Den Haag

Retouradres: Postbus 12600, 2500 DJ Den Haag

Bits of Freedom
t.a.v. [redacted]
Prinseneiland 97hs
1013 LN Amsterdam

VERZONDEN 23 DEC 2021

Uw brief van
10 september 2021
Ons kenmerk
157281
Contactpersoon
[redacted]
Dienst
Dienst Bedrijfsvoering
Afdeling
Juridische Zaken
Telefoonnummer
(070) 353 [redacted]

Datum 23/12/2021

Onderwerp
Besluit op Wob-verzoek inzake het onderzoek naar de werking en naleving van de Algemene Verordening gegevensbescherming onder diverse gemeenten.

Uw verzoek

Bij brief van 10 september 2021, heeft u met een beroep op de Wet openbaarheid van bestuur (hierna: Wob) een verzoek ingediend.

U verzoekt om openbaarmaking van:

1. Alle rapportages die zijn opgesteld door de functionaris gegevensbescherming inzake de naleving van de Algemene verordening gegevensbescherming, sinds 2017 tot op heden;
2. Alle bestuurlijke en ambtelijke reacties op de rapportages van de functionaris gegevensbescherming inzake de naleving van de Algemene verordening gegevensbescherming, sinds 2017 tot op heden;
3. Alle rapportages inzake de informatiebeveiliging, sinds 2017 tot op heden;
4. Alle bestuurlijke en ambtelijke reacties op de rapportages inzake de informatiebeveiliging, sinds 2017 tot op heden.

Bij brief van 19 november 2021 heeft u ons in gebreke gesteld vanwege het overschrijden van de wettelijke behandeltermijn. Wij hebben u ook schriftelijk laten weten waardoor wij niet tijdig op u verzoek hebben beslist. Hiervoor bieden wij nogmaals onze excuses voor aan.

Documentonderzoek

De inventarisatie naar de door u verzochte documenten is afgerond. Wij hebben de volgende documenten aangetroffen die aan uw verzoek voldoen:

1. Viermaands-rapportages over de periode juni 2018 t/m april 2021;
2. Jaarplan privacy 2020 gemeente Den Haag;
3. Jaarverslag Functionaris Gegevensbescherming 2019.

Wij wijzen u ook op de reeds openbare stukken over de door u genoemde onderwerpen. Deze zijn terug te vinden op www.denhaag.nl/bestuurlijkestukken door het RIS-nummer in te vullen in het zoekveld.

- Voortgang basisinfrastructuur IT, privacy en ISMS Gemeente Den Haag RIS 296464
- Voortgang privacy en informatieveiligheid gemeente Den Haag RIS 298148

- Beleidskader Gegevensbescherming Gemeente Den Haag RIS 299393
- Presentatie voor Rekeningencommissie + bijlagen RIS 29843
- Commissiebrief RC - voortgang gegevensbescherming en informatieveiligheid juni 2018 RIS 300386
- Voortgang gegevensbescherming, informatieveiligheid en ICT-organisatie Gemeente Den Haag RIS 303944
- Verantwoordelijkheden binnen de ICT-organisatie Gemeente Den Haag RIS 307573

Toetsingskader
De Wob kent het uitgangspunt dat documenten over een bestuurlijke aangelegenheid openbaar zijn, tenzij de belangen genoemd in artikel 10 van de Wob en/of de beperkingen genoemd in artikel 11 van de Wob zich tegen geheel of gedeeltelijke openbaarmaking verzetten.

Wij hebben uw verzoek getoetst aan de belangen genoemd in artikel 10 van de Wob en de beperkingen genoemd in artikel 11 van de Wob.

Overwegingen
Op grond van de Wob besluiten wij de aangetroffen documenten (deels) openbaar te maken. In de documenten zijn enkele passages onleesbaar gemaakt.

Buiten reikwijdte van verzoek
In de rapportages en verslagen wordt niet alleen gesproken over de AVG en informatiebeveiliging, maar ook over andere onderwerpen. Informatie over deze andere onderwerpen vallen buiten de reikwijdte van uw verzoek. Deze informatie hebben wij daarom gelakt en in de kantlijn aangeduid met de code "BR" (= buiten reikwijdte van het verzoek).

Artikel 10, lid 2, onderdeel e, Wob
Op grond van deze bepaling blijft het verstrekken van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer van de bij de bestuurlijke aangelegenheid betrokken personen. Wij hebben daarom de persoonsgegevens van ambtenaren die gelet op hun functie niet in de openbaarheid treden, onleesbaar gemaakt. Wij zijn van oordeel dat ten aanzien van deze gegevens het belang dat de persoonlijke levenssfeer van betrokkenen wordt geëerbiedigd, zwaarder moet wegen dan het belang van openbaarheid.

Artikel 10 aanhef en onder g, Wob
Op grond van deze bepaling blijft openbaarmaking van informatie achterwege voor zover het belang van openbaarheid niet opweegt tegen het belang van het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden. Wij hebben in zowel in de rapportages als in de verslagen van de functionaris voor de gegevensbescherming de volgende gegevens gelakt: namen van softwareprogramma's die de gemeente gebruikt en namen van ICT-bedrijven die met de gemeente samenwerken. Openbaarmaking van deze namen zou de betrokken bedrijven vanuit concurrentieoverwegingen onevenredig kunnen schaden. Openbaarmaking van de softwareprogramma's waar de gemeente mee werkt, zou de gemeente onevenredig kunnen schaden omdat die informatie gebruikt kan worden door kwaadwillenden.

Besluit
Onder verwijzing naar bovenstaande motivering, besluiten wij de documenten zoals hierboven genoemd (gedeeltelijk) openbaar te maken.

Wijze van verstrekking
Wij verstrekken de door u gevraagde documenten door deze aan u toe te zenden.

Plaatsing op internet
Dit besluit en de openbaar gemaakte documenten worden geanonimiseerd op wob.denhaag.nl geplaatst.

Burgemeester en wethouders van Den Haag,
namens dezen:
[redacted]
de algemeen directeur van de Bestuursdienst (plv),

[redacted]
Peter van Toor

Bezwaar
Bent u het niet eens met dit besluit? En bent u belanghebbende? Dan kunt u een bezwaarschrift indienen.
Stuur dit uiterlijk binnen zes weken na de datum bekendmaking van het besluit in.

Maakt u gebruik van internet? Dien uw bezwaarschrift dan in via www.denhaag.nl/bezwaar. U heeft hiervoor DigiD nodig. Op www.denhaag.nl/bezwaar vindt u meer informatie. E-mailen kan niet.

Beschikt u niet over internet, dan kunt u het bezwaarschrift ook opsturen naar het volgende adres:

Burgemeester en wethouders van Den Haag,
AWB / bezwaar
Postbus 12 600
2500 DJ DEN HAAG
Vermeld in uw bezwaarschrift:
naam, adres, telefoonnummer (waar wij u overdag kunnen bereiken) en emailadres;
de datum en handtekening;
een duidelijke omschrijving van het besluit waartegen u bezwaar maakt. Stuur een kopie van het besluit mee en noem het kenmerk;
de argumenten voor bezwaar.

Dient u namens iemand anders het bezwaar in? Stuur dan een schriftelijke en ondertekende verklaring (volmacht) mee waaruit blijkt dat u namens die persoon het bezwaar mag indienen.

Bij een spoedeisend belang kunt u na het indienen van een bezwaarschrift een verzoek om voorlopige voorziening indienen bij de rechtbank Den Haag.

Jaarplan privacy 2020 gemeente Den Haag

Auteur: Dr. 10.2.e , functionaris voor de gegevensbescherming

10 juni 2020

1. Inleiding

De gemeente Den Haag wil bij zijn dienstverlening aan de burger dat diens rechten in de persoonlijke levenssfeer worden beschermd. Om de bescherming van persoonsgegevens op een hoger niveau te brengen, is het van belang dat de gemeente in 2020 een volgend niveau bereikt in de privacy volwassenheid.

Binnen de gemeente Den Haag vormen de burgemeester en wethouders de verantwoordelijken. De AVG geeft de FG zowel toezichthoudende als adviserende bevoegdheden. De FG heeft echter geen verantwoordelijkheid voor de verwerking van persoonsgegevens en neemt hierover ook geen besluiten. In dit document geeft de FG aan welke stappen naar haar mening moeten worden gezet opdat de gemeente Den Haag (beter) aan de eisen van de AVG kan voldoen.

2. Executive summary

In dit jaarplan geeft de FG een aantal prioriteiten aan. Deze zijn voor een deel gelijk aan de prioriteiten uit 2019, omdat deze nog onverminderd actueel zijn. Voor 2020 staan de volgende hoofdpunten op de agenda:

- Het verwezenlijken van een privacy organisatie, die adviseert ten aanzien van de noodzakelijk maatregelen op het gebied van de bescherming van de persoonsgegevens en privacy vraagstukken en incidenten.
- Het afronden van het register van verwerkingen, zodat er een operationeel register is dat zowel door de diensten als door de FG kan worden geraadpleegd en waarvan een uittreksel kan worden gepubliceerd voor de burgers.
- Het tot stand brengen van een strategisch en tactisch privacy beleid zodat voor de organisatie helder is binnen welke kaders ze opereren en wat er van hen wordt verwacht.
- Het aanbesteden van een concern-brede bewustzijnscampagne, in samenwerking met security, data en informatiebeheer.
- Het verrichten van een nulmeting.

3. Prioriteiten 2020

Binnen de gemeente Den Haag heeft de FG de rol van strategisch en kaderstellend adviseur. De gemeente heeft in het Beleidskader en Reglement gegevensbescherming (RIS 299392) de verschillende taken en rollen vastgelegd. Dit betekent dat de FG in hoofdlijnen vaststelt hoe aan de open normen van de AVG moet worden voldaan. Bijvoorbeeld:

- De FG stelt een strategisch beleidskader voor privacy op;
- De FG bepaalt op hoofdlijnen de privacy governance;
- De FG schrijft gemeentebrede procedures voor;
- De FG bepaalt aan welke eisen het register van verwerkingen binnen de gemeente moet voldoen;
- De FG schrijft voor op welke wijze de diensten verantwoording over hun privacybeleid afleggen.

3.1 Privacy management binnen de gemeente: taken, rollen en verantwoordelijkheden

Privacy-management houdt in dat de verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen door de organisatie zijn vastgelegd en vastgesteld. Zonder een adequaat ingerichte organisatie is het niet mogelijk om doelen op het gebied van privacy te verwezenlijken. Het op orde brengen van het privacy management is derhalve de eerste prioriteit.

In het privacybeleid 2018[1] is vastgelegd, dat het college van B&W de verwerkingsverantwoordelijke is. De dagelijkse verantwoordelijkheid voor de bescherming van de persoonsgegevens ligt bij de AD's. Deze dienen ervoor te zorgen dat in hun werkprocessen voldoende aandacht wordt geschonken aan de risico's die de verwerking van persoonsgegevens met zich meebrengen en aan het treffen van toereikende maatregelen om deze risico's voldoende te beheersen.

De coördinatie van gegevensbescherming binnen de diensten is op dit moment belegd bij de Wbp-coördinatoren. Formeel heeft elke dienst 0,1 capaciteit voor deze coördinator beschikbaar. Hun taak is het behandelen van AVG-verzoeken.

In maart 2018 heeft de gemeente Den Haag de ambitie verwoord om het zogenaamde tien stappen plan van de Autoriteit Persoonsgegevens te implementeren om de Algemene Verordening Gegevensbescherming uit te voeren.[2] Nu, twee jaar later, stel ik als Functionaris gegevensbescherming (FG) vast dat de gemeente deze tien stappen nog niet volledig heeft doorlopen. Zo is er nog geen complete analyse van alle risico's binnen de wettelijk verplichte verwerkingen die zijn opgenomen in het gemeentebreed verwerkingsregister en de te nemen maatregelen om die te ondervangen en worden privacy vraagstukken bij de beleidsontwikkeling aan de voorkant vaak te laat meegenomen, zodat er vaak geen sprake is van privacy by design.

Inmiddels zijn de ambities van de gemeente Den Haag op bijvoorbeeld het gebied van datagedreven werken en smart cities alleen maar gegroeid en profileert Den Haag zich als de stad van vrede en recht én veiligheid.

Om de hierboven genoemde ambities – en nog vele andere - te verwezenlijken, is adequate privacybescherming essentieel. Hiervoor is het van belang dat de diensten worden ondersteund bij het ontwikkelen en implementeren van hun beleid door antwoord te geven op de vraag welke persoonsgegevens er worden verwerkt, welke risico's die verwerkingen met zich mee kunnen brengen en hoe die risico's beperkt kunnen worden. Alleen dan kunnen de diensten in control zijn.

Ook is het nodig dat de Functionaris voor de Gegevensbescherming (FG) wordt voorzien van meer systematische informatie uit de diensten. De FG kan de diensten dan ook voorzien van meer gerichte adviezen. Wanneer de diensten het overzicht van hun verwerkingen op orde hebben in de vorm van

---

[1] https://denhaag.raadsinformatie.nl/modules/13/Overige%20bestuurlijke%20stukken/442063

[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf

een register, waardoor zij beter in control zijn en kunnen vragen van de AP of burgers snel en accuraat beantwoord worden.

Het is een belangrijke positieve ontwikkeling dat verschillende gemeentelijke diensten op dit moment al zelfstandig bezig zijn met het invullen van de privacy functie. Op verschillende plaatsen binnen de organisatie zijn privacy officers aangesteld, ingehuurd of wordt de aanstelling hiervan onderzocht.

De FG adviseert het GMT echter in een separate notitie om de privacy capaciteit te bundelen en een gemeentebrede privacy office in te richten om de privacy bescherming te optimaliseren. Dit model heeft zijn waarde reeds bewezen in de security-organisatie van de gemeente Den Haag.

3.2 Privacy governance binnen de gemeente: sturing en controle op privacy

Privacy-governance houdt in dat alle processen waarbij persoonsgegevens worden verwerkt in een organisatie worden gestuurd en gecontroleerd. Zonder een goede privacy governance is het dus onmogelijk om te weten of de organisatie de gestelde doelen heeft bereikt. Om privacy governance mogelijk te maken, is een aantal andere zaken nodig.

1 Een register van verwerkingen
2 Uitvoeren van PIA's en DPIA's
3 Heldere en eenduidige procedures
4 Een meldplicht datalekken
5 Rechten van betrokkenen
6 Vergroten van het privacy-bewustzijn bij medewerkers
7 Verwerkersovereenkomsten
8 Rapporteren over de naleving van wet- en regelgeving en algemeen beleid van de gemeente in managementrapportages.

3.3.1 Heldere en eenduidige procedures

In 2019 is een begin gemaakt met het vastleggen van tactisch privacy beleid. In 2020 wordt verdergegaan met het formuleren van concern-breed tactisch privacy beleid. De procedures zullen worden vastgelegd in een gemeente-breed privacy handboek, zodat voor de diensten en medewerkers helder is wat er van hen wordt verwacht en binnen welke kaders zij opereren.

Het formuleren en vastleggen van beleid vindt voortdurend plaats. Veel elementen van de privacy governance zullen in dit privacy handboek worden opgenomen, zoals de meldplicht datalekken, de wijze waarop de gemeente invulling geeft aan de rechten van betrokkenen etcetera, de taken en rollen rondom het register van verwerkingen en de verplichtingen rondom het verrichten van risico analyses en (D)PIA's.

3.3.2 Register van verwerkingen

In 2019 heeft de FG de diverse registers op dienstniveau vervangen door één register dat deel uitmaakt van de applicatie 10.2.g . In dit register zijn alle wettelijk verplichte verwerkingen van de gemeente opgenomen. Gedurende een project in het laatste kwartaal van 2019 hebben de diensten de informatie uit dit register vergeleken met de feitelijke omstandigheden binnen de gemeente Den Haag.

Deze informatie moet nog in 10.2.g worden ingelezen. Dit project is medio 2020 voortgezet en zal eind 2020 zijn afgerond. Het is de bedoeling dat de privacy organisatie dan het bijhouden van het register op zich kan nemen. Wanneer alle wettelijke taken in het register zijn opgenomen, is het ook zaak dat alle verwerkingen die de gemeente verricht, maar die niet wettelijk verplicht zijn in het

register terecht komen, zodat het register een actueel en compleet overzicht van alle verwerkingen van persoonsgegevens binnen de gemeente geeft.

Conform de politieke wens zullen de delen uit het register die hiervoor geschikt zijn uiteindelijk worden gepubliceerd om bij te dragen aan de transparantie van de gemeente Den Haag bij het verwerken van persoonsgegevens. Het vullen en bijhouden van het register van verwerkingen is een taak en verantwoordelijkheid van de diensten zelf aangezien dat kennis van de lijntaken en processen vergt, de diensten zullen voldoende mensen en middelen beschikbaar moeten maken om hun overzicht bij te houden.

3.3.3 Uitvoeren van PIA's en DPIA's

De AVG kent een verplichte gegevensbeschermingseffectbeoordeling, ook wel aangeduid als DPIA. De verantwoordelijke is *verplicht* om een DPIA te verrichten wanneer de verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De AP heeft beleidsregels opgesteld om te bepalen of een DPIA verplicht is.[3] Wanneer na het verrichten van een DPIA blijkt dat er sprake is van een hoog risico, is de verantwoordelijke verplicht om de AP voorafgaand aan de verwerking te raadplegen.

Een verwerkingsverantwoordelijke is echter ook altijd verplicht om de risico's van zijn verwerkingen te kennen en maatregelen te treffen om deze risico's te beperken. Om de risico's in kaart te brengen, is het verrichten van een privacy impact assessment (PIA) volgens een uniform, gemeente-breed model het beste instrument.

- De FG zal in het tactische beleid vastleggen welk (D)PIA model er binnen de gemeente wordt gehanteerd. Ook zal in het beleid worden vastgelegd dat van alle verwerkingen waarvan na een risicoanalyse blijkt dat er persoonsgegevens worden verwerkt altijd een PIA wordt verricht. Het verrichten van (D)PIA's is een taak en verantwoordelijkheid van de diensten zelf, die hiervoor voldoende mensen en middelen beschikbaar moeten maken, omdat ook hiervoor een diepgaande kennis van de processen binnen een dienst noodzakelijk is.
- Daarnaast adviseert de FG de AD's om een aantal mensen zich te laten specialiseren in het faciliteren en schrijven van PIA's. Het blijkt in de praktijk dat materie-deskundigen te weinig PIA's verrichten om hier voldoende vaardigheden in te ontwikkelen.
- De FG zal in 2020 aandacht besteden aan situaties waarbij een voorafgaande raadpleging van de AP aan de orde is en de diensten hierover adviseren. Het is de verantwoordelijkheid van de diensten om al dan niet tot een voorafgaande raadpleging over te gaan.

3.3.4 Meldplicht datalekken

De meldplicht datalekken wordt door de AVG verplicht gesteld. De meldplicht datalekken geldt echter reeds sinds 1 januari 2016 op grond van nationale wetgeving. In 2020 is de procedure gewijzigd. De privacy coördinatoren zijn nu het eerste aanspreekpunt bij datalekken waarbij security niet de oorzaak is. Bij de afhandeling van datalekken werken de privacy coördinatoren nog steeds nauw samen met de security organisatie.

De FG zal in 2020 het proces voor de melding van datalekken verder stroomlijnen via 10.2.g.

3.3.5 Rechten van betrokkenen

De AVG stelt de betrokkene centraal. Ook het formuleren van procedures om de rechten van betrokkene te verwezenlijken, zoals het recht op inzage, correctie, verwijdering en dataportabiliteit, heeft daarom een hoge prioriteit. De FG zal door de privacy office uniforme, gemeente-brede procedures laten ontwikkelen om de rechten van betrokkenen te waarborgen.

---

[3] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia?qa=DPIA

3.4 Vergroten van privacy-bewustzijn

Omdat er nauwe samenhang bestaat tussen security-bewustzijn en dataprofessionaliteit, werkt de FG nauw samen met andere rollen binnen het CIO office om een samenhangende bewustzijnscampagne tot stand te brengen. Deze campagne zal niet alleen zijn gericht op het vergroten van kennis, maar vooral ook op het beïnvloeden van het gewenste gedrag van medewerkers van de gemeente.

In 2020 zal deze campagne voor 2 jaar worden aanbesteed. Hierna volgt een evaluatie waarna wordt besloten hoe hiermee in de toekomst zal worden omgegaan.

3.5 Volwassenheidsmeting

Om te bepalen waar de gemeente staat zal de FG in 2020 de diensten een volwassenheidsmeting laten verrichten om de privacy volwassenheid van de gemeente vast te stellen. Dat zal gebeuren op basis van het model van het CIP.

Het is van belang dat deze jaarlijks wordt herhaald, zodat een beeld ontstaat van de ontwikkelingen op privacy gebied binnen de gemeente.

Den Haag

Jaarverslag Functionaris Gegevensbescherming 2019

Datum
juni 2020
Versie
0.2
Auteur
mw. dr 10.2.e

Status
concept

Inhoudsopgave

1 Inleiding

Op 1 januari 2019 ben ik als nieuwe functionaris gegevensbescherming (FG) van de gemeente Den Haag aangetreden. Dit is het eerste jaarverslag van de Functionaris Gegevensbescherming sinds de Algemene Verordening Gegevensbescherming (AVG) in mei 2018 in werking trad.

2019 was een bijzonder jaar. De organisatie kreeg voor het eerst in volle omvang te maken met de AVG. Duidelijk werd dat de AVG grote invloed heeft op bijna alle processen van de gemeente en daarmee ook op het werk van de proceseigenaren.

2 De formele positie van de FG

Artikel 38 en 39 van de AVG regelen de positie, rol en taken van de FG. De gemeente Den Haag heeft de FG daarnaast een strategische en kaderstellende rol toebedeeld. In het Beleidskader en Reglement gegevensbescherming (RIS 299392) heeft de gemeente de verschillende taken en rollen van de FG vastgelegd.

- Het College van Burgemeester en Wethouders stelt het beleid vast. Zowel het College als de Raad kunnen de uitvoering van het beleid (laten) controleren. De Functionaris Gegevensbescherming bereidt dit beleid voor.
- De Chief Information Officer (CIO) geeft namens het College op dagelijkse basis invulling aan de sturende rol door besluitvorming in het College voor te bereiden en toe te zien op de uitvoering ervan. De taken inzake bescherming van persoonsgegevens die hieruit voortvloeien zijn toegewezen aan de Functionaris Gegevensbescherming (FG). De FG bevordert en adviseert ingevolge de AVG over de bescherming van persoonsgegevens en brengt eens per half jaar verslag uit.

2.1 De positie van de FG in de praktijk

De FG maakt onderdeel uit van de CIO office (directie informatie). Op dagelijkse basis rapporteert zij aan de CIO/directeur informatie. In het kader van de viermaandsrapportages rapporteert de FG aan de wethouder IT. Deze rapportages worden via het GMT geleid, waar de Gemeentesecretaris voorzitter van is.

De raad heeft in 2018 de vraag opgeworpen of de FG voldoende onafhankelijk kan opereren. De VNG stelt dat de FG rechtstreeks behoort te rapporteren aan het college van B&W over zijn werkzaamheden.

Daarnaast stelt de VNG dat dient te worden voorkomen dat de FG in een spagaat terecht komt als de FG zich (teveel) met uitvoerende taken bezig houdt. De FG controleert dan in feite zijn eigen uitvoerende werkzaamheden. Deze situatie kan zich ook voordoen bij de adviserende rol van de FG. Een dergelijke spagaat zou de geloofwaardigheid en betrouwbaarheid van de functie en de functionaris niet ten goede komen.

3 Advies en toezicht door de FG

De kerntaak van de FG is het geven van advies over de naleving van de privacy wetgeving en het houden van toezicht. Om informatie te verzamelen om gericht en proactief advies te geven en om na te gaan of de privacy regels op de juiste wijze worden nageleefd, heeft de FG informatie nodig. Bijvoorbeeld in de vorm van data protection impact assessments (DPIA's), de analyse van datalekken en audits.

In 2019 heeft de FG opdracht gegeven tot een tweetal audits. Beide audits waren het gevolg van een datalek. Dit laat zien, dat datalekken een belangrijk leereffect kunnen hebben en dat zij aanleiding kunnen vormen voor verbeteringen in de organisatie. Het is daarom van groot belang dat medewerkers zich vrij voelen om datalekken te rapporteren en zich geen zorgen hoeven te maken over nadelige gevolgen wanneer zij melding maken van een fout die tot een datalek heeft geleid.

Naar aanleiding van de uitkomsten en aanbevelingen van deze audits kan de FG op een later tijdstip de voortgang opnieuw beoordelen.

3.1 Toezicht door de AP

In oktober 2019 heeft de AP verschillende gemeenten benaderd met een verkennend onderzoek naar smart city toepassingen. Meer in het bijzonder wilde de AP nagaan in hoeverre gebruik was gemaakt van de DPIA en van de voorafgaande raadpleging. Een belangrijk leermoment was, dat de AP zich ook in het kader van een verkennend onderzoek altijd als toezichthouder kan opstellen. Medio 2020 zal in het kader van dit verkennend onderzoek nog een gesprek plaatsvinden tussen de AP, de wethouder, de CIO, de projectleider smart cities en de FG.

Inhoudelijke terugkoppeling over de verstrekte informatie heeft nog niet plaatsgevonden. De AP zal deze terugkoppeling niet bespreken met afzonderlijke gemeenten, maar met de VNG.

4 Privacy management binnen de gemeente: taken, rollen en verantwoordelijkheden

Privacy-management houdt in dat de verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen door de organisatie zijn vastgelegd en vastgesteld. Zonder een adequaat ingerichte organisatie is het niet mogelijk om andere doelen te verwezenlijken. Het op orde brengen van het privacy management was derhalve een van de eerste prioriteiten die de FG in haar jaarplan 2019 aangaf.

De FG heeft in 2019 vastgesteld dat de bestaande privacy organisatie van de gemeente Den Haag ontoereikend is. Binnen de diensten is onvoldoende kennis van privacy aanwezig, bijvoorbeeld om privacy impact assessments af te nemen. De AD's hebben hierdoor vaak onvoldoende zicht op de risico's die het verwerken van persoonsgegevens met zich mee kan brengen. Ook op centraal niveau ontbreekt een adequate privacy organisatie. Dit leidt ertoe, dat de FG niet beschikt over voldoende

informatie uit de organisatie om haar taken uit te oefenen. Haar advies is hierdoor vooral anekdotisch van aard en vindt hoofdzakelijk plaats naar aanleiding van incidenten, zoals bijvoorbeeld een datalek.

Daarom heeft de FG in 2019 een voorstel geformuleerd om een privacy organisatie binnen de gemeente Den Haag in te richten. Inmiddels is het oorspronkelijke voorstel achterhaald door actuele ontwikkelingen. De FG heeft het voorstel nu aangepast. Hopelijk zal het in 2020 door het GMT worden goedgekeurd.

Voor 2019 moet de FG vaststellen, dat de gemeente Den Haag nog niet beschikt over een toereikende privacy organisatie, waardoor de AD's onvoldoende kunnen worden geadviseerd over de risico's die gepaard gaan met de verwerking van persoonsgegevens.

5 Privacy governance binnen de gemeente: sturing en controle op privacy

Privacy-governance houdt in dat alle processen waarbij privacy wordt verwerkt in een organisatie worden gestuurd en gecontroleerd. Zonder een goede privacy governance is het dus onmogelijk om te weten of de organisatie de gestelde doelen heeft bereikt. Om privacy governance mogelijk te maken, is een aantal andere zaken nodig.

1 Een register van verwerkingen
2 Uitvoeren van PIA's en DPIA's
3 Heldere en eenduidige procedures
4 Een meldplicht datalekken
5 Rechten van betrokkenen
6 Vergroten van het privacy-bewustzijn bij medewerkers
7 Verwerkersovereenkomsten
8 Rapporteren over de naleving van wet- en regelgeving en algemeen beleid van de gemeente in managementrapportages.

5.1 Register van verwerkingen

De FG stelde in 2019 vast dat het bestaande register van verwerkingen van de gemeente Den Haag niet toereikend was. Ten eerste was het register niet actueel. Ten tweede voerden alle diensten een eigen register in de vorm van een excel bestand. De FG heeft daarom in haar jaarplan 2019 opgenomen dat een gemeentebreed verwerkingsregister tot stand moet komen. De FG heeft ook een aantal uitvoerende stappen gezet.

De FG heeft gekozen voor 10.2.g . In dit register zijn alle wettelijk verplichte verwerkingen van de gemeente reeds opgenomen, zodat 10.2.g niet alleen een register is, maar tegelijk een maatstaf vormt waarmee de gemeente Den Haag zichzelf kan vergelijken. Dit betekent wel dat alle verwerkingen die niet worden verricht op grond van een wettelijke verplichting vooralsnog ontbreken. Het is aan de diensten om aan te geven waar hun verwerkingen afwijken van 10.2.g en waarom dit het geval is. Afwijken van 10.2.g is mogelijk, mits dit kan worden uitgelegd.

In het laatste kwartaal van 2019 is een aantal consultants ingehuurd om het register van verwerkingen in samen werking met de diensten op orde te brengen. Omdat sommige diensten meer ondersteuning

en tijd nodig hadden dan aanvankelijk voorzien, waren bij het eind van het project echter nog lang niet alle verwerkingen van de gemeente Den Haag in 10.2.g opgenomen.

Op dit moment is de stand van zaken dat de verwerkingen van de gemeente zijn vergeleken met die in 10.2.g zodat een geactualiseerd overzicht tot stand is gekomen van de wettelijk verplichte verwerkingen van de gemeente. De FG adviseert derhalve om dit project in de eerste helft van 2020 voort te zetten.

5.2 PIA's en DPIA's

Op dit moment bestaat er alleen een decentraal overzicht van alle reeds gemaakte PIA's en DPIA's. Het is de bedoeling dat deze in de toekomst in 10.2.g worden opgenomen, zodat hierin een centraal overzicht van de verwerkingen en risico's te vinden is.

De AVG kent een verplichte gegevensbeschermingseffectbeoordeling, ook wel aangeduid als DPIA. De verantwoordelijke is verplicht om een DPIA te verrichten wanneer de verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De AP heeft beleidsregels opgesteld om te bepalen of een DPIA verplicht is. Wanneer na het verrichten van een DPIA blijkt dat er sprake is van een hoog risico, is de verantwoordelijke verplicht om de AP voorafgaand aan de verwerking te raadplegen. Omdat de AD's verantwoordelijk zijn voor de verwerkingen binnen hun dienst, zijn zij er ook verantwoordelijk voor dat (D)PIA's worden verricht en worden opgenomen in iNavigator.

In 2019 zijn de volgende PIA's en DPIA's aan de FG voorgelegd.

Onderwerp	**Dienst**	**PIA**	**DPIA**
Pilot vaste lasten pakket	SZW		X
Hallo werk	SZW		X
Edison	SZW		X
Onderzoek naar inkoop jeugdzorg door H10	GAD	X	
Risicoprofiel facilitycardbeheer	IDC	X	
Activiteitenregistratie BEC	BEC	X	
Intern cameratoezicht	IDC	X	
Factuurstromen GGD	IDC	X	
WvGG	OCW		X
Pilot Multi Disciplinair Overleg (MDO)	OCW		X
Landelijk onderzoek Gezondheidsmonitor Jeugd 2019 (GGD)	OCW		X
Daklozenopvang	OCW		X

Factuurstroom debiteuren boetes huisvuil	IDC	X	
Gegevensdeling mobiele devices	IDC	X	
Voortijdige schoolverlaters	OCW		X
Pilot bodycams	DSB		X
Haal Centraal	CIO		X
Zwembadpas	OCW		X

5.2.1 Voorafgaande raadpleging

De AVG schrijft in artikel 36 voor dat een verwerkingsverantwoordelijke overgaat tot een voorafgaande raadpleging van de Autoriteit Persoonsgegevens, wanneer uit een DPIA blijkt dat een verwerking een hoog risico zou opleveren, maar de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken.

De gemeente Den Haag heeft in 2019 geen gebruik gemaakt van voorafgaande raadpleging.

5.3 Heldere en eenduidige procedures

Een onmisbaar onderdeel van privacy management vormt strategisch, tactisch en operationeel privacybeleid. Privacy beleid is noodzakelijk om de organisatie te helpen bij de invulling van de open normen van de AVG.

Voordat de FG toezicht kan houden, moet voor de organisatie duidelijk zijn hoe de open normen van de AVG worden ingevuld.
De FG zal daarom in 2020 een strategisch privacy beleid opstellen dat aan het GMT zal worden voorgelegd ter goedkeuring. Daarnaast is de FG in het laatste kwartaal van 2019 gestart met het opstellen van een tactisch beleidskader. Wanneer er een functionerende privacy organisatie is, kan deze de invulling van het tactische beleidskader op zich nemen.

In januari 2020 heeft dit een conceptversie van een tactisch Haags privacybeleid opgeleverd. De bedoeling is dat deze gemeentebrede beleidsregels door de diensten worden toegepast, tenzij zij een goede reden hebben om van dit beleid af te wijken ('comply or explain'). Wanneer binnen de hele gemeente dezelfde beleidsregels worden toegepast, zal dit eraan bijdragen dat de gemeente meer als één organisatie zal gaan opereren op het gebied van privacy. Ook maakt eenvormig beleid het voor de FG eenvoudiger om toezicht te houden op de naleving van beleid. Het motto is: gemeentebreed waar het kan, dienstspecifiek waar het moet. Dit beleid zal in 2020 aan het GMT ter goedkeuring worden voorgelegd.

5.4 Meldplicht datalekken

Bij een datalek gaat het om het vrijkomen, wijzigen of vernietigen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Een ernstig datalek moet dan ook gemeld worden bij

Autoriteit Persoonsgegevens (AP) en in beginsel ook aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Datalekken zijn een risico voor de voor de burgers die het betreft en voor de organisatie en moeten daarom goed en snel worden afgehandeld. Daarnaast is het een wettelijke verplichting om datalekken tijdig en volledig te melden, dat wil zeggen binnen 72 uur na de ontdekking van het lek.

Ook moeten de betrokkenen zo snel mogelijk geïnformeerd worden en er moeten maatregelen worden genomen om het lek te dichten en de schade te beperken. De tabel op pagina 4 en 5 geeft de ontwikkeling van het aantal datalekken weer vanaf 2016, toen verplicht werd deze te melden bij de Autoriteit Persoonsgegevens. Datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens tenzij het risico voor betrokkenen gering is. In dat geval is een interne registratie voldoende.

Binnen de gemeente Den Haag worden alle privacy en security-incidenten centraal gemeld via een formulier op werknet en geregistreerd in 10.2.g Het tijdig (binnen 72 klokuren) kunnen afhandelen van datalekken is een belangrijke verplichting uit de AVG, die ook noodzakelijk is om de bescherming van persoonsgegevens binnen de organisatie te monitoren en te verbeteren. Daarnaast is de afhandeling van datalekken een van de manieren om de rechten van betrokkenen te waarborgen. Wanneer zich een datalek heeft voorgedaan, dat de rechten en vrijheden van betrokkenen kan schaden, dient de gemeente betrokken burgers te informeren, zodat zij hun eigen maatregelen kunnen treffen. Dit heeft dus ook concequenties voor de bereikbaarheid van de privacy contactpersonen om deze meldingen binnen 72 klokuren te kunnen behandelen en af te ronden.

Datalekken vormen een belangrijke bron van informatie voor de gemeente en kunnen voor de burger nadelige gevolgen hebben. Daarom is het belangrijk dat binnen de organisatie voortdurend aandacht wordt besteed aan het bewustzijn over wat een datalek is en hoe hiermee moet worden omgegaan. Daarom is het van belang dat, wanneer zich een datalek voordoet dat aan de AP moet worden gemeld, het incident ook wordt geanalyseerd. Op deze manier kan de organisatie leren en zich verbeteren, zodat de kans op herhaling van een incident wordt verkleind. De analyse van een datalek en het inzetten van een verbetertraject worden in het algemeen goed en serieus opgepakt.

Jaar	Gemeld aan AP	Niet gemeld aan AP	totaal
2019	122	140	262
2018	187	241	428
2017	14	57	71
2016	23	52	75

5.4.1 Privacy en integriteit

Verschillende datalekken hadden een relatie met integriteitsonderzoeken. Wanneer integriteitscoördinatoren een incident onderzochten, bleek soms dat medewerkers hun autorisaties hadden misbruikt voor niet-functionele inzage. In de praktijk blijkt dat voor medewerkers niet altijd helder is dat het feit dat zij beschikken over een autorisatie en daarmee toegang hebben tot bepaalde informatie, geen vrijbrief is om deze informatie in te zien zonder dat dit voor hun functie noodzakelijk is.

5.4.2 Veilig communiceren

Een veelvoorkomende oorzaak van datalekken is dat een mail onjuist wordt verstuurd. Het kan betekenen dat de mail naar één of meer verkeerde ontvangers wordt gestuurd of dat er een probleem is met de bijlage.

De AP rapporteert dat 67% van de datalekken wordt veroorzaakt doordat persoonsgegevens worden afgegeven of verstuurd aan de verkeerde ontvanger. Verder zijn de gemeenten met 33% van de meldingen koploper. Er valt dus veel winst te behalen wanneer de gemeente kans zou zien om de communicatie veiliger te maken.

De FG heeft in 2019 met een werkgroep met diverse specialisten en afnemers onderzocht wat de oplossing zou kunnen zijn en heeft in overeenstemming met de CISO aan de CIO geadviseerd om ervoor te zorgen dat binnen de gemeente kan worden gecommuniceerd conform de NTA 7615 norm. Deze norm is ook van toepassing op de gezondheidszorg, zodat de gemeente ook met ketenpartners veilig kan communiceren.

5.5 Rechten van betrokkene

Momenteel kunnen burgers via het mailadres fg@denhaag.nl de FG rechtstreeks benaderen. De FG heeft in 2019 45 verzoeken van betrokkenen geregistreerd. Hiervan waren er 13 bestemd voor DPZ en 14 gemeentebreed. De overige waren verdeeld over de overige diensten. Dit is geen ideaal werkproces. De FG fungeert hier vooral als coördinator die burgervragen uitzet bij de afdelingen.

In 2019 is eraan gewerkt om het mogelijk te maken om via de portal MijnDenHaag ook AVG verzoeken mogelijk te maken. Deze portal biedt de mogelijkheid tot identificatie door middel van DigiD.

In 2020 zal bij BEC-JZ een pilot van een half jaar starten met afhandeling van zoveel mogelijk verzoeken via deze portal. Omdat, zoals gezegd, het indienen van AVG-verzoeken vormvrij is, zullen burgers wel worden gestimuleerd om langs deze weg hun verzoeken in te dienen, maar zullen andere manieren om een verzoek te doen mogelijk blijven. Bijvoorbeeld, wanneer een burger aan de balie vraagt om zijn gegevens direct in te zien of te wijzigen.

5.6 Vergroten van het privacy bewustzijn van medewerkers

De FG werkt niet alleen samen met de CIO collega's bij het tot stand brengen van strategisch beleid, maar ook bij het organiseren van gezamenlijke interne bewustwording. Hiertoe werken de FG, CISO, CDO en de concernadviseur informatiebeheer samen in een aanbestedingstraject om een bewustwordingsprogramma aan te schaffen.

Deze aanbesteding moet ertoe leiden dat alle ambtenaren van de gemeente een samenhangend aanbod krijgen over het omgaan met data en informatie, vanaf het allereerste begin tot en met de archivering en uiteindelijk vernietiging. Naar verwachting zal dit medio 2020 resulteren in de selectie van een aanbieder die één jaar lang de bewustwording binnen de gemeente mag organiseren, met mogelijkheid voor verlenging tot in totaal 4 jaar.

5.6.1 Mindgame

In het najaar van 2019 is binnen de gemeente opnieuw het spel Gegevensweg gespeeld. Via vragen die zijn gerelateerd aan de werksituatie binnen de gemeente kunnen medewerkers vrijwillig hun kennis op het gebied van privacy en security testen. Er hadden zich 329 mensen aangemeld voor het spel.

Uit de analyse van de resultaten viel op dat dat er niet bekend is bij wie een datalek of beveiligingsincident gemeld moet worden. In ronde 1 wist 66% van de mensen dat er een formulier op Werknet te vinden was. In ronde 2wist zo'n 57% dat er een meldformulier is. Op het gebied van datalekken en het melden hiervan is nog veel te winnen.

5.6.2 Dag van de privacy

Op 28 januari 2020 heeft de FG voor medewerkers van de gemeente Den Haag de internationale Dag van de Privacy georganiseerd. Op deze dag bespraken deskundigen van binnen en buiten de gemeente hoe de bescherming van persoonsgegevens doorklinkt in de werkzaamheden van de gemeente. Bedoeling is om te laten zien hoe de privacy van burgers kan worden geraakt door de werkzaamheden van de gemeente en hoe de gemeente de privacy van burgers nog beter kan beschermen. Het aantal aanmeldingen was hoopgevend (> 100), maar helaas was het aantal deelnemers nauwelijks de helft.

Niettemin was de dag inhoudelijk een succes met een groot aantal interessante sprekers en workshops en zal deze dag volgend jaar opnieuw worden georganiseerd.

5.7 Verwerkersovereenkomsten

In 2019 heeft de VNG een standaardverwerkersovereenkomst geïntroduceerd die met ingang van 1 januari 2020 verplicht is. De gemeente Den Haag gebruikt sinds deze datum dan ook deze verwerkersovereenkomst. Advies over het gebruik van de verwerkersovereenkomst wordt gegeven door de juristen van BEC/JZ. Het is van groot belang om dit advies tijdig in te winnen, om ervoor te zorgen dat de belangen van de gemeente op de juiste wijze in de hoofdoverenkomst, de verwerkersovereenkomst en de hierbij behorende bijlagen zijn opgenomen.

6 Volwassenheidsmeting

Eind 2018 heeft de Gemeentelijke Accountants Dienst aan de hand van een door de FG vastgestelde vragenlijst 33 gesprekken gevoerd. Deze gesprekken hebben geresulteerd in een overzicht van het bewustzijn van privacy bij het hogere management. Deze eerste verkenning door de GAD heeft de FG aanleiding gegeven om in haar jaarplan een gemeentebrede volwassenheidsmeting voor te stellen. Deze volwassenheidsmeting kan een maatstaf bieden aan de hand waarvan de voortgang op verschillende terreinen systematisch in kaart kan worden gebracht. Zonder een dergelijke nulmeting is het onmogelijk om vast te stellen of inspanningen resultaat hebben, zo ja welk. Daarnaast kan een dergelijke meting aan bewustwording in de organisatie bijdragen.

Een dergelijke volwassenheidsmeting heeft in 2019 nog niet plaatsgevonden. De FG zal in 2020 de diensten een volwassenheidsmeting laten verrichten.

Den Haag

Viermaandelijkse wethoudersrapportage Informatiebeleid/ ICT

september - december 2019

Datum
3 februari 2020
Versie
0.11
Auteurs
10.2.e

Opdrachtgever
10.2.e

Status
concept

Inhoudsopgave

3 Gegevensbescherming

3.1 Privacy-organisatie

Het plan van de Functionaris Gegevensbescherming (FG) voor de privacy-organisatie wordt begin 2020 voorgelegd aan het GMT om invulling te geven aan de noodzakelijke organisatie om privacy goed te borgen binnen de gemeente. Kern van het voorstel is de inrichting van een centrale privacy-organisatie bij het BEC, bestaande uit privacy officers die de diensten adviseren en ondersteunen en die functioneel door de FG worden aangestuurd. Daarmee wordt dezelfde organisatie voorgesteld zoals die al een aantal jaar succesvol functioneert voor informatiebeveiliging.

3.2 Verwerkingsregister

De applicatie 10.2.g zal worden ingezet als gemeentebreed register van verwerkingen. Een register van verwerkingen is een verplichting op grond van de AVG, die de FG de noodzakelijke informatie biedt bij het uitoefenen van toezicht. Ook voor security en informatiebeheer zal 10.2.g de centrale registratie gaan vormen, zodat de samenhang tussen de verwerking van persoonsgegevens, informatiebeheer, werkprocessen en systemen wordt gewaarborgd. Een ander voordeel van 10.2.g is, dat alle wettelijke gemeentelijke processen al zijn ingevuld, zodat de verwerkingen van een de gemeente Den Haag met die van andere gemeenten kunnen worden vergeleken.
In oktober 2019 is een project gestart dat tot het eind van 2019 de diensten zal helpen om alle bestaande registraties in 10.2.g over te zetten. Een aantal diensten en dienstonderdelen heeft dit afgerond. Verschillende andere diensten blijken echter veel meer ondersteuning nodig te hebben. Als gevolg hiervan is 10.2.g nog niet compleet. Het project zal nog enige maanden worden voortgezet.

3.3 Tactisch beleidskader

In het kader van hetzelfde project heeft de FG een gemeentebreed tactisch beleidskader laten opstellen. Dit maakt voor diensten en medewerkers duidelijker wat van hen wordt verwacht. Dit tactische beleidskader heeft een aantal concrete producten opgeleverd, zoals een gemeentebrede procedure voor verzoeken van betrokkenen om hun rechten onder de AVG uit te oefenen. Op dit moment kunnen dergelijke verzoeken versnipperd door de hele gemeente binnenkomen. Hierdoor bestaat geen betrouwbaar inzicht in het aantal verzoeken, de onderwerpen of de wijze van afhandeling. De gemeente als organisatie dient hier inzicht in te hebben, wil zij in control zijn. Meer duidelijkheid over het verloop van processen kan ook leiden tot een betere dienstverlening aan burgers.

3.4 Toezicht

De kerntaak van de FG is het toezien op de naleving van de privacywetgeving. Hiervoor staan haar verschillende instrumenten ter beschikking. Naar aanleiding van verschillende signalen – een burgervraag, datalekken - heeft de FG in het laatste half jaar opdracht gegeven tot een tweetal audits.

3.5 Audit op het gebruik van BSN

Het gebruik van het BSN is alleen geoorloofd als hiervoor een wettelijke grondslag bestaat. Daarnaast is het BSN een gevoelig persoonsgegeven. Aanleiding voor deze audit was een vraag van een burger naar het gebruik van het BSN-nummer door de gemeente, waarbij de burger zelf aangaf dat hij betwijfelde of zijn BSN noodzakelijk was. Burgers kunnen grote hinder ondervinden wanneer hun BSN in verkeerde handen komt en onnodig of ongeoorloofd gebruik vergroot dit risico.
De audit is door interne gemeentelijke auditors van het BEC verricht. Naast de vraag in hoeverre het BSN op wettelijke basis wordt gebruikt bij het KCC, unit 14070, was deze audit gericht op het onderzoeken van mogelijke verbeterpunten of inconsistenties om corrigerende of proactieve/ verbeter acties voor te stellen.
De resultaten van de audit zijn door de directeur KCC van DPZ positief ontvangen. Naar aanleiding van de audit heeft het KCC aangegeven alle aanbevelingen op te volgen.
In de loop van 2019/2020 zal het BEC in overleg met de FG nog verder onderzoeken hoe gemeentebreed wordt omgegaan met het BSN. Hierbij zal aandacht worden besteed aan de zogeheten soft controls (menselijk handelen) en zal tevens worden onderzocht in hoeverre het verwerkingenregister een juist en betrouwbaar beeld geeft van het gebruik van het BSN binnen de gemeente.

3.6 Audit naar aanleiding van een datalek bij een verwerker

Aanleiding voor dit onderzoek was een datalek bij een verwerker van de Centrale Vastgoedorganisatie (CVDH), waarbij ook bijzondere persoonsgegevens van een burger waren gelekt. Mede omdat het ging om een datalek bij een verwerker, is dit onderzoek verricht door een externe auditor.
Het onderzoek leidde tot de conclusie dat verschillende afspraken en procedures tussen de gemeente en de verwerker onvoldoende waren vastgelegd. Bijvoorbeeld de wijze van het afhandelen van een datalek en het eventueel melden hiervan aan de AP. Ook was onvoldoende helder welke persoonsgegevens de verwerker nu precies voor de gemeente zou verwerken en voor welk doel en ontbrak op het moment dat het datalek zich voordeed een verwerkersovereenkomst. Binnen het betreffende organisatieonderdeel was geen medewerker belast met privacy.

3.7 Datalekken

In de periode augustus tot en met 17 december 2019 zijn zes datalekken aan de Autoriteit Persoonsgegevens (AP) gemeld.

3.8 Onderzoek naar smart cities door de Autoriteit Persoonsgegevens (AP)

In oktober 2019 heeft de AP verschillende gemeenten, waaronder Den Haag, benaderd met een verkennend onderzoek naar smart city-toepassingen. Met dit onderzoek beoogt de AP duurzame innovatie te stimuleren waarbij de privacy van betrokkenen in smart cities is gewaarborgd. Meer in het bijzonder wilde de AP nagaan in hoeverre gebruik was gemaakt van de data protection impact assessment (DPIA). Een DPIA is in bepaalde gevallen verplicht. Voor twee verwerkingen is een DPIA opgesteld, voor één een PIA. De gemeente Den Haag heeft 12 smart city verwerkingen gerapporteerd.

4 Informatieveiligheid

4.1 Terugblik

4.1.1 Ernstig phishing-incident door de CISO geëscaleerd

In het weekend van 26 oktober heeft een medewerker geklikt op een link in een phishing-mail en zijn inloggegevens achtergelaten. Deze inloggegevens zijn door een 'aanvaller' gebruikt om grote hoeveelheden aan spamberichten te versturen. Door de impact van deze aanval is besloten als maatregel multi factor-authentication (MFA) versneld uit te rollen. De migratie naar MFA is succesvol verlopen. Daarnaast is het proces verder geoptimaliseerd en zijn taken beter belegd binnen de organisatie.

In de periode september-december zijn in totaal zeven security incidenten geweest met de hoogste prio's 1 tot 3 te weten Prio 1: 0 | Prio 2: 1 | Prio 3: 6.

4.1.2 ENSIA 2019

In december is de zelfevaluatiefase van het jaarlijkse ENSIA-verantwoordingsproces over informatieveiligheid afgerond. Beheerders en lijnmanagers zijn actief betrokken geweest bij het beantwoorden van de vragen en het verzamelen van de documentatie t.b.v. de jaarlijkse IT-audit door de GAD. Er ontstond een goed samenspel tussen hen, de ISO's en de ENSIA-projectleider wat resulteerde in een soepel lopend verantwoordingsproces. De GAD zal de normen in het eerste kwartaal van 2020 toetsen en haar oordeel uitwerken in een Assurance rapportage. Na de Assurance rapportage start het bestuurlijke proces om uiterlijk 30 april 2020 de ondertekende collegeverklaring ENSIA vast te stellen.

4.1.3 Implementatie BIO & het ISMS

Vanaf 1 januari 2020 moet de gemeente voldoen aan de BIO[1]. De gemeente heeft in 2019 goede stappen gezet om hierop voorbereid te zijn. Zo is het nieuw aangeschafte tool ter ondersteuning van het Information Security Management System (ISMS), 10.2.g geïmplementeerd. Deze tool ondersteunt de (C)ISO's in het bijhouden en evalueren van de relevante informatieveiligheidsnormen van de gemeente. Het Beleidskader Informatieveiligheid 2019-2022 is op 17 december in het College vastgesteld.

4.1.4 Aanbesteding VNG GGI-Veilig

De VNG heeft de aanbesteding "GGI-Veilig" afgerond, waarmee de gemeente Den Haag security-producten en –diensten kan afnemen. Hiervoor is sinds september een raamovereenkomst beschikbaar voor deelnemende gemeente. De gemeente neemt op basis van deze raamovereenkomst producten en dienstern af middels minicompetities.

[1] Baseline Informatiebeveiliging Overheid. één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO 27000-normatiek

4.1.5 Hâck The Hague 2019

Het jaarlijks terugkerende evenement is wederom succesvol verlopen. In totaal hebben 79 internationale Ethische Hackers, 103 bevindingen gerapporteerd over zowel intern als extern gehoste webapplicaties. In samenwerking met het NCSC is de Early Bird Borrel voor de ONE Conference en de jaarlijkse *Capture The Flag* competitie aansluitend op Hack The Hague in het stadhuis georganiseerd. Tot volle tevredenheid van beide partijen. Na het evenement is onder coördinatie van het IDC-A en BEC-I gestart met het oplossen van de geconstateerde kwetsbaarheden. Van de 102 bevindingen staan er nog 44 open. Deze worden, in samenwerking met de hackers en de leveranciers, met prioriteit afgehandeld.

Een maand na de perspublicatie van de aankondiging van het evenement via de onlinemediakanalen en social mediakanalen is een bereik behaald van 19,5 miljoen views, waarvan 18% nationaal en 82% internationaal.

De gemeente Rotterdam heeft meegekeken bij deze editie en de Haagsche ervaringen gebruikt om, op kleine schaal, ook een Hackathon te organiseren in december. Ook Rotterdam spreekt over een succesvol evenement welke in juni 2020 navolging gaat krijgen. Een mooi voorbeeld van het succes van de Haagse formule en samenwerking binnen de Metropoolregio Den Haag - Rotterdam.

4.2 Vooruitblik komende 4 maanden

4.2.1 ISMS-proces en Securityorganisatie

Binnen de gemeente werken we volgens het ISMS, dat ondersteunt wordt door de tool 10.2.g Zoals dit in vele domeinen al het geval is (bijv. kwaliteit en milieu) is dit gebaseerd op een jaarlijkse Plan-Do-Check-Act cyclus. Een van de wijzigingen is dat de verantwoordingslast, zoals met ENSIA, over het jaar verspreid wordt om de werkdruk bij de ISO's en de lijnorganisatie te verminderen.

Onderdeel van het vastgestelde strategische beleidskader is de introductie van een jaarplan op security waarin de belangrijkste prioriteiten zijn opgenomen gebaseerd op de ambities en speerpunten uit het strategisch beleidskader informatieveiligheid. Het jaarplan wordt opgesteld onder regie van de CISO en bevat concrete acties capaciteit en planning.

Den Haag

Viermaandsrapportage Informatiebeleid/ICT Wethouder Guernaoui

Juni tot en met september 2018

Datum
Oktober 2018
Versie
1.0
Opsteller
10.2.e

Status
Definitief

Inhoudsopgave

1 Gegevensbescherming

In het eerste half jaar van 2018 is ingezet op de volgende punten uit het werkprogramma:

- Bewustwording binnen de gemeente
- Verdere invulling en aanscherping van het register van verwerkingen
- Registratie en opvolging van datalekken
- Inbedding van DPIA's (Data Protection Impact Assessments)
- Uitvoering van verwerkersovereenkomsten tussen de gemeente en derde partijen
- Acties betreffende het inzagerecht

Bewustwording
De Functionaris voor de Gegevensbescherming (FG) heeft samen met de Chief Information Security Officer (CISO) stevig ingezet op bewustwording in de gemeente. Dit heeft geleid tot:

- Het lanceren van een eerste versie van het spel Gegevensweg?!
  Het spel is door circa duizend ambtenaren gespeeld.
- Elke twee weken vindt een spreekuur over privacy & security plaats.
  De vragen en antwoorden uit deze spreekuren worden op Werknet gepubliceerd voor een verdere verspreiding van kennis.
- Iedere vijf weken vindt een privacy & security-overleg met de privacy- en security officers plaats.

Aanscherping register van werkingen
Voor de verdere invulling en aanscherping van het register van verwerkingen hebben alle gemeentelijke diensten de informatie aangeleverd per 1 juli 2018. De volgende stap in het vierde kwartaal van 2018 is de voorbereiding van het register voor externe publicatie, zodat het voor de burger inzichtelijk is welke (algemene en bijzondere) persoonsgegevens worden verwerkt.

Registratie en opvolging datalekken
Met de vergrote interne bewustwording over registratie en opvolging datalekken zijn meer ambtenaren bekend met de herziene procedure ingevolge de Algemene Verordening Gegevensbescherming (AVG). Het absolute aantal datalekken is in de eerste twee kwartalen van 2018 niet gestegen.

Inbedding DPIA's bij de grootschalige verwerking van persoonsgegevens
Sinds de inwerkingtreding van de AVG worden in de gemeente DPIA's uitgevoerd bij grootschalige verwerking van gevoelige gegevens. Een DPIA is geïntroduceerd met de AVG en wordt alleen uitgevoerd bij de grootschalige verwerking van gevoelige gegevens. Bij projecten van lichtere omvang in de verwerking van persoonsgegevens wordt hetzij een PIA (Privacy Impact Assessment) hetzij een *quick scan* uitgevoerd. Een PIA bestaat al onder Wbp en geschiedt bij elk project waarin persoonsgegevens worden verwerkt. Een quick scan wordt veelal voorafgaand aan een project gedaan om te zien of persoonsgegevens worden verwerkt. Voorafgaand aan elk project wordt een analyse gedaan van de privacy impact van een project.

Uitvoering verwerkersovereenkomsten tussen gemeente en derde partijen
De gemeente heeft verwerkersovereenkomsten afgesloten met derde partijen na gunning van een aanbesteding. Het overzicht van deze aanbestedingen is compleet. De gemeente sluit tevens (meervoudig onderhandse) overeenkomsten met kleine(re) derde partijen. De verantwoordelijkheid voor registratie hiervoor is recentelijk verschoven van de diensten naar BEC-I. Het overzicht wordt

voortdurend aangevuld. Inzicht in de compleetheid van deze overeenkomsten is op dit moment onvoldoende. Op het moment worden bij inkoop de verwerkersovereenkomsten bij de aanbestedingen verzameld. Het is aan de diensten om een overzicht van de onderhandse overeenkomsten te bewaren. Bewustwording wordt hierop vergroot door de privacy officers.

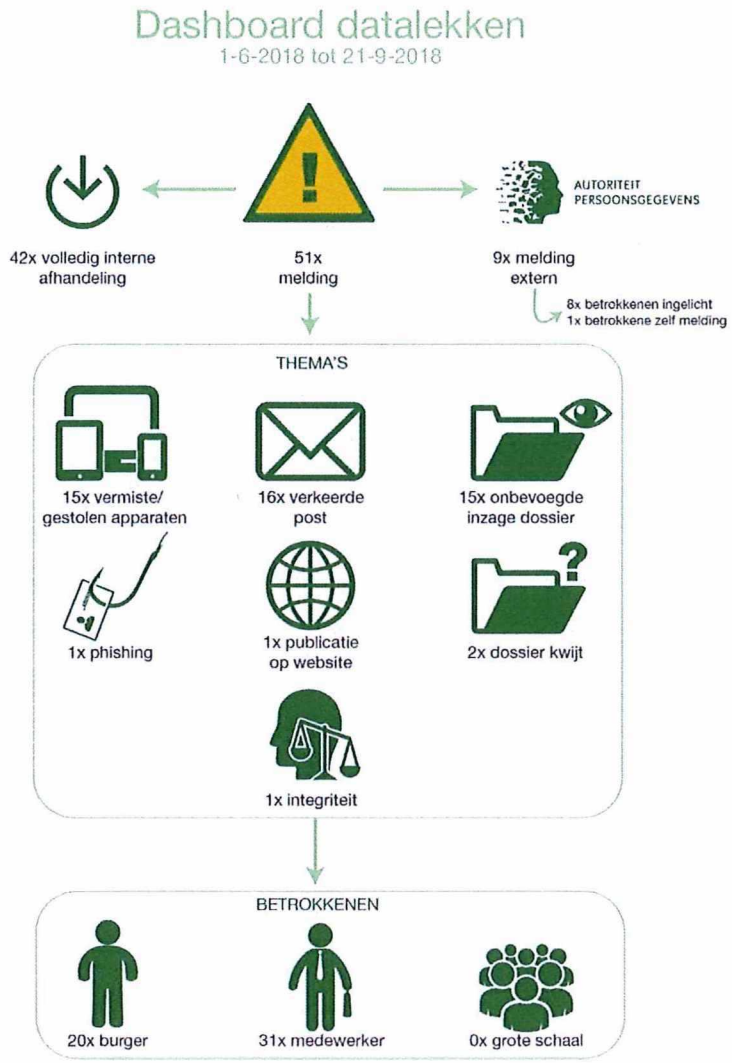
Inzagerecht

De procedure voor het inzagerecht is ingeregeld en inzichtelijk voor de burger. Tevens is de privacyverklaring van de gemeente aangepast aan de AVG. Het aantal inzageverzoeken is sinds de inwerkingtreding van de AVG niet gestegen.

Acties tweede helft 2018

De functionaris gegevensbescherming richt zich in de tweede helft van 2018 op de verdere inbedding van de beginselen van *privacy by design* en *privacy by default* in de gemeente. Een eerste rapportage over deze inbedding volgt in het eerste kwartaal van 2019.

Het volledige werkprogramma van gegevensbescherming wordt onderworpen aan een interne audit van de Gemeentelijke Accountantsdienst (GAD) in september en oktober 2018.



Conclusie naar aanleiding van het dashboard datalekken in het algemeen: het grootste deel van de datalekken betreffen menselijke fouten. De datalekken zijn voorts hersteld door a) daar waar mogelijk het lek te dichten; b) het proces te doorlopen dat geleid heeft tot de menselijke vergissing (b.v. vier-ogen-beginsel, doorlichting autorisatie en logging); c) technische maatregelen te treffen.

2 Informatieveiligheid

Hieronder staan de highlights van de afgelopen vier maanden en een vooruitblik op de komende vier maanden.

Highlights afgelopen 4 maanden

- **Eén ernstig incident door de CISO geëscaleerd**
  Er heeft 1 incident plaatsgevonden dat door de CISO is geëscaleerd naar bestuurlijk niveau. Dit betrof een melding op 31 augustus van CEO-fraude. Hiervoor is binnen de financiële lijn van het BEC een evaluatie uitgevoerd en op 24 september is aangifte gedaan namens de gemeente.

- **G5 ISO dag**
  Op 25 september waren alle ISO's en CISO's van de G5 te gast in Den Haag voor een eerste werkbijeenkomst. Tijdens de verschillende presentaties zijn organisatiestructuren, procedures en werkwijzen met elkaar gedeeld. De uitkomst is dat er op ISO-werkniveau vaker informatie met elkaar uitgewisseld zal worden (de G5 CISO's doen dit al iedere 6 weken).

- **One conference**
  Op 3 oktober heeft de gemeente Den Haag een side-event op de ONE Conference georganiseerd waar de CISO een paneldiscussie met de steden Atlanta en Manchester heeft gevoerd over het onderwerp "Cities under Cyber attack": Can a city be digital and resilient? Na afloop van de conferentie is in samenwerking met deze steden een artikel gepubliceerd dat ingebracht zal worden op de Smart City Expo World Congress Barcelona in november.

Highlights komende 4 maanden

- **Oplevering ENSIA**
  De komende periode zal in het teken staan van de oplevering van ENSIA (Eenduidige Normatiek Single Information Audit) waarmee verantwoording wordt afgelegd over de informatieveiligheid van de gemeente op specifieke processen.

- **Voorbereiding tweede rond bewustwordingsspel Gegevensweg?!**
  Naar verwachting zal begin 2019 de tweede ronde van het bewustwordingsspel Gegevensweg?! worden gelanceerd om de bewustwording op privacy & security gebied te verhogen onder alle medewerkers (zie ook hoofdstuk 3, Gegevensbescherming).

- **Aanbesteding ISMS-tool en opzegging contract**
  Ter ondersteuning van het ISMS proces, wordt gebruik gemaakt van een zogenaamd ISMS-tool. Op 27 september heeft het bedrijf 10.2.g het contract eenzijdig opgezegd zodat wij vanaf 1 januari 2019 niet meer over de tool kunnen beschikken. Aangezien het interne vullingsproces van het ISMS in december eindigt, is gekozen om in de tussentijd geen migratietraject te starten naar de nieuwe versie van de tool en de gebruikers (100+) onnodig te belasten. Parallel hieraan is in september een aanbestedingsprocedure gestart voor een nieuw ISMS tool. Door de tool tot eind 2018 te blijven gebruiken, verandert er voor de collega's die de ISMS-tool moeten vullen niets en met de GAD kan een werkbare situatie afgesproken worden die weinig afwijkt van de huidige processen. Een en ander wordt toegelicht in een aparte notitie.

Den Haag

Viermaandelijkse Rapportage IV-Beleid en ICT

Periode september – december 2020

Datum
Maart 2021
Versie
1.0
Auteurs
Adviseurs Dienst Bedrijfsvoering
Tijdelijke Organisatie I&A Keten

Opdrachtgever
10.2.e
TO I&A

Status
Definitief

Inhoudsopgave

4 Gegevensbescherming

4.1 Vooruitblik komende periode

4.1.1 Privacy-organisatie

De privacy organisatie is op 29 november in het GMT besproken. Het GMT heeft nog geen definitief besluit genomen, maar heeft gevraagd om een nadere uitwerking. Een belangrijke aanvulling is dat het GMT de wens heeft geuit dat er een kwartiermaker zal komen om de privacy office op te zetten en aan te sturen. De kwartiermaker zal zich richten op de opbouw en aansturing van de privacy organisatie en het opstellen en uitvoeren van beleid. De FG kan zich richten op toezicht. Het verder uitgewerkte voorstel zal begin 2021 worden voorgelegd aan het GMT.

4.1.2 Verwerkingsregister

10.2.g heeft het eindrapport voor het 10.2.g als gemeentebreed register van verwerkingen ingediend. In januari 2021 zullen de deelregisters van de verschillende diensten worden geüpload. Alle diensten hebben hun deelregisters afdoende gecontroleerd om dit mogelijk te maken, met uitzondering van DSO/DSB die dit echter zo spoedig mogelijk zullen realiseren. De privacy officers van de verschillende diensten krijgen momenteel een cursus om met het systeem om te gaan, zodat het register actueel gehouden kan worden en er ook op dienstniveau rapportages kunnen worden gemaakt.

Wanneer de gegevens zijn geüpload en de FG heeft kunnen vaststellen dat het register aan de minimumvereisten van de AVG voldoet, biedt 10.2.g ook de mogelijkheid om een uittreksel voor het publiek te publiceren. Aangezien dit een politieke wens is, zal deze publicatie zodra de informatie is geverifieerd plaatsvinden. Naar verwachting zal dit eind Q2 haalbaar zijn.

De volgende stap zal zijn, dat de niet-wettelijke verwerkingen in het register worden opgenomen. Dit zijn de verwerkingen met persoonsgegevens die de gemeente niet op grond van een wettelijke gemeentelijke taak verricht. Uiteindelijk zal het register een volledig en actueel beeld dienen te geven van de verwerkingen van persoonsgegevens in de gemeente Den Haag.

Model DPIA

10.2.g heeft een model DPIA opgeleverd, zodat binnen de gemeente op dezelfde wijze Data protection impact assessments worden afgenomen. In 2020 zijn 24 (D)PIA's verricht. De AP beveelt aan dat DPIA's elke 3 jaar worden geactualiseerd. Omdat de AVG in 2018 in werking is getreden, moet in 2021 duidelijk zijn op welke processen nog een DPIA moet worden verricht.

Een gemeentebreed model met uniforme werkwijze vergroot de onderlinge vergelijkbaarheid waardoor het gemakkelijker zal worden om onderling te leren en best practices over te nemen. Het model omvat niet alleen een rapportage maar ook een werkwijze, die er kort gezegd op neerkomt dat bij nieuwe verwerkingen van persoonsgegevens of bij belangrijke wijzigingen alle betrokken partijen bij elkaar komen om de risico's en mogelijke maatregelen in kaart te brengen. In dit model is de BIO-baseline toets geïntegreerd, zodat zoveel mogelijk wordt voorkomen dat privacy en security voor hetzelfde proces een risicoanalyse verrichten. De integratie van instrumenten moet de onderlinge uitwisseling van informatie vergemakkelijken.

4.1.3 Bewustwording

De bewustwordingscampagne is gestart met een inventarisatieronde, waarbij 10.2.g medewerkers uit de diverse doelgroepen bijeen heeft geroepen om te brainstormen over de vraag wat naar hun mening in hun specifieke functie de belangrijkste kennis en het belangrijkste gedrag is ten aanzien van privacy, security, data en informatiebeheer. Vanaf januari zullen de medewerkers met de producten van de campagne te maken krijgen.

Nulmeting

In het laatste kwartaal vindt een gemeentebrede nulmeting plaats naar de privacy volwassenheid van alle diensten. Deze nulmeting wordt uitgevoerd door 10.2.g Het rapport zal in januari worden opgeleverd. De resultaten van de nulmeting, de toets op het register van verwerkingen en een overzicht waar nog DPIA's dienen te worden uitgevoerd zullen zijn de basis voor de belangrijkste acties van de privacy organisatie in 2021. Daarbij zal de focus zijn op de verwerkingen met een hoog risico voor burgers. De uitkomst en de acties zullen worden gerapporteerd in de eerste vier maand rapportage over 2021

4.2 Terugblik afgelopen 4 maanden

4.2.1 Datalekken

In de periode 1 oktober 2020 - 10 december 2020 waren er 25 potentiële datalekken. Hiervan zijn er 11 aan de Autoriteit Persoonsgegevens gemeld. Het totale aantal datalekken ligt opvallend veel lager vergeleken met het vorige kwartaal. Er is geen pasklare verklaring voor het veel lagere aantal meldingen voorhanden. In de bewustwordingscampagne zal (opnieuw) ook aandacht aan datalekken worden geschonken. SZW heeft aangegeven mede om het risico op datalekken te verkleinen Zorgmail te gaan gebruiken en de FG heeft hierop positief geadviseerd.

De AP heeft op 15 december 2020 de gemeente Den Haag een brief gestuurd, omdat in de periode april tot en met november 2020 12 datalekken te laat (niet binnen 72 uur) aan de AP zijn gemeld en een afdoende motivatie voor het te laat melden ontbreekt. Melding aan de AP vindt plaats door de FG, die hiertoe pas kan overgaan als er een intern een melding bij haar is gedaan. De AP geeft nu een waarschuwing af en vraagt niet om een reactie, maar kan wanneer opnieuw datalekken te laat worden gemeld besluiten over te gaan tot een onderzoek en handhaving.

Een reden die diverse malen is aangegeven voor te late melding, is dat de ernst van het datalek niet meteen duidelijk was. De AP benadrukt, dat het voor het melden van een datalek niet nodig is dat alle informatie al beschikbaar is. Het onderzoek kan na de melding worden voortgezet en leiden tot een aanvulling van de melding. De FG heeft de privacy officers geadviseerd de brief van de AP in de MT's van de diensten te bespreken, zodat ook vanuit het management kan worden benadrukt dat tijdig melden van groot belang is.

5 Informatieveiligheid

5.1 Toelichting

In 2020 is de rapportage over informatieveiligheid gefaseerd verder geprofessionaliseerd. In de eerste fase zullen onderwerpen in deze rapportage gelabeld worden als elementen uit een wereldwijd gebruikt raamwerk, het Cyber Security Framework[1]. Dit model wordt met goedkeuring van het GMT (15 oktober 2020) binnen de gemeente gebruikt om focus aan te brengen in doelen en acties en deze te kunnen beoordelen en te verbeteren.

Identify - ID	Beheren van cybersecurityrisico's
Protect - PR	Waarborgen voor de bescherming van de diensten van de gemeente.
Detect - DE	Identificeren van cybersecurityincident
Respond - RS	Reageren op een gedetecteerd cybersecurityincident
Recover - RC	Plannen en onderhouden van de weerbaarheid om diensten te kunnen herstellen

5.2 Terugblik afgelopen 4 maanden

5.2.1 Jaarplan Security 2020 ID

Het jaarplan voor 2021 is i opgesteld. Verdere detaillering van de uitvoering zal begin 2021 in de roadmap worden opgenomen. Belangrijke onderwerpen in het jaarplan zijn de verdere implementatie van de BIO, vormgeven en intensiveren van het Expertisecentrum Security, implementatie van het NIST Cybersecurity Framework en activiteiten gericht op het verhogen van de digitale weerbaarheid, waaronder het opstellen van een cybercrisisplan en het houden van oefeningen. Doel is om vanuit het vakgebied informatieveiligheid invulling te geven aan de visie op digitalisering en de gemeentebrede en dienstspecifieke doelstellingen.

5.2.2 Audit en Compliance ID

Op 1 juli is de ENSIA-cyclus voor de zelfevaluatie over 2020 van start gegaan. In afstemming met de GAD zijn een aantal pre-audits op het proces op moment van schrijven afgerond of in afrondende fase. Doel hiervan is een verbetering in de ISMS-cyclus te bereiken en eigenaarschap bij de diensten. De pre-audits zijn nuttig gebleken voor de diensten die ervoor gekozen hebben om aan dit traject mee te doen (DPZ en IDC/A). Op basis van het pre-auditrapport worden plannen opgesteld om uiteindelijk wel aan de normen te voldoen door de verantwoordelijke partijen.

[1] National nstitute of Standards and Technology (2018) The N ST Cybersecurity Framework V1 1

5.2.3 Implementatie BIO & ISMS ID

GDH is goed op weg met de implementatie van de BIO, al zijn in het eindrapport na onderzoek door een extern bureau wel verbeterpunten geconstateerd. De verbeterpunten zijn geprioriteerd en worden opgepakt volgens planning binnen het Expertisecentrum Security. Onderdeel hiervan is het beleggen van eigenaarschap daar waar het hoort: zowel in de lijnorganisatie als binnen de securityketen zelf. Daarbij is eigenaarschap de eerste stap naar een daadwerkelijke Plan-Do-Check-Act (PDCA) cyclus waarbij GDH continu de effectiviteit van informatiebeveiliging als geheel verbetert. Blijvend aandachtspunt is eigenaarschap van informatie in de lijnorganisatie waar onder andere in het bewustwordingstraject aandacht aan zal worden besteed (zie hoofdstuk Gegevensbescherming).

5.2.4 Cybercrisisplan en bestuurlijke Cyberoefening RS

In oktober 2020 heeft het GMT besloten dat GDH de ontwikkelingsstap van preventie naar weerbaarheid gaat nemen, met als concrete invulling het kunnen reageren op en opvangen van verstoringen en incidenten met een maatschappelijke impact, ervan uitgaande dat het volledig voorkomen daarvan onmogelijk is. De securityketen vult deze opdracht in middels de implementatie van het NIST Cybersecurity Framework en door een Cyber crisisplan op te stellen en te beoefenen. Begin 2021 zal een eerste concept van het plan opgesteld zijn, wat in Q2 beoefend zal worden (indien de situatie rondom Covid-19 dit toelaat).

5.2.5 Incidenten SolarWinds en Citrix DE RS

Op de valreep van 2020 werd GDH geconfronteerd met twee grote dreigingen: SolarWinds en CitrixADC.

SolarWinds: Naar aanleiding van een grootschalige aanval op het Cybersecurity bedrijf FireEye bleek dat deze aanval werd uitgevoerd via een product van het bedrijf SolarWinds. Dit product was al in 2019 gecompromitteerd en de aanval lijkt te zijn uitgevoerd door een statelijke actor (Rusland). Direct is een interne analyse uitgevoerd op het GDH netwerk, waaruit geen compromittatie bleek. De netwerkleverancier van GDH, 10.2.g bleek wel gebruik te maken van het product. Er is intensief contact geweest met 10.2.g en zij hebben na uitgebreide checks geen indicatoren gevonden die wijzen op misbruik. Op basis van alle informatie is het zeer aannemelijk dat 10.2.g niet is geraakt door de Solarwinds problematiek. Indien dit wel het geval was geweest dan nog was de kans zeer klein dat het netwerk van Den Haag gecompromitteerd zou zijn. Dit vanwege de opzet van de beveiligingsmaatregelen op de verbinding tussen 10.2.g en GDH.

Citrix: 23 december kreeg GDH de melding vanuit Citrix en de IBD dat o.a. Nederlandse gemeenten melding hebben gemaakt van DDoS aanvallen op hun Citrix Netscaler omgeving. Er zijn diverse organisaties wereldwijd die hier hinder van hebben ondervonden. Dezelfde avond is in overleg met de eigen experts en op advies van Citrix besloten om de specifieke onderdelen van Citrix uit te schakelen waar deze aanval betrekking op had. Dit had verder geen consequenties voor de dienstverlening aangezien die componenten niet in gebruik waren.

5.2.5 Cyber security month en HTH21 DE RS

Tijdens de Cyber Security Month is vanuit GDH veel aandacht besteed aan het onderwerp cybersecurity. Onder meer is een internationaal Webinar over HTH21 georganiseerd, heeft de CISO deelgenomen aan Hacktalk – een evenement door en voor hackers – en op de ONE Conference deelgenomen aan een paneldiscussie over het Citrix incident, zijn artikelen/interviews met wethouder

Bruines, IoT Security Monitoring en HTH gepubliceerd, heeft GDH met de regio een prominente rol gespeeld in de Nationale Cyberoefening en heeft de CISO meegedaan aan een podcast over het belang van oefenen. Deze uitingen hebben bijgedragen aan het imago van GDH als voorloper op het gebied van Cybersecurity.

5.2.6 IT-CM TNO RC

Het IDC-A is, na goedkeuring door het GMT, in samenwerking met 10.2.g gestart aan de pilotfase van het programma IT Continuity Management om in het geval van een (cyber)crisis de belangrijkste IT-processen te kunnen blijven uitvoeren. Uitgangspunt in het plan van aanpak is de keuze voor een vitaal proces bij DPZ, paspoortuitgifte, om zo ervaring op te doen met een belangrijk, maar overzichtelijk proces binnen GDH. Inmiddels heeft er met de betrokken dienst afstemming plaats gehad en is het beoogde plan van aanpak gedeeld. Doel is te komen tot een generieke aanpak welke kan worden hergebruikt voor andere processen en diensten. De doelstelling hiervan is het verhogen van de weerbaarheid van de gemeente Den Haag. In het advies van 10.2.g zal ook ingegaan worden op het belang van Business Continuitymanagement (BCM), een verantwoordelijkheid van de diensten.

5.3 Vooruitblik komende 4 maanden

5.3.1 NIST CSF implementatie o.b.v. COBIT 2019 ID

Vanaf 11 januari zal gestart worden met het implementeren van het NIST CSF. Daartoe wordt de methodiek en programma aanpak van COBIT 2019 gehanteerd, met als doel het CSF aan te laten sluiten en te integreren met strategie en doelstellingen binnen de gemeente Den Haag. Daarmee wordt het CSF verbonden met de cybersecurity prioriteiten die volgen uit de doelstellingen vanuit de diensten en GDH breed.

5.3.2 Onderzoek technische digitale veiligheid PR

Dit jaar wordt er een onderzoek uitgevoerd naar de digitale veiligheid van de gemeente Den Haag. Een aantal pentesters zal van binnenuit de omgeving van de gemeente Den Haag gaan onderzoeken op de aanwezigheid van kwetsbaarheden. De scope van de opdracht, planning en daadwerkelijke uitvoering wordt nader bepaald in overleg met de Security keten.

5.3.3 Voorbereidingen Hack The Hague 2021 DE RS

Momenteel wordt onderzocht in welke vorm Hâck The Hague op maandag 27 september 2021 kan doorgaan. Daarbij wordt gekeken naar de variant van een online en een hybride evenement waarbij een deel van de hackers in het Atrium terecht zou kunnen en een deel virtueel kan deelnemen.

Den Haag

Viermaandsrapportage Informatiebeleid/ ICT Wethouder ICT

Mei - augustus 2019

Datum
augustus 2019
Versie
0.5
Auteur
CIO Office

Status
concept

Inhoudsopgave

2 Gegevensbescherming

2.1 Privacy-organisatie

De FG heeft op 13 juni 2019 een plan voor de privacy-organisatie voorgelegd aan het COIA, die dit zal doorgeleiden aan de BVB en vervolgens het GMT.

2.2 Nulmeting privacy-volwassenheid

Om vast te stellen wat de belangrijkste privacy-uitdagingen van de gemeente zijn, adviseert de FG dat alle diensten een nulmeting naar hun privacy-volwassenheid laten uitvoeren en deze jaarlijks herhalen. Geadviseerd wordt bovendien het model van het Centrum voor Informatiebeveiliging en Privacy (CIP) te gebruiken. Dan zijn de uitkomsten onderling vergelijkbaar. In het model van het CIP wordt niveau 3 gezien als het minimaal vereiste niveau van privacy-volwassenheid. De FG adviseert dat de nulmetingen dit jaar gedaan worden zodat ze als basis kunnen dienen voor verdere verbeteringen op het gebied van privacy voor het komende jaar.

2.3 Bewustwording

Het spreekuur over privacy & security vindt nog steeds elke twee weken plaats en wordt goed bezocht door collega's. De vragen en antwoorden uit deze spreekuren worden op Werknet gepubliceerd voor een verdere verspreiding van kennis[10.2.g] Het spreekuur biedt de FG en de CISO een goede inkijk in vraagstukken die op de werkvloer spelen.

2.4 Register van werkingen

Ten behoeve van het register van verwerkingen zal de reeds beschikbare applicatie[10.2.g] gebruikt gaan worden. In dit instrument is reeds een register van alle wettelijke verwerkingen van persoonsgegevens door de gemeente opgenomen dat als basis voor het Haagse register zal dienen.

2.5 Data protection impact assessment

DPIA's dienen te worden uitgevoerd bij grootschalige verwerking van gevoelige gegevens. De afgelopen periode is er echter slechts één DPIA uitgevoerd. De FG werkt aan een training om privacy officers en medewerkers te ondersteunen bij het uitvoeren van een DPIA.

2.6 Datalekken

Van mei tot en met juli 2019 zijn er 7 datalekken aan de Autoriteit Persoonsgegevens gemeld door de gemeente Den Haag. Dit is een daling ten opzichte van het eerste trimester. Naar aanleiding van één datalek heeft de FG de verantwoordelijke directeur verzocht een audit in te stellen bij een verwerker. De reden hiervan was dat uit de melding van het datalek de indruk ontstond, dat de verwerker vaker persoonsgegevens deelde met onbevoegden. De betreffende directie zal dit advies van de FG opvolgen. De rapportage m.b.t. BSN's was niet op tijd gereed om in dit rapport mee te nemen.

2.6.1 Externe ontwikkelingen met betrekking tot datalekken

Op 16 juli 2019 heeft de Autoriteit Persoonsgegevens het 10.2.g een boete van 460.000 euro opgelegd wegens een datalek, waarbij tientallen personeelsleden onnodig inzage hebben gehad in het dossier van een bekende Nederlander. Daarnaast heeft de AP een dwangsom opgelegd wanneer het ziekenhuis de beveiliging niet voor 2 oktober 2019 verbeterd heeft. De AP eist twee zaken van het 10.2.g een regelmatige controle van de logging van patiëntendossiers en beveiliging van deze dossiers met tweefactor authenticatie.

De AP eist dat andere organisaties lessen trekken uit een datalek dat aan de AP wereldkundig maakt. De gemeente Den Haag moet zich de vraag stellen of zij vergelijkbare risico's loopt als het 10.2.g . Samen met FG's van andere gemeenten wordt een brief voorbereid waarin de AP een aantal aanvullende vragen wordt gesteld om de uitspraak over het 10.2.g nader uit te leggen. Elke verwerkingsverantwoordelijke gemeente heeft hierin een eigen verantwoordelijkheid.

Omdat ook de gemeente Den Haag met bijzondere persoonsgegevens werkt, waaronder gezondheidsgegevens, adviseert de FG op dit moment dat Gemeente Den Haag nagaat hoe de logging ten aanzien van bijzondere persoonsgegevens plaatsvindt, een loggingbeleid te ontwikkelen en toe te zien op de naleving hiervan. Daarnaast adviseert de FG om in elk geval voor de verwerking van bijzondere persoonsgegevens tweefactor authenticatie in te voeren.

3 Informatieveiligheid

3.1 Terugblik

3.1.1 Twee ernstige incidenten door de CISO geëscaleerd

Op de vooravond van de Europese verkiezingen van 23 mei 2019 is afwijkend gedrag op ons netwerk geconstateerd. Het betrof verkeer vanaf thuiswerkplekken naar bepaalde poorten die o.a. wordt gebruikt bij ransomware aanvallen. De 2 bronnen zijn geïdentificeerd, de betreffende medewerkers geïnformeerd en de dreiging gemitigeerd. Normaliter wordt een dergelijke melding vanuit de externe monitoring van 10.2.g door de piketdienst aangenomen die daarna de juiste expertise inschakelt. Door de 'verhoogde dijkbewaking' in verband met de verkiezingen is nu direct actie ondernomen.

In de week van 22 juli is er in HalloWerk een inbreuk op de vertrouwelijkheid van persoonsgegevens vastgesteld. Tijdens pentesten is gebleken dat het in het burgerportaal HalloWerk technisch mogelijk is dat ingelogde burgers op vrij eenvoudige wijze persoonsgegevens van andere burgers kunnen inzien. In het samenwerkingsverband met Rotterdam is veel aandacht geweest voor privacy & security, waaronder een aantal uitgevoerde (externe) toetsen. De laatste pentest werd uitgevoerd op verzoek van Den Haag door de nieuwe leverancier (de vorige was failliet gegaan). Na constatering van de uitkomst van de pentest is er direct actie ondernemen om de risico's weg te nemen, zodat de privacy binnen HalloWerk gewaarborgd blijft. De eerste prioriteit betrof het technisch onmogelijk maken dat elkaars gegevens kunnen worden ingezien/gewijzigd. Er zijn 6 ernstige kwetsbaarheden gevonden die op 29 juli zijn opgelost. Een laatste kwetsbaarheid waarmee het mogelijk is om foto's te kunnen inzien of downloaden zonder in te loggen, is op 5 augustus met hoge prioriteit gerepareerd. Daarmee zijn alle hoge en midden kwetsbaarheden op het gebied van vertrouwelijkheid van het burgerportaal van Hallo Werk opgelost. De reeds geplande vervanging van het burgerportaal door de oplossing van de leverancier 10.2.e loopt op schema, en zal naar verwachting in de maand september worden afgerond.

Van de overige security incidenten zijn er in de periode april-juni in totaal 111 geweest, waarvan er 103 binnen de SLA zijn afgehandeld (prio 1: 1, prio 2: 3, prio 3: 6).

3.1.2 Implementatie BIO en ENSIA

2019 is een overgangsjaar van de BIG naar de BIO[1] in 2020. De gemeente heeft de eerste stappen genomen om hierop voorbereid te zijn. Zo is het nieuw aangeschafte Information Security Management System (ISMS)ISMS-tool, 10.2.g geïmplementeerd en wordt deze in het kader van ENSIA 2019 vanaf half augustus gevuld met de vragenlijsten en applicaties voor 2019. Ook volgen trainingen en voorlichtingssessies. In overleg met de diensten en de GAD wordt het ISMS-tool in eerste instantie alleen met de aan ENSIA gerelateerde applicaties gevuld om de kwaliteit te kunnen waarborgen. In tweede instantie volgen de, op basis van risicomanagement geselecteerde, bedrijfskritieke systemen.
Het Beleidskader informatieveiligheid is in het Concern Overleg I&A besproken met de opmerking dat er op tactisch niveau (BEC-i) eerst nog een additionele Roadmap moet worden toegevoegd om de benodigde capaciteit en middelen te onderbouwen. Verwachting is dat het beleidskader na de zomer aangeboden kan worden aan het GMT en het College.

[1] Baseline Informatiebeveiliging Overheid. één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO 27000-normatiek

Er is gestart met de communicatie over de verantwoording van ENSIA en de nieuwe informatiebeveiligingsnorm BIO richting de diensten. Voor de expertisemanagers, functioneel beheerders en de Business Partners worden voorlichtingssessies gehouden waarin de inhoud van de BIO wordt toegelicht en gezamenlijk afspraken worden gemaakt over de verdeling van taken en verantwoordelijkheden. Na de zomer zal de CISO, samen met de Business Partners I, de Algemeen Directeuren van de diensten spreken om ook daar bewustzijn en draagvlak te creëren voor ENSIA en de BIO.

3.1.3 Aanbesteding VNG GGI-Veilig

Inmiddels is de aanbesteding "GGI-Veilig" afgerond en de gunning definitief Vanaf september is het mogelijk om producten en diensten te gaan afnemen. De gemeente Den Haag doet mee in alle drie de percelen (Managed SIEM/SOC[2]-dienstverlening, aanvullende securityproducten/dienstverlening en Security expertise services). Middels minicompetities zullen de leveranciers binnen de 3 percelen worden geselecteerd voor de gemeente Den Haag. In eerste instantie richten wij ons op End-Point security en Managed SIEM/SOC-dienstverlening.

3.1.4 Oplevering ENSIA

Op 25 april 2019 is de ondertekende collegeverklaring ENSIA en bijbehorende GAD assuranceverklaring ingeleverd. Voor de eigen DigiD aansluiting bestonden 3 normen die niet aan de eisen voldeden. Aan de eerste norm moest voor 6 augustus 2019 voldaan worden en de positieve verklaring hiervoor is door de GAD afgegeven en inmiddels opgeleverd aan Logius. De overige twee openstaande normen moeten voor 6 oktober 2019 aan de eisen voldoen en liggen op planning om opgelost te worden. De openstaande normen bij Wigo4it zijn in een taskforce, opgezet door de SZW-lijn binnen de G4 en met Wigo4it aangepakt en de resultaten van een her-audit worden in september verwacht.

3.1.5 Risicoanalyses en beveiliging in de keten

Van alle dienstkritieke applicaties is een Business Impact Analyse uitgevoerd. Met de invoering van de BIO worden deze aangepast naar het daarin gebruikte Basis Betrouwbaarheidsniveau (BBN) en bijbehorende risicoanalysemethodiek. Deze is nog niet voorhanden vanuit de Overheid of de VNG (verwachting: eind 2019). In de tussentijd worden de meest kritische applicaties geanalyseerd en wordt een BBN toegekend voordat ze in het ISMS-tool worden opgenomen. Risicomanagement blijft zo gewaarborgd.

Het percentage ICT-contracten bij diensten waar security is meegenomen is gelijk aan het percentage ICT-contracten[3] dat is overdragen aan de contractmanager CLM. Zie de rapportage Contract en leveranciersmanagement voor het actuele percentage per dienst.

---

[2] SIEM is een proces dat alle beschikbare informatie binnen de ICT-infrastructuur, die een relatie heeft met informatieveiligheid, verzamelt en analyseert. Op basis van deze analyses kunnen kwetsbaarheden ontdekt worden en kunnen aanvallen en verdacht gedrag in een vroeg stadium worden gesignaleerd.
SOC staat voor Security Operations Center. Dit is de plek in de organisatie die alle IT-security gerelateerde zaken kan begeleiden en uitvoeren. Het SOC van Den Haag bevindt zich op de Leyweg.

[3] Gebaseerd op BIG, BIR, ISO en vanaf 2018 AVG.

3.2 Vooruitblik komende 4 maanden

3.2.1 Voorbereiding Hack The Hague 2019

In navolging van vorig jaar, is de scope van de wedstrijd verder uitgebreid met de intentie om uiteindelijk alle systemen van de gemeente en haar leveranciers onder de loep te laten nemen. Vanaf 30 juli zijn de leveranciers actief benaderd met de vraag deel te nemen. Hierbij is er ook de mogelijkheid om de wedstrijd ter plekke te volgen en het logo van de leverancier op banners te laten plaatsen. Het evenement zal op maandag 30 september 2019 worden gehouden, de dag voor de start van de ONE Conference. In overleg met het NCSC, de organisator van de ONE-conference, is besloten om elkaars evenementen te noemen in de communicatie. Daarnaast zal het stadhuis op dezelfde maandagavond plaats bieden aan nog eens 100 hackers die op uitnodiging van NCSC uit binnen- en buitenland komen voor een zogenaamd Capture The Flag hack-event. Tussen 17.00 en 19.00 zal een borrel met pizza plaatsvinden waar beide groepen hackers én nog eens 50 genodigden van de ONE-conference elkaar kunnen ontmoeten tijdens de prijsuitreiking.

Een maand na de perspublicatie via de online mediakanalen en social mediakanalen van 25 juli 2019 is een bereik behaald van 19,5 miljoen views, waarvan 18% nationaal en 82% internationaal. Dit heeft gezorgd voor in totaal 84 aanmeldingen, waarvan 12 internationale hackers.

3.2.2 Bewustwording

In maart en april dit jaar zijn 4 sessies gehouden van de Cybersecurity Table Top simulatie voor het management van de gemeente (top 36). Een 5e sessie zal op 13 september worden georganiseerd waarbij wethouder Guernaoui zal deelnemen, samen met de mensen die bij de eerste sessies niet konden deelnemen.

Daarnaast zal in Q4 van dit jaar een tweede ronde van het spel Gegevensweg!? worden uitgerold binnen de gemeente (in dezelfde periode als de Hackwedstrijd). Hierbij zal aandacht worden besteed aan de bewustwording van Privacy & Security van alle medewerkers van de gemeente. In tegenstelling tot vorig jaar krijgt dit jaar iedereen een uitnodiging waar in de eerste ronde de inschrijving al vrijblijvend was.

Ook zal dit jaar een aanbesteding starten voor een langdurig bewustwordingstraject (meerjarig). Hierbij zal de insteek zijn om een bewustwordingstraject aan te laten sluiten op verschillende doelgroepen en risico's. Bijvoorbeeld phishing en CEO-fraude, maar ook 'mystery guests' die fysiek onze panden proberen binnen te komen. De uitnodiging aan marktpartijen voor een marktverkenning zal begin augustus plaatsvinden.

3.2.3 Start realisatie virtueel hack team Den Haag

Van maandag 17 tot woensdag 19 juni is de eerste hack-training georganiseerd. Twee professionele hackers van 10.2.g hebben een cursus verzorgd voor een intern team van IDC/A. Deze goed gewaardeerde cursus zal door de security architecten verder worden uitgewerkt en verder worden toegespitst op de eigen vakdisciplines voor een directere aansluiting op de gemeente specifieke applicaties en werkzaamheden. Ook vanuit de GAD is er interesse om eind november 2019 de training te volgen voor auditers in G4 verband. De nadruk zal hierbij liggen op het lezen en interpreteren van pentestrapporten.

3.2.4 ONE-Conference

Van 1-3 oktober vindt de ONE-Conference plaats in het World Forum. Tijdens de 'One conference', dé internationale cyber security conferentie, worden in Den Haag veel prominente nationale en internationale sprekers verwacht die nieuwe ontwikkelingen, ideeën en inzichten delen. De gemeente heeft de CISO van New York als keynote speaker geregeld. Daarnaast zal een side-event worden georganiseerd om met CISO's van internationale steden in discussie te gaan met experts. De One Conference is een initiatief van het Nationaal Cybersecurity Centrum en het Ministerie van Economische Zaken en Klimaat in samenwerking met gemeente Den Haag.

Den Haag

Viermaandelijkse Rapportage IV-Beleid en ICT

mei - augustus 2021

Datum
3 oktober 2021
Versie
1.0
Dienst
Dienst Bedrijfsvoering (DBV)

Opdrachtgever
10.2.e
[redacted]

Opsteller
Team Strategie, Beleid en Ondersteuning (DBV/TO I&A)

Status
Conceptversie GMT

Inhoudsopgave

B.R.

3.5 B.R.

B.R.

B.R.

3.6 B.R.

B.R.

4 Gegevensbescherming

4.1 Privacy governance en organisatie

De voorbereiding voor het centraliseren van de privacy functie in een nieuwe expertisecentrum privacy in de TO I&A is afgerond en de adviesaanvraag is voorgelegd aan de Centrale Ondernemingsraad (COR). Na een positief advies van de COR start het expertisecentrum privacy (ECP) formeel en is de FG in de Bestuursdienst gepositioneerd op een (interne) onafhankelijkheid positie. Er is een Chief Privacy Officer/Expertisemanager Privacy geworven die het privacyteam gaat aansturen en verder ontwikkelen. Deze is per 1 september 2021 gestart.

In juni en juli hebben vier (decentrale) privacy officers (op het totaal van zeven privacy officers) hun ontslag ingediend voor een uitdaging elders en alle vier zijn per augustus en september uit dienst gegaan. Om de

continuïteit te borgen zijn per augustus tijdelijk ervaren senior privacy officers ingehuurd. De werving voor nieuwe privacy officers met een dienstverband bij de gemeente wordt in september 2021 gestart.

De AVG volwassenheidsscan is in de directieteams van de gemeentelijke (kern)diensten en het GMT besproken. Op basis van de volwassenheidsscan is afgesproken dat er een centraal plan van aanpak met roadmap komt om de gemeente op een hoger volwassenheidsniveau te brengen, met daarbij specifieke maatwerkacties per dienst waar nodig. Oplevering van het plan van aanpak en roadmap is voorzien in het najaar 2021.

4.2 Inzicht in verwerkingen

Nadat in begin 2021 is geconstateerd dat het beoogde systeem ter ondersteuning van het verwerkingsregister niet voldoet, is ervoor gekozen om het VNG-model verwerkingsregister te hanteren. De bestaande deelregisters van de gemeentelijke diensten zijn grotendeels omgezet naar het VNG-model en waar nodig geactualiseerd. In september 2021 worden de deelregisters conform VNG-model samengevoegd tot één centraal verwerkingsregister. Met het centrale verwerkingsregister voldoet de gemeente aan de wettelijke verplichting vanuit de AVG en heeft de gemeente beter inzicht in welke processen er mogelijke privacyrisico's zijn. Op basis van dit centrale verwerkingsregister start in september 2021 een project om de verwerkingen transparant te publiceren op denhaag.nl (tezamen met het algoritmeregister en sensorenregister).

4.3 Risicobeheersing (DPIA's)

In mei 2021 heeft het GMT het plan van aanpak, inclusief kaders, standaarden en templates voor de DPIA's vastgesteld. Daarmee is voldaan aan één van de aanbevelingen uit de AVG-volwassenheidsscan. Er is een begrotingsclaim ingediend voor (tijdelijk) extra capaciteit om DPIA's uit te voeren. Zodra de begroting (zonder afwijzing van deze claim) wordt vastgesteld, zullen er extra DPIA-experts worden geworven om DPIA's uit te voeren voor de diensten. Er zijn de afgelopen vier maanden een tiental DPIA's uitgevoerd, waaronder op WiFi-tellingen (naar aanleiding van het boetebesluit van de Autoriteit Persoonsgegevens (AP) aan de gemeente Enschede); het Urban Data Platform en Druktemeting op Scheveningen (Living Lab Scheveningen). De (inhoudelijke) kwaliteit van de DPIA's is merkbaar omhoog gegaan en met de procesaanpak (workshops met belangrijkste betrokkenen bij het project) wordt tevens veel (privacy)bewustwording gekweekt.

4.4 Datalekken

In de periode mei – augustus 2021 zijn 85 interne meldingen datalekken ontvangen (de vorige 4 maand periode waren er 90). 20 datalekken zijn aan de AP gemeld (vorige periode tevens 20). De meeste datalekken betreft het versturen van persoonsgegevens naar onbevoegden, doordat een e-mail of post verkeerd is geadresseerd. Als maatregel hierop zet de gemeente in het sociaal domein reeds een beveiligde mailapplicatie in (10.2.g Ook start een gemeentebreed project voor de implementatie van 10.2.g 10.2.g 10.2.g waarbij informatie geclassificeerd moet worden en zorg draagt dat vertrouwelijke en geheime informatie (waaronder persoonsgegevens) beveiligd worden.

4.5 Datalekken

Bij de start van (ICT-)projecten worden nu standaard de privacy officers betrokken om een eerste inschatting te maken van de privacy risico's van het project en te beoordelen of er een DPIA uitgevoerd dient te worden.

De (AP) heeft op 30 juli 2021 haar eindrapport en aanbevelingen smart cities gepubliceerd.[1] De gemeente Den Haag heeft informatie geleverd aan de AP voor dit rapport. De aanbevelingen uit het rapport neemt de gemeente tot zich en zal deze waar relevant en noodzakelijk gaan toepassen.

4.6 Transparantie en rechten van betrokkenen

In juli 2021 is het kwalitatieve onderzoek over communicatie omtrent privacy naar inwoners afgerond. Een aantal inwoners en experts zijn geïnterviewd over hoe de gemeente beter kan communiceren over privacy. De belangrijkste drie behoeften die uit het onderzoek komen: aan wie worden mijn persoonsgegevens verstrekt; hoe lang worden mijn persoonsgegevens bewaard; en wat doet de gemeente om de veiligheid (voorkomen datalekken) te garanderen? Dit onderzoek zal als basis fungeren voor een project dat in het najaar start om de privacy communicatie op de gemeentelijke website te verbeteren (inclusief de privacyverklaring).

4.7 Cultuur/bewustwording

In de gemeentebrede bewustwordingscampagne zal in september en oktober weer extra aandacht worden gegeven aan het thema "datalekken" om specifiek de meldingsbereidheid bij medewerkers (en managers) te vergroten. Er wordt vooral ingezet op kennis (herkennen van een mogelijk datalek) en gedrag (weten hoe en waar je een interne melding moet doen). De vastgestelde procedure voor meldingen datalekken is daarvoor voor medewerkers in een toegankelijke infographic omgezet; er wordt een video gemaakt over wat er gebeurt met een melding datalek; er worden presentaties gegeven in teamoverleggen en middels lijncommunicatie worden managers gevraagd om dit thema in hun teams te bespreken.

4.8 Advies FG

4.8.1 AVG volwassenheidsscan

In januari 2021 is de AVG volwassenheidsscan afgerond. De AVG is in mei 2018 in werking getreden, maar uit de scan komt naar voren dat volgens het onderzoeksbureau op basis van interviews en vragenlijsten, de gemiddelde score van de gemeente Den Haag te laag is en achterloopt bij waar zij had moeten kunnen staan (niveau 1 i.p.v. 3). De inspanningen tot verbetering dienen op korte termijn geïntensiveerd te worden. Nu de privacy-organisatie eerst nieuwe vaste privacy officers moet gaan werven, is het zaak dat diensten ook bottom-up aan de slag gaan met bevindingen uit deze volwassenheidsscan. Voor elke dienst is een specifieke analyse gemaakt die hiervoor voldoende aanknopingspunten biedt.

Essentieel is dat de MTs van de diensten op korte termijn meer inzicht in privacy krijgen. Eén van de instrumenten hiervoor is het register van verwerkingen. De FG beveelt aan binnen elke dienst een directeur wordt aangewezen die privacy in zijn/haar portefeuille heeft en aan wie op regelmatige basis wordt gerapporteerd. Omdat privacy vaak raakvlakken heeft met andere risico- 's – security, integriteit – zou aan een dergelijke directeur ook integraal over risico's gerapporteerd kunnen worden.

4.8.2 DPIA's

Een ander instrument om meer inzicht in privacy te krijgen is het uitvoeren van een DPIA. Het aantal DPIA's is nog steeds laag waardoor onvoldoende inzicht bestaat in de risico's van verwerkingen. Het is daarom van groot belang dat de gemeente hiervoor budget vrijmaakt. Vervolgens zal regelmatig moeten worden bezien of de in de DPIA's geïdentificeerde noodzakelijke maatregelen ook daadwerkelijk zijn genomen en of de risico's hiermee tot een aanvaardbaar niveau worden teruggebracht. Het uitvoeren van een DPIA moet dus het begin van een PDCA-cyclus vormen.

[1] AP publiceert aanbevelingen voor smart cities | Autoriteit Persoonsgegevens

De kwaliteit van de DPIA's gaat gestaag omhoog en biedt in het algemeen voldoende informatie voor een gericht privacy-advies. Uit de DPIA's die in de afgelopen periode zijn opgesteld, vielen twee punten op. Ten eerste heeft de gemeente als bestuursorgaan meestal een wettelijke grondslag nodig om persoonsgegevens te mogen verwerken. Deze grondslag moet voldoende specifiek zijn. Een situatie waarin een dergelijke grondslag vaak ontbreekt, is wanneer persoonsgegevens met andere organisaties worden gedeeld. Een tweede punt, is dat de verantwoordelijkheid voor de verwerking niet altijd helder is. Dit kan binnen de gemeente spelen, wanneer niet duidelijk is onder de verantwoordelijkheid van welke AD een verwerking valt. Daarnaast roepen samenwerkingsverbanden ook in dit opzicht vragen op. De rol van alle deelnemende partners vraagt vaak om nadere verduidelijking.

4.8.3 Datalekken

Voor het afhandelen van datalekken is een nieuwe procedure vastgesteld. Het is van belang dat nu de bezetting van de privacy-organisatie weer enigszins op orde is, privacy officers actiever met de FG gaan overleggen over datalekken en vooral over de vraag of deze al dan niet bij de AP moeten worden gemeld.

4.8.4 Privacy by design

De DPIA is ook een moment om privacy by design vast te leggen. Privacy by design is een breed begrip. Het kan erop duiden dat privacy beter wordt beschermd door bijvoorbeeld technische maatregelen, maar kan er ook toe leiden dat er minder persoonsgegevens worden verwerkt. Het is opvallend dat de business lang niet altijd de juiste partijen weet te vinden om vooraf het gesprek aan te gaan over privacy by design. Privacy officers kunnen in dat opzicht een bemiddelende rol spelen, maar dan is natuurlijk wel vereist dat zij zelf in een zeer vroeg stadium zijn betrokken.

4.8.5 Smart city

In het rapport over smart cities doet de Autoriteit Persoonsgegevens aanbevelingen die in feite op alle verwerkingen van persoonsgegevens van toepassing zijn. Zeer kort kan worden gesteld, dat ook voor smart city noodzakelijk is dat aan de basisvereisten van de AVG wordt voldaan. Zoals hierboven aangeven, dient de gemeente Den Haag in dat opzicht nog de nodige stappen te zetten.

De Autoriteit Persoonsgegevens (AP) benadrukt het belang van openbaarheid en democratische controle, juist bij smart cities. De AP wijst op de rol van de gemeenteraad en benadrukt dat gemeenteraden voldoende kennis en informatie over digitalisering en de inzet van smart city-toepassingen moeten krijgen om hun democratische taak goed uit te kunnen voeren. Ook adviseert de AP om burgers te betrekken, zodat zowel de problemen, de oplossingen als de risico's van de openbare ruimte in kaart worden gebracht. Dit laatste wordt in het Living Lab Schevingen (LLS) al in de praktijk gebracht, door burgers uit te nodigen bij overlegtafels. De betrokkenheid van burgers zou verder kunnen worden vergroot, door hen ook te betrekken bij het opstellen van DPIA's. De AVG formuleert dit zelfs als een verplichting, hoewel deze praktijk nog geen gemeengoed is.

5 Informatieveiligheid

Toelichting

In onderstaande rapportage zijn de onderwerpen gelabeld als elementen uit een wereldwijd gebruikt raamwerk, het NIST Cyber Security Framework[2]. Dit model wordt binnen de gemeente gebruikt om focus aan te brengen in doelen en acties en deze te kunnen beoordelen en te verbeteren.

Identify - ID	Beheren van cybersecurityrisico's
Protect - PR	Waarborgen voor de bescherming van de diensten van de gemeente.
Detect - DE	Identificeren van cybersecurityincident
Respond - RS	Reageren op een gedetecteerd cybersecurityincident
Recover - RC	Plannen en onderhouden van de weerbaarheid om diensten te kunnen herstellen

5.1 Terugblik afgelopen vier maanden

5.1.1 Voortgang jaarplan security 2021 ID

Belangrijke onderwerpen in het jaarplan zijn de verdere implementatie van de BIO, vormgeven en intensiveren van het Expertisecentrum Security en activiteiten gericht op het verhogen van de digitale weerbaarheid, namelijk implementatie van het NIST Cybersecurity Framework (CSF) en het opstellen van een cybercrisisplan inclusief het houden van oefeningen. Voor de implementatie van de BIO is gekozen voor extra begeleiding van de ISO's bij de invulling van de zelfevaluatie door de Diensten. Expertisecentrum Security zet stappen richting een meer professionele organisatie en werkt toe naar een duidelijker portfolio op basis van NIST CSF. Tot slot heeft de gemeente Den Haag in juni deelgenomen aan de nationale cyberoefening ISIDOOR, waarbij nauw is samengewerkt met directie Veiligheid. De oefening was een succes, waarbij de scope van de oefening de IT-organisatie tot en met de CIO betrof. De voortgang op het jaarplan is goed.

5.1.2 Audit en compliance ID

De jaarlijkse ENSIA-verantwoording is op 13 april in het college behandeld. De zelfevaluaties hebben uitgewezen dat niet volledig wordt voldaan aan alle geselecteerde normen. De op deze geldende uitzonderingen gerichte beheersmaatregelen voor DigiD en Suwinet zijn in verbeterplannen opgenomen en zijn bij de betreffende organisatieonderdelen belegd en worden gemonitord. Voor DigiD heeft het verbeterplan reeds geleid tot door de auditor geaccepteerde verbeteringen op de normen, waardoor een voorschot is genomen op de formele melding vanuit Logius na 1 mei. Op basis van de collegeverklaring stelt de GAD een assurance-rapport op. De DigiD pentest staat gepland voor de week van 13 september.

5.1.3 Implementatie BIO & ISMS ID

GDH werkt continu aan de verbetering van informatieveiligheid volgens de principes van de BIO. De verbeterpunten liggen met name op het vlak van beleid en de implementatie daarvan, het integrale bewustwordingstraject in 2021 en de verbetering en professionalisering van het ISMS-proces. Het beleid is aangevuld met missende stukken en er is in kaart gebracht welke stukken aan vernieuwing toe zijn. Voor het ISMS-proces is de procesbeschrijving vastgesteld en ontvangen de diensten extra begeleiding bij de

[2] National Institute of Standards and Technology (2018). The NIST Cybersecurity Framework. V1.1

zelfevaluatie. Blijvend aandachtspunt is eigenaarschap van informatie inclusief de veiligheid daarvan in de lijnorganisatie. We werken toe naar een goed werkende Plan-Do-Check-Act (PDCA) cyclus waarbij GDH continu de effectiviteit van informatiebeveiliging als geheel verbetert. Hiervoor is het Expertisecentrum Security echter afhankelijk van de Diensten (applicatie-eigenaren).

5.1.4 NIST CSF implementatie o.b.v. COBIT 2019 ID

Vanaf januari 2021 is gestart met het implementeren van het NIST CSF. Daartoe wordt de methodiek en programma aanpak van COBIT 2019 gehanteerd, met als doel het CSF aan te laten sluiten en te integreren met strategie en doelstellingen binnen de gemeente Den Haag. Daarmee wordt het CSF verbonden met de cybersecurity prioriteiten die volgen uit de doelstellingen vanuit de diensten en GDH breed. De nulmeting inclusief werkpakketten zit in de afrondende fase. Vanaf 2022 kunnen de werkpakketten geprioriteerd worden geïmplementeerd. Daarnaast wordt de eerste versie van een verbeterde rapportage eind augustus opgeleverd. Deze rapportage gaat helpen om informatieveiligheid en cybersecurity te duiden en het gesprek met de Diensten gerichter te voeren.

5.1.5 Grote incidenten DE

De afgelopen periode zijn er enkele incidenten geweest die invloed hebben gehad op de dienstverlening:

- Website Ombudsman offline:
  Op 10 juni waren er signalen dat de websites "ombudsman.denhaag.nl" en "jeugdombudsman.denhaag.nl" werden aangevallen. Uit voorzorg zijn de websites door de beheerders gecontroleerd down gebracht om schade en datalekken te voorkomen. Na onderzoek konden beide sites weer actief worden gemaakt. Er is geen schade ontstaan en er is geen data gelekt.
- Publicatie nieuwe website "Werkenvoordenhaag.nl" (10.2.g
  De nieuwe versie van de website bleek na livegang niet voldoende veilig te zijn. Er was geen pentest voor de livegang uitgevoerd en Security heeft enkele tests uitgevoerd waarbij mogelijke datalekken aan het licht kwamen. Op advies van Security is de website hierop offline gebracht. De oude website is online gebracht om de dienstverlening snel te kunnen herstellen.

In deze periode zijn er na het wereldwijde 10.2.g incident nog enkele kwetsbaarheden gemeld door de IBD. Geen van deze meldingen waren van toepassing op de gemeente Den Haag door de manier waarop het interne netwerk van de gemeente is ingericht.

5.2 Vooruitblik komende 4 maanden

5.2.1 Verhogen digitale weerbaarheid ID

In het kader van verhogen van digitale weerbaarheid wordt enerzijds NIST CSF geïmplementeerd en anderzijds een cybercrisisplan opgesteld en beoefend. In het tweede kwartaal is gestart met de training van de leden van het ECS omtrent NIST CSF, wat een vervolg zal krijgen in de komende tijd. Daarnaast wordt het concept cybercrisisplan geüpdatet op basis van de ervaringen in de oefening ISIDOOR. Dit nieuwe plan wordt na de bestuurlijke oefening in november definitief gemaakt en daarna aangeboden ter vaststelling aan het GMT.

5.2.2 Hâck The Hague 2021 DE RS

Voor dit jaar is vastgesteld dat Hâck The Hague als volledig digitaal evenement doorgaat op maandag 27 september met een maximum van 200 ethische hackers. De scope zijn alle systemen die via Internet bereikbaar zijn en van de leveranciers die deelnemen aan het evenement.

Het maximum aantal aanschrijvingen is bereikt en er zullen hackers uit circa 20 verschillende landen meedoen. Hoewel zij op afstand deelnemen, zal de presentatie van het evenement op het stadhuis plaatsvinden. Berichten op sociale media over Hâck The Hague 2021 worden vaker gedeeld dan voorgaande jaren en ook traditionele media hebben interesse getoond.

6 B.R.

B.R.

6.1 B.R.

6.1.1 B.R.

B.R.

6.1.2 B.R.

B.R.

Den Haag

Viermaandsrapportage Informatiebeleid / ICT Wethouder Guernaoui

Januari – april 2019

Datum
januari - april 2019
Versie
0.9
Auteur
CIO Office

Status
concept

Inhoudsopgave

2 Gegevensbescherming

Op 1 januari 2019 is de nieuwe functionaris voor de gegevensbescherming (FG) aangetreden. De FG heeft de eerste drie maanden benut om kennis te maken met de organisatie en zich te oriënteren op de stand van de bescherming van persoonsgegevens binnen de gemeente Den Haag. Daarbij was de voortgangsbrief van 28 augustus 2018 van de vorige FG aan de rekeningencommissie leidend.

2.1 Implementatie AVG

Privacy-organisatie
Om aan de verplichtingen van de AVG te voldoen, is een goed ingerichte privacy-organisatie noodzakelijk. Op dit moment hebben alleen de diensten OCW en SZW een fulltime privacy officer. DSB heeft een tijdelijke privacy officer aangesteld. Bij de overige diensten bestaat de privacy-organisatie voor het grootste deel uit voormalige Wbp-coördinatoren die een beperkt deel van hun takenpakket aan privacy besteden. Dit betekent dat er nog steeds een beroep gedaan wordt op de tijd van de Information Security Officers (ISO's). Er zijn dus te weinig deskundige medewerkers voor werkzaamheden als het adviseren van algemeen directeuren en het uitvoeren van privacy impact assessments. Dit is een belemmering in het verder groeien in privacy-volwassenheid en het invullen van de ambitie om koploper te zijn. Samen met het BEC stelt de FG daarom een plan op voor het GMT voor de inrichting van de gemeentelijke privacy-organisatie. In dit plan wordt de bezetting van de privacy-officers meegenomen. Naast de privacy-officers wordt ook ingegaan op de versterking van andere functies bij het BEC die betrekking hebben op privacy, denken aan juristen en privacy-auditors.

Nulmeting privacy-volwassenheid
Om vast te stellen wat de belangrijkste privacy-uitdagingen van de gemeente zijn, adviseert de FG dat de alle diensten een nulmeting naar hun privacy-volwassenheid laten uitvoeren en deze periodiek herhalen. Geadviseerd wordt bovendien het model van het Centrum voor Informatiebeveiliging en Privacy (CIP) te gebruiken. Dan zijn de uitkomsten onderling vergelijkbaar. Sommige diensten hebben dit al gedaan. In het model van het CIP wordt niveau 3 gezien als het minimaal vereiste niveau van privacy-volwassenheid.

Bewustwording
Het spreekuur over privacy & security vindt nog steeds elke twee weken plaats en wordt goed bezocht door collega's. De vragen en antwoorden uit deze spreekuren worden op Werknet gepubliceerd voor een verdere verspreiding van kennis. Het spreekuur biedt de FG en de CISO een goede inkijk in vraagstukken die op de werkvloer spelen.

Register van werkingen
De FG onderzoekt opties voor een nieuw register van verwerkingen, zodat betere rapportage mogelijk is. Betere rapportagemogelijkheden zijn voor de FG een voorwaarde om toezicht te kunnen houden. Het register dient volgens uniforme richtlijnen te worden ingevuld, zodat de informatie onderling vergelijkbaar is. Op dit punt is verbetering mogelijk. Als het nieuwe register is ingericht, wordt deze ook online gepubliceerd.

Data protection impact assessment
DPIA's dienen te worden uitgevoerd bij grootschalige verwerking van gevoelige gegevens. De afgelopen periode is er echter slechts één DPIA uitgevoerd. De FG stelt momenteel een eenvorming model DPIA op die gemeentebreed wordt vastgesteld.

Verwerkersovereenkomsten
De gemeente sluit verwerkersovereenkomsten af met derde partijen die persoonsgegevens verwerken onder de verantwoordelijkheid van de gemeente. De gemeente hanteert een door het college vastgestelde verwerkersovereenkomst. BEC-I registreert de verwerkersovereenkomsten die met derde partijen zijn afgesloten na gunning van een aanbesteding. Het overzicht wordt voortdurend aangevuld. De verwerkersovereenkomsten voor onderhands aanbesteedde contracten worden door de diensten zelf geregistreerd.

Rechten van betrokkenen
De FG stelt momenteel een gemeentebrede procedure op voor de rechten van betrokkenen, waaronder het inzagerecht. Binnen deze procedure wordt een oplossing gezocht voor het identificatievraagstuk. Dit houdt in dat de gemeente kan verantwoorden dat persoonsgegevens uitsluitend ter inzage worden gegeven aan de persoon zelf of aan diens wettelijke vertegenwoordiger.

2.2 Datalekken

In de eerste vier maanden van 2019 zijn er 27 datalekken aan de Autoriteit Persoonsgegevens gemeld. Dit is een daling ten opzicht van 2018.

Het grootste deel van de datalekken betreffen menselijke fouten. Hierbij gaat het om: het verliezen van telefoons en laptops, onvolledige adressering (huisnummer toevoeging ontbreekt), onjuiste mailadressen. In één geval was sprake van een datalek, waarbij geen gebruik werd gemaakt van de beschikbare beveiligde communicatiemogelijkheden. In twee gevallen was sprake van een datalek, dat het gevolg was van een niet-succesvolle security update. In drie gevallen was sprake van een datalek waarbij meerdere betrokkenen waren getroffen, namelijk tussen de 25-1000 betrokkenen. In twee gevallen was sprake van misbruik van autorisatie.

Opvallend is dat het aantal meldingen ten opzichte van het vorige half jaar sterk is gedaald. Met name de scherpe daling in het aantal onbevoegd geraadpleegde dossiers valt op, van 15 onbevoegde inzagen naar 2.

De datalekken zijn waar mogelijk hersteld door a) daar waar mogelijk het lek te dichten; b) het proces te doorlopen dat geleid heeft tot de menselijke vergissing (b.v. vier-ogen-beginsel, doorlichting autorisatie en logging); c) technische maatregelen te treffen.

Naar aanleiding van de inhoud van de datalekken heeft de FG opdracht gegeven tot een interne audit naar het onrechtmatig verwerken van BSN's. Het eerste onderzoek wordt verricht bij het klantcontactcentrum van DPZ, naar aanleiding van een klacht van een burger. Naar verwachting is in de volgende rapportage het resultaat bekend.

3 Informatieveiligheid

3.1 Terugblik

Drie ernstige incidenten door de CISO geëscaleerd
Op 20 maart heeft Wigo4it melding gedaan van een herzien oordeel van de externe auditor in het kader van het onderzoek voor ENSIA[1] 2018. Uit het onderzoek bleek o.a. dat autorisatiestructuren ontbraken, geen inzicht was in welke applicaties zijn gekoppeld met Suwinet[2] en niet vastgesteld kon worden dat Suwinet-data in voldoende mate beveiligd wordt. Aangezien deze situatie potentieel risico oplevert voor de bedrijfsvoering van SZW, is in G4-verband een taskforce opgericht die, samen met Wigo4it, zorgdraagt dat security-issues worden opgelost.

Bij OCW en SZW hebben twee gevallen van CEO-fraude[3] plaatsgevonden. Daarbij is geen informatie gelekt en is ook geen bedrag overgemaakt door snelle actie van de medewerkers die het direct hebben gemeld.

Implementatie BIO
2019 is een overgangsjaar van de BIG naar de BIO[4] in 2020. De gemeente heeft de eerste stappen genomen om hierop voorbereid te zijn. Belangrijke verschillen tussen de BIO en de BIG zijn dat de BIO uitgaat van drie Basis Betrouwbaarheidsniveaus (BBN's) met gekoppelde maatregelensets, koppeling met de ISO 2700x standaard en toewijzing van maatregelen aan een eindverantwoordelijke. De eerste stap waar nu mee is gestart, is het op basis van risicomanagement opnemen van de bedrijfskritieke systemen in het nieuwe ISMS-tool.

Aanbesteding ISMS tool
De aanbesteding van het nieuwe ISMS[5]-tool is eind vorig jaar gestart en begin april afgerond. Implementatie van het nieuwe tool is daarna direct gestart. Verwachting is dat in Q2 de tool is gevuld en gestart kan worden met het selecteren en beschrijven van de security-controls op basis van de BIO- normatiek.

Cybersecurity incident Table Tops
Op 14, 19 en 28 maart en 2 april hebben de bewustwordingssessies informatieveiligheid voor de gemeentelijke top plaatsgevonden. Het doel is de bewustwording op het gebied van informatieveiligheid te vergroten binnen deze doelgroep. Gelet op het deelnamepercentage van ongeveer 70% (123 personen) kan worden gesteld dat de gemeente Den Haag goed op weg is naar een steeds meer bewuste gemeentelijke top. De vier bewustwordingssessies zijn door deelnemers beoordeeld met een gemiddelde eindwaardering van een 8,0. Deelnemers gaven wel aan dat hun afdeling krap voldoende scoort op de mate waarin zij goed voorbereid zijn op een dergelijk incident. Er zal een laatste sessie worden gepland voor de resterende 30%. Wethouder Guernaoui neemt hier ook aan deel.

Onderzoek naar Digitale Veiligheid Interne ICT Systemen
IDC-A heeft in het eerste kwartaal van 2019 een onderzoek laten uitvoeren naar de digitale veiligheid van de interne ICT-Infrastructuur. De geconstateerde bevindingen hebben te maken met verouderde software, standaardconfiguraties en segmentatie van het netwerk en zijn als zodanig geclassificeerd. De bevindingen zijn als actiepunten uitgezet en in voor monitoring in 10.2.g geregistreerd.

Publicatie VNG GGI-Veilig
Met GGI-Veilig worden via de VNG producten en diensten voor operationele informatiebeveiliging aanbesteed. Na het eerder intrekken van de aanbesteding door de VNG in december 2018, heeft de werkgroep gewerkt aan de verbeteringen van de aanbestedingsprocedures. Dit heeft geresulteerd in een verbeterde publicatie in februari 2019. In april 2019 sluit de inschrijving en wordt gestart met de beoordeling van de inschrijvingen. De gemeente Den Haag neemt deel aan de expertgroep die hiervoor is opgericht. Den Haag doet mee in alle drie de percelen: managed SIEM/SOC dienstverlening, aanvullende security product/dienstverlening en security expertise services.

Oplevering ENSIA
Voor de verantwoording over informatieveiligheid past de gemeente het proces ENSIA (Eénduidige Normatiek Single Information Audit) toe. Middels de ENSIA-collegeverklaring geeft het college jaarlijks aan in hoeverre de beheersingsmaatregelen voldoen aan de normen die gelden voor de systemen DigiD, Suwinet en DKD-Inlezen en op welke onderdelen de gemeente niet voldoet aan deze normen. Hiervoor heeft de gemeente een zelfevaluatie uitgevoerd. In tegenstelling tot vorig jaar is er dit keer een relatief groot aantal bevindingen gerapporteerd. Het verschil heeft als reden dat 2017 een overgangsjaar was en het gebruik van

[1] Eenduidige Norma iek Single Information Audit
[2] Suwinet is een digitale infrastructuur die is ontwikkeld door en om ervoor te zorgen dat de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak.
[3] Bij CEO-fraude ontvangt een medewerker op de (financiële) administratie van een organisatie een e-mail van de 'baas'. Deze draagt hem of haar op een fors bedrag over te maken naar een (buitenlandse) rekening.
[4] Baseline Informatiebeveiliging Overheid. één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO 27000-normatiek
[5] Information Security Management System, ofwel een managementsysteem voor informatieveiligheid (gebaseerd op de PDCA-cyclus).

het landelijke systeem DKD-inlezen in dat jaar een summier onderdeel was van ENSIA. Op dit onderdeel zijn over het jaar 2018 de meeste bevindingen geconstateerd. Het college heeft de collegeverklaring op 24 april afgegeven. De GAD heeft op basis van deze verklaring een assurance-rapport opgesteld. Hiermee voldoet de gemeente aan de door het ministerie van BZK gestelde deadline van 1 mei.

3.2 Vooruitblik komende 4 maanden

Beleidskader informatieveiligheid en Roadmap 2019-2022
Het Beleidskader informatieveiligheid is in het Concern Overleg I&A van 16 januari goedgekeurd met de opmerking dat er op tactisch niveau (BEC-I) eerst nog een additionele Roadmap moet worden toegevoegd om de benodigde capaciteit en middelen te onderbouwen. Verwachting is dat het beleidskader rond de zomer wordt aangeboden aan het college.

Start realisatie virtueel hack team Den Haag
De komende periode wordt er vanuit het IDC-A een programma ontwikkeld waarbij interne medewerkers de mogelijkheid wordt gegeven zich verder te ontwikkelen als Ethische Hacker. Vanuit de training zal er een selectie gemaakt worden van vijftal potentiele kandidaten die het zogenaamde Red Team van Den Haag gaan vormen om zo de eigen systemen door eigen personeel te kunnen laten pentesten.

Den Haag

Viermaandelijkse wethoudersrapportage IV-Beleid en ICT

Periode januari - april 2020

Datum
mei 2020
Versie
0.10
Auteurs
CIO Office
IDC/A

Opdrachtgever
10.2.e

Status
concept

Inhoudsopgave

3 Gegevensbescherming

3.1 Vooruitblik komende periode

3.1.1 Privacy-organisatie

Het plan van de Functionaris Gegevensbescherming (FG) voor de privacy-organisatie wordt in het tweede kwartaal van 2020 voorgelegd aan het GMT om invulling te geven aan de noodzakelijke organisatie om privacy goed te borgen binnen de gemeente. Kern van het voorstel is de inrichting van een centrale privacy-organisatie bestaande uit privacy officers die de diensten adviseren en ondersteunen en die functioneel door de FG worden aangestuurd. Daarmee wordt een vergelijkbare organisatie voorgesteld zoals die al een aantal jaar succesvol functioneert voor informatiebeveiliging.

3.1.2 Verwerkingsregister

Het project om de applicatie 10.2.g in te zetten als gemeentebreed register van verwerkingen, zal in het tweede kwartaal van 2020 worden voortgezet. De diensten hebben een overzicht opgesteld van hun (wettelijke) verwerkingen. Dit overzicht moet nu worden opgenomen in 10.2.g zodat dit de Haagse werkelijkheid weergeeft. Om dit tot stand te brengen wordt externe versterking aangetrokken Het streven is dat alle verwerkingen van de GDH die op een wettelijke grondslag zijn gebaseerd over 4 maanden in het register zijn opgenomen.

3.1.3 Tactisch beleidskader

In het kader van hetzelfde project heeft de FG een gemeentebreed tactisch beleidskader laten opstellen. Aangezien de Algemene Verordening Gegevensbescherming veel open normen kent, maakt dit het voor diensten en medewerkers duidelijker wat van hen wordt verwacht. Het tactische beleidskader zal in het tweede kwartaal van 2020 aan het GMT ter goedkeuring voorgelegd worden.

3.2 Terugblik afgelopen 4 maanden

3.2.1 Toezicht

De FG heeft in het eerste kwartaal van 2020 opdracht gegeven tot het verrichten van een onderzoek, naar aanleiding van een datalek in het laatste kwartaal van 2019 dat in de pers kwam voordat het intern was opgemerkt. Het ging om het versturen van stukken in bezwaar en beroep naar de verkeerde ontvanger. De reden om opdracht te geven voor een onderzoek was, om na te gaan hoe het werkproces kon worden verbeterd om de privacy beter te bescherming. Om de uitkomsten van het onderzoek zo goed mogelijk toepasbaar te maken, is er in overleg met het verantwoordelijke dienstonderdeel voor gekozen om een privacy impact assessment op het proces te laten verrichten door een externe. Het bleek lastig om afspraken te maken met betrokken medewerkers die de nodige informatie moesten verstrekken, waardoor het onderzoek vertraging heeft opgelopen. Een eindrapport wordt eind mei 2020 verwacht.

Datalekken
In de periode 20 december 2019 tot 20 april 2020 zijn van de 74 potentiele datalekken er 44 aan de Autoriteit Persoonsgegevens (AP) gemeld. Dit hogere aantal meldingen aan de AP is op zichzelf geen reden tot zorg, maar kan ook worden uitgelegd als een teken dat de meldingsbereidheid groot is.

Hieronder wordt een aantal datalekken nader toegelicht. De reden hiervan is, dat er bij deze datalekken sprake is van fouten of situaties die zich vaker voordoen, maar die met meer bewustzijn in veel gevallen voorkomen kunnen worden. In andere gevallen kan een technische oplossing worden geboden.

Een betrekkelijk groot aantal datalekken wordt telkens veroorzaakt door verkeerd verstuurde mails. Voor een deel zijn deze datalekken moeilijk te voorkomen. Zelfs wanneer gebruik wordt gemaakt van (beveiligde) zorgmail, kan een verkeerd geadresseerde mail leiden tot een datalek.
Een belangrijke oorzaak van datalekken wordt gevormd door het versturen van bijlages met persoonsgegevens in e-mails. De risico's op datalekken zouden aanzienlijk kunnen worden verkleind, wanneer medewerkers op afstand samen zouden werken in dossiers. Verkeerd geadresseerde mails aan collega's hoeven dan immers zelf niet of nauwelijks meer gevoelige informatie te bevatten.
Ook voor communicatie met burgers zou het aanbeveling verdienen dat burgers op afstand toegang verleend zou kunnen worden tot stukken.

Twee verkeerd verstuurde mails leidden tot een intern datalek. In beide gevallen betrof het – binnen 24 uur – de situatie waarbij een mail met persoonsgegevens naar een dienstpostbus werd verstuurd waarna de mail bij een voltallige directie belandde. Nader onderzoek wees uit dat het bestaan van dergelijke dienstpostbussen die iedereen kan gebruiken in strijd is met intern beleid. Dienstpostbussen horen alleen toegankelijk te zijn voor een beperkt aantal ondersteuners om het risico op incidenten zoals deze zo klein mogelijk te maken. Deze dienstpostbus is dan ook afgesloten.

Er ontstaat ook steeds meer oog voor de samenloop tussen privacy en integriteit. Helaas doet zich van tijd tot tijd de situatie voor dat medewerkers gebruik maken van hun autorisaties om niet-functionele inzage te doen. In het afgelopen kwartaal is hiervan éénmaal melding gedaan. Dit komt op verschillende manieren aan het licht. Eén ervan is dat burgers zich (soms rechtstreeks bij de FG) beklagen. Zowel bij de privacy coördinatoren als bij de integriteitscoördinatoren bestaat een toenemend bewustzijn dat tussen deze twee disciplines raakvlakken bestaan en dat het van belang is dat we elkaar tijdig informeren. Voor privacy geldt hierbij, dat wanneer er sprake is van een incident met grote impact, dit binnen 72 uur aan de Autoriteit Persoonsgegevens moet worden gemeld.

In vier gevallen was sprake van een datalek met duidelijke security kenmerken, bijvoorbeeld omdat er sprake was van een hack of technisch falen. In drie van deze gevallen is door de security organisatie een uitgebreide analyse verricht waarna verbeteringen zijn doorgevoerd. In het vierde geval wordt overleg gevoerd met de leverancier. Deze 'plaatst vraagtekens' bij de stelling dat hier sprake is van een datalek. De gemeente Den Haag zoekt hier samenwerking met de VNG en G5-gemeenten die gebruik maken van dezelfde leverancier.

3.2.2 Dag van de privacy

Op 28 januari heeft de FG de dag van de privacy georganiseerd. Op deze datum wordt wereldwijd aandacht besteed aan de internationale dag van de privacy. Voor de vijftig deelnemers waren gedurende de dag verschillende workshops over privacy op diverse locaties op het Spui. Aan de dag van de privacy is belangeloos medewerking verleend door zowel interne als externe deskundigen op het gebied van privacy, security en integriteit. Gegevensbescherming

4 Informatieveiligheid

4.1 Toelichting

Identify - ID	Beheren van cybersecurityrisico's
Protect - PR	Waarborgen voor de bescherming van de diensten van de gemeente.
Detect - DE	Identificeren van cybersecurityincident
Respond - RS	Reageren op een gedetecteerd cybersecurityincident
Recover - RC	Plannen en onderhouden van de weerbaarheid om diensten te kunnen herstellen

4.2 Terugblik afgelopen 4 maanden

4.2.1 Aansturing en samenwerking in de Expertiseketen Security ID

De aansturing van de Expertiseketen Security is ingericht zoals is opgenomen in het Strategisch Beleidskader Informatieveiligheid 2019-2022. Concreet wordt de Expertiseketen Security, die verspreid is over de organisaties BSD, BEC en IDC, functioneel aangestuurd door de CISO. Besluiten worden door de CISO genomen na een advies van vertegenwoordigers uit BEC en IDC. Het is de verantwoordelijkheid van de CISO om, naast het geven van richting, erop toe te zien dat er een effectieve en efficiënte organisatie staat die passend is voor de realisatie van de ambities van gemeente Den Haag op het gebied van informatiebeveiliging.

4.2.2 Opstellen Jaarplan Security 2020 ID

Binnen de Expertiseketen Security is gewerkt aan het jaarplan Security voor 2020. Belangrijke onderdelen in de Roadmap betreffen de implementatie van de BIO en het opstellen van een Cyber Crisisplan. Daarnaast wordt er ingezet op verdere professionalisering van de Expertiseketen Security door het opstellen van een opleidingsplan waarbij naast generieke (reeds aanwezige) kennis, wordt ingezet op specialisatie. Het Jaarplan 2020 zal binnenkort aan het GMT worden aangeboden ter besluitvorming.

4.2.3 Audit en Compliance ID

Op 14 april heeft het college ingestemd met de collegeverklaring ENSIA over 2019. In december 2019 heeft de zelfevaluatie plaatsgevonden. Aan de hand van de input heeft de GAD een steekproef gedaan en na het opleveren van additionele bewijslast bleek dat voor DigiD aan alle normen was voldaan, maar dat dit niet voor Suwinet gold. Dit is opgenomen in verbeterplannen, zijn belegd en worden gemonitord. In het proces rond ENSIA is een aantal leerpunten naar voren gekomen die met elkaar zijn gedeeld en als verbeterpunten voor het proces voor ENSIA 2020 opgenomen.

4.2.4 Implementatie BIO & ISMS ID

De tooling om te ondersteunen bij het doorlopen van het ISMS is door de leverancier geoptimaliseerd volgens de eisen en wensen van de gemeente. Voor het eerst worden de BIO-controls waarover verantwoording moet worden afgelegd, op verschillende momenten in het jaar uitgezet bij de collega's die deze moeten onderbouwen. Voorheen gebeurde dit in een "big bang" in september waardoor de werkdruk aan het einde van het jaar te hoog was. Deze ingreep leidt nu al tot positieve reacties en draagt bij aan het speerpunt om de lijn te helpen bij het invullen van het eigenaarschap voor

informatieveiligheid. Daarnaast zijn de eerste, vanuit de BIO verplichte, tactische beleidsdocumenten opgeleverd.

4.2.5 Incidenten en hoge impact kwetsbaarheden RS

De eerste vier maanden van 2020 was een forse toename van zogenaamde zero-day kwetsbaarheden bij meerdere leveranciers te zien, waaronder 10.2.g 10.2.g en 10.2.g Door verdere optimalisatie van het release en patch proces van het IDC is voor alle bekende zero-day kwetsbaarheden vroegtijdig actie ondernomen – ruim voordat de kwetsbaarheid misbruikt kon worden. De grootste impact had de zogenaamde '10.2.g-gate". De 10.2.g componenten met als taak toegang te verlenen tot de VDI-omgeving bleek kwetsbaar. In december 2019 is reeds door het IDC-A de work-around toegepast en na het beschikbaar komen van de patch is de omgeving door de interne securityspecialisten en twee externe partijen (10.2.g en 10.2.e gecontroleerd en niet-kwetsbaar bevonden. De geleerde lessen worden verwerkt in het op te stellen Cyber-crisisplan dat nog dit jaar wordt opgesteld en beoefend.

4.3 Vooruitblik komende 4 maanden

4.3.1 Verhogen van professionaliteit van de Expertiseketen Security ID

Onderdeel van de samenwerking in de Expertiseketen Security is het verder professionaliseren van het advies dat aan de diensten wordt geleverd. Dit vereist meer kennis op tactisch en strategisch niveau. Dit wordt gefaciliteerd door, onder andere, meerdere ISO's een dienst te laten adviseren. Binnen het sociale domein zullen vanaf de zomer bijvoorbeeld vier ISO's de werkzaamheden voor OCW en SZW onderling verdelen. Dit betekent een betere continuïteit bij afwezigheid, maar het zorgt er ook voor dat we de talenten en vaardigheden van ISO's beter kunnen inzetten waar deze nodig zijn.

4.3.2 Uniforme rapportage in de lijn ID

Met het strategisch beleidskader en het jaarplan (nog vast te stellen door het GMT) is een nieuwe cyclus en manier van werken ingeluid waar ook rapportage onderdeel van is. Zo zal er volgens de cyclus van de Wethouderrapportage 3 keer per jaar worden gerapporteerd in de lijn – op basis van dezelfde informatie. Dit zijn rapportages aan: 1. de directies van de verschillende diensten door de ISO's (waardoor hun strategische positie ook wordt verbeterd), 2. het GMT en 3. de Wethouder. Uitgangspunt van deze rapportages is dat ze direct gerelateerd zijn aan de primaire processen van de diensten, besluiten in de lijn moeten ondersteunen en voor alle doelgroepen te begrijpen zijn. Uiteindelijk zou deze rapportage ook geschikt gemaakt kunnen worden voor communicatie aan de Raad.

4.3.3 Voorbereidingen Hack The Hague 2020 DE RS

Het is, gelet op de huidige situatie inzake Corona, nog niet duidelijk of, en zo ja, in welke vorm het evenement in 2020 doorgang kan vinden. De voorbereidingen zijn in volle gang en er wordt rekening gehouden met een 'normale' variant in het Atrium, maar ook een volledig 'externe' variant waarbij de hackers vanaf hun eigen werkplek deelnemen. Er is nauw contact met het NCSC om eventuele besluiten op elkaar af te stemmen. Binnenkort wordt een voorstel aan de wethouder aangeboden.

Den Haag

Viermaandelijkse wethoudersrapportage IV-Beleid en ICT

Periode mei - augustus 2020

Datum
september 2020
Versie
1.0
Auteurs
CIO Office
IDC/A

Opdrachtgever
10.2.e
[redacted]

Status
Definitief

Inhoudsopgave

3 Gegevensbescherming

3.1 Vooruitblik komende periode

3.1.1 Privacy-organisatie

Het plan van de Functionaris Gegevensbescherming (FG) voor de privacy-organisatie is voor de zomer besproken in het BVB dat een aantal wijzigingen heeft voorgesteld. Het zal na de zomer opnieuw in het BVB geagendeerd worden. Kern van het voorstel is de inrichting van een centrale privacy-organisatie bestaande uit privacy officers die de diensten adviseren en ondersteunen en die functioneel door de FG worden aangestuurd. Daarmee wordt een vergelijkbare organisatie voorgesteld zoals die al een aantal jaar succesvol functioneert voor informatiebeveiliging.

3.1.2 Verwerkingsregister

Het project om de applicatie 10.2.g in te zetten als gemeentebreed register van verwerkingen, is in het tweede kwartaal van 2020 voortgezet en loopt door tot half oktober 2020. De bedoeling is, dat de losse en incomplete overzichten per dienst in één systeem worden gebundeld. De diensten hebben een overzicht opgesteld van hun (wettelijke) verwerkingen. Dit overzicht moet nu worden opgenomen in 10.2.g zodat dit de gemeentebrede verwerking van persoonsgegevens weergeeft. Om dit tot stand te brengen is externe versterking aangetrokken De diensten hebben aangeven dat alle verwerkingen van de GDH die op een wettelijke grondslag zijn gebaseerd op 1 oktober 2020 in het register kunnen zijn opgenomen. Het sociaal domein heeft aangegeven dat 1 oktober 2020 niet haalbaar is, maar heeft toegezegd een externe in te huren, zodat hun deel van het register op 1 januari 2021 zal zijn gevuld. De volgende stap zal zijn, dat de niet-wettelijke verwerkingen in het register worden opgenomen. Dit zijn de verwerkingen met persoonsgegevens die de gemeente niet op grond van een wettelijke gemeentelijke taak verricht.

3.1.3 Tactisch beleidskader

Met behulp van dezelfde consultants heeft de FG een gemeentebreed tactisch beleidskader laten opstellen. Aangezien de Algemene Verordening Gegevensbescherming veel open normen kent, maakt dit het voor diensten en medewerkers duidelijker wat van hen wordt verwacht. Het tactische beleidskader zal in 2020 aan het GMT ter goedkeuring worden voorgelegd .

3.1.4 Bewustwording

In juli 2020 heeft 10.2.g de aanbesteding gewonnen om de komende 2 jaar een gemeentebrede bewustwordingscampagne te organiseren. Doel van deze campagne is om ambtenaren de juiste kennis mee te geven om, om te gaan met privacy, security, datagedreven werken en informatiebeheer. Naast verschillen vertonen deze terreinen ook veel raakvlakken. De bedoeling is om het ambtenaren zo eenvoudig mogelijk te maken om op de juiste wijze te handelen op deze terreinen. Deze campagne is aanvullend ten opzichte van de bewustwording die diensten zelf organiseren over dienst specifieke onderwerpen.

3.1.5 Rechten van betrokkenen via MijnDenHaag

Om een beter overzicht te krijgen over de aantallen mensen die hun rechten als betrokkene willen uitoefenen, heeft de FG is samenwerking met BEC-JZ georganiseerd dat betrokkenen dit via MijnDenHaag.nl kunnen doen. BEC-JZ zal de backoffice bemannen. Er was afgesproken dat gedurende

zes maanden een pilot zou plaatsvinden. Door corona is dit echter nog niet in praktijk gebracht. Er is nog geen nieuwe planning bekend.

3.2 Terugblik afgelopen 4 maanden

Datalekken
In de periode 1 mei 2020 tot 1 september 2020 waren er 143 potentiële datalekken. Hiervan zijn er 14 aan de Autoriteit Persoonsgegevens gemeld. Eén melding is ingetrokken, omdat het bij nader inzien geen datalek betrof. De reden om deze datalekken te melden, was in de meeste gevallen dat er bijzondere of gevoelige persoonsgegevens waren betrokken bij het datalek. Het gaat dan bijvoorbeeld om gezondheidsgegevens of het BSN. De oorzaak van de datalekken was in de meeste gevallen menselijk handelen. Bijvoorbeeld het versturen van een brief aan de verkeerde betrokkene doordat een verkeerd (email)adres werd gebruikt.

Corona-app
Samen met de FG's van de GGD-en is de gemeente Den Haag ook betrokken bij de gesprekken tussen het ministerie van VWS en de GGD-en over de corona-meldingsapp. In Den Haag maakt de GGD onderdeel uit van de gemeentelijke organisatie. Andere GGD-en zijn van de gemeenten onafhankelijke organisaties. VWS heeft uiteindelijk deze app zelf ontwikkeld, zonder tussenkomst van derde partijen. De toepassing van de app wordt in beheer aan 10.2.g gegeven. Het was de bedoeling dat de app op 1 september officieel zou worden gelanceerd, maar de minister heeft aangegeven te willen voldoen aan de eis van de AP voor een wettelijke grondslag. Momenteel worden er al proeven gedaan in GGD Drenthe, GGD IJsselland, GGD Twente, GGD Noord- en Oost-Gelderland en GGD Gelderland-Zuid.
Ook op bestuurlijk niveau is door wethouder Bruines via de VNG overleg geweest met VWS over de introductie en het delen van alle relevante informatie door VWS met alle gemeenten. Op basis van dat overleg heeft de VNG bestuurlijk besloten de introductie van de app actief te ondersteunen.[1]

[1]De Autoriteit Persoonsgegevens heeft een advies uitgebracht over de app. Via deze link de kamerbrief over de CoronaMelder (incl. bijlagen) is de kamerbrief te lezen. In bijlage 2 en 3 staan het advies van de AP en reactie van de landsadvocaat.

4 Informatieveiligheid

4.1 Toelichting

In 2020 zal de rapportage over informatieveiligheid gefaseerd verder geprofessionaliseerd worden. In de eerste fase zullen onderwerpen in deze rapportage gelabeld worden als elementen uit een wereldwijd gebruikt raamwerk, het Cyber Security Framework[2]. Dit model wordt binnen de gemeente gebruikt om focus aan te brengen in doelen en acties en deze te kunnen beoordelen en te verbeteren.

Identify - ID	Beheren van cybersecurityrisico's
Protect - PR	Waarborgen voor de bescherming van de diensten van de gemeente.
Detect - DE	Identificeren van cybersecurityincident
Respond - RS	Reageren op een gedetecteerd cybersecurityincident
Recover - RC	Plannen en onderhouden van de weerbaarheid om diensten te kunnen herstellen

4.2 Terugblik afgelopen 4 maanden

4.2.1 Aansturing en samenwerking in de Expertiseketen Security ID

In het tweede kwartaal zijn overleggen binnen de securityketen geïntensiveerd en gestructureerd. De Werkgroep Informatieveiligheid – bestaande uit een vertegenwoordiging vanuit BEC-I, IDC-A en CIO – wordt wekelijks gehouden op basis van agenda en vastlegging van besluiten binnen de securityketen op strategisch-beleidsmatig niveau. Daarnaast is er ook wekelijks operationeel-tactisch overleg tussen het concern en de ISO's vanuit BEC-I en de securitymanagers/architecten van IDC-A.
Onderzocht wordt hoe en op welke wijze de besluiten in deze overleggen een plek kunnen krijgen binnen de nieuwe governance structuur in het kader van de BC I&A.

4.2.2 Jaarplan Security 2020 ID

De expertiseketen Security heeft het jaarplan Security voor 2020 opgeleverd. Belangrijke onderdelen in de Roadmap betreffen de implementatie van de BIO en het opstellen van een Cyber Crisisplan. Daarnaast wordt er ingezet op verdere professionalisering van de Expertiseketen Security door het opstellen van een opleidingsplan waarbij naast generieke (reeds aanwezige) kennis, wordt ingezet op specialisatie.

4.2.3 Audit en Compliance ID

Op 1 juli is de nieuwe ENSIA-cyclus voor de zelfevaluatie gestart (over 2020). Om dit verantwoordingsproces adequaat en efficiënt in te richten zijn in juni kick-off bijeenkomsten met de diensten georganiseerd. In afstemming met de GAD zal in 2020 op onderdelen van de ENSIA een pre-audit plaatsvinden, met als doel de kwaliteit van het proces verder te verbeteren.

4.2.4 Implementatie BIO & ISMS ID

Afgelopen half jaar is door een extern bureau geadviseerd ten behoeve van het implementeren van de BIO binnen GDH. Op 31 juli heeft dit bureau de eindrapportage opgeleverd. Geconcludeerd kan worden dat GDH goed op weg is met de implementatie. Doch ook is gebleken dat er veel tijd is gaan zitten in het verzamelen, genereren en updaten van benodigde beleidsdocumenten teneinde te kunnen voldoen aan de beheersmaatregelen binnen de BIO. Ook is gebleken dat er nog meer aandacht nodig is voor het

[2] National Institute of Standards and Technology (2018). The NIST Cybersecurity Framework. V1.1

eigenaarschap van processen en applicaties binnen GDH. Daarbij is eveneens goed op te merken dat het voldoen aan de BIO een onderdeel is van een integraal Security Management System (ISMS) waarbij zowel een (PDCA) proces (Plan Do Check Act) (zie ook 1.3.2).

4.2.5 VNG-GGI-Veilig: Penetratietests ID

Vanuit de securityketen is de afgelopen twee maanden gewerkt aan de minicompetitie inzake aanbesteding penetratietests. Het pakket van eisen is samengesteld en gepubliceerd. De nota van inlichtingen, de inschrijvingen en de beoordeling van deze inschrijvingen hebben plaatsgevonden. Gunning is gegaan naar een samenwerkingsverband tussen 10.2.g en 10.2.g Op dit moment is het IDC-A bezig met de verdere afhechting van het contract, de voorwaarden en werkwijze. Afnemen van diensten kan vanaf 1 augustus 2020.

4.2.6 IT-CM TNO ID

Het IDC-A is, in samenwerking met 10.2.g gestart aan een programma IT Continuity Management om in het geval van een (cyber)crisis de belangrijkste IT-processen te kunnen blijven uitvoeren. Het plan van aanpak en de criteria zijn besproken om te bepalen welk primair proces van de gemeente Den Haag in aanmerking komt. Inmiddels heeft er met de betrokken dienst afstemming plaats gehad en is het beoogde plan van aanpak gedeeld. Naar verwachting kan in september worden gestart. Doel is te komen tot een generieke aanpak welke kan worden hergebruikt voor andere processen en diensten. De doelstelling hiervan is het verhogen van de weerbaarheid van de gemeente Den Haag.

4.2.7 VNG GGI-Veilig: EndPoint Protection PR

De implementatie van de nieuwe, moderne oplossing is gestart. In de implementatie fase heeft het project vertraging opgelopen. Deze vertraging heeft nog geen impact op de livegang. De verwachting is nog steeds dat voor 24 september de bestaande oplossing is vervangen op alle 10.2.g 10.2.g gerelateerde platformen. De 10.2.g platformen volgen later. Dit heeft geen consequenties voor het huidige contract met 10.2.g Dit contract wordt per 24 september 2020 beëindigd.

4.3 Vooruitblik komende 4 maanden

4.3.1 NIST CSF implementatie o.b.v. COBIT 2019 ID

Het NIST Cybersecurity Framework (CSF) is voor het eerst gebruikt als indeling voor het Jaarplan Security 2020. Het voornemen bestaat de indeling ook te gaan hanteren voor de viermaandelijkse rapportages. Komende periode zal de voorbereiding starten van het implementeren van het NIST CSF. Daartoe wordt de methodiek en programma aanpak van COBIT 2019 gehanteerd, met als doel het CSF aan te laten sluiten en te integreren met strategie en doelstellingen binnen de gemeente Den Haag. Daarmee wordt het CSF verbonden met de cybersecurity prioriteiten die volgen uit de doelstellingen vanuit de diensten en GDH breed.

4.3.2 Onderzoek technische digitale veiligheid PR

Dit jaar wordt er een onderzoek uitgevoerd naar de digitale veiligheid van de gemeente Den Haag. Een aantal pentesters zal van binnenuit de omgeving van de gemeente Den Haag gaan onderzoeken op de aanwezigheid van kwetsbaarheden. De scope van de opdracht, planning en daadwerkelijke uitvoering wordt nader bepaald in overleg met de Security keten.

4.3.3 Voorbereidingen Hack The Hague 2020 DE RS

Vanwege de situatie omtrent Corona kan het evenement in 2020 geen doorgang vinden en is verplaatst naar 27 september 2021. In aanloop hiernaar wordt een content marketingstrategie uitgevoerd. Hierbij zal ook aansluiting worden gezocht bij (digitale) evenementen als de ONE Conference en de Nationale Cyberoefening. Deelnemers en leveranciers zijn geïnformeerd.

Den Haag

Viermaandelijkse Rapportage IV-Beleid en ICT

Periode januari – april 2021

Datum
mei 2021
Versie
1.0

Opdrachtgever
10.2.e

Status
definitief

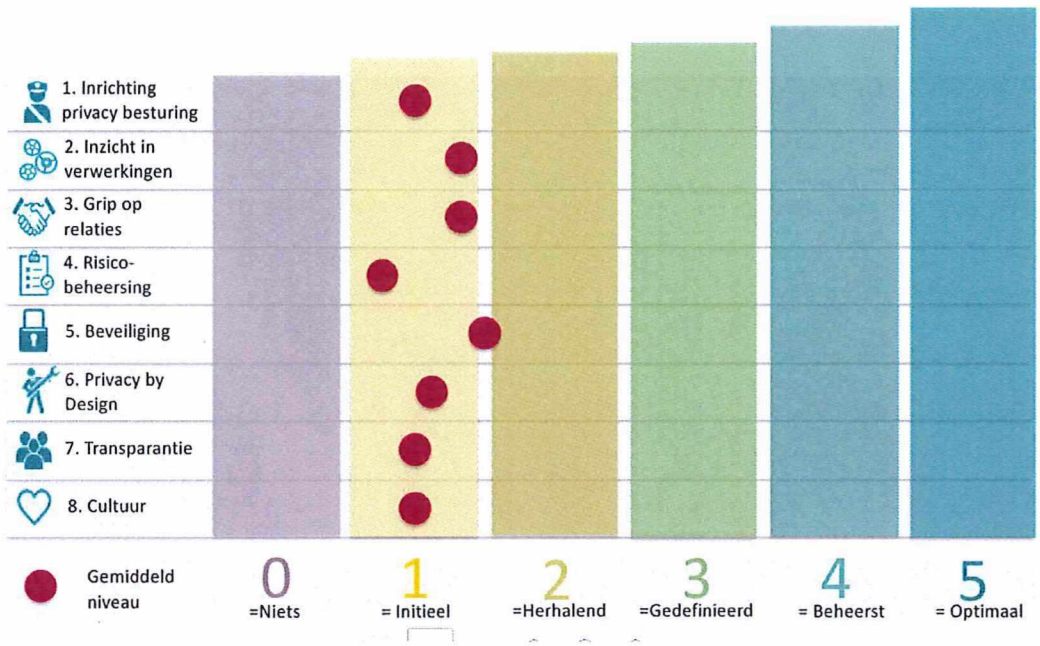
Inhoudsopgave

4 Gegevensbescherming/ Privacy

4.1 Toelichting

In februari 2021 is de rapportage Volwassenheidsscan AVG (Algemene Verordening Gegevensbescherming) opgeleverd en in mei besproken in het GMT. Het doel van deze scan is het creëren van een gemeentebreed inzicht in de mate van volwassenheid op het gebied van de AVG. De scan is gebaseerd op het volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP) en hanteert daarvoor een achttal privacythema's, welke ook voortaan wordt gebruikt voor jaarplannen en rapportages (waaronder per heden ook deze viermaandelijkse rapportage). Het rapport bevat per thema ook aanbevelingen voor de gemeente om het volgende volwassenheidsniveau te bereiken. Op alle acht de thema's staat de gemeente concernbreed gemiddeld op volwassenheidsniveau 1 (zie hieronder afbeelding 2: volwassenheidsbepaling). De privacy organisatie werkt momenteel aan een nieuw jaarplan 2021-2022 op basis van de volwassenheidsscan en aanbevelingen, dat – na vaststelling door het GMT – als doel heeft om eind 2022 concernbreed op niveau 3 te staan.

Afbeelding 2 volwassenheidsbepaling



4.2 Inrichting privacy besturing

Het GMT heeft begin februari 2021 het principebesluit genomen tot de oprichting van een centrale privacy organisatie in de TO I&A van de Dienst Bedrijfsvoering. De adviesaanvraag wordt in mei voorgelegd aan de COR. Als de COR een positief advies geeft en het GMT een definitief besluit neemt zal de privacy organisatie worden ingericht als expertisecentrum privacy. In het expertisecentrum komen dan de privacy officers die in de huidige situatie gedecentraliseerd zijn georganiseerd bij de diensten. Het GMT heeft tevens besloten om de interne toezichthoudende rol van de FG te scheiden van het maken van beleid en de coördinatie op de uitvoering (inclusief functionele aansturing van de privacy organisatie).

Daartoe is vanaf januari een medewerker voor 2 dagen vrijgemaakt om tijdelijk invulling te geven aan de rol van kwartiermaker privacyorganisatie/chief privacy officer. Deze stuurt sinds eind januari functioneel de privacy officers aan (feitelijke privacy organisatie). Een fulltime (interim) chief privacy officer wordt momenteel geworven. De FG wordt als intern toezichthouder gepositioneerd nabij de gemeentesecretaris in de Bestuursdienst. Op deze wijze wordt de scheiding tussen toezicht en uitvoering bewerkstelligd en de onafhankelijke positie van de FG versterkt. Dit laatste is een aandachtspunt geweest van zowel de Rekeningencommissie als de GAD.

4.3 Inzicht in verwerkingen

In februari zijn de deelregisters van de diensten geïmporteerd naar het ondersteunende systeem (10.2.g voor het verwerkingsregister en hebben de privacy officers een cursus gehad voor het gebruik van het systeem. Helaas is na controle gebleken dat het importeren niet is geslaagd, waardoor het ondersteunende systeem momenteel niet bruikbaar is als verwerkingsregister. De gemeente is bezig met de leverancier om te onderzoeken hoe dit verholpen kan worden. In de tussentijd werkt de privacy organisatie aan en met een versimpelde en eenduidig centraal verwerkingsregister, zodat de gemeente daarmee voldoet aan haar wettelijke verplichting om een verwerkingsregister bij te houden. Daarnaast is een projectopdracht uitgewerkt om in het najaar het verwerkingsregister via denhaag.nl te publiceren, tezamen met het algoritmeregister en het sensorenregister.

4.4 Grip op relaties

Op dit thema zijn de afgelopen 4 maanden geen noemenswaardige ontwikkelingen gebeurd om te vermelden in deze rapportage.

4.4.1 Risicobeheersing

Het uitvoeren van data protection impact assessements (DPIA) is een wettelijke verplichting uit de AVG bij bepaalde risicovolle verwerkingen. De gemeente heeft een aanzienlijke achterstand in te halen op het uitvoeren van DPIA's op risicovolle verwerkingen (zowel bestaande processen als nieuwe projecten). De eerste inschatting is dat het tussen circa 200 tot 300 DPIA's gaat. De privacy organisatie heeft in maart een aanpak op de DPIA's opgesteld die in mei voor besluitvorming naar het GMT gaat. In de aanpak wordt voorgesteld om tijdelijk extra capaciteit (2 Fte) in te zetten om de achterstand in twee jaar in te halen. Daarnaast is een aantal gemeentebrede tactische kaders en standaarden opgesteld (zoals een model DPIA en het privacy risico analyse proces). Met de vaststelling van deze kaders is meteen een aanbeveling uit de volwassenheidsscan opgevolgd.

4.5 Beveiliging (Privacy)

Onder het thema beveiliging valt ook de meldplicht datalekken. In de periode januari-april zijn 90 interne meldingen datalekken ontvangen. 20 datalekken zijn aan de AP gemeld. Hiervan zijn er 6 te laat gemeld. In alle gevallen is de oorzaak van te late melding dat het datalek intern te laat is ontdekt als datalek of te laat intern is gemeld. Eén dossier springt eruit (dossiers op ruimtelijkeplannen.nl niet geanonimiseerd). Het incident was al in oktober 2019 opgemerkt, maar niet als datalek gemeld aan de FG of de AP. Ook de destijds door de privacy officer gesignaleerde maatregelen zijn niet genomen. Inmiddels is het datalek gemeld bij de AP en worden de vereiste maatregelen getroffen. De brief van de AP eind 2020 en het onderzoek van de GAD over de bewustwording onder ambtenaren over de meldplicht datalekken, hebben aanleiding gegeven tot het herzien van de procedure

meldplicht datalekken. De privacy organisatie heeft in januari en februari de procedure geëvalueerd en een aantal knelpunten gesignaleerd en verbeterd in een herziene procedure. De procedure is in april door het GMT vastgesteld en wordt in mei door het college B&W vastgesteld. In de herziene procedure is het mandaat om een melding te doen bij de Autoriteit Persoonsgegevens (AP) belegd bij de privacy officer in plaats van de FG. Dit komt ten goede van de snelheid om tijdig een datalek te melden aan de AP en ook het borgen van de toezichthoudende rol van de FG. Daarnaast is een centraal datalekkenregister ingericht dat alle privacy officers hanteren en op basis van dat register kan er ook eenduidig gerapporteerd worden over de datalekken. Een belangrijk aandachtspunt bij de procedure meldplicht datalekken is de bewustwording bij elke medewerker om een datalek te herkennen en daar direct ook intern melding van te maken. Daarover is in de maanden januari tot en met april extra aandacht aan gegeven via Werknet artikelen en presentaties door privacy officers in diverse teamoverleggen. Bewustwording over de meldplicht datalekken onder medewerkers is een van de belangrijke onderwerpen die als eerste aan bod komen in de integrale bewustwordingscampagne Informatiebewust werken (PSDI). Zie ook thema "Cultuur".

4.5 Privacy by design

Op dit thema zijn de afgelopen 4 maanden geen noemenswaardige ontwikkelingen gebeurd om te vermelden in deze rapportage.

4.6 Transparantie

De afgelopen maanden is het onderzoek naar communicatie over privacy richting inwoners in voorbereiding geweest. Het aanpassen van de privacyverklaring op denhaag.nl (aanbeveling uit volwassenheidsscan), het kunnen doen van een AVG-inzage verzoek via MijnDenHaag en de relatie met (de publicatie van) het verwerkingsregister zijn daar onderdeel van. Burgers kunnen per 15 april jl. via MijnDenHaag een inzageverzoek AVG doen. Onderdeel van communicatie over privacy richting inwoners is ook een onderzoek met inwoners middels de Stadskamer.

4.7 Cultuur

In het thema Cultuur staat de bewustwordingscampagne Informatiebewust werken centraal. Dit is een integrale bewustwordingscampagne op de disciplines Privacy, Security, Data en Informatiebeheer (PSDI). In januari en februari zijn de voorbereidende producten van de campagne opgeleverd, zoals de Deep Dives (inzichten vanuit de beoogde doelgroepen), PSDI Principes, de Body of Knowledge & Skills (benodigde kennis en competenties), communicatieaanpak en de aanpak voor de Monitor. In maart is de Monitor Informatiebewust werken uitgezet onder 2.094 medewerkers (afspiegeling van de diensten en doelgroepen). 653 medewerkers hebben de monitor ingevuld (31% response). De resultaten een onderbouwing op welke onderwerpen en bij welke doelgroepen de eerste interventies gepleegd dienen te worden om zowel houding, gedrag en kennis op de vier disciplines te versterken. De interventies gaan vanaf juni 2021 van start.

4.8 Advies FG

11.1 [redacted]

5 Informatieveiligheid

5.1 Terugblik afgelopen 4 maanden

5.2.1 Voortgang jaarplan Security 2021 ID

Het jaarplan voor 2021 is in de afgelopen periode verder uitgewerkt en op hoofdlijnen ingevuld. Belangrijke onderwerpen in het jaarplan zijn de verdere implementatie van de BIO, vormgeven en intensiveren van het Expertisecentrum Security en activiteiten gericht op het verhogen van de digitale weerbaarheid, namelijk implementatie van het NIST Cybersecurity Framework en het opstellen van een cybercrisisplan inclusief het houden van oefeningen. De voortgang op het jaarplan is goed.

5.2.2 Audit en Compliance ID

De jaarlijkse ENSIA-verantwoording is op 13 april in het college behandeld. De zelfevaluaties hebben uitgewezen dat niet volledig wordt voldaan aan alle geselecteerde normen. De op deze geldende uitzonderingen gerichte beheersmaatregelen voor DigiD en Suwinet zijn in verbeterplannen opgenomen en zijn bij de betreffende organisatieonderdelen belegd en worden gemonitord. Voor DigiD heeft het verbeterplan reeds geleid tot door de auditor geaccepteerde verbeteringen op de normen, waardoor een voorschot is genomen op de formele melding vanuit Logius na 1 mei. Op basis van de collegeverklaring stelt de GAD een assurance-rapport op.

5.2.3 Implementatie BIO & ISMS ID

GDH is goed bezig met de implementatie van de BIO, waarbij de doelstelling van de BIO om continue verbetering na te streven leidt tot doorlopend verbeterpunten. De verbeterpunten liggen met name op het vlak van beleid en de implementatie daarvan, het integrale bewustwordingstraject in 2021 en de verbetering en professionalisering van het ISMS-proces. De verbeterpunten zijn geprioriteerd en worden opgepakt volgens planning binnen het Expertisecentrum Security. Blijvend aandachtspunt is eigenaarschap van informatie in de lijnorganisatie. Goed belegd eigenaarschap is de eerste stap naar een daadwerkelijke Plan-Do-Check-Act (PDCA) cyclus waarbij GDH continu de effectiviteit van informatiebeveiliging als geheel verbetert. In de cyclus voor 2021 is het verantwoordingsproces verder geoptimaliseerd en wordt in de komende periode ingezet op verbeterplannen voor de applicaties in de verantwoording.

5.1.1 NIST CSF implementatie o.b.v. COBIT 2019 ID

Vanaf januari 2021 is gestart met het implementeren van het NIST CSF. Daartoe wordt de methodiek en programma aanpak van COBIT 2019 gehanteerd, met als doel het CSF aan te laten sluiten en te integreren met strategie en doelstellingen binnen de gemeente Den Haag. Daarmee wordt het CSF verbonden met de cybersecurity prioriteiten die volgen uit de doelstellingen vanuit de diensten en GDH breed. In het eerste en deels tweede kwartaal van 2021 wordt de nulmeting uitgevoerd, zodat werkpakketten gevormd kunnen worden om tot implementatie te komen. Deze werkpakketten worden geprioriteerd en uitgezet op de roadmap 2021-2023.

5.1.2 Grote incidenten DE

In deze periode is een groot incident geweest die wereldwijde impact had, namelijk meerdere kwetsbaarheden in 10.2.g 10.2.g (e-mail) servers. Deze kwetsbaarheden werden op zeer korte tijd misbruikt, ook in Nederland. Nog voor de melding van de IBD en het NCSC was GDH op de hoogte en zijn voorbereidingen getroffen om patches uit te rollen. Later bleek dat er met name in de dienstverlening richting het RIEC problemen ontstonden door de patches en zijn deze deels teruggedraaid. Dit was ten aanzien van de beveiliging geen issue door de manier waarop het interne netwerk van de gemeente is ingericht.

5.2 Vooruitblik komende 4 maanden

5.2.1 Verhogen digitale weerbaarheid ID

In het kader van verhogen van digitale weerbaarheid wordt enerzijds NIST CSF geïmplementeerd en anderzijds het opstellen en beoefenen van een cybercrisisplan. In het tweede kwartaal wordt gestart met de training van de leden van het ECS omtrent NIST CSF en worden de werkpakket gevormd. Deze werkpakketten worden geprioriteerd en gepland in de roadmap 2021-2023. Daarnaast wordt het cybercrisisplan in eerste concept afgerond in Q2, waarna de beoefening van de uitvoering gaat starten. In juni zal ECS deelnemen aan een nationale cyberoefening ISIDOOR, waarna een oefening in samenwerking met directie Veiligheid zal plaatsvinden. Tot slot zal in Q4 een oefening gepland worden waarin zowel IT-, organisatorische- als bestuurlijke componenten worden meegenomen.

5.2.2 Onderzoek technische digitale veiligheid PR

Dit jaar wordt er een onderzoek uitgevoerd naar de digitale veiligheid van de gemeente Den Haag. Een aantal pentesters zal van binnenuit de omgeving van de gemeente Den Haag gaan onderzoeken op de aanwezigheid van kwetsbaarheden.

5.2.3 Voorbereidingen Hack The Hague 2021 DE RS

Voor dit jaar is vastgesteld dat Hâck The Hague als volledig digitaal evenement doorgaat op maandag 27 september met een maximum van 200 ethische hackers. Tevens wordt er aandacht besteed aan meer inclusie binnen de deelnemersgroep. Zo zetten we o.a. in op meer vrouwelijke deelnemers.