Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Rijksbreed onderzoek sturing en beheersing informatiebeveiliging 2020

Definitief

Colofon

Titel	Rijksbreed onderzoek beheersing informatiebeveiliging 2020
Uitgebracht aan	CIO Rijk als voorzitter van het CIO-beraad
Datum	16 november 2021
Kenmerk	2021-0000231538
Referentienummer	2020-BZK-042

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

In opdracht van CIO Rijk hebben wij voor het vierde achtereenvolgende jaar onderzoek gedaan naar de sturing en beheersing van informatiebeveiliging op centraal departementaal niveau aan de hand van de 'Handreiking bij Volwassenheidsmodel Informatiebeveiliging' van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA).

Dit jaar hebben wij het aandachtsgebied Risicomanagement onderzocht. Daarnaast hebben wij onderzocht in hoeverre de departementen opvolging hebben gegeven aan de aanbevelingen uit 2019 op de overige hierboven genoemde aandachtsgebieden. Aanvullend hebben wij inzicht verschaft in de feitelijke inrichting van informatiebeveiliging bij de departementen. Hiervoor is de beveiliging van de Active Directory (AD) geselecteerd.
In dit hoofdstuk zijn de belangrijkste bevindingen uiteengezet.

Departementen blijven werken aan de centrale beheersing van informatiebeveiliging, maar nog niet alle verwachte elementen aanwezig

Alle departementen hebben het afgelopen jaar activiteiten ondernomen om de sturing en beheersing op informatiebeveiliging te verbeteren. Voor een klein deel van de departementen heeft dit ook geresulteerd in een groei in volwassenheid, voornamelijk ten aanzien van het versterken van het risicomanagementbeleid. Hierbij valt het op dat er een groot verschil zit in de volwassenheid van de departementen. Twee departementen hebben de door henzelf gestelde ambitie op alle onderwerpen behaald. De overige departementen zitten nog niet (of alleen op deelonderwerpen) op het gedefinieerde ambitieniveau.

Uit ons rijksbrede beeld komt naar voren dat bevindingen die wij de afgelopen jaren rapporteerden op het gebied van risicomanagement nog steeds standhouden. Zo heeft het grootste deel van de departementen geen volledig zicht op risico's en kwetsbaarheden van kritieke systemen. Daarnaast ontbreken soms nog fundamentele beleidstukken, zoals voor risico- en incidentmanagement. Wij beschouwen dit als een belangrijke basis voor informatiebeveiliging en vinden het zorgelijk dat dit terugkerende bevindingen zijn.

Opvolging van aanbevelingen door alle departementen opgestart, vaak nog niet volledig afgerond

In dit rapport beschrijven we ook de mate van opvolging van de vorig jaar door ons gerapporteerde aanbevelingen. Alle departementen hebben opvolging gegeven aan (een deel van) de door ons gerapporteerde aanbevelingen uit 2019. Zo zijn 15 van

de 39 aanbevelingen uit 2019 volledig opgevolgd. De overige aanbevelingen zijn deels opgevolgd, 5 aanbevelingen hebben geen opvolging gehad. De nog (deels) openstaande aanbevelingen betreffen een diversiteit aan onderwerpen, waaronder het afronden en implementeren van beleid en processen of juist het verhogen van het inzicht in de status van kritieke systemen.

Inzicht in feitelijke veiligheid nog altijd op onderdelen niet aanwezig

Op basis van de centrale monitoring van departementen zelf, signaleren wij dat ongeveer 65 procent van de kritieke systemen beschikt over een QuickScan of risicoanalyse die uitgevoerd is in de afgelopen drie jaar. Daarbij is ongeveer 25 procent van deze systemen de afgelopen drie jaar ook onderworpen aan een audit of pentest. Dit is een stijging ten opzichte van onze inventarisatie vorig jaar (respectievelijk 35 en 15 procent), voornamelijk als gevolg van de grote inspanning die twee departementen hebben geleverd. Een groot deel van de systemen die kritiek zijn voor het functioneren van de Rijksoverheid beschikt echter nog niet over een risicoanalyse of beveiligingsonderzoek (resp. 144 en 293 van de 400 kritieke systemen). Wanneer er op centraal niveau geen inzicht bestaat in de feitelijke veiligheid van de kritieke systemen, kunnen er zonder dit te weten beveiligingsrisico's bestaan.

Kwetsbaarheden aangetroffen op Active Directories

Ieder departement maakt gebruik van de Active Directory (AD) om gebruikers toegang te bieden tot de digitale werkplek en andere benodigde applicaties. Bij een hack proberen aanvallers vaak de hoogste rechten binnen een AD te verkrijgen om zich zo toegang tot andere onderdelen van de IT-infrastructuur te verschaffen. Een onveilig geconfigureerde AD kan daarom tot serieuze beveiligingsrisico's leiden.
De belangrijkste bevindingen die uit ons onderzoek naar voren zijn gekomen zijn:

a) Het gebruik van verouderde systemen en protocollen met bekende kwetsbaarheden (zogenaamde *legacy)* en
b) De op onderdelen beperkte beveiliging van beheeraccounts met hoge rechten, waardoor ze minder beschermd zijn tegen diefstal van inloggegevens.

Deze bevindingen verhogen het aanvalsoppervlak van de systemen van de Rijksoverheid. Het afgelopen jaar is gebleken dat gevonden kwetsbaarheden in softwareproducten[1] actief worden misbruikt. Hierdoor neemt het belang van adequate beveiliging van interne systemen verder toe.

Aanbevelingen CIO Rijk

Op basis van het uitgevoerde onderzoek bij de elf departementen, en bij de afdeling van CIO Rijk zelf, geven wij de volgende aanbevelingen voor het komende jaar:

- Benut de versterkte regierol om o.a. aan de hand van rijksbrede best-practices het inzicht op centraal departementaal niveau in de feitelijke veiligheid van (kritieke) systemen te bevorderen. Laat deze onderwerpen

[1] Zoals Citrix, Microsoft Exchange of diverse VPN-oplossingen

actief terugkomen in bijvoorbeeld het CISO- en CIO-beraad, in de gesprekken met de departementale sleutelfiguren en in het jaarlijks door departementen opgestelde informatiebeveiligingsbeeld.

- Stimuleer op deze wijze ook de departementen om vanuit de tweede lijn (alsmede de IT-serviceorganisaties) opvolging te geven aan de bevindingen uit de deelonderzoeken ten aanzien van de beveiliging van de Active Directory.

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

Alle organisaties binnen de Rijksoverheid moeten voldoen aan het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR). In het VIR zijn eisen voor de beheersing van informatiebeveiliging beschreven, zoals het uitvoeren van risicoanalyses voor informatiesystemen. De afgelopen jaren heeft de ADR rijksbrede onderzoeken uitgevoerd naar de sturing en beheersing op het gebied van informatiebeveiliging.

In het onderzoek van 2017 is de volwassenheid van de departementen op het gebied van informatiebeveiliging geïntroduceerd. De focus betrof de sturing en beheersing van informatiebeveiliging op centraal niveau. In 2018 en 2019 is hier vervolg aan gegeven en zijn opnieuw vier aandachtsgebieden uit het NBA/NOREA-model onderzocht: governance, organisatie, risicomanagement en incidentmanagement. In 2018 hebben de CIO's, voorafgaand aan ons onderzoek, het gewenste niveau voor de door ons onderzochte aandachtsgebieden vastgesteld.

Om wederom een actueel beeld te verkrijgen van de beheersing van informatiebeveiliging heeft CIO Rijk (DGOO), als voorzitter van het CIO-beraad, de ADR dit jaar opnieuw gevraagd onderzoek uit te voeren naar dit onderwerp.

1.1.1 Onderzoek naar sturing op en beheersing van informatiebeveiliging

Dit jaar hebben wij verdere focus aangebracht in de scope van het onderzoek door het thema risicomanagement en de opvolging van de aanbevelingen uit 2019 te onderzoeken. Risicomanagement is integraal onderzocht, omdat dit een belangrijke basis vormt voor het gericht sturen op informatiebeveiliging en het verkrijgen van inzicht in de feitelijke veiligheid van de informatiesystemen. In ons vorige onderzoek hebben wij diverse bevindingen en ontwikkelpunten over risicomanagement gerapporteerd.

1.1.2 Onderzoek naar beveiliging van de Active Directory

Aanvullend hebben wij inzicht verschaft in de daadwerkelijke inrichting van informatiebeveiliging bij de departementen. Hiervoor hebben wij de beveiliging van de Active Directory (AD) geselecteerd. Ieder departement maakt gebruik van de AD om gebruikers toegang te bieden tot de digitale werkplek en andere benodigde applicaties. Bij een hack proberen aanvallers vaak de hoogste rechten binnen een AD te verkrijgen om zo andere onderdelen van de IT-infrastructuur te kunnen bereiken. Een onveilig geconfigureerde AD kan daarom tot serieuze beveiligingsrisico's leiden. Bij dit deelonderzoek hebben we gebruik gemaakt van

een open source tool (PingCastle) die erop gericht is om snel inzicht te geven in de beveiligingsinstellingen van een AD-domein.

1.2 Doelstelling en onderzoeksvragen

Een gedetailleerde verantwoording van ons onderzoek hebben wij opgenomen in hoofdstuk 6. Hieronder lichten we kort de doelstelling en onderzoeksvragen toe.

De **doelstelling** van het onderzoek is drieledig, namelijk:

- Het inzichtelijk maken van de sturing en beheersing op het gebied van informatiebeveiliging op centraal departementaal niveau, door middel van het onderzoeken van de opvolging van de aanbevelingen uit het voorgaande onderzoek en het integraal onderzoeken van het aandachtsgebied Risicomanagement.
- Het inzichtelijk maken van de inrichting van informatiebeveiliging, gericht op de beveiliging van de Active Directory.
- Het adviseren over verbetermogelijkheden vanuit beide deelonderzoeken.

Gezamenlijk dienen deze doelstellingen ertoe goede voorbeelden en verbeterpunten te identificeren in de sturing, beheersing en inrichting van informatiebeveiliging op departementaal en rijksbreed niveau.

In dit onderzoek hebben wij de volgende vier **onderzoeksvragen** beantwoord:

1. Wat is het huidige volwassenheidsniveau bij elk departement ten aanzien van het aandachtsgebied Risicomanagement en hoe verhoudt dit zich tot het gewenste ambitieniveau?
2. Wat is de status van opvolging van aanbevelingen uit 2019 (ADR en AR) op departementaal en rijksbreed niveau?
3. Welke mogelijk onveilige instellingen bevatten de onderzochte AD-domeinen?
4. Welke verbeteringen zijn mogelijk in de sturing, beheersing en inrichting van informatiebeveiliging vanuit de bovenstaande onderzoeksvragen bij elk departement en op rijksbreed niveau?

1.3 Afbakening

Zoals hierboven aangegeven richt het onderzoek zich enerzijds op de sturing en beheersing van informatiebeveiliging en anderzijds de inrichting van feitelijke informatiebeveiligingsmaatregelen.

1.3.1 Onderzoek naar sturing op en beheersing van informatiebeveiliging: risicomanagement

Het onderzoeksobject betreft de sturing en beheersing op het gebied van informatiebeveiliging op **centraal departementaal niveau**. Hoewel wij de decentrale beheersing niet onderzoeken, onderzoeken wij wel de gemaakte

afspraken tussen het centrale en decentrale niveau en de ontvangen stuurinformatie.

Het onderzoek richt zich op **opzet** en **bestaan**: er is een beschrijving van beheersmaatregelen deze functioneren conform omschrijving. We richten ons niet op het functioneren van de beheersmaatregelen over een langere tijd (werking).

We hebben ten aanzien van sturing op en beheersing van informatiebeveiliging drie **aspecten** onderzocht:

- de opvolging van de aanbevelingen van de ADR uit 2019;
- de verrichte werkzaamheden rondom de opvolging van de aanbevelingen van de Algemene Rekenkamer uit 2019;
- het aandachtsgebied "risicomanagement", conform het NBA-volwassenheidsmodel.[2]

1.3.2 Onderzoek naar de inrichting van informatiebeveiliging: de beveiliging van de Active Directory

Wij hebben **domeinen** in productie onderzocht, die worden gebruikt voor de kantoorautomatisering van de kerndepartementen.[3]

Het onderzoek richt zich voornamelijk op het **bestaan** van een selectie beveiligingsmaatregelen op het gebied van: gebruikers- en beheeraccounts met hoge rechten, wachtwoordinstellingen, risicovolle protocollen en diverse overige mogelijke kwetsbare configuraties. In beperkte mate hebben wij de **opzet** onderzocht om een beeld te krijgen van gemaakte keuzes voor de inrichting van de AD-domeinen. Gezien dit onderzoek een eerste scan betreft van de Active Directory, hebben we ons niet gericht op de werking van beveiligingsmaatregelen, noch op de *trust*-relaties tussen de verschillende domeinen, noch op autorisaties en gebruikersbeheer.

1.4 Leeswijzer

In dit onderzoeksrapport geven wij antwoord op de vier onderzoeksvragen. In de volgende secties rapporteren wij over:

- de opvolging van de aanbevelingen uit 2019 (hoofdstuk 2);
- de sturing op en de beheersing van informatiebeveiliging (hoofdstuk 3);
- de beveiliging van de Active Directory (hoofdstuk 4) en
- de Rijksbrede verbetermogelijkheden op de sturing, beheersing en inrichting van informatiebeveiliging (hoofdstuk 5).

In hoofdstuk 6 verantwoorden wij de wijze van onderzoek. Daarna zijn de volgende bijlagen opgenomen:

[2] Zie bijlage 1. Zie ook §2.6.1. van de opdrachtbevestiging "Rijksbreed onderzoek sturing en beheersing informatiebeveiliging 2020", d.d. 28-09-2020.
[3] Zie hoofdstuk 6 voor een gedetailleerd overzicht van de scope.

- het referentiekader voor het deelonderzoek naar sturing en beheersing van informatiebeveiliging (bijlage 1);
- het referentiekader voor het deelonderzoek naar de Active Directory (bijlage 2);

2 Opvolging van de aanbevelingen uit 2019: sturing en beheersing op het gebied van informatiebeveiliging

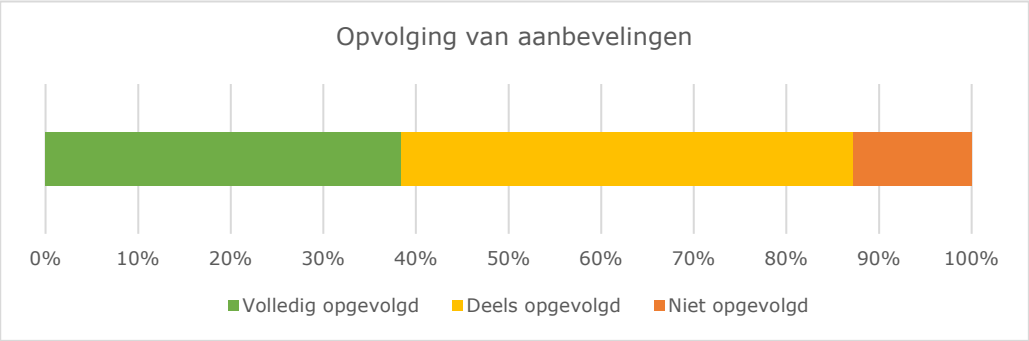
In dit hoofdstuk geven wij antwoord op de tweede onderzoeksvraag: "Wat is de status van opvolging van aanbevelingen uit 2019 (ADR en AR) op departementaal en rijksbreed niveau?"

Hierbij schetsen wij zowel een beeld van de opvolging van de aanbevelingen op departementaal niveau (sectie 2.1.), als van de aanbevelingen die wij vorig jaar hebben meegegeven aan de CIO Rijk (sectie 2.2).

In dit hoofdstuk geven wij geen overzicht van de werkzaamheden die zijn verricht rondom de opvolging van de aanbevelingen van de Algemene Rekenkamer. De departementen hebben deze beschrijving reeds ontvangen in de deelrapportages.

2.1 Activiteiten opgestart voor opvolging aanbevelingen op departementaal niveau, afronding dient veelal nog plaats te vinden

Alle departementen hebben in 2020 gewerkt aan de opvolging van aanbevelingen over 2019. De mate van opvolging is zichtbaar in de volgende figuur.



De volledig **opgevolgde aanbevelingen** relateren zich vaak aan het vernieuwen van beleid en het beleggen van taken en verantwoordelijkheden ten behoeve van de IB-organisatie. Anderzijds zien we ook dat er is gewerkt aan het verhogen van contactmomenten tussen strategisch-, tactisch- en operationeel niveau binnen de IB-organisaties van departementen, met als voornaamste doel de stuurinformatie te verbeteren.

De aanbeveling die het vaakst **open blijft staan** betreft het verkrijgen van meer inzicht in de feitelijke veiligheid van kritieke systemen. Bij de helft van de departementen ontbreekt nog een volledig overzicht van IB-risico's en uitgevoerde risicoanalyses- en beveiligingsonderzoeken.

Tot slot zijn er ook **deels opgevolgde aanbevelingen**. Hierbij zijn de benodigde activiteiten voor het opvolgen van de aanbeveling(en) vaak al gedeeltelijk uitgevoerd, maar nog niet tot afronding gebracht. Ook heeft het 'gedeeltelijk opvolgen' van een bevinding in een aantal gevallen te maken met het feit dat de organisatie voor het eerst de PDCA-cyclus doorloopt na aangebrachte wijzigingen in de IB-organisatie.

2.2 Diverse activiteiten opgestart door CIO Rijk voor opvolging aanbevelingen, risicomanagement blijft nog een rijksbreed aandachtspunt

Aanbevelingen 2019

De directie CIO Rijk heeft de verantwoordelijkheid om de vormgeving van ICT binnen de Rijksoverheid te bevorderen door kaders te stellen en toezicht te houden op de naleving daarvan. In 2019 hebben wij, naar aanleiding van onze bevindingen uit het rijksbrede onderzoek, daartoe ook aanbevelingen gedaan aan CIO Rijk:

1. Stimuleer de departementen actief om het inzicht in de feitelijke veiligheid van de (kritieke) systemen te verhogen, door onder andere periodiek risicoanalyses en beveiligingsonderzoeken uit te voeren en de belangrijkste uitkomsten centraal bij te houden;
2. Neem bij de evaluatie van de pilot van het informatiebeveiligingsbeeld ook mee welke informatie over kritieke systemen centraal minimaal dient te worden ontvangen om over voldoende sturingsinformatie te beschikken.
3. In 2019 is gestart met het opstellen van (verbeterde) CISO- en CIO-profielen. Zet de ingezette lijn voort om op rijksbreed niveau verduidelijking aan te brengen in de verdeling van verantwoordelijkheden op het gebied van informatiebeveiliging;
4. Onderzoek hierbij ook, in samenspraak met de departementen, de optimale inrichting van tweedelijns toezicht op het gebied van informatiebeveiliging, rekening houdend met de verschillende karakteristieken van de departementen.

Opvolging aanbevelingen 2020

DGOO/CIO Rijk voert periodiek CISO-gesprekken met de departementen. Hierbij worden relevante ontwikkelingen besproken, evenals de opvolging van bevindingen uit onze departementale deelrapporten over informatiebeveiliging. In deze gesprekken wordt ook ingegaan op de inhoud van de jaarlijkse In Control Verklaringen (ICV) / Informatiebeveiligingsbeelden (IBB). Ten tijde van het onderzoek was een deel van de CISO-verslagen beschikbaar. Hieruit komt naar

voren dat verschillende onderwerpen op het gebied van informatiebeveiliging worden besproken, waaronder de ICV/IBB en expliciet het thema 'feitelijke veiligheid'. Hierbij wordt de stand van zaken besproken en worden ook vervolgvragen gesteld, maar de departementen worden niet actief gestimuleerd om het inzicht verder te verhogen. De aanbeveling is daarom deels opgevolgd.

In juli 2020 is door de ICBR ingestemd met het nieuwe Informatiebeveiligingsbeeld (IBB). Dit IBB vervangt de In Control Verklaring (BIR). Het sjabloon bevat de minimaal te rapporteren informatie, maar dit betreft geen specifieke informatie over de kritieke systemen. Het IBB zou door CIO Rijk kunnen worden benut om de mate van centraal inzicht in de feitelijke veiligheid van de kritieke systemen bij de departementen te bevorderen. De evaluatie van het gebruik van het IBB heeft nog niet plaatsgevonden en zal naar verwachting eind 2021 plaatsvinden. DGOO heeft aangegeven hierbij ook de inhoud van het sjabloon mee te willen nemen. Deze aanbeveling is daarom nog niet opgevolgd.

In 2020 zijn de verbeterde CISO- en CIO-profielen definitief gemaakt en is ook het besluit CIO-stelsel door de Ministerraad goedgekeurd. De departementen dienen eind september 2021 over een plan van aanpak te beschikken om het nieuwe stelsel te implementeren in de organisatie. Met dit besluit wil BZK het besturingsmodel en het besluitvormingsproces van het CIO-stelsel verstevigen en verduidelijken. Een andere belangrijke ontwikkeling is het aanstellen van een CISO Rijk die ook als voorzitter van het CISO-overleg optreedt. De derde aanbeveling is hiermee opgevolgd.

De introductie van het Informatiebeveiligingsbeeld heeft o.a. als doel om het tweedelijnstoezicht (van de CISO) te versterken. Het vernieuwde CISO-profiel draagt hier ook aan bij. Het is echter niet gebleken dat de inrichting van tweedelijnstoezicht in zijn geheel is geëvalueerd, waarbij ook bijvoorbeeld rollen naast de centrale CISO zijn meegenomen. De vierde aanbeveling is daarmee deels opgevolgd.

3 Sturing en beheersing op het gebied van informatiebeveiliging: risicomanagement

In dit hoofdstuk geven wij antwoord op onze eerste onderzoeksvraag: "Wat is het huidige volwassenheidsniveau bij elk departement ten aanzien van het aandachtsgebied Risicomanagement en hoe verhoudt dit zich tot het gewenste ambitieniveau?"

Doelstelling risicomanagement binnen informatiebeveiliging

Risicomanagement draagt zorg voor het op gestructureerde wijze identificeren en beheersen van informatiebeveiligingsrisico's zodanig dat de risico's in lijn zijn met de risicobereidheid en het risicoraamwerk van de organisatie.

Om inzicht te krijgen in het risicoprofiel van de organisatie is het van belang om analyses uit te voeren. Met een risicoraamwerk voor informatiebeveiliging dat in lijn is met het organisatiebrede model, kunnen risico's juist worden ingeschat en kan het behalen van bedrijfsdoelstellingen ondersteund worden. Bij het uitvoeren van risicoanalyses worden plannen opgesteld om risico's te verkleinen of te accepteren. Door het uitvoeren en monitoren van deze verbeterplannen wordt schade aan de organisatie vermeden.

(Naar: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, NBA)

Voor het aandachtsgebied "risicomanagement" hebben wij de volgende thema's onderzocht:

- *Information risk management framework* (RM.01, zie §3.2)
- *Risk assessment* (RM.02, zie §3.3)
- *Risk action and mitigation plan, including risk acceptance* (RM.03, zie §3.4)

Voor wat betreft het risicomanagement van informatiebeveiliging signaleren wij de volgende ontwikkelingen en aandachtspunten:

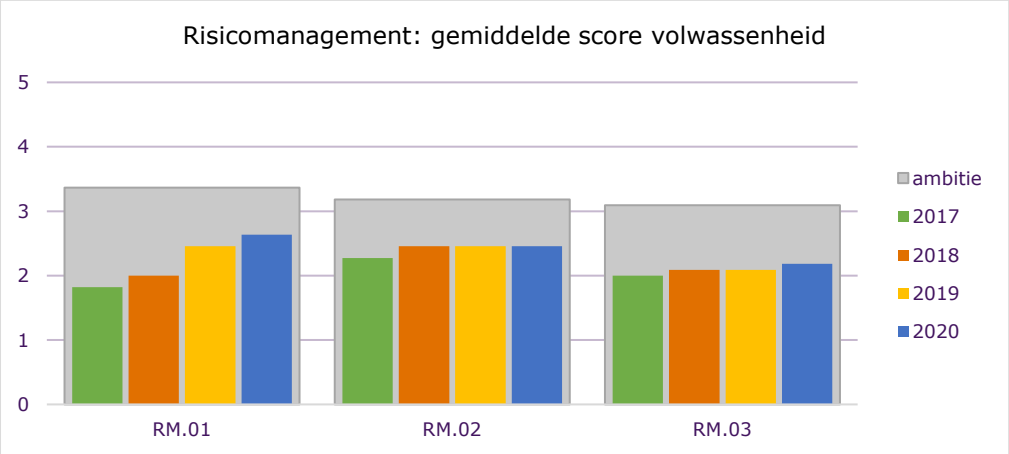
- Lichte groei in volwassenheid op het gebied van risicomanagement, maar ambitie veelal nog niet behaald;

- Risicomanagementbeleid bijna overal aanwezig, definiëren van risicobereidheid en –acceptatie blijft nog achter;
- Op onderdelen groei in verkregen sturingsinformatie van deelorganisaties, diepgang vaak nog beperkt;
- Centraal inzicht in feitelijke veiligheid van kritieke systemen op onderdelen niet aanwezig.

In de volgende paragrafen gaan wij nader in op deze bevindingen.

3.1 Lichte groei in volwassenheid op het gebied van risicomanagement, maar ambitie veelal nog niet behaald

In onderstaand figuur zijn de gemiddelde scores voor Risicomanagement (verdeeld over RM.01, RM.02, RM.03) opgenomen. Hierbij is onderscheid gemaakt tussen de scores voor 2017, 2018, 2019, 2020 en het gewenste ambitieniveau.

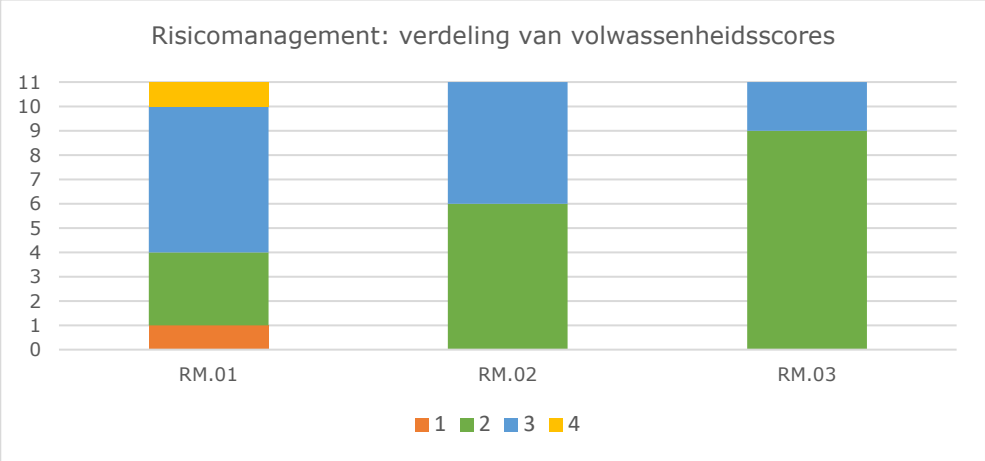


Figuur 1. *Gemiddelde scores aandachtsgebied Risicomanagement*

We rapporteren vooruitgang op de volwassenheid van RM.01: het *information risk management framework*. Ook hebben wij voor dit aandachtsgebied voor het eerst de volwassenheid van een departement gerapporteerd als “beheerst en meetbaar” (niveau 4).

Zoals blijkt uit figuur 1, merken we op dat er beperkte, meetbare vooruitgang is op de *scores va*n RM.02 en RM.03. Dat betekent niet dat geen van de departementen acties hebben ondernomen, maar dat deze niet hebben geleid tot een hoger volwassenheidsniveau.
Zo hebben vier departementen, ondanks eventuele verbeteracties, nog geen volledig zicht op de uitgevoerde risicoanalyses op kritieke systemen. Bij een deel hiervan ontbreekt bijvoorbeeld informatie vanuit de dienstonderdelen, maar bij andere departementen zijn de risicoanalyses niet uitgevoerd of sterk verouderd. Vijf departementen beschikken over een actueel overzicht van kritieke systemen en bijbehorende risicoanalyses. Overigens hebben ook deze departementen niet voor alle kritieke systemen een recente risicoanalyse beschikbaar. Twee departementen

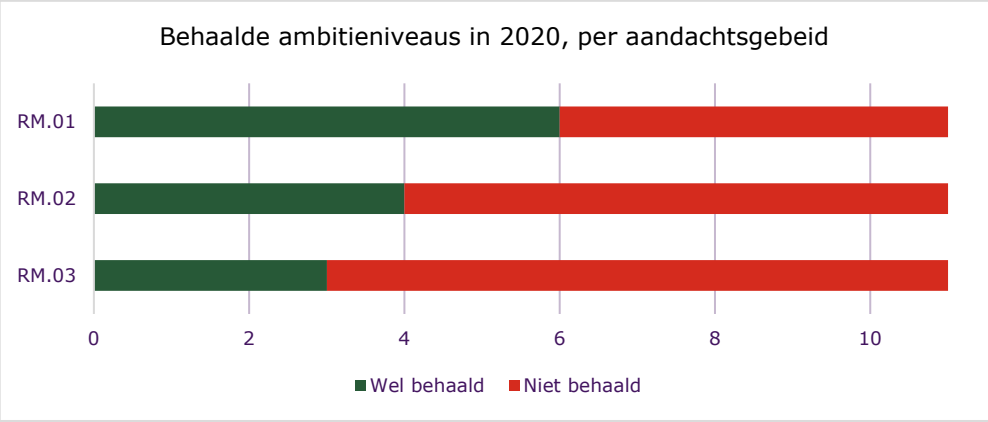
stellen volgens de geldende risicoclassificaties géén kritieke systemen te gebruiken. Tot slot zien we dat bij de helft van de departementen (op onderdelen) actief gestuurd wordt vanuit het overzicht van kritieke systemen, de overige departementen doen dit nog niet.
Deze verschillen in scores zijn terug te zien in de verdeling van volwassenheidsscores:



Figuur 2. *Verdeling van de volwassenheidsscores voor het aandachtsgebied Risicomanagement*

Uit het onderzoek komt ook naar voren dat er een groot verschil in scores is tussen de departementen, waarbij een kwart voor geen van de thema's niveau 3 behaalt.

De relatie tussen de volwassenheidsniveaus en de vastgestelde ambitie van de departementen is zichtbaar in figuur 3. Hierin wordt per aandachtsgebied weergegeven hoeveel departementen het door henzelf vastgestelde ambitieniveau hebben behaald.



Figuur 3. *Behaalde ambitieniveaus in 2020 binnen de elf departementen, ingedeeld per aandachtsgebied van het volwassenheidsmodel.*

Uit ons onderzoek komt naar voren dat twee departementen de door henzelf gestelde ambitieniveaus op alle onderwerpen hebben gehaald en dat dit voor vier van de departementen voor geen van de thema's het geval is. De overige vijf

departementen voldoen op één (4 departementen) of twee thema's (1 departement) aan hun ambitieniveau.

Daarnaast hebben twee departementen op basis van voortschrijdend inzicht het ambitieniveau bijgesteld, dit betreft zowel verlagingen als verhogingen.

3.2 Risicomanagementbeleid bijna overal aanwezig, definiëren van risicobereidheid blijft nog achter

Nagenoeg alle departementen (m.u.v. één departement waar het risicomanagementbeleid tijdens het onderzoek nog in een eerste conceptfase zat) beschikken over een recent en geformaliseerd risicomanagementbeleid. Hierbij valt een onderscheid te maken tussen:

- een integraal, organisatiebreed beleid dat geldt voor het gehele departement en dienstonderdelen;
- een op hoofdlijnen beschreven beleid, dat decentraal verder uitgewerkt dient te worden.

Ondanks dat bijna alle departementen over een recent formeel beleid beschikken, verschilt de mate van diepgang nog wel sterk per departement. Wij hebben onderzocht in hoeverre het beleid richtlijnen omschrijft voor de volgende elementen: a) risicobereidheid, b) risico-eigenaarschap, c) risicoproces, d) risicobeoordeling, e) risicomitigatie en f) risicoacceptatie.
Zes departementen benoemen alle elementen in hun beleid. Vier departementen hebben niet alle, maar wel de meeste elementen opgenomen.

We constateren dat voornamelijk de risicobereidheid niet formeel is beschreven. Risicobereidheid is van belang voor het beheersen van risico's tot een geaccepteerd niveau. Momenteel is dit vaak nog informeel vormgegeven.

Een aantal departementen heeft de intentie om het beleid in 2021 te herijken om bijvoorbeeld nieuwe elementen toe te voegen of om het beleid niet te laten verouderen (minimaal eens per drie jaar te actualiseren en opnieuw vast te stellen).

3.3 Op onderdelen groei in verkregen sturingsinformatie van deelorganisaties, diepgang vaak nog beperkt

Op centraal departementaal niveau ontvangen de CIO-offices sturingsinformatie vanuit hun organisatieonderdelen. De wijze van aggregatie hiervan, de frequentie en de diepgang verschillen per departement.

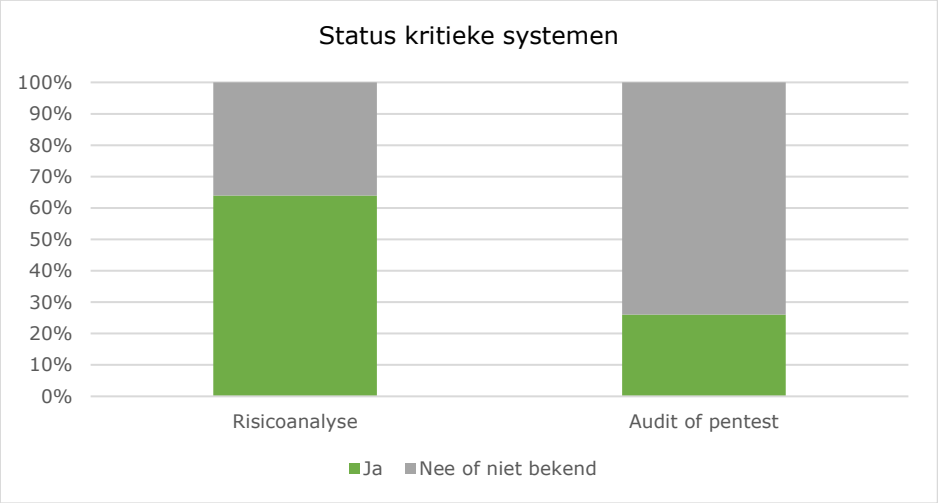
Bij het merendeel van de departementen zien we dat het centrale inzicht verloopt via de jaarlijkse cyclus op het IB-proces; de In Control Verklaring (ICV) of het nieuwe Informatiebeveiligingsbeeld (IBB). Dienstonderdelen leveren hierbij input aan, vaak via een deel-ICV.

Gedurende de jaarlijkse cyclus van het IB-proces halen de meeste departementen ook tussentijds sturingsinformatie op bij de deelorganisaties. Dit vindt op verschillende manieren plaats. Voorbeelden hiervan zijn periodieke (control)gesprekken vanuit de CISO-office, het opvragen van zelfevaluaties, proef-ICV's of toezichtrapportages.

De departementen gebruiken verschillende formats en tools om stuurinformatie te verzamelen. Voorbeelden hiervan zijn risicolijsten, risicokaarten op basis van te beschermen belangen (TBB), GRC-tooling of een samenwerkingsruimte op het intranet.
Departementen ondernemen steeds meer activiteiten om relevante informatie vanuit de dienstonderdelen op centraal niveau te verzamelen en structureren. De status van kritieke systemen is op centraal niveau vaak echter nog niet volledig bekend. De meeste departementen houden bij wanneer voor het laatst een QuickScan (QS) of risicoanalyse uit is gevoerd en ongeveer de helft vult dit aan met uitgevoerde beveiligingsonderzoeken en lopende verbeteracties. De overige departementen hebben hier op centraal niveau geen zicht op. Een klein deel houdt ook de restrisico's bij. Overigens geven twee departementen aan niet over kritieke systemen te beschikken.

3.4 Centraal inzicht in feitelijke veiligheid van kritieke systemen op onderdelen niet aanwezig

In de praktijk blijkt ook dat voor een groot deel van de kritieke systemen uit deze centrale vastlegging nog niet naar voren komt dat er recentelijk a) een QuickScan of risicoanalyse of b) een audit of pentest uit is gevoerd.
'Recent' definiëren we hierbij als maximaal drie jaar oud. Zie hiervoor ook de onderstaande figuur (fig. 5).



Figuur 4 *- Rijksbrede status van de kritieke systemen*

Op basis van de centrale monitoring van departementen zelf, signaleren wij dat ongeveer 65 procent van de kritieke systemen beschikt over een recente risicoanalyse en ongeveer 25 procent van de kritieke systemen de afgelopen drie

jaar is onderworpen aan een audit of pentest. Hierbij constateren wij een significante groei ten opzichte van het voorgaande onderzoek in 2019, waarbij de percentages respectievelijk 35 en 15 procent betroffen. De stijging in het aantal risicoanalyses/QuickScans is voornamelijk veroorzaakt doortwee departementen die een inhaalslag hebben uitgevoerd en/of hun overzichten sterk hebben verbeterd.

Het is echter van belang om op te merken dat een derde van de geregistreerde kritieke systemen nog steeds niet beschikt over een recente risicobepaling, en dat een minderheid van de systemen maar recentelijk is getoetst op feitelijke veiligheid. Een informatiesysteem is kritiek als bij falen de uitvoering van een kerntaak niet langer kan worden gegarandeerd of een te beschermen belang van de organisatie niet langer kan worden beschermd (bron: *Toelichting model in control verklaring inzake informatiebeveiliging 2019, 23 augustus 2019*). Wanneer er op centraal niveau geen inzicht bestaat in de feitelijke veiligheid van de kritieke systemen, kunnen er zonder dit te weten beveiligingsrisico's bestaan.

4 Beveiliging van de Active Directory

In dit hoofdstuk geven wij antwoord op de derde onderzoeksvraag: “welke mogelijk onveilige instellingen bevatten de onderzochte Active Directory domeinen?”.

Hierbij schetsen wij op hoofdlijnen het Rijksbrede beeld dat naar voren is gekomen uit de resultaten van de PingCastle-tool voor de dertien onderzochte domeinen bij vier verschillende IT-serviceorganisaties. Alleen bevindingen die in meerdere deelrapportages zijn gerapporteerd, zijn hieronder opgenomen.

Wij signaleren de volgende ontwikkelingen en aandachtspunten:

- Aanvullende beveiligingsopties voor beheeraccounts niet altijd benut;
- Aandacht nodig voor inactieve beheeraccounts en mogelijke aanvalspaden;
- Verouderde en onveilige functionaliteiten in gebruik;
- Verouderde Windows-versies aangetroffen. Gebruik van ESU (Extended Security Update) en bijbehorend risicomanagement niet onderzocht;
- Aandacht voor MS Azure en monitoring van de AD gevraagd.

De detailbevindingen zijn opgenomen in de deelrapportages die aan de departementen uit zijn gebracht.

5 Rijksbrede goede voorbeelden en verbetermogelijkheden

Vanuit ons onderzoek hebben wij deelrapportages opgeleverd aan de departementen. In deze rapportages hebben wij aanbevelingen geschreven die specifiek zijn voor die departementen. De aanbevelingen dringen veelal aan op het verstevigen van de centrale regierol en het ophalen van stuurinformatie vanuit de dienstonderdelen. Ook het delen en inzetten van rijksbrede best-practices is een aanbeveling die aan meerdere departementen is meegegeven.

In dit hoofdstuk gaan wij nader in op de Rijksbrede aanbevelingen voor de CIO Rijk voor zowel de sturing en beheersing, als de inrichting van informatiebeveiliging. Daarnaast geven wij aan wat volgens de onderzoekers goede voorbeelden zijn voor andere departementen op deze gebieden. Op deze wijze kan het delen en inzetten van best practices verder worden gestimuleerd.

5.1 Aanbevelingen aan CIO Rijk

Op basis van het uitgevoerde onderzoek bij de elf departementen, en bij de afdeling van CIO Rijk zelf, geven wij de volgende aanbevelingen:

- Benut de versterkte regierol om o.a. aan de hand van rijksbrede best-practices het inzicht op centraal departementaal niveau in de feitelijke veiligheid van (kritieke) systemen te bevorderen. Laat deze onderwerpen actief terugkomen in bijvoorbeeld het CISO- en CIO-beraad, in de gesprekken met de departementale sleutelfiguren en in het jaarlijks door departementen opgestelde informatiebeveiligingsbeeld.
- Stimuleer op deze wijze ook de departementen om vanuit de tweede lijn (alsmede de IT-serviceorganisaties) opvolging te geven aan de bevindingen uit de deelonderzoeken ten aanzien van de beveiliging van de Active Directory.

5.2 Goede voorbeelden

Voorgaande jaren hebben wij telkens goede voorbeelden op departementsniveau opgenomen in onze overkoepelende rapportage. Wij zijn van mening dat deze voorbeelden nog altijd voor departementen bruikbaar zullen zijn, zoals het *risicoregister van J&V*. In de volgende secties zijn een aantal goede voorbeelden uitgelicht onder de activiteiten die in 2020 zijn ondernomen.

5.2.1 Risk letters: verantwoordelijkheid eerste lijn

Het ministerie van Algemene Zaken legt in haar nieuwe proces verantwoordelijkheid voor IB-risico's expliciet in de eerste lijn. Vanuit het departementale CISO-office

worden, op basis van geïdentificeerde IB-risico's, zogeheten *Risk Letters* verzonden aan de betreffende systeemeigenaar. Deze bevatten de gelopen risico's en een advies en tijdlijn voor het uitvoeren van de verbeteringen. Centraal wordt vervolgens gemonitord op de voortgang op deze verbeterplannen. Wel merken we op dat dit proces nog relatief nieuw is en de werking van de beheersingsmaatregelen nog deels moet worden aangetoond.

5.2.2 Red teaming: inzicht in de feitelijke veiligheid van het netwerk

Het ministerie van Financiën heeft het afgelopen jaar ethische hackers ingeschakeld om de beveiliging van een specifieke IT-omgeving te toetsen. Specifiek voor de Active Directory heeft ook de IT-serviceorganisatie DICTU het afgelopen jaar ethische hackers ingezet voor dit doel. Op deze manier kan actief inzicht worden gewonnen in eventuele zwakke plekken om de beveiliging naar een hoger niveau te tillen.

5.2.3 Control-gesprekken voor inzicht in decentrale ontwikkelingen

Bij dit onderzoek zien we een jaarlijkse toename in het aantal departement dat tussendoor formele gesprekken voert met haar deelorganisaties. Voorgaande jaren noemden we al de *toezichtscyclus van SZW*. Ten tijde van ons onderzoek heeft ook het ministerie van Binnenlandse Zaken en Koninkrijksrelaties de gesprekscyclus uitgebreid, door viermaandelijks gesprekken met de CIO's van de dienstonderdelen over de ontwikkelingen rondom IB (alsmede andere i-onderwerpen) te starten. Ter voorbereiding voor het IB-gedeelte vindt een gesprek plaats tussen de betreffende CISO's en wordt een I-Agenda opgesteld. Het gesprek wordt inhoudelijk voorbereid op basis van de interne rapportages die de onderdelen opstellen als onderdeel van het IB-Beeld BZK. De ICV's en proef-ICV's zijn hiermee vervallen. De gesprekscyclus zal volgens planning eind 2021 voor het eerst volledig zijn doorlopen.

5.2.4 CISO-brieven: actieve sturing op informatiebeveiliging

Vorige jaren rapporteerden wij over de ICV-cyclus van BZK, waarbij de deelorganisaties van reactie op de deel-ICV's worden voorzien. Dit jaar hebben we een vergelijkbare ontwikkeling bij EZK aangetroffen. Eens per jaar worden zogenaamde CISO-brieven gestuurd met specifieke aanbevelingen per organisatie. De inhoud en opvolging van deze aanbevelingen wordt in de CISO-gesprekken met dienstonderdelen meegenomen. Ook kunnen de aanbevelingen terugkomen in periodieke gesprekken tussen de pSG en hoofden van de dienstonderdelen.

6 Verantwoording onderzoek

6.1 Werkzaamheden en afbakening

6.1.1 Uitgevoerde werkzaamheden

In de periode van eind september 2020 tot en met medio februari 2021 hebben wij veldwerkzaamheden uitgevoerd bij de departementen.

Onderzoek naar sturing op en beheersing van informatiebeveiliging

De departementen hebben middels een zelfevaluatie het gewenste en huidige niveau van informatiebeveiliging, met onderbouwing, aangegeven. Hierin hebben de departementen ook de status van de opvolgingen van de aanbevelingen aangegeven.

De zelfevaluatie is tijdens een kick-off toegelicht en in detail besproken tijdens interviews op centraal niveau met betrokkenen (bijv. CISO, CIO, CISO-office, BVA). De departementen hebben deze betrokkenen aangewezen. Bij sommige departementen is naar aanleiding van deze interviews aanvullende informatie opgevraagd.

Ieder departement heeft het onderzoeksteam van de ADR een terugkoppeling gegeven in het kader van hoor/wederhoor. Deze terugkoppeling betrof het huidige volwassenheidsniveau. Er is gebruik gemaakt van een standaard presentatieweergave met een indicatie per departement.

Onderzoek naar de beveiliging van de Active Directory

Er is een beknopte vragenlijst opgesteld met daarin vragen over de configuratie van de Active Directory. Deze is ingevuld op basis van één of meerdere gesprekken met de beheerders van de betreffende AD-domeinen. Beheerders hebben vooraf de ADR van onderbouwende documentatie voorzien. Ieder departement heeft de verantwoordelijke betrokkenen aangewezen.

Per AD-domein is gebruik gemaakt van de tool PingCastle[4] voor het vaststellen van de huidige instellingen gedurende de onderzoeksperiode. Voor het onderzoek is een selectie gemaakt van de controles (*rules*) in PingCastle.

Ieder departement heeft het onderzoeksteam van de ADR een terugkoppeling gegeven in het kader van hoor/wederhoor. Deze terugkoppeling betrof de aangetroffen situatie. Er is gebruik gemaakt van een standaard presentatieweergave met een indicatie per departement.

[4] PingCastle 2.9.1.0

6.1.2 *Object van onderzoek*

Onderzoek naar sturing op en beheersing van informatiebeveiliging

Zoals hiervoor kort beschreven zal dit deelproject uit de volgende onderdelen bestaan:

- Onderzoek naar de opvolging van aanbevelingen uit het voorgaande ADR-rapport (over 2019).
- Onderzoek naar de werkzaamheden die uitgevoerd zijn om opvolging te geven aan de aanbevelingen van de Algemene Rekenkamer in het verantwoordingsonderzoek over 2019[5].
- Integraal onderzoek naar het aandachtsgebied Risicomanagement uit het NBA-volwassenheidsmodel (op dezelfde wijze als in het onderzoek over 2019).

Afbakening

Het object van onderzoek betreft telkens de sturing en beheersing op het gebied van informatiebeveiliging op centraal departementaal niveau (veelal bij het CIO-office en/of Beveiligingsambtenaar) voor het gehele departement. Sturing en beheersing van informatiebeveiliging op centraal departementaal niveau dient om invulling te geven aan art. 3 en art. 4 van het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR:2007).

Ons onderzoek richt zich op opzet (is er een beschrijving van de maatregelen) en bestaan (functioneren de maatregelen op het moment van onderzoek conform de opzet?) van de aandachtsgebieden zoals in de vorige sectie omschreven. Wij richten ons bij dit onderzoek niet op de beheersing van informatiebeveiliging op decentraal (dienstonderdeel) niveau, wel onderzoeken wij de gemaakte afspraken tussen centraal en decentraal omtrent informatiebeveiliging en de aanwezigheid van stuurinformatie op centraal niveau. Ook richt ons onderzoek zich niet op de werking (het functioneren van de maatregelen over een langere tijd).

Opvolging aanbevelingen

Onderzoek naar de opvolging van aanbevelingen bestaat uit a) indexeren welke aanbevelingen in 2019 af zijn gegeven, en op basis van welk risico en/of gap deze afgegeven zijn en b) onderzoeken welke werkzaamheden door het departement uit zijn gevoerd om het oorspronkelijke risico en/of gap weg te nemen. Indien er aanleiding is om te vermoeden dat er door de uitgevoerde werkzaamheden aanvullende risico's zijn ontstaan, zullen deze ook mee worden genomen in het onderzoek.

[5] Deze zijn niet opgenomen in dit eindrapport, wel in de deelrapporten.

Aandachtsgebied risicomanagement
Om het object van onderzoek 'de sturing en beheersing op het gebied van informatiebeveiliging' volgens het VIR:2007 te verduidelijken gebruikt dit onderzoek een selectie aandachtsgebieden uit een NBA-volwassenheidsmodel over informatiebeveiliging. Het NBA-volwassenheidsmodel wordt in bijlage 1 verder toegelicht.

In de centrale beheersing speelt de veiligheid van kritieke systemen een belangrijke rol. Wij beschouwen het centrale ICV-dossier van een departement als de eigen verantwoording over informatiebeveiliging. De minimale verwachting is dat uit het centrale dossier blijkt wat de status is van informatiebeveiliging voor de kritieke systemen van het departement, en dat centraal toezicht ingericht is op de betrouwbare werking van de kritieke systemen. Om dit inzicht te krijgen maakt de ADR onder meer gebruik van eerder door de ADR uitgevoerde IB-gerelateerde onderzoeken op een departement. De frequentie van het toezicht is gebaseerd op basis van risicoafweging bij het departement. Indien een departement geen kritieke systemen (volgens de rijksbreed vastgestelde definitie) kent, zal het onderzoek zich richten op de bedrijfskritische systemen van een departement.

Onderzoek naar de beveiliging van de Active Directory
Zoals hiervoor kort beschreven zal dit deelproject zich richten op de Active Directory (AD) domeinen van de departementen die gebruikt worden voor de kantoorautomatisering. Per AD-domein zal worden onderzocht of best practices op het gebied van beveiliging en configuratie toe zijn gepast.

Afbakening
Het deelproject richt zich op de domeinen in productie die worden gebruikt voor de kantoorautomatisering van de kerndepartementen. Domeinen die worden gebruikt voor bijvoorbeeld test-, acceptatie- of beheeromgevingen vallen buiten de scope, evenals mogelijke *trust*-relaties[6] tussen verschillende domeinen.

Het onderzoek richt zich voornamelijk op het *bestaan* (zijn de maatregelen ingeregeld op het moment van onderzoek) van een selectie beveiligingsmaatregelen op het gebied van:

- Gebruikers-/beheeraccounts met hoge rechten;
- Wachtwoordinstellingen;
- Risicovolle protocollen;
- Diverse overige mogelijke kwetsbare configuraties.

Het onderzoek zal zich in beperkte mate ook op de *opzet* richten (is er een beschrijving van de maatregelen?) om een beeld te kunnen krijgen van de keuzes die ten grondslag liggen aan de inrichting van de AD-domeinen. Wij richten ons bij

[6] Een trust-relatie tussen domeinen biedt de mogelijkheid om objecten, zoals user accounts, buiten het eigen domein te gebruiken.

dit onderzoek niet op *trust*-relaties tussen verschillende domeinen of op autorisaties en gebruikersbeheer. Ook richt ons onderzoek zich niet op de werking (het functioneren van de maatregelen over een langere tijd).

6.1.3 Gehanteerde referentiekader

Voor het onderzoek naar de sturing op en beheersing van informatiebeveiliging hebben wij het aandachtsgebied "risicomanagement" gehanteerd vanuit de "Handreiking Volwassenheidsmodel Informatiebeveiliging". Het referentiekader is opgesteld door de Ledengroep Intern en Overheidsaccountants (LIO) van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA). Het doel van het referentiekader is organisaties te ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging. Deze hebben wij in Bijlage 1 van dit rapport opgenomen.

Er is gekozen voor dit aandachtsgebied op basis van de relatief lage volwassenheidsscores in 2019 in vergelijking met de gestelde ambitieniveaus. Daarnaast beschouwen wij risicomanagement als een belangrijke basis voor het verkrijgen en onderhouden van inzicht in de feitelijke veiligheid van informatiesystemen.

Voor het onderzoek naar de inrichting van informatiebeveiliging naar de Active Directory is een referentiekader samengesteld op basis van een selectie uit de beveiligingsadviezen van Microsoft, de ANSSI Active Directory Security Assessment Checklist en literatuur over bekende kwetsbare instellingen. Dit referentiekader is tijdens de opdrachtformulering afgestemd met DGOO. Het referentiekader is opgenomen in Bijlage 2 van dit rapport.

De tool PingCastie maakt gebruik van rules om vast te stellen of een bepaalde configuratiekwetsbaarheid aanwezig is in een AD-domein. Voor dit onderzoek is een selectie gemaakt van deze rules om het bestaan van kwetsbaarheden in de bovenstaande onderwerpen te onderzoeken. Zie hiervoor eveneens Bijlage 2. Deze selectie hebben wij toegepast op AD-Domeinen in scope en naar aanleiding van de resultaten zijn uitzonderingenrapportages opgesteld.

6.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van

kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

6.3 Verspreiding rapport

De opdrachtgever, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

7 Ondertekening

's-Gravenhage, 16 november 2021

Projectleider

Auditdienst Rijk

Pijnacker, 16 november 2021

Deelprojectleider Active Directory

Auditdienst Rijk

8 Managementreactie

In deze rapportage is een rijksbreed beeld geschetst van het per departement onderzochte deelgebied Risicomanagement, de mate waarin opvolging is gegeven aan de aanbevelingen die de ADR vorig jaar heeft gedaan en de beveiliging van de Active Directory als onderdeel van de feitelijke inrichting van informatiebeveiliging. De deelrapporten waarop deze rapportage is gebaseerd zijn door de ADR besproken met de CISO's van de kerndepartementen.
De CIO Rijk en de kerndepartementen spreken hun waardering uit voor de wijze waarop de ADR de onderzoeken heeft uitgevoerd en de resultaten daarvan heeft toegelicht.

In het besef dat op het gebied van informatiebeveiliging nog veel werk moet worden verzet stellen wij het op prijs dat de ADR erkenning geeft voor de activiteiten die alle departementen hebben ondernomen om de sturing en beheersing op informatiebeveiliging te verbeteren voor de wederom rijksbreed geconstateerde lichte groei in volwassenheid die daarmee is bereikt.

Tot slot herkennen wij ons in de hoofdlijn van de bevindingen en nemen wij de aanbevelingen van de ADR over. Het versterken van het inzicht op centraal departementaal niveau in de feitelijke veiligheid van (kritieke) systemen is inmiddels al onderwerp van gesprekken met de departementen, waarin de compleetheid van het risicobeeld (zoals het zicht op kritische systemen en de uitgevoerde risicoanalyses en securitytesten) wordt besproken.

Ook zal onderzocht worden of in het voorbeeldsjabloon voor het informatieveiligheidsbeeld hier meer nadruk of handvatten voor nodig zijn. De noodzaak voor bestuurders om inzicht te hebben in risico's die te maken hebben met informatiebeveiliging of cybersecurity is ook benoemd als een van de speerpunten voor digitale weerbaarheid in de nieuwe I-strategie van de Rijksoverheid. De opvolging van bevindingen rond het AD-onderzoek zal vanuit CIO Rijk actief worden gestimuleerd.

CIO Rijk en voorzitter van het CIO-beraad

Bijlage 1: Referentiekader aandachtsgebied "risicomanagement"

Het aandachtsgebied "risicomanagement" is als volgt uitgewerkt in het NBA-volwassenheidsmodel:

Aandachtsgebied	**Referentie NBA volwassenheidsmodel**	**Onderdeel[7]**
Risicomanagement	RM.01	Information risk management framework
	RM.02	Risk assessment
	RM.03	Risk action and mitigation plan (including risk acceptance)

De volgende vijf niveaus en bijbehorende leidende criteria zijn in het volwassenheidsmodel onderkend:

Niveau	**Naam**	**Omschrijving**	**Criteria**
1	Initieel	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2	Herhaalbaar	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd • Uitvoering is consistent en standaard • Informeel en grotendeels gedocumenteerd
3	Gedefinieerd	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar.	• Control gedefinieerd o.b.v. risico assessment • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken eenduidig toegewezen • Opzet, bestaan en effectieve werking aantoonbaar
4	Beheerst en meetbaar	De effectiviteit van de beheersmaatregelen wordt	• Periodieke (control) evaluatie en opvolging vindt plaats

[7] In dit onderzoek wordt de benaming van het NBA volwassenheidsmodel aangehouden in het Engels.

		periodiek geëvalueerd en kwalitatief gecontroleerd.	• Rapportage management vindt plaats
5	Continu verbeteren	Een ecosysteem is verankerd en draagt zorg voor een continue en effectieve controle en risico beheersing	• Self-assessment, gap en root cause analyses • Real time monitoring • Inzet automated tooling

Bijlage 2: Referentiekader voor de beveiliging van de Active Directory

Categorieen	PingCastle rules
Gebruikers/beheeraccounts met hoge rechten	• At least one Administrator Account can be delegated (P-Delegated) • At least one Domain controller is not owned correctly (P-DCOwner) • Check for Dangerous rights found in OU delegation (P-DangerousExtendedRight) • Ensure that Exchange did not introduce security vulnerabilities • Ensure that GPO items cannot be modified by any user • Ensure that the privilege to log on Domain Controllers are not granted to everyone by GPO • Check for inactive Administrator Accounts • Check for Native administrator usage • Check for Number of Administrator accounts above the baseline • Check if there is a control path involving everyone-like groups. • Check if there is a control path involving too much users or computers. • Check if Service Accounts are domain administrators • Ensure that dangerous privileges are not granted to everyone by GPO • Check for suspicious account(s) used in administrator activities • Check if admin accounts are vulnerable to the kerberoast attack. (P-Kerberoasting)
Wachtwoordinstellingen	• Check if all admin passwords are changed on the field. (P-AdminPwdTooOld) • Mitigate golden ticket attack via a regular change of the krbtgt password • Check for Accounts using Smart Card with unchanged password for a long time • Check if the LAPS tool to handle the native local administrator password is installed • Check for GPO which enable reversible passwords • Find Password GPO • Check for GPO allowing accounts without password to be accessed from the network • Check for Short password length in password policy

Risicovolle protocollen	• Check the use of Kerberos with weak encryption (DES algorithm) • DC Vulnerability (SMB v1)
Diverse overige mogelijke kwetsbare configuraties	• Check if all privileged accounts are in the special group Protected Users. (P-ProtectedUsers) • Ensure that all login scripts cannot be modified by any user (P-DelegationLoginScript) • Ensure the "automatic administrative logon" feature of the recovery mode is not enabled • Ensure that the printer spooler cannot be abused to get the DC Credentials • Check for local backdoor stored in SID History • Obsolete OS hele categorie • DC Vulnerability (MS14-068) • DC Vulnerability (MS17-010) • Retrieve data from the domain without any account

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