijn we gestart met het uitvoeren van de herhaalonderzoeken. In overleg met de leidinggevenden worden de medewerkers aangeschreven door [redacted] voor het aanleveren van een aanvraag. De verwachte doorlooptijd van het hele project (Min JenV), om iedere medewerker te voorzien van een actueel VGB, is 5 jaar.

Stafafdeling Bedrijfsvoering

Datum
20 november 2017

Ons kenmerk
123456

Toelichting indeling vertrouwensfuncties
In het MT d.d. 20 november werd een vraag gesteld naar de criteria voor A, B of C onderzoek. Bij onderhavig besluit gaat het er om functieprofielen samen te voegen ten behoeve van harmonisering en eenduidigheid.

De en de leidinggevende kunnen de volgende criteria gebruiken voor het vast stellen van het gewenste niveau van onderzoek voor de uitvoerende taken van de medewerker;

-
-
-
-
-
-

Indien er afwegingen in dit kader moeten worden gemaakt, ook gelet op nieuwe NCTV-brede programma's waaraan medewerkers van verschillende afdelingen samenwerken, kan de beveiligingscoördinator een adviserende rol hierbij spelen.

Document vrijgegeven bij publicatie

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

~~Dep. VERTROUWELIJK~~

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. [redacted]
Postbus 20010
2500 EA Den Haag

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
[redacted]

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 11 december 2023
Onderwerp Melding mogelijk onrechtmatig bezit EU-gerubriceerde stukken

Geachte heer [redacted],

Naar aanleiding van de aanhouding van een medewerker en een oud-medewerker van de NCTV, ben ik door u geïnformeerd dat de medewerker ervan wordt verdacht onrechtmatig in het bezit te zijn van gerubriceerde documenten. Op grond van de informatie van de AIVD, acht ik het voorstelbaar dat hier ook documenten tussen zitten die een EU-rubricering kennen.

In dat kader ben ik op grond van artikel 14, derde lid, van het besluit 2013/488 inzake de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie verplicht melding te maken van dit feit aan de in Nederland bevoegde instantie. De taak van National Security Authority (NSA) is ondergebracht bij de AIVD. Derhalve doe ik via deze brief formeel melding van het feit dat er mogelijk EU-gerubriceerde informatie onrechtmatig in bezit was van een medewerker van de NCTV, waarbij deze informatie mogelijk terecht is gekomen bij onbevoegden.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd,

[redacted]

Met vriendelijke groet,

[redacted]

Pieter-Jaap Aalbersberg
Nationaal Coördinator Terrorismebestrijding en Veiligheid

~~**Dep. VERTROUWELIJK**~~

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NCTV/Pieter-Jaap Aalbersberg

Postadres
Postbus 20010
2500 EA Den Haag

Contact

Ons kenmerk

Uw kenmerk

Bijlagen
0

Datum 21 december 2023
Betreft Reactie op uw melding aangaande mogelijk onrechtmatig bezit gerubriceerde EU-stukken

Geachte heer Aalbersberg,

Bedankt voor uw brief van 11 december jl. (uw kenmerk waarin u melding maakt van het feit dat er mogelijk gerubriceerde EU-informatie onrechtmatig in bezit was van een medewerker van de NCTV. In deze brief geef ik een reactie vanuit de rol van National Security Authority (NSA). De NSA meent in dezen dat redelijkerwijs aan te nemen is dat EU-gerubriceerde informatie in gevaar is geraakt.

Conform artikel 14, vierde lid, van het besluit 2013/488 van de Raad van de Europese Unie, inzake de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie, moeten er in dit geval maatregelen genomen worden om herhaling te voorkomen. Daarom heeft de NSA onder andere de actuele accreditatiestatus van het informatiesysteem bij de NCTV beoordeeld. Hieruit blijkt dat het informatiesysteem van de NCTV op dit moment niet over de benodigde accreditatie voor de opslag en verwerking van gerubriceerde EU-informatie beschikt. Om een accreditatie af te geven, dient de NSA middels een inspectie te verifiëren of de beveiliging van het informatiesysteem voldoet aan de beveiligingseisen uit het besluit 2013/488.

In het verlengde van uw melding en het ontbreken van de accreditatie, gaat de NSA graag met u in gesprek over het inspectieproces en mogelijke andere maatregelen om herhaling te voorkomen. Ik vertrouw erop u hiermee voldoende geïnformeerd te hebben.

Hoogachtend,
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties,

de Algemene Inlichtingen- en Veiligheidsdienst

~~**Dep. VERTROUWELIJK**~~

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Document vrijgegeven bij publicatie

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Afdeling Strategie, Staf en Juridische zaken

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Contactpersoon

M

nota

Risicobeheersingsproces en aanvraag accreditatie

Datum
29 februari 2024

Projectnaam
Informatiebeveiliging

Ons kenmerk

Indienend MT-lid

Doel nota
☐ Ter bespreking ☒ Ter Besluitvorming ☐ Ter informatie ☐ Anders, namelijk:

Aanleiding
Sinds de aanhoudingen van twee (oud-)collega's van de NCTV is het buitenwerking gesteld voor de verwerking van staatsgeheime informatie van derden. Om het onderhavige weer in gebruik te nemen, is accreditatie van het systeem door SG JenV een voorwaarde. Met vaststelling van voorliggende stukken worden zijn de processen afgerond om deze accreditatie aan te vragen.

Gevraagde acties en advies
Risicobeheersingsproces :
- Instemmen met vaststelling van quickscan, risicoanalyse en risicoregister.
- Instemmen met voorgestelde risicobehandelplannen.
- Instemmen met voorlopige acceptatie van de restrisico's door de organisatie.

Aanvraag accreditatie en vervolgstappen voor heringebruikname systemen:
- Instemmen met aanvraag van accreditatie van het bij en door de NCTV.
- Kennisnemen van vervolgstappen voor heringebruikname systemen.

Toelichting op het advies
Het beheersen van de risico's van het is een randvoorwaarde voor accreditatie. Hiervoor is het risicobeheersingsproces doorlopen.
Na instemming met voorgestelde besluiten is de NCTV klaar voor de aanvraag van toestemming voor het gebruik van het voor verwerking van staatsgeheime informatie.
De hierboven genoemde onderdelen worden toegelicht in twee bijgesloten nota's.

Bijlagen
- Nota Risicobeheersing .
- Nota Aanvraag accreditatie en vervolgstappen voor heringebruikname systemen.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~**Dep. VERTROUWELIJK**~~
MT NCTV

Afdeling Strategie, Staf en Juridische zaken

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum
12 maart 2024

Ons kenmerk
[redacted]

nota

Risicobeheersing [redacted] NCTV

Aanleiding

In het kader van de heringebruikname van [redacted] binnen de NCTV is een aantal processen doorlopen t.b.v. de risicobeheersing. In deze nota worden deze processen nader toegelicht.

Gevraagde besluiten

- Instemmen met vaststelling van quickscan, risicoanalyse en risicoregister.
- Instemmen met de voorgestelde risicobehandelplannen.
- Instemmen met voorlopige acceptatie van de restrisico's door de organisatie.

Samenvatting

Voor [redacted] is het risicobeheerproces gevolgd, met als resultaat dat alle geïdentificeerde risico's die er zijn bij ingebruikname van het netwerk, na het nemen van maatregelen op een acceptabel niveau zijn en gebruik van [redacted] als veilig kan worden beschouwd.

In het risicobeheerproces zijn een quickscan en een risicoanalyse uitgevoerd. Uit de risicoanalyse zijn tien risico's geïdentificeerd die, volgens het vastgestelde NCTV-beleid, behandeling door mitigerende maatregelen of acceptatie vereisen. Voor deze risico's zijn behandelplannen opgesteld met daarin mitigerende maatregelen of het voorstel tot acceptatie. Voor een risico op niveau laag is tevens een behandelplan opgesteld. Deze behandelplannen worden na akkoord van de systeemeigenaar uitgevoerd. Voor één risico wordt acceptatie zonder mitigerende maatregelen voorgesteld. Totdat de behandelplannen uitgevoerd zijn, wordt geadviseerd de bestaande risico's voorlopig te accepteren. In de bijlage 'Risicoregister' zijn alle risico's opgenomen die behandeling vereisen.

Met het vaststellen van de hierboven genoemde stukken en het accepteren van (rest)risico's wordt tevens door het MT NCTV verklaard dat voor [redacted] voldaan wordt aan het geldende beleid (*statement of compliance*).

Afdeling Strategie, Staf en Juridische zaken

Datum
12 maart 2024

Ons kenmerk
[redacted]

Doorlopen traject: quickscan, risicoanalyse, risicobehandeling en risicoacceptatie

Als onderdeel van het traject voor accreditatie van [redacted] is het risicobeheerproces uitgevoerd voor [redacted]. Het risicobeheerproces van de NCTV is beschreven in het [redacted].

Quickscan voor het bepalen van het vereiste beveiligingsniveau

Als eerste is er een quickscan uitgevoerd. In de quickscan zijn de belangrijkste kenmerken van [redacted] vastgelegd. Onderdeel is de vaststelling van de systeemeigenaar. In dit geval is het voorstel het eigenaarschap te beleggen bij het MT NCTV, gedelegeerd aan het afdelingshoofd [redacted]

Uit de quickscan bleek dat de informatie die op [redacted] verwerkt wordt beveiligd moet worden op [redacted][2]. Conform het beleid wordt er, als het BBN-niveau hoger is dan BBN2, een risicoanalyse uitgevoerd om te bepalen welke risico's er bestaan en welke extra maatregelen genomen moeten worden om deze risico's te reduceren.

Risicoanalyse voor het bepalen van specifieke risico's van [redacted]

De risicoanalyse die uitgevoerd is leverde een groot aantal risico's met een lage risicoscore op. Volgens het risicobeheerbeleid van de NCTV zijn voor lage risico's geen aanvullende maatregelen nodig, deze risico's worden geaccepteerd. In het hierboven genoemde Beleid Risicobeheer informatiebeveiliging NCTV is beschreven dat risico's op niveau 'laag' acceptabele risico's zijn, beheersing ervan vindt plaats door reguliere managementactiviteiten.

Naast de lage risico's zijn er elf risico's geïdentificeerd die wel behandeling door de systeemeigenaar vereisen, waarna het restrisico laag en daarmee acceptabel wordt. Dit betrof drie risico's op niveau hoog, zeven risico's op niveau midden en een risico op niveau laag[3]. Deze risico's zijn opgenomen in het risicoregister.

Behandelplan voor geïdentificeerde risico's

Voor de elf geïdentificeerde risico's die opgenomen zijn in het risicoregister is volgens het risicobeheerproces van de NCTV risicobehandeling nodig. Het doel van behandeling wordt vastgelegd in risicobehandelplannen, die opgesteld zijn. De behandelplannen beschrijven welk risico het betreft, wat de inschaling in kans en impact is en welke behandeling voorgesteld wordt (acceptatie van het risico, vermijden van het risico, mitigeren van het risico of overdragen van het risico).

---

[1] Beleid Risicobeheer informatiebeveiliging NCTV, kenmerk [redacted]. Vastgesteld door MT NCTV dd. 31 januari 2024. NB Voor het [redacted] is een eerdere versie van het beleidsdocument gebruikt, omdat het beleidsdocument nog niet definitief en vastgesteld was ten tijde van de risicoanalyse.

[2] BBN-niveaus (basisbeveiligingsniveaus) zijn gedefinieerd in de Baseline Informatiebeveiliging Overheid (BIO) en geven een basisniveau van beveiliging, waaraan eisen of maatregelen gekoppeld zijn. [redacted]

[3] Omdat de impact van het als laag ingeschatte risico hoog is en de kans zich aan de bovenkant van het lage spectrum bevindt, worden hiervoor toch mitigerende maatregelen voorgesteld.

Afdeling Strategie, Staf en Juridische zaken

Datum
12 maart 2024

Ons kenmerk

Voor een van de risico's op niveau midden is in het behandelplan voorgesteld het te accepteren zonder verdere maatregelen. Nadere beschouwing van dit risico leerde dat de kans op midden gescoord was, maar dat dit dicht tegen laag aan zat.

Voor de overige risico's zijn behandelplannen opgesteld waarin voorgesteld wordt om mitigerende maatregelen te nemen. Deze maatregelen moeten het risico dat overblijft (het restrisico) tot een acceptabel, laag niveau reduceren. In het risicoregister is deze resulterende score ook opgenomen. De uitwerking van de benodigde maatregelen gebeurt door de actiehouder.

Leer- en verbeterpunten tijdens het proces
Op basis van de ervaringen met het uitvoeren van de quickscan en de risicoanalyse is er tijdens het proces voor gekozen om de methodiek voor beide onderdelen aan te scherpen.

Voor de quickscan is gekozen voor een versimpelde versie van de scan, in lijn met de geadviseerde methodiek door de Baseline Informatiebeveiliging Overheid (BIO). De in eerste instantie door de NCTV gekozen methodiek bleek complex, zonder extra waarde toe te voegen.

Voor de risicoanalyse zijn gedurende het traject twee wijzigingen doorgevoerd. Ten eerste is ervoor gekozen om in de toekomst een versimpelde lijst van mogelijke risico's te gebruiken, zonder dat dit tot een minder goed resultaat leidt. Dit maakt het proces sneller en daarmee werkbaarder. Ten tweede is ervoor gekozen om risico's in de toekomst in te schalen op een 5x5-matrix, in plaats van een 3x3-matrix. Dit biedt de mogelijkheid kans en impact van risico's met meer detail in te schalen. Gebruik ervan zou problemen die in het voorliggende traject tegengekomen zijn vermijden. Deze methodiek is tevens opgenomen in het reeds vastgestelde Beleid Risicobeheer informatiebeveiliging NCTV.

Bijlagen
- Quickscan .
- Risicoanalyse .
- Risicoregister.
- Risicobehandelplannen.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

~~Dep. VERTROUWELIJK~~

Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. dhr. [redacted]
Postbus 20010
2500 EA Den Haag

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
[redacted]

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 9 oktober 2024
Onderwerp Mogelijke inspectie NSA bij de NCTV

Geachte heer [redacted],

In reactie op uw brief van 7 oktober jl. (uw kenmerk: [redacted]), informeer ik u over het volgende. De NCTV heeft na de arrestatie van twee oud-medewerkers van de NCTV, de stroom voor EU en NAVO-gerubriceerde informatie stilgelegd. Hierover is de [redacted] geïnformeerd, alsmede medewerkers binnen uw organisatie die zich bezighouden met de NSA-taak. Deze stroom is sindsdien niet heropgestart.

In het kader van prioritering heb ik mij in de afgelopen periode geconcentreerd op het heropstarten van ons staatsgeheime netwerk [redacted], om zo staatsgeheim (nationaal) gerubriceerde informatie te kunnen verwerken. Hiervoor is de NCTV reeds op 8 april jl. geaccrediteerd door de secretaris-generaal van het ministerie van Justitie en Veiligheid. De AIVD heeft een afschrift van deze accreditatie ontvangen. Ten einde de tijdelijke accreditatie (IATO) voor het verwerken van staatsgeheime informatie in april 2025 te verlengen, dan wel om te zetten in een meer permanente accreditatie (FATO), zijn er nog een aantal activiteiten nodig binnen mijn organisatie die absolute prioriteit vergen.

Accreditatie om ook weer EU en NAVO-gerubriceerde informatie te kunnen ontvangen is hiermee lager in de prioriteit komen te staan dan de nationale accreditatie. Dit is een bewuste keuze geweest, gelet op mijn verantwoordelijkheid als Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Dit betekent echter dat op dit moment de processen binnen mijn organisatie nog niet op orde zijn om EU of NAVO-gerubriceerde informatie te ontvangen. Zodra wij de capaciteit hebben om ook de accreditatie rond EU en NAVO-gerubriceerd materiaal op te starten, zullen wij, in nauwe afstemming met de NSA, ernaar streven volledig te voldoen aan alle criteria die zijn gesteld aan de omgang met deze informatie en afspraken maken met u over het doen van een inspectie. Tot dat moment is het weinig zinvol om een inspectie bij de NCTV te doen, aangezien er op dit moment geen EU en NAVO-gerubriceerde informatiestromen lopen binnen mijn organisatie. Dit zal ook niet gebeuren, totdat de NSA en de secretaris-generaal van JenV hier expliciet toestemming voor hebben gegeven.

Vertrouwende u hiermee voldoende te hebben geïnformeerd,

Hoogachtend,

Pieter-Jaap Aalbersberg
Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV