Informatiebeveiliging en privacy

Bestuurlijke nota

Rekenkamer Hoeksche Waard

Februari 2022

Samenstelling rekenkamer Hoeksche Waard:

Mevrouw mr. drs. A.M.M. (Sandra) van Breugel (voorzitter)
Mevrouw A. (Lize) Kooijman MSc
De heer mr. drs. J. (Jelle) Stelpstra
Mevrouw drs. P. (Patricia) Feelders (secretaris-onderzoeker)

Inhoudsopgave

Voorwoord

Informatiebeveiliging en privacy kan best een technisch onderwerp zijn. Wanneer doe je het als gemeente goed en hoe beoordeel je dat als gemeenteraad? Dat is lastig en tegelijkertijd kunnen de gevolgen van kwetsbaarheden ten aanzien van informatiebeveiliging en privacy groot zijn, zo blijkt uit de voorbeelden die we geven in de paragraaf over de aanleiding voor dit onderzoek.

De Rekenkamer Hoeksche Waard (RK HW) heeft gemeend dat zij de gemeenteraad kan helpen door de informatiebeveiliging en privacy te onderzoeken: niet alleen beleidsmatig, maar ook technisch en praktisch. Lukt het om digitaal of fysiek binnen te dringen bij de gemeente? Dit is niet gedaan door een echte hacker, maar door een ethisch hacker.

De gemeenteraad krijgt met dit onderzoek een beeld van de stand van zaken van informatiebeveiliging en privacy en aanbevelingen aan het college en aan de gemeenteraad zelf om nog sterker te worden op dit onderwerp. Is de gemeente Hoeksche Waard dan beschermd tegen iedere cyberaanval? Die garantie is nooit te geven. Het blijft een proces van alert zijn en blijven.

Dit onderzoek bestaat uit een bestuurlijke nota die is geschreven door de RK HW zelf en uit twee feitenonderzoeken. Eén naar het meer beleidsmatige deel van het onderwerp door Prae Advies en één naar het meer praktische deel door Hoffmann. Vanzelfsprekend is de RK HW verantwoordelijk en aanspreekbaar voor alle drie de onderdelen. Het beleidsmatige deel (onderzoek door Prae Advies) is, voordat de conclusies door de RK HW zijn getrokken, aangeboden aan de ambtelijke organisatie voor een feitencheck. De ambtelijke organisatie heeft hierop een schriftelijke reactie gegeven. Die is door de RK HW grotendeels overgenomen in de eindversie.

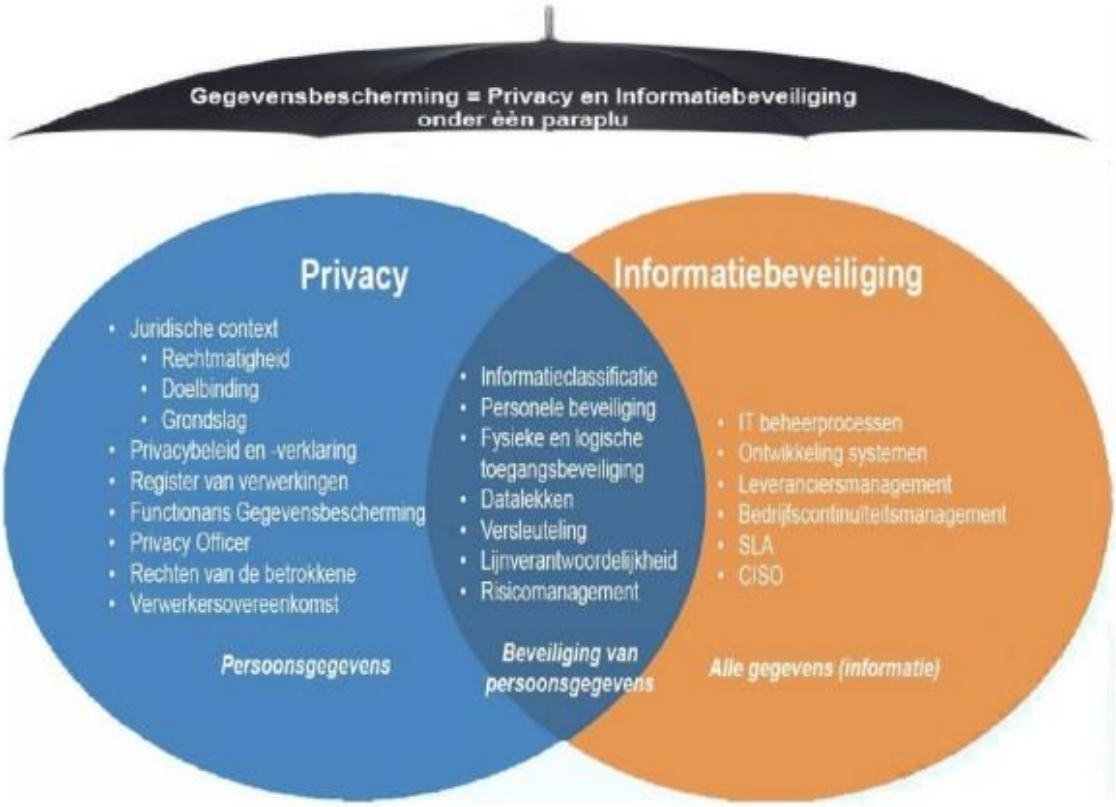
De RK HW bedankt de beide onderzoeksbureaus voor hun werkzaamheden. Ook dank aan de betrokken ambtenaren en het gemeentebestuur voor de prettige en constructieve samenwerking. In het bijzonder kijkt de RK HW terug op een waardevolle en goede samenwerking met de CISO.

Hierbij wenst de RK HW de gemeenteraad veel succes met het stellen van kaders en het controleren daarvan voor de informatiebeveiliging en privacy bij de gemeente Hoeksche Waard. Met dit onderzoek in handen kan de raad hopelijk een goede dialoog voeren met het college. De RK HW wenst ook het college en de ambtelijke organisatie veel succes met de ontwikkelingen op dit belangrijke beleidsterrein. De impact van een hack kan groot zijn op inwoners en bedrijven. Dat wil niemand, ook de RK HW niet. Met dit onderzoek beoogt de RK HW een bijdrage te hebben geleverd aan het up-to-date houden van de informatiebeveiliging en privacy in de gemeente Hoeksche Waard.

De Rekenkamer Hoeksche Waard.

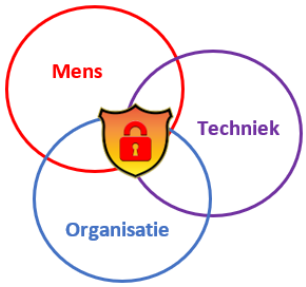
Aanleiding

Informatiebeveiliging en privacy zijn actuele onderwerpen die een reëel risico vormen voor een gemeente. Gemeenten beheren en verwerken veel persoonsgegevens, tegenwoordig meer dan vroeger, door bijvoorbeeld de decentralisaties in het sociaal domein. Informatiebeveiliging en privacy zijn nauw met elkaar verbonden, zoals onderstaande figuur illustreert.



Bron: Gemeente Utrecht (2019). *Beleid voor gegevensbescherming 2019-2022*

Organisaties die persoonsgegevens gebruiken moeten deze volgens de Algemene verordening gegevensbescherming (AVG) beveiligen. Volgens de AVG moeten persoonsgegevens "worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt."



Het gaat hierbij niet alleen om techniek, maar ook om hoe je als organisatie met persoonsgegevens omgaat. Met andere woorden: de menselijke factor en de cultuur van de ambtelijke organisatie zijn medebepalend.

Door de coronacrisis en het massale thuiswerken is bij 36 procent van de gemeenten de informatieveiligheid afgenomen.[1] De Autoriteit Persoonsgegevens meldt dat in 2020 de meeste datalekken zijn veroorzaakt doordat persoonsgegevens naar een verkeerde ontvanger gaan.[2] Dit type datalek is de belangrijkste oorzaak voor de stijging van het aantal datalekken bij de overheid (in 2020 13% meer datalekken dan in 2019). De sector Openbaar Bestuur staat op een gedeelde tweede plaats als het gaat om het aantal datalekmeldingen in 2020.
De Autoriteit Persoonsgegevens ziet in 2020 een toename in het aantal datalekken door hacking, malware of phishing. Ook gemeenten zijn een doelwit van hackers. Een voorbeeld is de hack op 1 december 2020 bij de gemeente Hof van Twente, waarbij gegevens op de servers van de gemeente ontoegankelijk werden gemaakt voor de gemeente, de back-up deels vernietigd was en de gemeente wekenlang stillag.[3]

Informatiebeveiliging en privacy zijn actuele onderwerpen die een reëel risico vormen voor een gemeente en daarom heeft de RK HW hiernaar onderzoek gedaan. Dit onderzoek is de RK HW niet gestart om de vinger te heffen wat er niet goed gaat, maar om een preventieve bijdrage te leveren aan de gemeente op dit beleidsterrein. De ambtelijke organisatie kan hier haar voordeel mee doen.

Onderzoeksmethode

De RK HW heeft besloten om het onderzoek op te splitsen in twee delen en elk deel te gunnen aan een onderzoeksbureau dat voor dat deel bij uitstek geschikt is. Het onderzoek naar het beleidsmatige deel van informatiebeveiliging en privacy is uitgevoerd door Prae Advies door middel van deskresearch en interviews. Het praktische en technische deel van het onderzoek is uitgevoerd door Hoffmann. Hoffmann heeft digitale en fysieke penetratietesten uitgevoerd en een phishingmail naar medewerkers en raad verzonden. Beide bureaus voerden het onderzoek in opdracht van de RK HW uit. De RK HW is verantwoordelijk voor het onderzoek en de uiteindelijke rapportage.

Als bijlage bij dit bestuurlijke deel vindt u de nota van bevindingen van Prae Advies. Gezien de aard van de bevindingen van Hoffmann zijn deze niet op detailniveau opgenomen in de nota van bevindingen. Uiteraard worden deze bevindingen wel gedeeld met betrokkenen van de ambtelijke organisatie, zodat zij die kunnen gebruiken om kwetsbaarheden op te lossen. Eén kwetsbaarheid die acute actie vergde, is tijdens het onderzoek direct gemeld aan de ambtelijke organisatie en die heeft dat doortastend opgepakt.

Gezien het onderwerp worden er relatief veel technische termen en afkortingen gebruikt. De RK HW heeft geprobeerd deze zoveel mogelijk uit te schrijven danwel toe te lichten. In de nota van bevindingen van Prae Advies is tevens een verklarende woordenlijst opgenomen.

Centrale vraag

De onderzoeksvraag luidt:

“Hoe heeft de gemeente Hoeksche Waard de beveiliging van informatie en privacy georganiseerd en geborgd?”

[1] https://www.binnenlandsbestuur.nl/digitaal/nieuws/thuiswerken-bedreigt-informatieveiligheid.16315532.lynkx
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf
[3] https://www.hofvantwente.nl/actueel/veelgestelde-vragen-cyberaanvalhack-gemeentehuis

Onderzoeksvragen

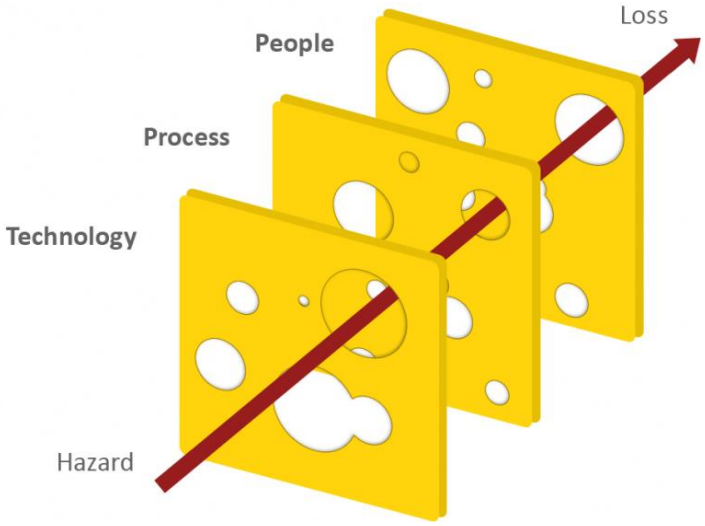
De deelvragen bij dit onderzoek zijn als volgt:

1. **Beleid van de gemeente:** Welk beleid voert de gemeente Hoeksche Waard op het gebied van informatiebeveiliging? In hoeverre stuurt het college van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatiebeveiliging, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO)?
2. **Risico's bij informatiebeveiliging en privacy:** Welke risico's bij informatiebeveiliging en privacy heeft de gemeente benoemd? In hoeverre worden risico's beheerst dan wel geaccepteerd? Op welke wijze zijn de (eind)verantwoordelijken aangewezen en de autorisaties geregeld? Welke maatregelen worden genomen om risico's te laten afnemen?
3. **Bewust omgaan met informatiebeveiliging:** Op welke manier zet de gemeente in op het bewust omgaan met informatie? Hoe gaan de medewerkers van de gemeente in de praktijk om met informatiebeveiliging? In hoeverre dragen bestuur en medewerkers het informatiebeveiligingsbeleid uit? Op welke manier rapporteert en bespreekt de organisatie het functioneren van informatiebeveiliging op management- en bestuursniveau (college en raad)?
4. **Bewust omgaan met privacy**: Hoe heeft de gemeente de Algemene verordening gegevensbescherming (AVG) van de EU geïmplementeerd in haar werkwijzen? Hoe worden medewerkers hierop actief getraind? In hoeverre dragen bestuur en medewerkers het privacybeleid uit?
5. **Toetsen van informatiebeveiliging:** In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden? Wat zijn de gevolgen voor inwoners en ondernemers als toegang door onbevoegden wordt verkregen? In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of pen-testen? In hoeverre is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en hoe ziet het incidentenmanagementproces eruit?
6. **Toetsen van partners en leveranciers op informatiebeveiliging:** Op welke manier toetst de gemeente partners en leveranciers op informatiebeveiligingsaspecten?
7. **Lerende houding t.o.v. informatiebeveiliging:** Hoe houdt de gemeente kennis over informatiebeveiliging vast, hoe bouwt zij hierop voort en leert ze hiervan? Op welke wijze wordt aandacht besteed aan de verdere bewustwording bij medewerkers van de gemeente?
8. **Opvolging onderzoek Rekenkamercommissie Hoeksche Waard 2016:** Welke opvolging is gegeven aan het onderzoek van de rekenkamercommissie Hoeksche Waard uit 2016 getiteld "ICT-samenwerking en informatiebeveiliging van de vijf Hoeksche Waard gemeenten"?[4]

Algemeen beeld

Zoals eerder aangegeven is er bij informatiebeveiliging sprake van een samenspel van techniek, organisatie en mensen. Een veelgebruikt figuur hierbij is het gatenkaasmodel (zie onderstaand figuur). Dit model geeft aan dat een systeem uit meerdere lagen bestaat, waarbij het risico van een dreiging verkleind wordt door op elke laag een beveiliging toe te passen.

[4] De VVD-fractie heeft hier in 2019 ook technische vragen over gesteld, deze konden toen nog niet volledig worden beantwoord omdat de gemeente Hoeksche Waard nog bezig was een aantal zaken te implementeren.



Bron: Het gatenkaasmodel van prof. James Reason, aangepast aan cybersecurity.[5]

Het gatenkaasmodel geeft inzicht in de impact en schade die veroorzaakt wordt door tekortkomingen in de ICT-technologie, processen (het opvolgen en het monitoren ervan) en tot slot de menskant. De theorie geeft inzicht dat als er menselijke fouten worden gemaakt, en die worden er gemaakt in een lerende organisatie, de techniek het mogelijk maakt om bijtijds de menselijke fout inzichtelijk te maken zodat de schade beperkt blijft. Ook geeft het model inzicht dat als er een calamiteit plaatsvindt met grote gevolgen, dit te maken heeft met zwakte in de techniek *én* het niet volgen van processen *én* het niet adequaat monitoren *én* de menselijke fouten die zijn gemaakt. Het is een systeem. Het model impliceert niet dat als de techniek op orde is dat er geen calamiteiten kunnen gebeuren.

Het algemene beeld dat de RK HW heeft gekregen in de gemeente Hoeksche Waard is dat de technische kant en het organisatorische aspect van informatiebeveiliging en privacy goed zijn, maar aan de mens-kant kwetsbaarder is. Het is menselijk om fouten te maken. Terecht besteedt de gemeente Hoeksche Waard aandacht aan de bewustwording van mensen door instrumenten in te zetten als trainingen.

Uit het onderzoek is gebleken dat het niet mogelijk was om het netwerk van de gemeente Hoeksche Waard van buitenaf te benaderen. Dat is een belangrijke eerste waarborg voor informatiebeveiliging. Eenmaal op het netwerk, bleek uit het onderzoek dat er diverse verbeteringen mogelijk zijn. Ook bleek dat er een groot bewustzijn is over het onderwerp, dat beleid en uitvoering ten aanzien van informatiebeveiliging en privacy steeds sterker worden en dat de ambities groot zijn.
Uit het onderzoek blijken diverse voorbeelden waarbij het menselijk handelen de zwakste schakel lijkt te zijn ten aanzien van informatiebeveiliging en privacy. Te gemakkelijk toegankelijke ruimtes, open kasten of zwak gekozen wachtwoorden kunnen leiden tot risico's.

Het algemene beeld van de RK HW is dan ook dat de basis voor informatiebeveiliging en privacy op orde is, maar dat het onderwerp tevens dagelijkse aandacht vergt. De ontwikkelingen gaan snel, de gemeente moet alert blijven. Een kleine onzorgvuldigheid ten aanzien van dit onderwerp heeft immers potentieel grote gevolgen. De gevolgen van een hack kunnen een grote impact hebben op de gemeente.

Hierna gaan we gedetailleerder in op de conclusies uit het onderzoek.

[5] Verkregen op 3 februari 2022 van https://securityandpeople.com/2017/07/human-errors-in-cyber-security-a-swiss-cheese-of-failures/

Conclusies

Om de onderzoeksvragen te beantwoorden is gebruik gemaakt van een normenkader. Onderstaand worden per onderzoeksvraag de normen besproken met bijbehorende conclusie.

Onderzoeksvraag 1: Beleid van de gemeente

Normen onderzoeksvraag 1. Beleid van de gemeente
- Het college stelt het integrale beleid ten aanzien van informatiebeveiliging en privacy vast.
- Er vindt sturing plaats op basis van de BIO.
- Op onderdelen van informatiebeveiliging en privacy is beleid geformuleerd en zijn richtlijnen opgesteld, zoals gebruik van wachtwoorden, 2 factor authenticatie, mobiele datadragers, autorisaties en monitoring, protocol datalekken, wijzigingsbeleid enz.

Strategisch beleid

Het strategisch beleid op informatiebeveiliging is voor de periode 2020-2024 beschreven volgens de BIO (Baseline informatiebeveiliging Overheid, dit zijn vastgestelde richtlijnen voor alle gemeenten in Nederland) en is vastgesteld door college. Verantwoordelijkheden zijn beschreven en belegd. Het beleid op privacy is volgens de AVG (Algemene Verordening Gegevensbescherming) en is ook door college vastgesteld.
Functies op informatiebeveiliging en privacy zijn ingevuld bij de gemeente Hoeksche Waard op strategisch niveau, met de CISO (Chief Information Security Officer), FG (Functionaris Gegevensbescherming) en PO (Privacy Officer). Ten aanzien van privacy is de functie ook op tactisch niveau ingevuld. Voor informatiebeveiliging is op tactisch niveau echter nog niet in een functie voorzien. Wel wordt een TISO (Technical Information Security Officer) geworven die hierbij een rol zou kunnen vervullen.
De CISO en PO zijn bij het team Control ondergebracht in het Privacy & Informatieveiligheidsteam (PIV). Regelmatig overleg is er met de concerncontroller en de externe FG. Twee jaar geleden is een stuurgroep met teammanagers ingesteld naast het PIV, maar die rol moet nog nader worden ingevuld.
Sturing vindt in principe plaats op basis van de BIO, die risicogeoriënteerd van opzet is.

Protocollen

De gemeente heeft meerdere protocollen opgesteld, zoals een wachtwoordenbeleid, back-up en restorebeleid, toegangsrechten, enz. Een integraal continuïteitsplan ontbreekt en deze wordt door de teammanager ICT opgesteld. De verdeling van verantwoordelijkheden hierop voor ICT en de vakteams, zoals Integrale veiligheid, moet nog worden vastgelegd in het beleid.

Conclusie 1: Het beleid van de gemeente Hoeksche Waard op het gebied van informatiebeveiliging en privacy is grotendeels op orde.

Onderzoeksvraag 2: Risico's bij informatiebeveiliging en privacy

Normen onderzoeksvraag 2. Risico's bij informatiebeveiliging en privacy
- Het informatiebeveiligingsbeleid is opgesteld aan de hand van een GAP-analyse.
- Jaarlijks wordt op basis van een risicoanalyse het informatiebeveiligingsplan ingevuld.
- De gemeente neemt maatregelen om risico's te verlagen.

Planvorming

Het informatiebeveiligingsplan of implementatieplan wordt tweejaarlijks opgesteld op basis van een risicoanalyse. De capaciteit op tactisch niveau ontbreekt om een plan jaarlijks op te

stellen. Overigens schrijft de BIO voor dat er periodiek een dergelijk plan wordt opgesteld, zonder een jaartermijn te noemen.

Maatregelen

Op basis van de jaarlijkse ENSIA-rapportages[6] en de pentesten worden maatregelen getroffen om de gesignaleerde risico's aan te pakken. Informatieveiligheid wordt halfjaarlijks gemonitord op basis van een meting van de vordering op de 112 BIO-maatregelen. Dat is op te vatten als een gap-analyse tussen enerzijds de aangetroffen realiteit en de BIO-norm.
Ook over opzet, bestaan en werking van AVG-beleid wordt halfjaarlijks gerapporteerd. Daarnaast rapporteert de gemeente over informatiebeveiliging op de VNG-site 'waarstaatjegemeente.nl', die openbaar is en voor externe partijen te benaderen is.
Het volwassenheidsniveau op informatiebeveiliging (op basis van de NOREA-norm[7]) van de gemeente is groeiende en wordt eind 2021 op niveau 2 gewaardeerd (schaal 1 tot en met 5; cijfer 3 betekent in control).
De beheersingsmaatregelen zijn in opzet aanwezig, maar worden op informele wijze toegepast. De proceseigenaren in de lijn zijn nog niet in staat om de risicoanalyses op te stellen en maatregelen te prioriteren die nodig zijn voor het implementatieplan. Dat vormt een risico op ineffectiviteit. Dat wil zeggen dat op operationeel niveau de kennis om de risico's te inventariseren en prioriteren niet aanwezig is, en ook niet met externe ondersteuning wordt opgepakt. In het plan voor 2022 wordt voorgesteld voorlopig de risico's te accepteren en de verantwoordelijkheid voor een programma om maatregelen daarop te nemen op directieniveau te beleggen.

Conclusie 2: De risico's bij informatiebeveiliging en privacy bij de gemeente Hoeksche Waard zouden meer in kaart gebracht kunnen worden, met name op tactisch niveau ontbreekt de kennis.

Onderzoeksvraag 3: Bewust omgaan met informatiebeveiliging

Normen onderzoeksvraag 3. Bewust omgaan met informatiebeveiliging
- Het beleid ten aanzien van informatiebeveiliging wordt gepubliceerd voor werknemers en relevante externe partijen.
- Medewerkers krijgen cursussen, trainingen e.d. hoe om te gaan met informatie.
- Medewerkers weten wat ze wel en niet mogen/moeten doen met gegevens en herkennen incidenten en rapporteren deze ook daadwerkelijk.
- Het bestuur en medewerkers dragen het beleid ten aanzien van informatiebeveiliging actief uit.
- Over het functioneren van informatiebeveiliging wordt gerapporteerd aan het management, bij voorkeur op basis van een ISMS (Information Security Management System).
- Over het functioneren van informatiebeveiliging wordt gerapporteerd aan de raad, in ieder geval jaarlijks in het kader van ENSIA.
- De CISO is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren.

Beleid

Het beleid, de protocollen en de standaarden met betrekking tot informatiebeveiliging en privacy worden voor de medewerkers gepubliceerd.Het merendeel is op het intranet aanwezig en beschikbaar voor medewerkers.

E-learning

Medewerkers krijgen via e-learning op de Hoeksche Campus een gevarieerd en wisselend aanbod aan cursussen en trainingen over informatiebeveiliging en privacy. Voor nieuwe medewerkers zijn deze trainingen verplicht om meteen mee te beginnen en voor de andere medewerkers zijn die deels jaarlijks verplicht. Daar wordt niet altijd door teammanagers op

[6] ENSIA (Eenduidige Normatiek Single Information Audit), dit wordt door gemeenten gebruikt om zich te verantwoorden over de staat van hun informatiebeveiliging.
[7] https://www.norea.nl/download/?id=6223

gestuurd. De functionarissen op informatiebeveiliging en privacy geven aan deelname van de medewerkers te gaan volgen.

Bewustzijn

Bewustwording op informatiebeveiliging en privacy neemt volgens de respondenten toe en de functionarissen krijgen steeds meer vragen hierover. De bereidheid om incidenten te melden, zoals phishingmails of (vermoede) datalekken, neemt toe. Bewustzijn kan altijd beter en vergt continu aandacht, zoals ook blijkt uit de testen die in het kader van dit rekenkameronderzoek zijn uitgevoerd. Het kan altijd beter en de gemeente werkt daar continu aan door middel van e-learning (Hoeksche Campus). Er zijn verplichte modules, maar die zitten nog niet in het blikveld van alle medewerkers.

Rapportages

De CISO rapporteert halfjaarlijks aan directie en college over de voortgang van de BIO-maatregelen. De jaarlijkse ENSIA-rapportage gebeurt nog niet met behulp van een Information Security Management System (ISMS). Er is in aanzet een ISMS aanwezig, maar dat is nog niet geheel uitgerold en gevuld omdat team Control en de FG met andere informatiesystemen werken. Dat betekent een risico op ineffectiviteit en inefficiëntie, omdat de informatie op informatiebeveiliging, benodigd voor de rapportages niet geautomatiseerd verzameld en verwerkt wordt.

Informatie raad

De raad krijgt in het kader van de P&C-cyclus gerapporteerd over informatiebeveiliging. Dat gebeurt in het jaarverslag van de gemeente en in de jaarlijkse ENSIA-rapportage. In de ENSIA doet de gemeente verslag van de (zelf)audits op verschillende applicaties, zoals DigiD en Suwinet[8]. Met de ENSIA-systematiek rapporteert de gemeente verticaal aan de landelijke toezichthouders en horizontaal aan de gemeenteraad als lokale toezichthouder. Daarmee voldoet het college aan de minimumeisen van de BIO. Er wordt geen gebruik gemaakt van de zogenoemde “vrije ruimte” die de ENSIA biedt om de raad aanvullend te informeren over informatiebeveiliging en privacy.

Positie CISO

De CISO is in principe geëquipeerd en gepositioneerd om diens taak te kunnen uitvoeren bij team Control, en met een eigen lijn naar de portefeuillehouder op informatiebeveiliging en de burgemeester. Er ontbreekt een tactische capaciteit op informatiebeveiliging, waardoor de CISO ook nog veel op tactisch en operationeel terrein bezig is. Er wordt een TISO geworven om op technisch vlak daarin te voorzien.

Conclusie 3: De gemeente Hoeksche Waard stimuleert het bewust omgaan met informatiebeveiliging.

Onderzoeksvraag 4. Bewust omgaan met privacy

Normen onderzoeksvraag 4. Bewust omgaan met privacy
- De gemeente werkt volgens de regels van de AVG.
- Medewerkers krijgen cursussen, trainingen e.d. hoe zij moeten werken in overeenstemming met de AVG.
- Het bestuur en medewerkers dragen het beleid ten aanzien van privacy actief uit.
- De FG is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren.

AVG

De gemeente werkt op het gebied van privacy in principe volgens de regels die de AVG voorschrijft. De FG constateert in zijn halfjaarlijkse rapportages aan het college een stijgende lijn in het uitdragen van beleid en sturing door het bestuur.

[8] Suwinet is een digitale infrastructuur waarin partijen als UWV, Sociale Verzekerings Bank (SVB) en gemeenten gegevens kunnen uitwisselen.

DPIA's

Een DPIA (Data Protection Impact Assessment) wordt uitgevoerd wanneer gegevensverwerking waarschijnlijk een hoog risico oplevert. Het uitvoeren van DPIA's komt langzaam maar zeker van de grond. Twee zijn afgerond en vier zijn in een afrondende fase. De proceseigenaren zijn daarvoor in principe de opdrachtgever. Op operationeel gebied van privacy hebben de proceseigenaren nog veel ondersteuning nodig.

FG

De FG is als extern adviseur gepositioneerd en geëquipeerd om de taak adequaat uit te voeren, mede omdat er op tactisch niveau ondersteuning is. De gemeente is bezig met de opstart van een AVG-werkprogramma. Door de aandacht voor de operationele uitvoering komt de PO vooralsnog niet toe aan de werking van een structureel activiteitenprogramma.

Conclusie 4: De gemeente Hoeksche Waard werkt in principe volgens de regels van de AVG en besteedt extra aandacht aan de DPIA's.

Onderzoeksvraag 5. Toetsen van informatiebeveiliging

Normen onderzoeksvraag 5. Toetsen van informatiebeveiliging
- Gegevens zijn goed beschermd tegen ongewenste invloeden van buitenaf.
- Er wordt jaarlijks een beveiligingsaudit uitgevoerd.
- Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd.
- Op de systemen is logging geïnstalleerd en er is capaciteit aanwezig om deze te monitoren.

Testen

De gemeente laat jaarlijks door externen verschillende pentesten uitvoeren om de informatiebeveiliging (techniek) en het risicobewustzijn van medewerkers te testen. Op de geconstateerde risico's worden verbetermaatregelen getroffen. Dat gebeurt ook naar aanleiding van de jaarlijkse ENSIA-rapportages en de (zelf)audits die de gemeente uitvoert, of laat uitvoeren. Met name de audits op Suwinet en DigiD zijn streng en de collegeverklaring over deze twee audits moet worden gecheckt door een gecertificeerde auditor. De rapportage over de BRP en Reisdocumenten, en andere applicaties, verloopt vooralsnog via een apart traject, maar maakt wel onderdeel uit van ENSIA.

Pentesten

In het kader van het rekenkameronderzoek zijn in opdracht van de Rekenkamer door Hoffmann diverse pentesten uitgevoerd: een externe en een interne netwerktest, een wifi-netwerktest, een mystery guest (fysieke inlooptest) en een phishingmail. De eerste drie zijn vooral gericht op de techniek, de laatste twee grotendeels op de mens (bewustzijn). Samenvattend kwamen uit de testen een paar kritieke bevindingen naar voren en voor het merendeel punten die meer aandacht behoeven. Deze worden naar aanleiding van dit rapport met de gemeente gedeeld en kunnen successievelijk worden verholpen.

Externe netwerktest

Uit de externe netwerktest, uitgevoerd in opdracht van de Rekenkamer, blijkt dat het moeilijk is om ongeautoriseerd van buiten het gemeentelijke netwerk naar binnen te komen. Een kritiek risico met betrekking tot een server is meteen met en door de CISO opgepakt. De overige bevindingen uit de testen zijn van lager risico en betreffen onder andere risico op spoofing (verzenden van een email uit naam van de gemeente), multifactor authenticatie (2FA) en zwakke wachtwoorden.

Interne netwerktest

Uit de interne netwerktest blijkt dat het mogelijk was om ongeautoriseerd toegang te krijgen tot het systeem van de gemeente, maar het lukte niet om het domein onder controle te krijgen. Verder zijn onder andere wachtwoorden en bijzondere persoonsgegevens aangetroffen.

Mystery guest

Uit de inlooptest die de RK HW heeft laten uitvoeren blijkt dat een mystery guest ongehinderd over meerdere dagen toegang kon krijgen tot een drietal servicepunten. Daarbij is geprobeerd technisch toegang te krijgen tot de informatiesystemen en is het risicobewustzijn van medewerkers getest. De mystery guest is gedurende de test nauwelijks aangesproken door medewerkers en heeft (vertrouwelijke) informatie kunnen inzien, waaronder privacygevoelige WMO-aanvragen.

Mail-phishing

Om het bewustzijn bij medewerkers en (burger)raadsleden te toetsen is in opdracht van de Rekenkamer door Hoffmann een phishing mail verzonden. 22% van de medewerkers en 3% van de (burger)raadsleden hebben op de link in de mail geklikt. Respectievelijk 6% en 3% heeft een gebruikersnaam en wachtwoord ingevoerd waarmee een kwaadwillende op het netwerk kan komen. Deze resultaten zijn gemiddeld in vergelijking met andere gemeenten die door Hoffmann zijn onderzocht, maar maken duidelijk dat medewerkers en (burger)raadsleden hierop nog kunnen leren.

Logging

Een manier om informatiebeveiliging en de ongeautoriseerde toegang tot gegevens te toetsen is logging[9]. Een aantal systemen wordt gelogd omdat dat wettelijk afgedwongen is, zoals bij DigiD en Suwinet. Daarnaast past de gemeente logging op een aantal andere systemen toe. De logging en de check daarop is nog niet in een procedure vastgelegd. Procedure is dat bij verdacht verkeer achteraf kan worden gecheckt wie toegang had tot welke informatie en dat systemen door systeembeheer kunnen worden gecontroleerd op inbraken en uitval. Ook de firewall wordt elke twee weken gecheckt op verdacht verkeer.

Conclusie 5: De technische informatiebeveiliging van de gemeente Hoeksche Waard is merendeels op orde, maar de menselijke kant vertoont kwetsbaarheden.

Onderzoeksvraag 6. Toetsen van partners en leveranciers op informatiebeveiliging

Normen onderzoeksvraag 6. Toetsen van partners en leveranciers op informatiebeveiliging

- De gemeente heeft in beeld met welke partners (bijzondere) persoonsgegevens worden gedeeld met behulp van het verwerkingsregister.
- De gemeente maakt met partners en leveranciers afspraken over het veilig uitwisselen en verwerken van persoonsgegevens en de daarvoor te nemen maatregelen, bij voorkeur op basis van 'privacy by design'.
- Partners en leveranciers rapporteren jaarlijks over het verwerken van persoonsgegevens.

Verwerkingsregister

De gemeente heeft in beeld met welke partijen (bijzondere) persoonsgegevens worden gedeeld, met behulp van het verwerkingsregister. Bij contracten met partners die namens of voor de gemeente persoonsgegevens verwerken moeten verwerkersovereenkomsten worden afgesloten. Om de proceseigenaren te helpen bij het bepalen of zo'n verwerkersovereenkomst nodig is wordt een checklist gebruikt.

[9] Bijhouden wie waar toegang tot heeft.

Aanbestedingen

Bij nieuwe aanbestedingen en contracten wordt in principe voldaan aan de eisen die informatiebeveiliging en privacy stellen. Bij alle nieuwe aanbestedingen en contracten wordt door de proceseigenaar gecheckt of (bijzondere) persoonsgegevens worden verwerkt en of een verwerkersovereenkomst nodig is. Daarbij dient ook gecontroleerd te worden of 'privacy by design'[10] als uitgangspunt is genomen voor de uitvoering van de opdracht.
Het bovenstaande geldt voor alle aanbestedingstrajecten van softwarepakketten die centraal worden gecheckt door de CISO en PO. Echter, er is geen standaard centrale controle op aanbestedingen en contracten beneden de €50.000.
Er lopen oude contracten die waarschijnlijk niet volledig voldoen wat betreft de voorwaarden die de AVG stelt. Deze moeten bij vernieuwing worden aangepast aan de nieuwe wet- en regelgeving, en dan gelden de bovenstaande richtlijnen. Als de gemeente meer zekerheid zou willen verkrijgen over, van, voor de AVG-risico's in die contracten zou daarvan een tussentijdse scan kunnen worden gemaakt.

Third Party Memorandum

De partners en leveranciers moeten bij het afsluiten van contracten met een verwerkersovereenkomst op een onafhankelijke wijze kunnen aantonen dat zij voldoen aan de gestelde veiligheidseisen. Dat kunnen ze doen door een accountantsverklaring te overleggen of een Third Party Memorandum (TPM) en ze moeten zich bereid verklaren mee te werken aan een controle en datalekprocedure, als de gemeente dat verlangt of daartoe verplicht is.

Conclusie 6: De gemeente Hoeksche Waard heeft in beeld met welke partijen (bijzondere) persoonsgegevens worden gedeeld, maar bij kleinere of oudere contracten kunnen zich risico's voordoen op het gebied van informatiebeveiliging en/of privacy.

Onderzoeksvraag 7. Lerende houding ten opzichte van informatiebeveiliging

Normen onderzoeksvraag 7. Lerende houding t.o.v. informatiebeveiliging
- De gemeente heeft procedures om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren.
- Het ISMS, indien aanwezig, is gekoppeld aan de PDCA-cyclus.

Incidentmanagement

De Rekenkamer heeft een protocol aangetroffen hoe om te gaan met (de melding van) datalekken. Er is een handelwijze afgesproken hoe om te gaan met incidenten. Deze worden bijgehouden in Topdesk en worden halfjaarlijks geanalyseerd door de CISO en PO. Veelvoorkomende of serieuze incidenten, zoals datalekken, worden geëvalueerd met het betreffende team. Aangegeven is dat erover wordt gedacht om een geautomatiseerd systeem te implementeren om dreigingen te monitoren en te analyseren (SOC/SIEM[11]). Er is ook geen protocol aangetroffen voor een groot informatiebeveiligingsincident.

ISMS

Aan een Information Security Management System is een beleidsleercyclus, of PDCA (Plan-Do-Check-Act) cyclus, gekoppeld. Zoals hiervoor al is geconstateerd, is dat voor informatiebeveiliging niet geheel uitgerold en gevuld. Daardoor kan niet optimaal worden gebruikgemaakt van deze tool. Activiteiten moeten vanuit verschillende systemen handmatig worden overgezet en dat is een risico op inefficiëntie.

[10] Al bij het ontwerp rekening houden met privacy.
[11] https://www.vngrealisatie.nl/nieuws/siem-en-soc-verhogen-digitale-weerbaarheid

Conclusie 7: De gemeente Hoeksche Waard kan de lerende houding ten opzichte van informatiebeveiliging verder versterken.

Onderzoeksvraag 8. Opvolging onderzoek Rekenkamercommissie Hoeksche Waard 2016

Normen onderzoeksvraag 8. Opvolging onderzoek Rekenkamercommissie Hoeksche Waard 2016
- De gemeente heeft gevolg gegeven aan de aanbevelingen van het Rekenkamercommissie-rapport Hoeksche Waard uit 2016.

Aanbevelingen 2016 Een van de 5 aanbevelingen uit 2016 is geheel opgevolgd. Dat betreft de prioritering van maatregelen op basis van een classificatie van risico's. Zoals eerder in deze conclusies aangegeven, is het beleid van de BIO en de uitvoering ervan door de gemeente risicogestuurd. Het implementatieplan kon echter, vanwege het ontbreken van een door het lijnmanagement opgestelde en onderbouwde risicoanalyse, niet adequaat worden opgesteld. In aanzet is die aanbeveling wel geïmplementeerd, maar in de uitvoering is die nog niet geheel opgevolgd.

Vier aanbevelingen zijn deels opgevolgd, mede door de fusie en corona. Aangegeven wordt dat alsnog met de vier aanbevelingen aan de slag wordt gegaan, zoals de businesscase die eind 2021 wordt verwacht en de aanvulling op de rapportages met aanbevolen prestatie-indicatoren op doelmatigheid en dagelijks beheer.

Conclusie 8: De aanbevelingen uit het onderzoek van de Rekenkamercommissie Hoeksche Waard 2016 zijn deels opgevolgd.

Aanbevelingen

De materie rondom informatiebeveiliging en privacy is complex. Met het oog op de nota van bevindingen kunnen de volgende aanbevelingen worden gedaan.

Aanbevelingen aan het college

1. Stel jaarlijks de ambitie vast ten aanzien van informatiebeveiliging en privacy en voorzie die ambitie van de nodige middelen.
2. Neem in deze ambitie versterking van het volwassenheidsniveau van de organisatie mee.
3. Neem noodzakelijke maatregelen, op basis van een risicoanalyse. Gebruik hierbij mede de pentesten die in het kader van het rekenkameronderzoek zijn uitgevoerd op de systemen (techniek) en de mens.
4. Versterk de capaciteit op de tactische kant van informatiebeveiliging, een eerste stap met het werven van een TISO is gezet, en evalueer de capaciteit en inzet op de tactische kant van privacy.
5. Ondersteun het proceseigenaarschap van het lijnmanagement, zodat deze in staat is het opdrachtgeverschap op informatiebeveiliging en privacy in te vullen.
6. Breid de standaard controle op aanbestedingen en contracten op informatiebeveiliging en 'privacy by design' uit naar contracten met een bedrag dat lager is dan €50.000.
7. Blijf investeren in leren over en bewustzijn ten aanzien van informatieveiligheid en privacy bij medewerkers.
8. Maak een keuze voor een informatiemanagementsysteem dat door de gehele organisatie wordt gebruikt.
9. Besteed aandacht aan de protocollen/procedures, zoals het incidentmanagement en het integrale bedrijfscontinuïteitsplan.

Aanbevelingen aan de raad

10. Geef het college de opdracht om binnen 4 maanden de aanbevelingen aan het college in een plan van aanpak aan u te presenteren.
11. Geef nadere invulling van uw taak als controleur van de uitvoering van het beleid op informatiebeveiliging en privacy door:
    a. Met het college afspraken te maken wanneer en waarover u ten aanzien van informatie-beveiliging en privacy geïnformeerd wil worden;
    b. Om toezending te vragen van de halfjaarlijkse rapportages van de FG en de CISO en deze in de raad te bespreken;
    c. Afspraken te maken met het college over de 'vrije ruimte' in de ENSIA-rapportage voor de verantwoording aan u als raad;
    d. U te laten bijstaan door de FG en CISO als 'externe' adviseurs en u indien gewenst voor een second opinion door een andere externe adviseur te laten bijstaan.

Noot: Datagedreven werken met algoritmes

Het openbaar bestuur moet het hoofd bieden aan grote digitale bedreigingen en staat ook voor grote digitale opgaven. Een van de opgaven is het werken met grote bestanden met groepen (bijzondere) persoonsgegevens. Dit zogenoemde datagedreven werken waarbij algoritmes in beeld komen is relatief nieuw voor gemeenten, maar gaat met rasse schreden voort. Het is nog vaak zoeken hoe gemeenten hiermee omgaan en hoe de aspecten van informatiebeveiliging en privacy daarin geborgd kunnen worden. En, 'last but not least' wat de rol van de raad daarin is. Het omgaan met algoritmes maakte geen deel uit van de onderzoeksopdracht. Zijdelings kwam het wel ter sprake tijdens de interviews en in sommige documenten. De RK HW wil de raad aansporen de vinger aan de pols te houden bij deze turbulente ontwikkelingen.

Bijlage: Rapportage met bevindingen Prae Advies

Informatiebeveiliging en privacy
Gemeente Hoeksche Waard

Rapport

Rekenkamer Hoeksche Waard

23 december 2021

Auteur: drs. Etienne Lemmens,

Prae Advies en onderzoek

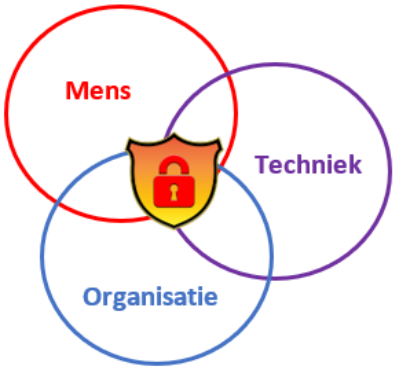
Inhoudsopgave

1 Inleiding

De Rekenkamer Hoeksche Waard (RK HW) vindt in deze tijd informatie-beveiliging en privacy van belang, iedere organisatie loopt op dit terrein risico's. Ook gemeenten, denk bijvoorbeeld aan de hack bij de gemeente Hof van Twente. De RK HW is geïnteresseerd hoe het staat met het beleid en de uitvoering van de informatiebeveiliging en privacy in de gemeenten Hoeksche Waard. Om die reden heeft de RK HW aan Prae advies BV en Hoffmann BV opdracht gegeven om hier onderzoek naar de verrichten.

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonlijke en gevoelige data. Gemeenten zijn daarbij kwetsbaar gebleken, zoals onder andere blijkt uit datalekken en grote incidenten bij gemeenten en recente onderzoeken van rekenkamers. Wat gebeurt er bijvoorbeeld als die informatie op straat komt te liggen? Of als de digitale dienstverlening aan burgers niet meer mogelijk is? Naast financiële, juridische en technische gevolgen kunnen deze crises de privacy van burgers en het imago van de gemeente aantasten.

De Rekenkamer Hoeksche Waard wil de gemeenteraad inzicht geven in de stand van zaken op het gebied van informatiebeveiliging en privacy in de gemeente. Ten aanzien van informatiebeveiliging spelen drie aspecten een cruciale en op elkaar ingrijpende rol: mens – techniek – organisatie. In het rekenkameronderzoek wordt ingegaan op deze drie aspecten.



Op de technische infrastructuur zijn door Hoffmann pentesten uitgevoerd. Vanwege de vertrouwelijke aard wordt de gemeente over de resultaten daarvan apart gerapporteerd. De rekenkamer heeft Prae Advies en Onderzoek gevraagd de organisatorische en menselijke aspecten van informatiebeveiliging en privacy te onderzoeken. Daar waar dat zinvol is wordt in dit rapport ingegaan op de resultaten uit de technische testen.

1.1 Leeswijzer

Deze nota van bevindingen betreft het beleidsdeel van het rekenkameronderzoek naar informatiebeveiliging en privacy. Hoffmann heeft voor de rekenkamer Hoeksche Waard, naast dit beleidsonderzoek, een technisch onderzoek uitgevoerd naar informatiebeveiliging en privacy. Het technisch onderzoek bestaat uit drie delen. De techniek, een inlooptest in de gebouwen van de gemeente door een mysterie guest en tot slot een phishing mail die de onderzoekers naar alle ambtenaren en raads- en burgerleden heeft gezonden. De resultaten van de eerste twee onderdelen van het technisch onderzoek (techniek en inlooptest) zijn in de interviews in het beleidsonderzoek meegenomen. Om die reden refereert dit

beleidsonderzoek aan het technische onderzoek dat door de Hoffmann is uitgevoerd.

In hoofdstuk 2 gaan we in op de doelstelling en de onderzoeksvragen. In hoofdstuk 3 behandelen we de gehanteerde onderzoeksaanpak om de vragen te beantwoorden. Vanaf hoofdstuk 4 volgt de beantwoording van de onderzoeksvragen. In hoofdstuk 4 worden de eerste 2 onderzoeksvragen beantwoord. In de hoofdstukken 5 tot en met 10 komen respectievelijk de onderzoeksvragen 3 tot en met 8 aan bod. De bevindingen uit de interviews zijn getoetst door de bij dit onderzoek betrokken respondenten.

In de bijlagen is achtereenvolgens een verklarende woordenlijst opgenomen, de bestudeerde documenten en geïnterviewde respondenten, de normen gekoppeld aan de onderzoeksvragen, een samenvatting van de resultaten van de pentesten, het schema van NOREA en de aanbevelingen van het onderzoek van de Rekenkamercommissie Hoeksche Waard naar informatiebeveiliging uit 2016.

2 Doelstelling en onderzoeksvragen

2.1 Centrale onderzoeksvraag

De Rekenkamer Hoeksche Waard wil met dit onderzoek de volgende centrale vraag beantwoorden:

"Hoe heeft de gemeente Hoeksche Waard de beveiliging van informatie en privacy georganiseerd en geborgd?"

2.2 Onderzoeksvragen

De centrale onderzoeksvraag wordt uitgewerkt aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 1.

Tabel 1. Onderzoeksvragen

1.	**Beleid van de gemeente**: Welk beleid voert de gemeente Hoeksche Waard op het gebied van informatiebeveiliging? In hoeverre stuurt het college van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatiebeveiliging, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO)? [1]
2.	**Risico's bij informatiebeveiliging en privacy**: Welke risico's bij informatiebeveiliging en privacy heeft de gemeente benoemd? In hoeverre worden risico's beheerst dan wel geaccepteerd? Op welke wijze zijn de (eind)verantwoordelijken aangewezen en de autorisaties geregeld? Welke maatregelen worden genomen om risico's te laten afnemen?
3.	**Bewust omgaan met informatiebeveiliging**: Op welke manier zet de gemeente in op het bewust omgaan met informatie? Hoe gaan de medewerkers van de gemeente in de praktijk om met informatiebeveiliging? In hoeverre dragen bestuur en medewerkers het informatiebeveiligingsbeleid uit? Op welke manier rapporteert en bespreekt de organisatie het functioneren van informatiebeveiliging op management- en bestuursniveau (college en raad)?
4.	**Bewust omgaan met privacy**: Hoe heeft de gemeente de Algemene verordening gegevensbescherming (AVG) van de EU geïmplementeerd in haar werkwijzen? Hoe worden medewerkers hierop actief getraind? In hoeverre dragen bestuur en medewerkers het privacybeleid uit?

[1] Gemeenten hebben in 2013 in VNG-verband afgesproken te voldoen aan de maatregelen van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO.)
Vanaf 25 mei 2016 schrijft de Algemene Verordening Gegevensbescherming (AVG of GDPR) voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeenten zelf.

5. **Toetsen van informatiebeveiliging**: In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden? Wat zijn de gevolgen voor inwoners en ondernemers als toegang door onbevoegden wordt verkregen? In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of pen-testen? In hoeverre is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en hoe ziet het incidentenmanagementproces eruit?
6. **Toetsen van partners en leveranciers op informatiebeveiliging**: Heeft de gemeente in beeld met welke partners informatie en persoonsgegevens worden gedeeld? Op welke manier toetst de gemeente haar partners en leveranciers op privacy- en informatiebeveiligingsaspecten? Met partners en leveranciers zijn afspraken gemaakt op basis van 'privacy by design'.
7. **Lerende houding t.o.v. informatiebeveiliging**: Hoe houdt de gemeente kennis over informatiebeveiliging vast, hoe bouwt zij hierop voort en leert ze hiervan? Op welke wijze wordt aandacht besteed aan de verdere bewustwording bij medewerkers van de gemeente?
8. **Opvolging onderzoek Rekenkamercommissie Hoeksche Waard 2016**: Welke opvolging is gegeven aan het onderzoek van de rekenkamercommissie Hoeksche Waard uit 2016 getiteld "ICT-samenwerking en informatiebeveiliging van de vijf Hoeksche Waard gemeenten"? (zie bijlage 5.)

Voor de normen bij deze onderzoeksvragen verwijzen we naar bijlage 3.

3 Aanpak

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch en interviewverslagen. De documenten bevatten beleid en rapportages van de gemeente Hoeksche Waard op het gebied van informatiebeveiliging. De documenten die zijn bestudeerd zijn in bijlage 2 opgenomen, evenals de functies van de in totaal vier bestuurders en van de functionarissen van de gemeente Hoeksche Waard die zijn geïnterviewd. De deskresearch en interviews vonden plaats in de periode oktober-november 2021.

De pentesten zijn in de periode augustus-november 2021 uitgevoerd door Hoffmann. Zie voor een samenvatting van de resultaten bijlage 4. De resultaten zijn met de ambtelijke organisatie gedeeld.

Hieronder volgen in de hoofdstukken 4 tot en met 10 de bevindingen in de volgorde van de onderzoeksvragen (zie tabel 1).

4 Beleid van de gemeente

Onderzoeksvragen 1 en 2

In dit hoofdstuk geven we antwoord op de eerste twee onderzoeksvragen. Vraag 1: Welk beleid voert de gemeente Hoeksche Waard op het gebied van informatiebeveiliging? In hoeverre stuurt het college van B&W op de afspraken die benoemd zijn in de VNG Resolutie 'Informatiebeveiliging, randvoorwaarde voor de professionele gemeente' en in het bijzonder op de implementatie van de Baseline Informatiebeveiliging Nederlandse Overheid (BIO)?

Vraag 2: Welke risico's bij informatiebeveiliging en privacy heeft de gemeente benoemd? In hoeverre worden risico's beheerst dan wel geaccepteerd? Op welke wijze zijn de (eind)verantwoordelijken aangewezen en de autorisaties geregeld? Welke maatregelen worden genomen om risico's te laten afnemen?

Strategisch Informatie-beveiligingsbeleid

Het Strategisch Informatiebeveiligingsbeleid 2021-2024 is in april 2021 vastgesteld door het college op basis van de Baseline Informatiebeveiliging Overheid (BIO).[2] In het strategisch beleid is opgenomen: "Het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen." In het Strategisch Informatiebeveiligingsbeleid 2021-2024 staan de diverse rollen en functies op informatiebeveiliging beschreven. Tevens is opgenomen dat de gemeenteraad hier toezicht op moet houden.

Privacy & Informatie-veiligheidsteam (PIV)

De functionarissen op informatiebeveiliging en privacy, Chief Information Security Officer (CISO) en Privacy Officer (PO) vormen samen het Privacy & Informatieveiligheidsteam (PIV). Dat is een subteam van Control, dat in de gemeente Hoeksche Waard tweewekelijks bijeenkomt, en indien nodig vaker. Daar komen de lijnen van de Algemene Verordening Gegevensbescherming (AVG) en BIO bijeen en worden informatie-beveiliging en privacy samen besproken. De Functionaris Gegevens-bescherming (FG) en concerncontroller sluiten een keer per maand aan bij het teamoverleg van team PIV. Naast het Privacy & Informatieveiligheidsteam is sinds een jaar een stuurgroep geformeerd met teammanagers of hun vertegenwoordigers (van control, inkoop, integrale veiligheid, communicatie, informatiemanagement, DIV en HR.) De portefeuillehouder sluit in beginsel ook bij deze stuurgroep aan. De stuurgroep komt eens per kwartaal bijeen. De rol van deze stuurgroep moet zich nog uitkristalliseren en daar is een discussie over gaande. Geconstateerd wordt door een enkele respondent dat men veel op detailniveau met elkaar praat, terwijl het de bedoeling was strategische

[2] De Baseline Informatiebeveiliging Overheid (BIO) bevat een op risicomanagement gericht pakket aan maatregelen op informatiebeveiliging voor de gehele overheidssector.

kwesties te bespreken. Een van de respondenten noemt de stuurgroep meer een klankbordgroep.
Op gegevensbescherming zijn de rollen op strategisch en tactisch/-operationeel niveau belegd met respectievelijk de FG en de privacy officers. Op informatiebeveiliging is deze met de CISO alleen op strategisch niveau belegd. Dat wil zeggen dat er geen security officer is die informatie-beveiliging op operationeel terrein in het pakket heeft. Wel wordt eind 2021/begin 2022 voor een Technical Information Security Officer (TISO) geworven, voor de technische informatiebeveiliging. Deze heeft o.a. de rol de architectuur op informatieveiligheid te beoordelen en te controleren. De regie op de technische kant van informatiebeveiliging komt bij deze functie te liggen.

Aanwezige kennis

In interviews wordt aangegeven dat er in de organisatie voldoende kennis aanwezig is op informatiebeveiliging en privacy om adequaat beleid in te richten en uit te voeren. Waar nodig kan externe kennis verkregen worden. Zo wordt de CISO ten behoeve van de halfjaarlijkse BIO-meting onder-steund door externen. Ook aan middelen op ICT, informatiebeveiliging en privacy is voldoende om de taak naar behoren uit te voeren.

Respondenten geven aan dat er steeds beter op de BIO wordt gepresteerd, zeker voor een jonge organisatie die begin 2019 is ontstaan en die van ver moest komen gezien de focus die gericht was op het proces van herindeling. De gemeente Hoeksche Waard is het resultaat van een fusieorganisatie, met een erfenis van verschillende culturen en systemen, dit biedt ook de kans het anders en goed aan te pakken. Meerdere respondenten ervaren de wil bij het bestuur en management om het goed te doen op informatiebeveiliging en privacy.

Volwassenheid

De volwassenheid van de gemeente Hoeksche Waard op informatie-beveiliging laat een groei zien van 1,5 (op een schaal van 5) in 2020 naar 1,8 in april 2021, op basis van de BIO-meting.[3] Deze verbetering is voornamelijk te danken aan het toenemend vastleggen van maatregelen en procedures. In het nog niet vastgestelde CISO-verslag van oktober 2021 is een groei naar niveau 2 geconstateerd. Een organisatie is volgens deze schaal in control op niveau 3. [4] Het cijfer is bedoeld als meetinstrument om de ontwikkelingen op objectieve gronden vast te stellen, niet als een oordeel van goed of slecht. Veel organisaties en ook gemeenten zijn in ontwikkeling op dit nieuwe beleidsterrein, zo ook de gemeente Hoeksche Waard, die ambities toont.

---

[3] De volwassenheid op informatiebeveiliging wordt gemeten op een schaal van 1-5, ontwikkeld door de Nederlandse Orde van Register EDP-Auditors (NOREA). De vijf niveaus van volwassenheid: 1. Initieel; 2. Herhaalbaar; 3. Gedefinieerd; 4. Beheerst en meetbaar; 5. Continu verbeteren. Zie voor nadere uitleg bijlage 5.

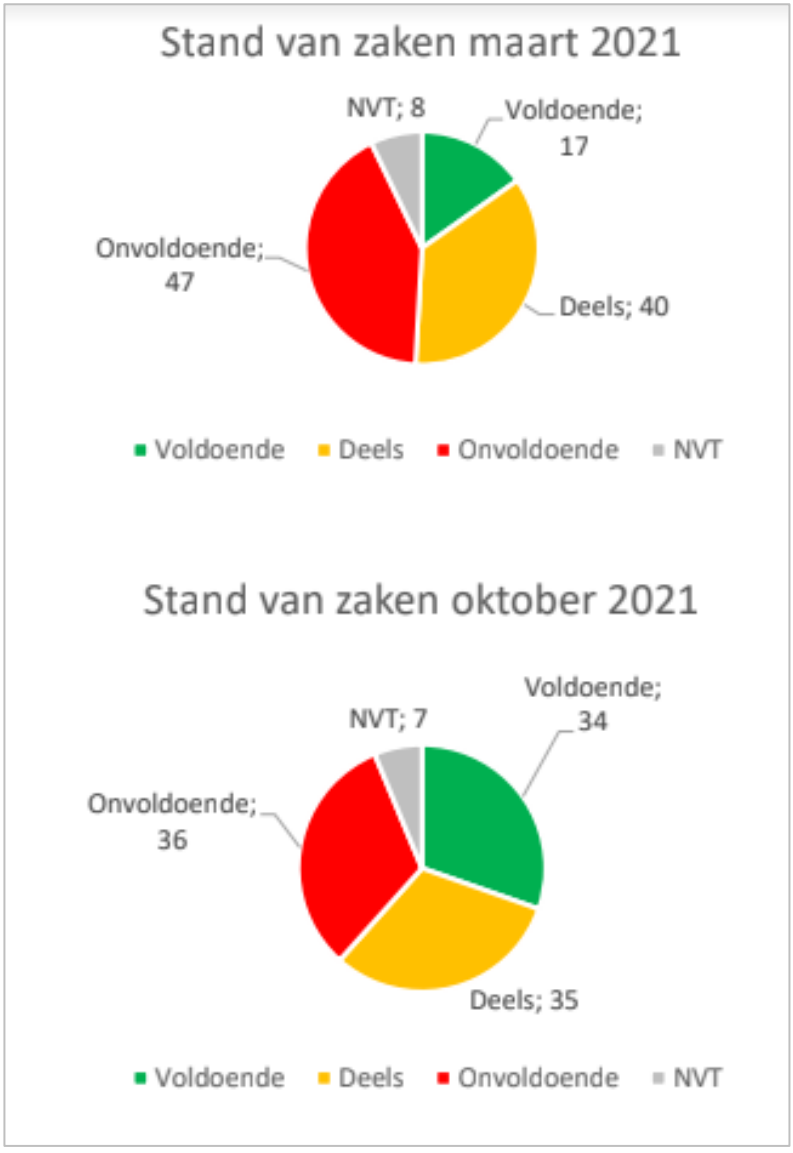
[4] Implementatieplan voorzet BIO, Gemeente Hoeksche Waard, september 2021.

Ambitie

De organisatie zou, om te voldoen aan de wetgeving, door moeten ontwikkelen naar niveau 3. De ambitie om dat op korte termijn te realiseren is uitgesproken, maar nog niet bestuurlijk vastgesteld. Deze ambitie wordt door een aantal respondenten op dit moment als een nog te grote stap gezien. Uit interviews blijkt dat al wel veel in overeenstemming met de BIO wordt gedaan, maar nog niet alles is vastgelegd en er zijn nog open einden.

Implementatieplan

Dat beeld wordt bevestigd in het Implementatieplan voorzet BIO. Dit plan is het resultaat van de tweejaarlijkse tussenevaluatie van het informatie-beveiligingsbeleid. Hiervoor wordt gebruik gemaakt van de halfjaarlijkse meting van de vorderingen op 112 BIO-maatregelen. De laatste is uitgevoerd in oktober 2021. In de grafiek hieronder is de voortgang op de mate van realisatie van de maatregelen weergegeven ten opzichte van de eerdere meting in maart 2021.



Het aantal maatregelen waar voldoende op is gescoord is van 17 naar 34 toegenomen en aantal maatregelen waarop onvoldoende is gescoord is afgenomen van 47 naar 36.

Uit de meting, die aan het implementatieplan ten grondslag ligt, moet een activiteitenplan per afdeling naar voren komen. De teammanagers is gevraagd op basis van een maatregelenlijst een risicoanalyse te maken. Welke maatregelen moeten worden geïmplementeerd en van welke zijn de risico's vooralsnog acceptabel? Geconstateerd wordt dat de risicoanalyses en voor een groot deel de 'bewijzen' daaronder ontbreken. Geconcludeerd wordt dat daar geen sluitend overzicht van maatregelen of planning voor een implementatieplan voor de BIO van te maken is.

In het Implementatieplan worden meerdere adviezen gegeven om alsnog planmatig in een programma de maatregelen op de BIO te implementeren:[5]

- Accepteer formeel alle tekortkomingen (ondertekend door de directeur bedrijfsvoering) randvoorwaardelijk is dat deze formalisering alleen kan indien vergezeld van een risicoanalyse.
- Beleg opdrachtgeverschap bij een directielid, opdrachtgever moet direct betrokken zijn en gecommitteerd met mandaat.
- Geef een hoge prioriteit aan het programma.
- Benoem een programma en projectleider (schatting doorlooptijd 8 maanden) (note, deze rol kan i.v.m. mogelijke belangenverstrengeling en toezichthoudende rol niet bij een CISO belegd worden)
- PM en PL stelt samen met de teammanagers een plan van aanpak op incl. planning en uitvoerenden, uitgezet in tijd om de tekortkomingen te adresseren.
- Teammanagers moeten voor relevante maatregelen een planning maken waarbij aangegeven wordt wanneer de maatregel is/wordt geïmplementeerd.
- Opdrachtgever/directie moet verantwoordelijken resultaat verantwoordelijk maken
- PM rapporteert periodiek de voortgang aan opdrachtgever
- Voortgang programma moet voor de duur van het programma vast onderdeel op de agenda van het directie overleg worden.

Op moment van schrijven moet het implementatieplan nog vastgesteld worden.

Inhaalslag op privacy

De FG constateerde over 2020 een inhaalslag op privacy.[6] Het privacybeleid is 2021 geactualiseerd met een plan van aanpak gebaseerd op de AVG. De gemeente is bezig met de opstart van een AVG-werkprogramma, met als doel om op de middellange termijn op het gewenste niveau te komen. Hierbij wordt uitgegaan van de ambitie die verwoord is in het visiedocument 'Kompas 2018': "Met de ambitie van gemeente Hoeksche Waard om de bedoeling van de Algemene Verordening Gegevensbescherming na te leven, wordt handen en voeten gegeven aan de pijler “100% dienstverlenend”."

[5] Implementatieplan voorzet BIO, Gemeente Hoeksche Waard, oktober 2021, pagina 11.
[6] FG verslag april 2021.

Protocollen

Met het vastleggen van protocollen is men bezig, o.a. vanuit ICT. Protocollen zijn erop:

- wachtwoordenbeleid
- back-up- en restorebeleid
- toegangsrechtenbeleid
- inlogprocedure
- testomgevingsbeleid
- mobile device management
- patch- en releasemanagement
- datalekprotocol

De protocollen staan gepubliceerd op intranet van de gemeente en zijn bereikbaar voor de medewerkers. Hierbij wordt er vaak op gewezen dat Hoeksche Waard een jonge en zich ontwikkelende organisatie is. Een citaat van een van de respondenten: "We zijn niet bezig met op papier zetten, maar met de dagelijkse casuïstiek die langskomt." Dat heeft volgens enkele respondenten grotendeels te maken met capaciteit. Er ontbreken nog wel stukken, zoals een integraal continuïteitsbeleid, waar informatiebeveiliging onderdeel van uitmaakt. Het continuïteitsplan heeft de eerste prioriteit in een nog op te zetten projectportfolio. Een eerste versie is vanwege corona met stoom en kokend water tot stand gekomen. Zo is in de interviews aangegeven dat corona op veel dossiers negatief uitwerkt, maar op informatiebeveiliging heeft de crisis genoodzaakt tot stevig doorpakken. Zo is bijvoorbeeld onder hoge druk het veilig thuiswerken voor de medewerkers geregeld.

Continuïteitsplan

Op dit moment is er geen continuïteitsplan, team Integrale Veiligheid heeft dit in haar portefeuille. Aan de nieuwe versie van het continuïteitsplan wordt gewerkt door de teammanager ICT, met behulp van een externe. Vraag die beantwoord moet worden, is welke verantwoordelijkheden bij de vakteams en welke bij ICT liggen. Het plan wordt besproken met de andere betrokken teammanager en directeur (resp. integrale veiligheid en fysiek domein.) Daarna moet het plan in de praktijk getest worden en kan het definitief vastgesteld worden in het directieteam.

'In control'

De vraag is of de gemeente in control is. In control is op informatiebeveiliging en privacy een lastig begrip, aangezien dit zich in een constante ontwikkeling bevindt. In het kader van de verplichte jaarlijkse verantwoordingsrapportage Eenduidige Normatiek Single Information Audit (ENSIA) is een collegeverklaring verplicht met een 'in control'-statement. Voor het jaar 2020 heeft het college in 2021 een dergelijke verklaring afgegeven? Een 100%-garantie dat een hack voorkomen kan worden is door niemand te geven. Een kleine menselijke maar fatale fout is snel gemaakt en de ontwikkelingen aan de criminele kant van het spectrum gaan heel hard. De gemeente Hoeksche Waard is in control in de zin dat de gemeente risicoanalyses uitvoert, maatregelen vanuit de BIO prioriteert en uitvoert. Kortom, er wordt op gestuurd.

ENSIA

Bij de vorige ENSIA-rapportage bleek de gemeente minder in control. Om in control te zijn moeten de afdelingen aan de slag zijn met de verbeter-maatregelen die uit de verschillende audits, testen en rapportages naar voren komen. Omdat het managementinformatiesysteem op informatiebeveiliging (Information Security Management System, ISMS) nog niet goed gevuld was, moest die informatie van veel afdelingen komen en was die slechts fragmentarisch aanwezig. Er wordt volgens respondenten aan gewerkt om daarmee in control te komen.

Risicomanagement

Bedoeling van BIO en AVG is om met behulp van risicoanalyses het gesprek aan te gaan en aan de slag te gaan met informatiebeveiliging en privacy. Op risicomanagement zijn zeker nog open eindjes en verbeterpunten, zo blijkt uit de interviews. Zoals logging (zie hoofdstuk 7) en risicomanagement op updates of autorisaties (zie hieronder en hoofdstuk 7). Belangrijk wordt gevonden dat er proceseigenaren in de organisatie zijn, die zich verantwoordelijk voelen op informatiebeveiliging en privacy. Zij moeten een vorm van interne accountability tonen, en niet alleen wijzen naar de CISO of de FG. De proceseigenaren in de lijn worden betrokken bij de risicoanalyses en de prioritering van de maatregelen. Die interne accountability begint te groeien, ervaren respondenten. Bestuurlijk bij college en de raad, in de uitvoering door de proceseigenaren in de organisatie, ondersteund door professionals die in het PIV zitten (CISO en PO).

Informatiebeveiligingsplan

Het directieteam (DT) stelt 1x per 2 jaar een informatiebeveiligingsplan vast. Het directieteam vindt een breed gedragen informatiebeveiligingsplan belangrijk, om die reden mochten de teammanagers meedenken om tot een gedragen plan te komen. Dit vergt tijd. Op dit moment is er geen informatiebeveiligingsplan. De organisatie werkt eraan, het is niet duidelijk op welke termijn het informatieplan door het DT wordt vastgesteld.

De maatregelen om de risico's die geprioriteerd zijn af te laten nemen worden in het informatiebeveiligingsplan opgenomen en gemonitord. De gemeente stuurt op risico's in het kader van de BIO. Risico's worden afgewogen op basis van een GAP- en risicoanalyse.

Risico acceptatie: MDM

Een voorbeeld daarvan is risico acceptatie ten aanzien van Mobile device management (MDM): Medewerkers hebben te maken met beleid op Company owned device (COD) en Bring your own device (BYOD). Iedere medewerker heeft van de gemeente een laptop gekregen die van de benodigde essentiële beveiliging is voorzien. Binnen het netwerk kan met een Single Sign On (SSO) met één password toegang verkregen worden tot alle applicaties waar de medewerker rechten toe heeft. Als niet op het netwerk wordt gewerkt moet met behulp van multi factor authentication (MFA of 2 FA) van de app authenticator ingelogd worden.

Apparatuur raadsleden

Soms worden ten behoeve van de gebruiksvriendelijkheid concessies gedaan aan de informatiebeveiliging op basis van MFA. Uit de interviews blijkt dat de iPads die raadsleden hebben gekregen niet op basis van het vastgestelde MDM-beleid worden uitgerold. Zo heeft de gemeenteraad vooralsnog de risico's geaccepteerd dat raadsleden over iPads beschikken zonder beleid op informatiebeveiliging en privacy. Raadsleden kunnen wel terecht bij de Servicedesk van de gemeente voor vragen en eventuele problemen, maar ze kunnen op afstand niet bij het netwerk. De raadsleden kregen ondersteuning bij het installeren van een bedrijfsportal en Teams. Met name het onbeveiligde mailgebruik is een achilleshiel, geeft een van de respondenten aan. Deze situatie wordt nog gedoogd tot de verkiezingen in maart 2022. Vanaf dan wordt de nieuwe raad meegenomen in de omgeving waar de hele gemeente mee werkt, met alle veiligheidseisen op informatiebeveiliging en gegevensbescherming van dien. Ook is er het plan de mobiele telefoons voor zakelijk en privégebruik te scheiden van elkaar.

Autorisaties

De autorisaties, toegang tot data uit de systemen, zijn geregeld in het toegangsrechtenbeleid. De autorisaties staan geregistreerd in een database, de Active Directory (AD) genaamd, die beheerd wordt door functioneel beheerders van ICT. De gegevens daarin worden door ICT alleen aangepast naar aanleiding van een bericht van de teammanager, proceseigenaar via HRM. Dat bericht bevat niet de specifieke autorisaties, maar het functieprofiel waarop de autorisaties zijn gebaseerd. Daarmee zijn de autorisaties in principe niet aan individuele medewerkers gerelateerd, maar aan de functie die zij op dat moment vervullen. Zij zien alleen de mappen en bestanden waarop zij vanuit hun functie rechten toe hebben.

Die toekenning van rechten gebeurt automatisch bij in- en uitdiensttreding op basis van een melding van HRM. Bij een functiewisseling gebeurt dat in principe ook zo. Deze worden door de teammanager doorgegeven aan HRM via Topdesk, en deze geeft dat door aan ICT. De servicedesk maakt dan ook een tag aan, op basis van de functie van de medewerker.

Techniek

Er is zonering ingesteld in de systemen, zodat niet iedereen die binnen is zomaar overal ongehinderd bij alle data kan. Nieuwe applicaties, patches en updates worden eerst in een testomgeving uitgeprobeerd. De uitbreidingen en nieuwe functionaliteiten worden in een Excel bestand opgenomen en systematisch nagelopen. Bij goed bevinden vindt er overleg plaats met het betreffende team om de applicatie/patch/update te installeren en worden de gebruikers op de hoogte gesteld.

Aansluiting IBD

Een ander aspect is de aansluiting op de Informatiebeveiligingsdienst gemeente (IBD) van de VNG. Daartoe moet aan vier voorwaarden voldaan zijn:

- Een algemeen contactpersoon informatiebeveiliging (ACIB) aanwijzen, dat is de PO. Deze functionaris krijgt meldingen van de IBD van

algemene aard, bijvoorbeeld meldingen dat software geüpdatet moet worden.

- Een vertrouwd contactpersoon informatiebeveiliging (VCIB) aanwijzen, dat zijn de CISO en de systeembeheerder. Deze krijgen beveiligings-meldingen die vertrouwelijk van aard zijn en niet met het publiek gedeeld moeten worden;
- De derde stap is het doorgeven van alle IP-adressen (van de in de gemeente in gebruik zijnde apparaten) en URL's (adressen van de bij de gemeente gebruikte internetsites).
- De vierde en laatste stap is het aanleveren van de bij de gemeente in gebruik zijnde hard- en software (de ICT-foto).

Als die vier stappen zijn doorlopen is de aansluiting compleet en krijgt de gemeente van de IBD op maat toegesneden (waarschuwings)meldingen en adviezen. Uit de interviews blijkt dat bij de gemeente Hoeksche Waard de aansluiting compleet is, de gemeente voldoet aan de gestelde eisen.

5 Bewust omgaan met informatiebeveiliging

Onderzoeksvraag 3

In dit hoofdstuk beantwoorden we onderzoeksvraag 3: Op welke manier zet de gemeente in op het bewust omgaan met informatie? Hoe gaan de medewerkers van de gemeente in de praktijk om met informatiebeveiliging? In hoeverre dragen bestuur en medewerkers het informatie-beveiligingsbeleid uit? Op welke manier rapporteert en bespreekt de organisatie het functioneren van informatiebeveiliging op management- en bestuursniveau (college en raad)?

Rapportages

Er wordt regelmatig halfjaarlijks gerapporteerd aan management en college. Verticale verantwoording richting landelijke organen, horizontale verantwoording richting raad in het jaarverslag en in de jaarlijkse ENSIA-rapportage. De ENSIA gaat vergezeld van een in control statement van college, de Collegeverklaring Informatiebeveiliging. Dat wordt onafhankelijk getoetst en met een zogenoemde 'assuranceverklaring' naar de raad gestuurd.

Uit de audits, o.a. op Suwinet en DigiD, en de zelfaudits op de andere applicaties, komen verbetermaatregelen. De gemeente Hoeksche Waard


VNG

VRAAG 1 2 3 4 5 6 7 8 9 10 11

INHOUD

Deze rapportage bestaat uit de volgende onderdelen:

- Vraag 1: Heeft uw gemeente informatieveiligheid als onderdeel van de collegeambities opgenomen?
- Vraag 2: Heeft uw gemeente informatieveiligheid onderdeel gemaakt van de portefeuille van een van de leden van het college van het B&W?
- Vraag 3: Heeft uw gemeente in het jaarverslag een paragraaf aangaande informatieveiligheid opgenomen?
- Vraag 4: Is er een werkend systeem van controle en rapportages over informatiebeveiliging aan het bestuur?
- Vraag 5: Heeft het bestuur zicht op alle risico's waarvoor nog geen of onvoldoende maatregelen getroffen zijn?
- Vraag 6: Is er een informatiebeveiligingsbeleid vastgesteld dat voldoet aan de voorwaarden uit de BIO?
- Vraag 7: Heeft u de eisen uit relevante wetgeving vertaald naar maatregelen?
- Vraag 8: Zijn alle controls en maatregelen die van toepassing zijn toebedeeld aan een verantwoordelijke?
- Vraag 9: Wordt door het management het belang van deelname aan opleiding en training op het gebied van informatiebeveiliging benadrukt en gestimuleerd?
- Vraag 10: Zijn medewerkers op de hoogte van de regels en verplichtingen met betrekking tot informatiebeveiliging en de verantwoordelijkheid die voor hun functie van toepassing is?
- Vraag 11: Is het bestuur bekend met de 10 bestuurlijke principes voor informatiebeveiliging?

GEMEENTE HOEKSCHE WAARD

Hieronder vindt u de beantwoording, namens gemeente Hoeksche Waard, in 2020. De vragenlijst over de status van informatieveiligheid is in 2020 aangepast ten opzichte van voorgaande jaren in verband met de overgang van BIG naar BIO. De eerste 3 vragen in het rapport zijn wel gelijk gebleven. Daarom worden voor de eerste 3 vragen ook de beantwoording in 2016, 2017, 2018 en/of 2019 (indien de gemeente deze toen heeft aangeleverd) getoond. Daarnaast worden bij alle vragen de geaggregeerde resultaten van alle responderende gemeenten in 2020 getoond.

De **gemeente Hoeksche Waard** behoort tot de **gemeentegrootteklasse van 50.000 - 100.000 inwoners.**

beantwoordt ook de vragen over informatiebeveiliging op

Bron: Waarstaatjegemeente.nl.

'waarstaatjegemeente.nl' van de VNG. [7] Zie onderstaande voor een overzicht van de hoofdcategorieën vragen over informatiebeveiliging op de site van de VNG.

ENSIA en ISMS

De CISO was tot en met 2021 de coördinator van de ENSIA-rapportages, daarna alleen voor de externe DigiD en Suwinet audits. De ENSIA verantwoording wordt in de verschillende teams georganiseerd en bijgehouden. Er is geen Information security management system (ISMS), dat de ENSIA-rapportage ondersteunt, dat over de gehele organisatie is uitgerold. Uit de interviews blijkt dat dat mede komt omdat concern control, CISO en FG verschillende applicaties gebruiken.

Halfjaarlijks rapporteert de CISO aan het directieteam (DT) over de stand van zaken met betrekking tot de BIO-maatregelen normering. Dat gebeurt met behulp van de applicatie k2c. Vanwege de capaciteit wordt de CISO bij de uitvoering van de metingen ondersteund door een extern bureau. De FG rapporteert ook twee keer per jaar aan het DT over de voortgang op privacy-maatregelen, hierover meer in hoofdstuk 6.

Aandacht

In interviews wordt gemeld dat acceptatie en begrip voor de maatregelen op informatiebeveiliging in alle lijnen en lagen van de organisatie aanwezig is. Bij sommige afdelingen is er veel aandacht voor informatiebeveiliging en gegevensbescherming, omdat ze al veel langer met het thema te maken hebben. Dat zijn teams als Publiekszaken en Sociaal domein (werk en inkomen, en schuldhulpverlening). Daar komen de onderwerpen informatiebeveiliging en privacy regelmatig langs op de teamoverleggen. Daar is de bereidheid elkaar aan te spreken, op bijv. niet houden aan clean desk en clear screen, groter dan op andere afdelingen. Vanwege het vele thuiswerken door corona hoefde dat het laatste anderhalf jaar uiteraard minder te gebeuren.

Betrokkenheid bestuur

Het gemeentebestuur moet, zoals gesteld in de BIO, het informatie-beveiligings- en privacybeleid uitdragen. Door meerdere respondenten wordt opgemerkt dat het bestuur betrokken is op deze beleidsterreinen. Tevens wordt geconstateerd dat informatiebeveiliging geen topprioriteit is. Een uitzondering hierop is het volgende voorbeeld van de steun voor de ambtenaren op informatiebeveiliging en privacy: de wethouder brak een lans voor informatiebeveiliging om de raad naar dezelfde beveiligde omgeving als de organisatie te brengen. Dit wordt na de verkiezingen van maart 2022 gestart.

---

[7] Tijdens de Buitengewone Algemene Ledenvergadering van de VNG op 29 november 2013 hebben de gemeenten ingestemd met de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'. Een van de afspraken waaraan gemeenten zich met de resolutie gecommitteerd hebben, is dat zij inzicht geven in de wijze waarop zij invulling geven aan de informatieveiligheid via Waarstaatjegemeente.nl.

Bereikbaarheid functionarissen

Tijdens meerdere interviews wordt gemeld dat de functionarissen op informatiebeveiliging en privacy makkelijk en laagdrempelig te bereiken zijn en snel en adequaat reageren op adviesvragen. Ze hebben ook een wekelijks inloopspreekuur, op maandagochtend 10.00-12.00 uur. Daarnaast kunnen de medewerkers veel informatie, protocollen en procedures op het gebied van informatiebeveiliging en privacy vinden op intranet.

6 Bewust omgaan met privacy

Onderzoeksvraag 4

In dit hoofdstuk geven we antwoord op vraag 4: Hoe heeft de gemeente de Algemene verordening gegevensbescherming (AVG) van de EU geïmplementeerd in haar werkwijzen? Hoe worden medewerkers hierop actief getraind? In hoeverre dragen bestuur en medewerkers het privacybeleid uit?

Privacybeleid is 2021 geactualiseerd, met een plan van aanpak gebaseerd op de AVG. De FG geeft aan dat privacybeleid een kwestie van risicobeheersing is, waarin de vraag centraal staat "Hoe ga je met je inwoners om?" Dat is o.a. in informatiesystemen waarmee de link naar informatiebeveiliging is gelegd.

Omgaan met persoonsgegevens

Op het gebied van gegevensbescherming is er onder andere een (wettelijk verplicht) datalekprotocol, verwerkingsregister en een privacystatement over hoe de gemeente omgaat met de persoonsgegevens van inwoners.[8]

Alertheid privacy

Er wordt in sommige teams zeer alert gereageerd op gegevensbescherming. Zo worden bij handhaving persoonsgegevens verwerkt. Zoals bij de sluiting van hennepkwekerijen in panden. Dan moet de gebruiker en eigenaar van de panden nagetrokken kunnen worden. Of zoals Bibob procedures bij sommige vergunningentrajecten. Daarbij wordt gelet op dataminimalisatie, waarbij in principe alleen die gegevens opgevraagd en verwerkt worden om een besluit te kunnen nemen. Bij het team Financiën moet bijvoorbeeld geverifieerd worden of naam en bankrekening matchen, en dat gebeurde door een kopie van een bankpas en bij de boeking te voegen en mee te sturen naar een andere afdeling. De kopie van de bankpas wordt tegenwoordig niet meer bij de boeking gevoegd en alleen gebruikt ter controle.

Toename alertheid

De alertheid in de organisatie neemt wel toe bij de meeste medewerkers, merken respondenten. De vragen of gegevens ingezien of naar derden verzonden mogen worden, of een incident een datalek is, nemen onderling en richting CISO en PO toe. Ook bij functioneel beheerders van ICT komen vragen binnen, zoals een medewerker die vroeg of hij op basis van een BSN-nummer kon checken of een inwoner bekend is in andere registraties van de gemeente. Op de vraag naar de grondslag waarop de gegevens verwerkt zouden mogen worden kwam geen passend antwoord. Het bewustzijn is nog niet bij iedereen op dezelfde gewenste hoogte.

Afspraken met derden

Schoonmakers komen uiteraard ook in de gebouwen. Er wordt naar gestreefd om de medewerkers van het schoonmaakbedrijf in beeld te hebben en een VOG te verlangen. Uit de interviews blijkt dat wel eens een

[8] Voor de privacyverklaring van de gemeente Hoeksche Waard, zie https://www.gemeentehw.nl/privacyverklaring/ .

overleg met het schoonmaakbedrijf vervalt en dat het beeld van de schoonmakers niet actueel is. Procedureel zouden daarop betere borgingsmomenten gepland kunnen worden.

Uit interviews blijkt dat de alertheid binnen de gemeentelijke organisatie toeneemt, maar dat derden soms nog niet zover zijn. Bijvoorbeeld deelt de gemeente op veiligheid gegevens met politie, veiligheidsregio, belastingdienst en het Regionale Informatie- en Expertise Centrum (RIEC). Met het RIEC wordt een beveiligde omgeving gecreëerd waarin gegevens gedeeld kunnen worden.

FG en PO

De werkzaamheden van de privacy officers (PO) bestaan onder andere het organiseren en begeleiden van data protection impact assessments (dpia's), bijwerken van verwerkingsregister, bijdragen aan verslagen van de FG. De omvang van de functionarissen op privacy is nu 2 medewerkers van elk 0,75 fte PO en 0,1 fte FG, allen ondergebracht bij Control. Voorheen waren er 2 fte (1 fte PO en 1 fte FG), dus feitelijk een vermindering van menskracht. Dat bleek dit jaar voldoende om toe te komen aan de zaken die moeten gebeuren. De functionarissen geven aan dat er nu ook nog veel operationele inzet wordt gepleegd, wat verder gaat dan de lijn te ondersteunen met advies. De vraag wordt nog of de huidige capaciteit voldoende is om aan een structureel activiteitenprogramma te werken. Dat vinden respondenten lastig nu al te zeggen.

DPIA's

Maatregelen worden getroffen naar aanleiding van de dpia's. Daarvan zijn de volgende processen in de gemeentelijke organisatie afgerond:

- DPIA Dashboard
- DPIA Peutermonitor [9]

Lopend (afrondende fase):

- DPIA Vroegsignalering
- DPIA Schulddienstverlening
- DPIA Stougjesdijk
- DPIA Track & trace

Zoals eerder gemeld zijn dit processen of projecten binnen de gemeente waarin persoonsgegevens worden verwerkt. Uit de dpia's komen verbetermaatregelen voort, ook uit de gemelde incidenten en mogelijke datalekken. Het opstellen van de dpia's en de opvolging van de verbetermaatregelen liggen bij de proceseigenaren in de lijn. In principe moet de lijn in staat zijn de dpia's zelf uit te voeren en hoeft de PO dit proces slechts te volgen en waar nodig advies geven. Maar gelet op het volwassenheidsniveau van de organisatie moeten medewerkers hierbij geholpen worden. Daardoor is de PO nog grotendeels operationeel en uitvoerend actief hierop.

[9] De Peutermonitor wordt georganiseerd in samenwerking met de GGD en Careyn, en levert een factsheet op die inzicht geeft in de gezondheid van 2-jarige peuters.

Beveiligd mailverkeer

Beveiligd uitwisselen van gegevens, via de mail, gebeurt via Zivver, een applicatie voor beveiligd mailverkeer. Dat gebeurt in ieder geval door de teams die met persoonsgegevens werken.

Geen NAW-gegevens

Het Team sociaal domein registreert geen NAW-gegevens in de systemen of agenda's voor de huisbezoeken, maar klantnummers. Dat maakt het veiliger, maar lastiger om te verwerken, omdat de nummers steeds terugvertaald moeten worden. Met zorgverleners worden gegevens gedeeld met behulp van de applicatie WmoNed. Zij kunnen dan alleen de data van de eigen klanten inzien en raadplegen. Als de zorgverleners daar niet mee (kunnen) werken, wordt Zivver gebruikt om gegevens te delen.

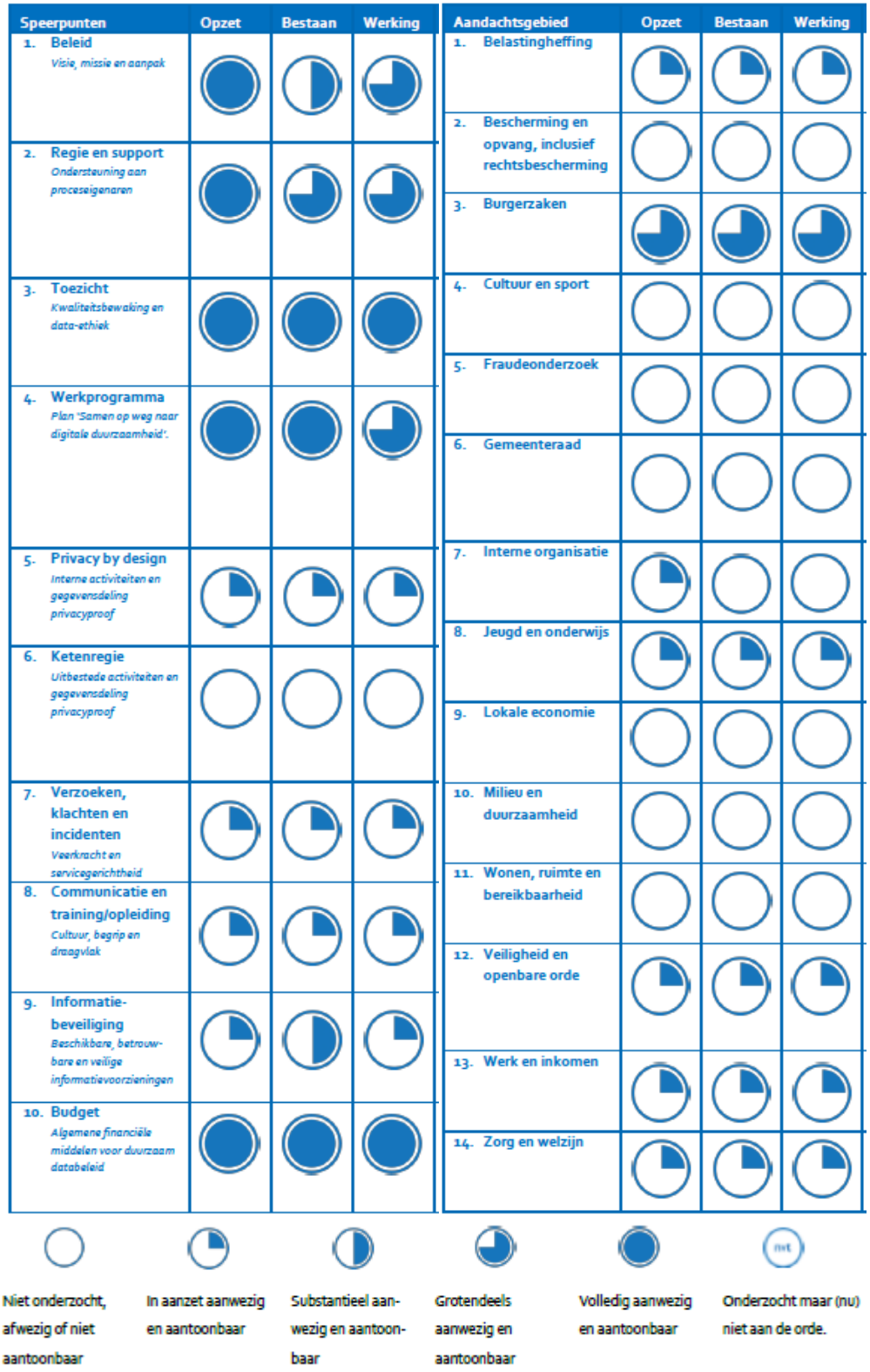
Het komt voor dat derden onbeveiligd gegevens versturen. Dan gaan de medewerkers met die partij in gesprek. Oplossing is dan om een lege mail via Zivver te sturen, waar de andere partij beveiligd op kan antwoorden.

Check op externe partij

Ook bij Publiekszaken wordt beveiligd gecommuniceerd via Zivver. Soms worden partijen waarmee wordt gecommuniceerd gecheckt. In het geval van een gerechtelijke procedure of erfenis wordt bijvoorbeeld gecheckt of een advocaat of notaris op de lijst van de advocatuur of het notariaat staat.

De FG rapporteert sinds 2018 met een bestuurlijke dashbordrapportage. Deze bevat grafieken, 'blauwe bolletjes', om te beoordelen hoe de gemeente scoort op 10 speerpunten of kritieke prestatie indicatoren (KPI's), in vergelijking met andere organisaties, en op 14 hoofdprocessen. Gescoord wordt op opzet, bestaan en werking van AVG-maatregelen op KPI's en hoofdprocessen. Zie hierna voor een voorbeeld van een dergelijke rapportage van april 2021.

Voorbeeld van het dashboard in de FG-rapportage op 10 KPI's en 24 hoofdprocessen.



De FG noemt deze rapportages het DPMS, een dataprotection managementsysteem, naar analogie van het ISMS voor informatiebeveiliging. Het laatste tussenrapport van de FG, van oktober 2021, adresseert het eigenaarschap op AVG (college/ burgemeester,

PIV/beleidsthema's kwaliteit en informatiebeheer, raad) en de agendering van onderwerpen als digitalisering en datagedreven werken. De FG constateerde geen noodzaak tot bijsturing.

7 Toetsen van informatiebeveiliging

Onderzoeksvraag 5

In dit hoofdstuk geven we antwoord op vraag 5: In hoeverre zijn gegevens bij de gemeente beschermd tegen de toegang door onbevoegden? Wat zijn de gevolgen voor inwoners en ondernemers als toegang door onbevoegden wordt verkregen? In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of pen-testen? In hoeverre is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en hoe ziet het incidentenmanagementproces eruit?

Pentesten

Volgens een aantal respondenten beschikt de gemeente Hoeksche Waard over 'state of the art'-materiaal op ICT. Om dat te checken worden elk jaar pentesten op steeds verschillende onderdelen uitgevoerd. Dat gebeurt meestal op initiatief van de CISO. De laatste pentest dateert na het uitrollen van Office365, najaar 2020.

De CISO organiseert ook phishing mail-campagnes, om het klikgedrag van de medewerkers te beproeven. Deze worden door externen uitgevoerd. Begin 2021 heeft de CISO de laatste phishing mail in de organisatie uitgezet. Deze vorm van phishing is niet vergelijkbaar met de phishing mail die de Rekenkamer heeft laten uitvoeren.

Een enkele respondent heeft de suggestie om in de toekomst een hackaton te organiseren zoals in de gemeente Den Haag wordt gehouden. Een groot aantal hackers wordt daarbij uitgenodigd om te proberen in de gemeentelijke systemen te komen.

Pentesten rekenkameronderzoek

In het kader van het rekenkameronderzoek zijn ook pentesten uitgevoerd, door een ethische hacker van Hoffmann in de periode september 2021 tot en met november 2021. Deze bestonden uit een Mystery guest bezoek en enkele technische testen. De technische testen zijn bedoeld om te achterhalen of de informatiesystemen van de gemeente voldoende beveiligd zijn tegen het risico van hacken. Ze zijn uitgevoerd zonder enige voorkennis, zogenoemde 'blackboxtesten', zoals een echte kwaadwillende hacker ook tewerk moet gaan. Onderzocht is of de systemen vanaf internet te benaderen zijn (externe pentest) en vanuit de servicepunten (interne pentest.) Ook het Wifi-netwerk is getest op locatie.

Resultaten

Over één kritiek risico, dat te maken had met een mailserver, is de CISO meteen geïnformeerd en is onmiddellijk actie ondernomen om het risico te verhelpen. De overige resultaten van de pentesten worden zo spoedig mogelijk gedeeld met de gemeente zodat hierop verbetermaatregelen getroffen kunnen worden. Highlights van de resultaten zijn in onderstaand kader weergegeven, de uitgebreidere versie is opgenomen in bijlage 4.

Highlights resultaten technische pentesten Hoffmann.

- Systemen van buitenaf redelijk goed beveiligd
- Op 1 kritiek risico bevinding uit de pentest, ten aanzien van een mailserver, is de CISO geïnformeerd en is actie ondernomen
- Aantal minder zware risico's op de systemen vanuit een externe netwerkpentest
- Zwakke wachtwoorden gevonden, terwijl wachtwoordenbeleid wordt afgedwongen voor alle gebruikers, daardoor zijn 284 geldige gebruikersnamen achterhaald
- Een actief gebruikersaccount van medewerker die niet meer in dienst is
- Meer zwakke wachtwoorden gevonden door aanval op de Active Directory, plus open laptop
- Het is mogelijk om zonder Multi Factor Authenticatie (MFA) in te loggen op systeem en applicaties
- Een domein heeft geen SPF (Sender Policy Framework) records, daardoor is het mogelijk vanuit dat domein e-mails te versturen
- Ongeautoriseerde toegang gekregen tot systeem, geen volledige controle
- Werkstations kunnen ongeautoriseerd worden aangepast

Open cultuur en informatiebeveiliging	Uit de interviews en bestudeerde stukken blijkt dat de gemeente kiest voor een open uitstraling en stijl. Bij de toegang tot de gebouwen speelt het spanningsveld tussen enerzijds de open cultuur die de gemeente richting inwoners wil uitstralen en anderzijds de restricties die informatiebeveiliging en gegevensbescherming opleggen. De risico's van de open opstelling zijn bekend en worden bestuurlijk geaccepteerd.
Toegangsprocedure	Uitgangspunt is dat de niet-publieke zones afgeschermd zijn. De medewerkers hebben een tag, waarmee ze toegang verkrijgen tot deze ruimten. Raadsleden en burgerleden hebben hun eigen tag, met dezelfde toegangsrechten als collegeleden. Zij kunnen 's avonds en in de weekends naar binnen. De leveranciers of reparateurs moeten eerst worden aangemeld en worden bij de receptie geregistreerd in Topdesk. Als de leveranciers niet zijn aangemeld, wordt de aanmelding via de receptie afgerond. In principe lopen de bodes mee als leveranciers e.d. de niet-publieke ruimten binnen gaan. Respondenten geven daarbij aan dat er niet de gehele dag iemand bij blijft, als de reparateur of installateur een dag bezig moet zijn. Wel wordt gevraagd of ze zich willen afmelden als ze vertrekken. Uit de interviews blijkt dat het ook wel eens voorkomt dat een timmerman of schilder aan het werk is gegaan zonder dat dat bekend was bij de receptie.
Inlooptest/mystery guest	De laatste inlooptest door de gemeente zelf geïnitieerd was in april 2021. De bevindingen van de inlooptest zijn besproken en teammanagers hebben onder leiding van de directeuren de prioriteiten bepaald. Naar aanleiding van de test heeft facilitair in het Jaarplan 2022 verbetering van de toegangsprocedure opgenomen. Er is budget aangevraagd en verkregen voor een nieuw systeem dat begin 2022 wordt getest. Ook wordt overwogen om de herkenbaarheid van de medewerkers op locatie te verbeteren, door bijvoorbeeld het dragen van een ID of pas.

In het kader van dit rekenkameronderzoek zijn bij de verschillende gebouwen inlooptesten gehouden.[10] De mystery guest kon verschillende dagen achter elkaar ongeautoriseerd vrij toegang verkrijgen tot niet-publieke ruimten. Een aantal medewerkers geeft aan dat deuren ook wel eens open staan op een wig, ondanks de vergrendeling. Vanwege het gemak omdat er heen en weer gelopen moest worden. Daarnaast bleek de aangebrachte fysieke beveiliging niet overal goed te functioneren en kan deze op een aantal punten verbeteren. Daar zal de inzet op modernisering bij helpen. Ook in de houding van medewerkers tegenover bezoekers zijn verbeterpunten te constateren. De mystery guest kon binnenkomen door met een medewerker mee te lopen. Op een enkel servicepunt werd de clean desk policy goed nageleefd, op andere locaties waren (bijzondere) persoonsgegevens in te zien.

Bewustzijn

Getracht wordt medewerkers en bestuurders erop te wijzen dat niet iedereen met hun tag mag meelopen door de vergrendelde deuren. De gemeente HW komt voort uit een fusie van meerdere kleinere gemeenten. In de kleinere organisaties was het makkelijker iedere medewerker te kennen. De sfeer is anoniemer in een grotere organisatie. Ook speelt het thuiswerken tijdens de coronapandemie een rol. In het afgelopen anderhalf jaar zijn 180 nieuwe medewerkers begonnen en zijn er veel tijdelijke krachten ingehuurd, die de meeste vaste medewerkers hoogstens van het beeldscherm kennen. Een aantal respondenten geeft aan niet aan elk nieuw gezicht te vragen wat hij/zij hier komt doen. Zij zouden het gênant vinden om er dan achter te komen dat diegene een medewerker is. Dan wordt er gemakshalve van uitgegaan dat diegene terecht door de check bij de receptie is gekomen. In een van de vroegere gemeenten is getracht met een bezoekerspas te werken die zichtbaar gedragen zou moeten worden. Maar niet iedereen droeg deze zichtbaar.

Nieuwe toegangsprocedure per 2022

De toegang tot de gebouwen, van de servicepunten, is momenteel nog geregeld met drie verschillende systemen. Uit de interviews blijkt dat het streven is deze te stroomlijnen met één modern systeem. De resultaten van de inlooptest van de gemeente vorig jaar waren de aanleiding middelen te vragen om de toegang tot de ruimten in de gebouwen te moderniseren en professionaliseren. De exploitatie en het beheer van de gebouwen worden per 1-1-2022 anders georganiseerd.[11]

Uit de interviews blijkt dat het nieuwe systeem met zogenoemde smart credentials al op één locatie is geïnstalleerd. Dat betekent dat je met

[10] De test met de mystery guest, in het kader van het rekenkameronderzoek, is uitgevoerd vóór de verbetermaatregelen naar aanleiding van de gemeentelijke test zijn doorgevoerd.

[11] Exploitatie en het groot onderhoud van de gebouwen van de gemeente Hoeksche Waard komt per 1-1-2022 bij BRES BV te liggen. Behalve de gebouwen waar de werkplekken van de ambtenaren zijn gehuisvest (twee gemeentehuizen, twee werven en HWwerkt) en het klein onderhoud. Bres is een BV die volledig in handen van de gemeente is. Daarnaast zijn er drie servicepunten die zich in verzorgingstehuizen bevinden, die niet van de gemeente of BRES zijn. En een servicepunt in een dorpshuis, dat wel gemeentelijk vastgoed is.

behulp van een app op de smartphone of smartwatch toegang kunt krijgen, waardoor een tag niet meer nodig zou zijn. Dit proces wordt ondersteund door de CISO en FG. Als er een definitief besluit genomen is, wordt het systeem uitgerold naar de andere locaties.

Clean desk/clear screen

Enkele medewerkers geven aan dat de bureaus in de werkruimtes eigenlijk niet zo spannend zijn, vanwege de clean desk en clear screen policy. Maar deze wordt blijkbaar niet overal even goed nageleefd, zo laten de inlooptesten zien. Medewerkers geven aan dat op de navolging van de regels door andere medewerkers en leiding werd gehamerd, in ieder geval in de pre-corona periode dat iedereen nog op kantoor werkte. Het zijn niet alleen op de bureaus en beeldschermen waar risico's op datalekken zich voordoen. Er zijn kasten met dossiers die open staan en archiefruimten die bereikbaar zijn, zo laat de inlooptest zien. In sommige van deze kasten bevonden zich vertrouwelijke gegevens zoals medische gegevens in combinatie met NAW-gegevens en geboortedatum van personen die een aanvraag deden voor een voorziening.

Autorisaties en profiel

In hoofdstuk 4 is al ingegaan op het autorisatiebeleid, het verlenen van toegangsrechten tot data in systemen. Bij indiensttreding uiteraard, omdat een nieuwe medewerker op basis van zijn/haar functieprofiel toegang moet hebben tot data en applicaties om te kunnen werken. Bij uitdiensttreding houden die rechten in principe op. Deze meldingen worden door de teammanager of applicatiebeheerder via Topdesk gedaan aan HRM, die de functioneel beheerder van ICT het functieprofiel doorgeeft. Deze kent de medewerker op basis daarvan toegangsrechten toe, of verwijdert deze. Volgens respondenten werkt dat snel.

Functiewisseling

Feitelijk krijgt een medewerker bij functiewisseling een ander profiel met andere autorisaties en dat moet in principe ook via HRM lopen. Enkele respondenten zijn niet zo zeker dat wijzigingen in autorisaties op die wijze of snel doorgevoerd worden. Uit interviews blijkt dat bij een functie-wisseling niet altijd HRM wordt betrokken. En aangegeven wordt dat weliswaar het grootste deel van de autorisaties in een functieprofiel zijn geregeld, maar nieuwe wetgeving of nieuwe taken zijn niet altijd direct aan functieprofielen opgehangen. Daardoor kan het voorkomen dat medewerkers te weinig of te veel rechten hebben.

Respondenten van team ICT geven aan dat de check naar aanleiding van een melding vanuit HRM dat de functie van een medewerker wijzigt (in- of uitdiensttreding of wijziging) goed gaat. Fouten kunnen ontstaan omdat teammanagers niet goed doorvragen of medewerkers nog de juiste rechten hebben.

Check op de profielen

ICT geeft aan dat een keer per kwartaal de lijst met functieprofielen wordt nagelopen, in overleg met HRM. Vanuit ICT wordt aangegeven dat als een account 30 dagen niet gebruikt is bij de teammanager wordt gecheckt of

diegene nog in die functie werkzaam is. Bij de technische pentesten bleek er toch een gebruikersaccount actief van een medewerker die niet meer in dienst was.

Logging

Op een aantal systemen wordt het dataverkeer bijgehouden, gelogd. Dat wil zeggen dat bijgehouden wordt welke informatie door welke accounts wordt opgevraagd, zoals het raadplegen van klantgegevens van inwoners. Als er reden is om te twijfelen aan de rechtmatigheid van activiteiten in applicaties kan gericht worden onderzocht wie wanneer welke informatie heeft opgevraagd. De logging ligt volgens een van de respondenten nog niet helemaal in procedures vast, omdat soms onduidelijk is wat er gelogd moet worden. Een aantal systemen worden via de logging gemonitord op inbraken en uitval, door systeembeheer. De firewall wordt elke twee weken actief gecontroleerd, dat doet systeem- en netwerkbeheer. Het gebeurt, maar de procedures liggen niet vast, blijkt uit de interviews. Op enkele systemen is logging wettelijk verplicht, zoals Suwinet.

Uitwijk

Belangrijk onderdeel van een continuïteitsplan is de uitwijk. Bij een calamiteit moet met de systemen uitgeweken kunnen worden naar een andere locatie, zodat de gemeentelijke dienstverlening snel weer opgepakt kan worden. Er zijn twee datacenters ingericht, zodat de infrastructuur, data en applicaties van de andere gebruikt kan worden als er één uitvalt. De uitwijk wordt jaarlijks getest, tijdens een weekend dat de updates en patches worden geïnstalleerd. In 2021 is de uitwijkprocedure twee keer getest. Daar kwamen verbeterpunten uit voort die opgepakt zijn. De volgende test staat begin 2022 op de planning.

Incident response team

Geconstateerd wordt dat er op ICT geen 'incident-' of 'Computer Emergency Response Team' (CERT) is. Dat is een multidisciplinair samengesteld team dat bij kritieke incidenten de benodigde acties kan oppakken en (laten) uitvoeren. In interviews is aangegeven dat de vorming van zo'n team op de planning staat. Aangegeven is dat bij de bestrijding van een calamiteit een coördinator uit het team Integrale Veiligheid komt, ICT uitvoerend in actie komt en de CISO de rol van adviseur is.

Applicatie bij leverancier

Niet alle applicaties draaien op lokale systemen bij de gemeenten, maar enkele draaien bij een leverancier (als Software as a service [SAAS]). Daar zijn uiteraard contracten voor afgesloten. Bij die contracten horen verwerkersovereenkomsten als persoonsgegevens onderdeel van het dataverkeer uitmaken. En in die contracten is informatiebeveiliging geadresseerd en de continuïteit geborgd.[12]

Rol gemeenteraad

In het strategische informatiebeveiligingsbeleid staat dat de gemeenteraad de uitvoering van het beleid controleert. De ENSIA-rapportage wordt met

[12] Bij navraag blijkt dat een van de leveranciers ISO-gecertificeerd is, op de ISO-norm op informatiebeveiliging. Ieder jaar voert de leverancier een pentest uit.

de raad gedeeld, met het 'in control'-statement van het college. Enkele respondenten vinden dat de raad meer in de rol moet komen en in positie moet worden gebracht. Het inhoudelijke gesprek wordt nergens met de raad gevoerd. De raad meenemen op bijv. de wijze waarop geprobeerd wordt datalekken te voorkomen.

8 Toetsen van partners en leveranciers op informatiebeveiliging

Onderzoeksvraag 6

In dit hoofdstuk geven we antwoord op vraag 6: Heeft de gemeente in beeld met welke partners informatie en persoonsgegevens worden gedeeld? Op welke manier toetst de gemeente haar partners en leveranciers op privacy- en informatiebeveiligingsaspecten? Met partners en leveranciers zijn afspraken gemaakt op basis van 'privacy by design'.

Verwerkingsregister

Het verwerkingsregister is actueel, zodat de gemeente in beeld heeft met welke partijen en op welke wijze persoonsgegevens worden gedeeld met en verwerkt door derden. Bij nieuwe aanbestedingen moet gecheckt worden of er persoonsgegevens worden verwerkt. En zo ja, moeten er verwerkingsovereenkomsten onder de contracten liggen.

Respondenten geven aan dat zij merken dat leveranciers meer en meer met informatiebeveiliging en privacy bezig zijn. Uit de interviews blijkt dat de medewerkers daar alert op zijn. Nieuwe aanbestedingen boven € 50.000 en aankoop van softwarepakketten moeten via een formulier opgestart worden. Daar zitten de componenten privacy en informatiebeveiliging als vast onderdeel van de procedure in. Ook heeft de CISO een toets daarop. Op de nieuwe contracten onder €50.000 ligt geen procedure vast en is geen centrale controle ingeregeld. Onduidelijk is in hoeverre oude contracten maatregelen hebben op informatiebeveiliging en privacy. Als de contracten vernieuwd worden komen ze vanzelf langs.

Standaard overeenkomst

Er zijn standaard verwerkingsovereenkomsten, volgens het VNG-model. Volgens de deelnemers aan de PIV-groep is er contact met de afdeling Inkoop om het gebruik van deze overeenkomsten goed in te regelen. Het moeten eigenlijk de proceseigenaren zijn die dit oppakken. De CISO en PO ondersteunen hen door een checklist op te stellen zodat zij zelf kunnen bepalen of persoonsgegevens worden verwerkt, of en wie een verwerker is, enz. Als er dan een overeenkomst gesloten is moet deze daarna op aspecten van informatiebeveiliging en privacy gecontroleerd worden door de CISO of PO. Hierop wordt ingegaan bij de e-learning (zie hoofdstuk 9).

Span of control

Respondenten geven aan dat werken in een grotere gemeente, zoals de fusiegemeente Hoeksche Waard, anders is dan in een kleinere gemeente, zoals voor de herindeling. Gevolg hiervan is dat er meer collega's en meer inhuur is en dat men die niet of nauwelijks kent. Voor de teammanagers betekent het een grotere span of control. En in een grotere organisatie moet meer erop vertrouwd worden dat de procedures gevolgd worden. Dat geldt zowel voor de eigen medewerkers als de partners en de leveranciers. Gelet op de taakvolwassenheid van de organisatie wordt dat als een uitdaging gezien, door de respondenten.

9 Lerende houding t.o.v. informatiebeveiliging

Onderzoeksvraag 7

In dit hoofdstuk geven we antwoord op vraag 7: Hoe houdt de gemeente kennis over informatiebeveiliging vast, hoe bouwt zij hierop voort en leert ze hiervan? Op welke wijze wordt aandacht besteed aan de verdere bewustwording bij medewerkers van de gemeente?

Bewustzijn groeit, kan altijd beter

Bijna alle respondenten geven als antwoord op de vraag "wat kan beter op het gebied van informatiebeveiliging en privacy?" dat het bewustzijn hierop weliswaar al hoger is dan voorheen, maar altijd beter kan. Dat onderwerp vergt continu aandacht. Alertere houding en reactie op bijvoorbeeld phishing mails en het doorgeven van incidenten en mogelijke datalekken. Fouten en incidenten zijn niet altijd te voorkomen, zoals een mail met namen en mailadressen in de CC in plaats van de BCC. Zo'n recent incident valt dan mee, maar wordt wel meteen opgeschaald naar de FG. De bereidheid om incidenten te melden neemt toe en de functionarissen zien dat de meldingen meestal op de juiste wijze binnenkomen. Bij een phishingmail werd, naast het feit dat een aantal medewerkers op de 'foute' link klikte, ook snel melding gemaakt dat een phishing mail in omloop was. Alleen werd deze melding naar de gehele organisatie gestuurd, in plaats van via de CISO of PO te delen.

De PIV-leden krijgen steeds meer vragen en zij publiceren regelmatig over informatiebeveiliging en privacy op intranet. Het is de bedoeling dat PO en de CISO regelmatig langsgaan bij de vakinhoudelijke teams om presentaties te geven over informatiebeveiliging en privacy. Dat is er door corona niet volledig van gekomen. De verwachting is dat deze activiteit in het eerste kwartaal van 2022 wordt afgerond. Op basis van de behoeften van de vakinhoudelijke teams kunnen verdiepingssessies gegeven worden.

Teamoverleggen

Teammanagers geven aan regelmatig te sturen op informatiebeveiliging en privacy. In sommige team overleggen worden bijvoorbeeld structureel wijzigingen in beleid en aanpak met betrekking tot informatiebeveiliging en privacy besproken en nieuwe modules op e-learning aangekondigd. Ook worden nieuwe medewerkers geïntroduceerd op beginselen van informatiebeveiliging en privacy of wordt een nieuwe medewerker op de CISO- of PO-functie geïntroduceerd.

ISMS-PDCA

Incidenten worden bijgehouden in Topdesk. Deze worden halfjaarlijks geanalyseerd door de CISO en PO. Bij veel voorkomende of meer serieuze incidenten, zoals een datalek, vindt een evaluatie plaats in het betreffende team met de CISO of PO. Inzet is het incident in de toekomst te voorkomen. Zoals aangegeven is een informatiemanagementsysteem op informatie-beveiliging (ISMS) aanwezig. Deze kan gebruikt worden voor documenteren en administreren, zodat bijvoorbeeld de ENSIA-rapportage gevuld kan worden. Om continu te kunnen verbeteren en leren kan het ISMS

gekoppeld worden aan een beleidsleercyclus. De Plan-Do-Check-Act-cyclus (PDCA) is de meest gebruikelijke, waarmee doelstellingen, activiteiten, rapportages en evaluaties ingepland kunnen worden. Zoals eerder geconstateerd is het ISMS niet volledig uitgerold en gevuld en wordt alleen gebruikt voor het bijhouden van de BIO-richtlijnen, niet voor de ENSIA-rapportages. Het overzetten van activiteiten in het kader van de ENSIA-rapportages gaat op basis van handwerk.

E-learning

Op de Hoeksche Campus is gestart met e-learning over informatie-beveiliging en privacy. Deze cursus is voor alle medewerkers verplicht om jaarlijks te volgen en de nieuwe medewerkers moeten er meteen mee aan de slag. PO en CISO breiden de e-learning constant uit met nieuwe modules. Respondenten noemen onder andere modules over phishing mails, wachtwoorden en clear screen policy. De teammanagers zijn erop gewezen dat ze erop moeten sturen dat medewerkers de modules ook daadwerkelijk volgen, in ieder geval jaarlijks 1x de basis over informatie-beveiliging en gegevensbescherming. Alle respondenten weten dat e-learning er is, maar nog niet iedereen heeft dit jaar de verplichte modules gevolgd en nog niet bij iedereen is bekend welke modules er momenteel gevolgd kunnen worden. Aangegeven is dat de medewerkers, die nog niet de verplichte modules hebben gevolgd, een reminder hebben gekregen. PO en CISO geven aan dat zij de deelname van medewerkers halfjaarlijks gaan evalueren.

Gevarieerd aanbod

Lichte kritiek vanuit de medewerkers is dat e-learning die wordt aangeboden een extensieve manier van kennis opdoen is en generiek en weinig toegesneden is op het eigen werkterrein. Daarmee wordt aan awareness gewerkt, maar dat kan snel wegzakken in de drukke waan van de dag. De CISO en PO geven aan awareness evenementen te organiseren, zoals lezingen en een VR-game/escaperoom. Daarmee wordt op een afwisselende en ludieke manier gewerkt. Begin 2021 is bijvoorbeeld een meeting geweest over gegevensbescherming. Daar heeft Maria Genova, journaliste en schrijfster van onder andere *Komt een vrouw bij de hacker*, uitleg gegeven over de risico's. Voor begin 2022 staat een lezing door een ethisch hacker op de planning.

10 Opvolging onderzoek Rekenkamercommissie Hoeksche Waard 2016

Onderzoeksvraag 8

In dit hoofdstuk geven we antwoord op vraag 8: Welke opvolging is gegeven aan het onderzoek van de rekenkamercommissie Hoeksche Waard uit 2016 getiteld “ICT-samenwerking en informatiebeveiliging van de vijf Hoeksche Waard gemeenten”? (zie bijlage 2)

Aanbevelingen 2016

In 2016 heeft de Rekenkamercommissie Hoeksche Waard in een onderzoek naar informatiebeveiliging de volgende vijf aanbevelingen geformuleerd:

1. De Rekenkamercommissie Hoeksche Waard beveelt de ISHW aan om zich te focussen op de realisatie van excellente dienstverlening tegen een acceptabele prijs. Om zicht te krijgen op de consequenties van deze aanbeveling en voor het nemen van besluiten adviseert de Rekenkamer-commissie Hoeksche Waard om aan de gemeenteraden een geactuali-seerde businesscase voor te leggen waarin verschillende scenario's inclusief kostenplaatjes zijn uitgewerkt voor een verdere ontwikkeling van het ISHW.
2. De Rekenkamercommissie Hoeksche Waard beveelt, gelet op de als hoog-risico geclassificeerde risico's, aan om op het gebied van informatie-beveiliging prioriteit te schenken aan de implementatie van het uitvoerings-plan informatiebeveiliging, zodat de vele acties opgenomen in dit plan worden uitgevoerd.
3. De Rekenkamercommissie Hoeksche Waard beveelt het ISHW aan om adequate ICT-beheerprocessen in te richten.
4. De Rekenkamercommissie Hoeksche Waard beveelt de gemeenteraden aan om bij toekomstige besluitvorming aan de hand van een businesscase voor de toetsing van het realiteitsgehalte van gepresenteerde cijfers benchmarkgegevens te gebruiken alsmede voor de toetsing van de volledigheid van de businesscase een instrument toe te passen als de bij het rapport toegevoegde checklist.
5. De Rekenkamercommissie Hoeksche Waard beveelt aan om in de bestuursrapportage aandacht te besteden aan de ontwikkeling van prestatie-indicatoren op het gebied van verbetering van doelmatigheid en efficiency én het dagelijks beheer.

Samenwerking ICT

De aanbevelingen uit 2016 zijn gericht op de toenmalige nog niet gefuseerde situatie, van vijf gemeenten die op ICT samenwerkten in ISHW (ICT Samenwerking Hoeksche Waard). ISHW bestaat vanaf de fusie van 1-1-2019 niet meer en is opgegaan in twee teams, ICT-beheer en Informatie-management. De organisatorische context is dusdanig gewijzigd dat het lastig is de opvolging van de aanbevelingen te traceren. De ambtelijke organisatie is verzocht antwoord te geven op de vraag naar de opvolging.

In de onderstaande tabel zijn de aanbevelingen opgenomen in de 2e kolom. In de 3e kolom de tekst met de eventuele opvolging. In de 4e kolom is met een kleur de mate van opvolging aangegeven (rood = niet opgevolgd, oranje = deels opgevolgd, groen = opgevolgd.)

Tabel 2. Opvolging aanbevelingen Rekenkameronderzoek, *ICT-samenwerking en informatie-beveiliging van de vijf Hoeksche Waard gemeenten,* 2016.

	Aanbeveling	Opvolging	
1	De Rekenkamercommissie Hoeksche Waard beveelt de ISHW aan om zich te focussen op de realisatie van excellente dienstverlening tegen een acceptabele prijs. Om zicht te krijgen op de consequenties van deze aanbeveling en voor het nemen van besluiten adviseert de Rekenkamercommissie Hoeksche Waard om aan de gemeenteraden een geactualiseerde businesscase voor te leggen waarin verschillende scenario's inclusief kostenplaatjes zijn uitgewerkt voor een verdere ontwikkeling van het ISHW.	Op basis van een businesscase zou ISHW zich moeten focussen op de realisatie van excellente dienstverlening tegen een acceptabele prijs. In de reactie is aangegeven dat er momenteel een benchmark onderzoek loopt, waarbij de businesscase van de Hoeksche Waard vergeleken wordt met andere gemeenten. Op basis daarvan worden scenario's uitgewerkt. Dat zou eind 2021 opgeleverd moeten worden. In de tussentijd is hard gewerkt aan de fusie en de formatie van de teams ICT-beheer en Informatiemanagement. Daarna kwam door corona een periode waarin hard gewerkt moest worden om iedereen veilig op afstand aan het werk te houden, met een laptop en programmatuur. Geconstateerd kan worden dat de fusie en de pandemie daarna de opvolging van de eerste aanbeveling vertraagd heeft. Maar dat gemeld wordt dat de aanbeveling na 5 jaar gerealiseerd gaat worden.	
2	De Rekenkamercommissie Hoeksche Waard beveelt, gelet op de als hoog-risico geclassificeerde risico's, aan om op het gebied van informatie-beveiliging prioriteit te schenken aan de implementatie van het uitvoeringsplan informatiebeveiliging, zodat de vele acties opgenomen in dit plan worden uitgevoerd.	Er is niet na te gaan of en hoe de in 2016 als hoog-risico geclassificeerde risico's prioriteit zijn geschonken. Momenteel wordt aan deze aanbeveling opvolging gegeven door de implementatie van het tweejaarlijkse informatiebeveiligingsplan die op basis van halfjaarlijkse metingen op de BIO wordt gemonitord. Daarnaast worden de risico's naar aanleiding van de pentesten en audits in het kader van ENSIA opgepakt. In deze zin is aanbeveling 2 gerealiseerd in het informatiebeveiligingsbeleid van de Hoeksche Waard.	
3	De Rekenkamercommissie Hoeksche Waard beveelt het ISHW aan om adequate ICT-beheerprocessen in te richten	Inrichting van adequate ICT-beheerprocessen is een punt dat continu aandacht vergt. Momenteel is de gemeente op informatiebeveiliging op een volwassenheidsniveau van 2. Dat wil zeggen dat de beheersingsmaatregelen aanwezig zijn en op consistente maar informele wijze worden toegepast. De ambitie om naar niveau 3 door te ontwikkelen, feitelijk 'in control' zijn, is nog niet vastgesteld en vergt zeker nog de nodige formalisatie van de uitvoering van de beheersingsmaatregelen.	

4	De Rekenkamercommissie Hoeksche Waard beveelt de gemeenteraden aan om bij toekomstige besluitvorming aan de hand van een businesscase voor de toetsing van het realiteitsgehalte van gepresenteerde cijfers benchmarkgegevens te gebruiken alsmede voor de toetsing van de volledigheid van de businesscase een instrument toe te passen als de bij het rapport toegevoegde checklist.	Zoals bij de opvolging van de eerste aanbeveling is geconstateerd is er nog geen businesscase of benchmark opgesteld die aan de raad ter toetsing is voorgelegd. Deze wordt eind 2021 verwacht. In de reactie wordt aangegeven dat het streven is deze jaarlijks uit te voeren en aan de raad voor te leggen. Deze vierde aanbeveling is nog niet volledig gerealiseerd.	
5	De Rekenkamercommissie Hoeksche Waard beveelt aan om in de bestuursrapportage aandacht te besteden aan de ontwikkeling van prestatie-indicatoren op het gebied van verbetering van doelmatigheid en efficiency én het dagelijks beheer.	Op het gebied informatiebeveiliging en privacy wordt op basis van prestatie-indicatoren en processen de voortgang op BIO en AVG door de FG en CISO bijgehouden en gerapporteerd aan het Directieteam en de colleges. Meer specifiek rapportages op verbetering van doelmatigheid en efficiency en dagelijks beheer, zoals in de aanbeveling is opgenomen, zijn nog niet gerealiseerd. In de reactie wordt aangegeven dat de aanwezige rapportages op incidentafhandeling in 2022 aangevuld kunnen worden met de in de aanbeveling aangeduide prestatie-indicatoren. Kortom, zoals bedoeld in het rapport van de Rekenkamercommissie Hoeksche Waard is deze aanbeveling nog niet volledig opgevolgd.	

Uiteindelijk is een aanbeveling volledig opgevolgd en zijn vier aanbevelingen deels opgevolgd.

Tot slot

Zoals eerder gemeld is het rekenkamerrapport uit 2016 voor een groot deel door de ontwikkelingen van de fusie van gemeenten en de pandemie daarna ingehaald. Een aanbeveling (nr. 2) is gerealiseerd, de andere aanbevelingen zijn nog niet geheel gerealiseerd.

Bijlage 1. In informatiebeveiliging en privacy veel voorkomende termen en afkortingen

2FA	Twee factor authenticatie, zo wordt op 2 verschillende manieren gecheckt of degene die inlogt degene is die hij/zij aangeeft te zijn
2-staps-verificatie	zie 2FA
ACIB	Algemeen Contactpersoon Informatiebeveiliging, ontvangt berichten van algemene aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
Active Directory (AD)	De Active Directory is een database waarin onder andere accounts en inloggegevens zijn opgenomen.
AP	Autoriteit Persoonsgegevens
Applicatie	Softwareprogramma, zoals de BAG, BRP, SUWInet enz.
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert (GDPR = General Data Protection Regulation)
BAG	Basisregistratie Adressen en Gebouwen, applicatie met onder andere gegevens over adressen en gebouwen in de gemeente
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband
BIO	Baseline Informatiebeveiliging Overheid, verwachting is dat hier de BIR en BIG in zullen opgaan vanaf 2020
BIR	Baseline Informatiebeveiliging Rijksdienst, geldt als basis voor de BIG
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligingsrisico's van de informatie/applicaties zijn geënt
BRP	Basisregistratie Personen, applicatie met persoonsgegevens van de inwoners
BYOD	Bring your own device, betekent dat medewerkers en externen hun eigen apparaten (laptops, smartphones, usb-sticks enz.) meenemen en inloggen op het gemeentelijk systeem
CERT	Computer Emergency Response Team, multidisciplinair samengesteld team dat kan acteren op incidenten en crises
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
CYOD	Choose your own device, beleid dat inhoudt dat medewerkers en eventueel externen apparaten (laptops, smartphones, usb-sticks enz.) kunnen kiezen uit een beperkt assortiment, waarop de veiligheidsmaatregelen al zijn aangebracht
Dongel	Een USB-modem waarmee (beveiligde) toegang tot internet verkregen kan worden
DPIA (ook PIA)	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting

	gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
Firewall	Een firewall is een systeem dat de middelen van een netwerk of computer kan beschermen tegen misbruik van buitenaf.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIG geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie AVG)
GBA	Gemeentelijke Basisadministratie
GR	Gemeenschappelijke regeling
iBabs	Vergadertool op internet, meestal gebruikt voor papierloos vergaderen voor bijvoorbeeld gemeenteraden.
IBD	Informatiebeveiligingsdienst voor gemeenten
ICT	Informatie- en communicatietechnologie
IP-adres	Internetprotocol adres, bestaande uit (momenteel) 4 setjes van drie cijfers. Met behulp van deze set cijfers is elke computer en apparaat dat op internet is aangesloten te traceren
IPv6	Is de opvolger van het traditionele IP-adres. De oude IP-adressen, eigenlijk IPv4, raakten op. Onder andere vanwege de groei van het aantal apparaten dat op internet aangesloten wordt
ISMS	Information securitymanagement system
KING	Kwaliteitsinstituut Nederlandse Gemeenten, heet tegenwoordig VNG Realisatie
NFC	Near Field Communication, contactloze communicatie op korte afstand (vergelijkbaar is de ov-chipkaart)
OWASP	Open Web Application Security Project
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidsleercyclus
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PIA (ook DPIA)	Privacy impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
PKI-certificaat	Public Key Infrastructure. Een PKI(overheid)-certificaat is een internationale standaard voor de digitale ondertekening bij het versturen van gegevens en berichten.
Privacy by default	Onderdeel van privacy by design, waarbij de standaardinstellingen zo privacy-vriendelijk mogelijk zijn ingesteld
Privacy by design	Betekent dat bij het ontwerp van producten en diensten nagedacht wordt over privacy
RIVG	Rijksdienst voor Identiteitsgegevens
SAAS	Software-as-a-Service is een model waarbij softwaretoepassingen via internet worden aangeleverd.
Smart credentials	Smartphone of smartwatch voorzien van een sleutel app
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
Spoofing	Het verzenden van e-mails waarbij het e-mailadres van de afzender vervalst is
Token	Een fysiek apparaat waarmee toegang verkregen kan worden tot een elektronisch beveiligde bron of netwerk

TPM	Third Party Memorandum. Verklaring dat de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen inzake informatiebeveiliging
Url	Uniform Resource Locator. Verwijst naar een uniek adres waarmee de locatie van een webpagina op internet wordt aangegeven of een e-mailadres
VCIB	Vertrouwd Contactpersoon Informatiebeveiliging, ontvangt berichten van vertrouwelijke aard van de Informatiebeveiligingsdienst voor gemeenten (IBD)
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)
VPN	Virtueel privé netwerk (versleutelde beveiligde verbinding)

Bijlage 2. Lijst geraadpleegde stukken en lijst respondenten

De geraadpleegde stukken en de geïnterviewde personen zijn hieronder weergegeven, per onderdeel/gemeente.

Geraadpleegde stukken

- 1.2 Verklaring van toepasselijkheid ISO27001 ZorgNed
- 1.3 Verklaring van toepasselijkheid NEN7510 ZorgNed
- Backup en Restore Procedure 2020
- Bijlage 1 FG-verslag 08-2020
- Bijlage 2 CISO Verslag 08 2020
- BIO - Backup en Restore beleid 2020
- BIO - Toegangsrechtenbeleid 2020
- CISO Verslag April 2021
- Collegevoorstel FG en CISO verslag April 2021 Def
- DigiTrust Certificaat ISO 27001 ZorgNed Automatisering
- DigiTrust Certificaat NEN 7510 ZorgNed Automatisering
- Envelop-procedure definitief 2020
- FG verslag April 2021
- Implementatieplan voorzet BIO, Gemeente Hoeksche Waard, september 2021
- Informatiebeveiligingsbeleid 2020-2024 gemeente HW v1.0
- Inkoop- en aanbestedingsbeleid 2019
- Inlogprocedure 2020
- Jaarstukken-2020-RAAD HW
- Management 2020 accountant IT omgeving evaluatie (PIV)
- MDM beleid 2021
- Netwerkbeleid 2020
- Nieuwe Bruikleenovereenkomst 2.0
- Patch- en releasemanagement Netwerkgebied 1.0 2021
- Privacybeleid gemeente Hoeksche Waard, 11-05-2021
- Security Baselines 2020
- Testomgevingbeleid 2020
- Tussenrapport AVG, 12-10-2021
- Voorstel FG en CISO verslag def

Functies van geïnterviewde respondenten

- Chief Information Security Officer (CISO)
- Functionaris Gegevensbescherming (FG)
- 2 Privacy Officers
- Teammanagers I, II, III
- Directeur
- Portefeuillehouder
- 2 medewerkers Team Integrale Veiligheid
- 3 medewerkers Team Financiën
- 2 medewerkers Team Publiekszaken
- 3 medewerkers Team Facilitair
- 4 medewerkers Team Sociaal Domein
- 3 medewerkers Team ICT-beheer en Informatiemanagement

Bijlage 3. Onderzoeksvragen en normen

De onderstaande normen zijn voornamelijk ontleend aan de BIO en de AVG. Mogelijk kunnen de gemeentelijke beleidsplannen aanvullende normen opleveren, waaraan de uitvoering van de informatiebeveiliging getoetst wordt.

Onderzoeksvragen	Normen
1. Beleid van de gemeente	- Het college stelt het integrale beleid ten aanzien van informatiebeveiliging en privacy vast. - Er vindt sturing plaats op basis van de BIO. - Op onderdelen van informatiebeveiliging en privacy is beleid geformuleerd en zijn richtlijnen opgesteld, zoals gebruik van wachtwoorden, 2 factor authenticatie, mobiele datadragers, autorisaties en monitoring, protocol datalekken, wijzigingsbeleid enz.
2. Risico's bij informatiebeveiliging en privacy	- Het informatiebeveiligingsbeleid is opgesteld aan de hand van een GAP-analyse. - Jaarlijks wordt op basis van een risicoanalyse het informatie-beveiligingsplan ingevuld. - De gemeente neemt maatregelen om risico's te verlagen.
3. Bewust omgaan met informatiebeveiliging	- Het beleid ten aanzien van informatiebeveiliging wordt gepubliceerd voor werknemers en relevante externe partijen. - Medewerkers krijgen cursussen, trainingen e.d. hoe om te gaan met informatie. - Medewerkers weten wat ze wel en niet mogen/moeten doen met gegevens en herkennen incidenten en rapporteren deze ook daadwerkelijk. - Het bestuur en medewerkers dragen het beleid ten aanzien van informatiebeveiliging actief uit. - Over het functioneren van informatiebeveiliging wordt gerapporteerd aan het management, bij voorkeur op basis van een ISMS (Information Security Management System). - Over het functioneren van informatiebeveiliging wordt gerapporteerd aan de raad, in ieder geval jaarlijks in het kader van ENSIA. - De CISO is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren.
4. Bewust omgaan met privacy	- De gemeente werkt conform de regels van de AVG. - Medewerkers krijgen cursussen, trainingen e.d. hoe zij moeten werken conform AVG. - Het bestuur en medewerkers dragen het beleid ten aanzien van privacy actief uit. - De FG is gepositioneerd en geëquipeerd om diens taak adequaat uit te voeren.
5. Toetsen van informatiebeveiliging	- Gegevens zijn goed beschermd tegen ongewenste invloeden van buitenaf. - Er wordt jaarlijks een beveiligingsaudit uitgevoerd. - Er is een procedure vastgesteld voor de wijze waarop informatiebeveiligingsgebeurtenissen en zwakke plekken in de beveiliging worden beheerd en gerapporteerd. - Op de systemen is logging geïnstalleerd en er is capaciteit aanwezig om deze te monitoren.

6. Toetsen van partners en leveranciers op informatiebeveiliging	- De gemeente heeft in beeld met welke partners (bijzondere) persoonsgegevens worden gedeeld met behulp van het verwerkingsregister. - De gemeente maakt met partners en leveranciers afspraken over het veilig uitwisselen en verwerken van persoonsgegevens en de daarvoor te nemen maatregelen, bij voorkeur op basis van 'privacy by design'. - Partners en leveranciers rapporteren jaarlijks over het verwerken van persoonsgegevens.
7. Lerende houding t.o.v. informatiebeveiliging	- De gemeente heeft procedures om te leren van beveiligingsmeldingen met als doel beheersmaatregelen te verbeteren. - Het ISMS, indien aanwezig, is gekoppeld aan de PDCA-cyclus.
8. Opvolging onderzoek Rekenkamercommissie Hoeksche Waard 2016	- De gemeente heeft gevolg gegeven aan de aanbevelingen van het Rekenkamercommissie-rapport Hoeksche Waard uit 2016.

Bijlage 4. Resultaten Pentesten

- Inlooptest
  - Meerdere dagen ongeautoriseerd fysieke toegang gekregen op verschillende servicepunten
  - Niet aangesproken en (zeer) vertrouwelijke informatie (persoons- en medische gegevens) in kunnen zien
  - Meegelift op een toegangspas en toegang verkregen tot beveiligde deel (Oud-Beijerland)
  - Deur defect (Maasdam)
  - Ingelogd op fat client
  - Onbeheerde laptop wethouderkamer (Maasdam)
  - Post (niet vertrouwelijk) ingezien kamer burgemeester
  - Kasten dicht, clean desk, niemand aanwezig (gebouw Streona, Strijen)
  - Verouderd besturingssysteem (Windows 7, niet meer ondersteund met beveiligingsupdates)

- Externe pentest
  - Systemen goed beveiligd, lastig om van buitenaf in de systemen te komen
  - 20 accounts met zwak wachtwoord (OWA gevoelig voor password spraying, daarna in Office365 met gebruikersnaam, wachtwoord en MFA), wel 284 geldige gebruikersnamen achterhaald
  - Domein strijen.nl geen SPF-records > spoofing
  - Minder risico:
    - Systeem lekt IP-adres, lokale domein
    - Websites zonder security headers
    - Standaard, test en reproductiesystemen op internet aangetroffen
    - PHP-pagina die systeem en configuratie instellingen publiceert
    - Kaart viewer laat parkeerplaatsen in Nijmegen zien
  - mail.oud-beijerland.nl verwijst naar mailserver niet van gemeente Hoeksche Waard

- Interne pentest
  - Ongeautoriseerd toegang tot het systeem gekregen, geen volledige controle kunnen krijgen over het systeem
  - Met behulp van de door de externe pentest verkregen 20 gebruikersaccounts ingelogd op fat client > command prompt en Powershell gestart > aanval op AD > zwakke wachtwoorden gevonden
  - Intern inloggen op Citrix zonder MFA
    - inlog op mailbox wethouders > mails vanuit wethoudersaccount kunnen versturen
    - in mailboxen wachtwoorden, BSN-nummers en legitimatiebewijs wethouder(s) aangetroffen
    - ingelogd op Key2Financien
  - Op Fat-client
    - geen BIOS-wachtwoord > opstartprocedure kunnen wijzigen
    - geen disk encryptie > bestanden raadpleegbaar
    - beperkte administrator rechten > applicaties installeren
  - Een van de 20 gebruikersaccounts van medewerker niet meer in dienst, maar account was wel actief

- Laptop in vergaderzaal met een zeer eenvoudig wachtwoord bevatte documenten en browsergeschiedenis

- Wifi netwerk
  - Niet in kunnen inloggen zonder MFA
  - Vanaf parkeerplaats ingelogd op netwerk 'HW'

Oordeel: beveiligingsniveau onvoldoende, op onderdelen afdoende maar verscherping van informatiebeveiligingsniveau gewenst en op punten nodig.

Kritiek: niet melden bij receptie, geen tourniquets, defecte deur

- Mail-phishing
  - Ruim 700 verstuurde phishing e-mails naar medewerkers en raads- en burgerleden
  - 22% van de medewerkers en 2% van de raads- en burgerleden hebben link geopend
  - Resp. 6% en 3% hebben gebruikersnaam en wachtwoord ingevoerd

Aanbevelingen:

- Het uitvoeren van een sluitende verificatie door beveiliging/receptie bij onbekende gezichten of afwijkend gedrag;
- Het laten repareren van defecte deuren met paslezer;
- Plaats een muur of een deur bij de reproruimte in Oud-Beijerland;
- Het opstellen/ uitvoeren van een beleid met betrekking tot het opslaan van vertrouwelijke informatie;
- Voer controles uit voor het verhogen van de clean desk policy;
- Het risicobewustzijn van medewerkers te verhogen:
  - Verhogen van het veilige gedrag van medewerkers met betrekking tot het meeliften van ongeautoriseerde personen;
  - Verhogen van het veilige gedrag van medewerkers met betrekking tot het achterlaten van laptops.

Bijlage 5. Volwassenheidsniveau NOREA

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen 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	Beheersingsmaatregelen 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	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

Bron: Handreiking bij Volwassenheidsmodel Informatiebeveiliging, januari 2019, NBA.