Rapport ”Tussen beeldscherm en bureaustoel”

Informatiebeveiliging en privacy
Gemeenten De Wolden en Hoogeveen

Figuur 1 Jan Alexander via Pixabay.

Rekenkamercommissies De Wolden en Hoogeveen

November 2023

Auteur: drs. Etienne Lemmens

Prae Advies en onderzoek, Utrecht

Inhoudsopgave

Samenvatting, conclusies en aanbevelingen

Samenvatting

Informatieveiligheid

Informatieveiligheid binnen de gemeente is van groot belang. Voor inwoners om te garanderen dat de gemeentelijke dienstverlening doorgaat, dat paspoorten verstrekt worden, dat inwoners kunnen vertrouwen op inkomensondersteuning met waarborg van hun persoonsgegevens. Maar ook van groot belang is de bescherming van gegevens over ruimtelijke projecten, financiën en veiligheid in de stad. Gezien recente hacks blijken gemeenten daarop kwetsbaar en de financiële impact bij lokale overheden en instellingen onderstrepen het belang van het op orde hebben van informatieveiligheid. Cybercriminelen, op individueel en statelijk niveau, liggen op de loer. De ontwikkelingen gaan razendsnel, mede door Artificiële Intelligentie (AI).

BIO, AVG, NIS2

Gemeenten hebben op vrijwillige basis in VNG-verband afgesproken de maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) te implementeren. Daarmee borgen ze op basisniveau de beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens die gemeenten verwerken. Vanuit de EU is vanaf 2018 de Algemene Verordening Gegevens-bescherming (AVG) van kracht om de privacy van persoonsgegevens te garanderen. Vanaf oktober 2024 worden met de Network and Information Security directive (NIS2) vanuit de EU de richtlijnen voor cyberbeveiliging en weerbaarheid van essentiële diensten strakker in wetgeving vormgegeven.

Rekenkameronderzoek

De rekenkamercommissies de Wolden en Hoogeveen hebben onderzoek uitgevoerd naar de informatieveiligheid binnen de SWO om de gemeenteraden inzicht te geven in de opgaven, de stand van zaken, de doelmatigheid en doeltreffendheid van de informatieveiligheid van de gemeenten. En om aanbevelingen voor mogelijke verbeteringen te doen naar aanleiding van de bevindingen en conclusies. Doel is om een gedegen beeld te krijgen van de aanwezige kwetsbaarheden, van het beveiligingsniveau van zowel de organisatie, mens als techniek (ICT).

In mei en juni 2023 zijn in opdracht van de Rekenkamercommissies door ethische hackers verschillende testen uitgevoerd op de systemen van de SWO, en phishing mails verstuurd naar medewerkers van de SWO en raadsleden van De Wolden en Hoogeveen. Daarnaast zijn de beleidsdocumenten op informatiebeveiliging en privacy bestudeerd en interviews gehouden met sleutelpersonen. Ook is een casestudie gedaan naar de wijze waarop de SWO met een brok informatie omgaat, specifiek met betrekking tot de aanvraag voor een Wmo-voorziening.

Hoofdvraag en -conclusie

De hoofdvraag die de rekenkamercommissies willen beantwoorden is “Hoe doelmatig, doeltreffend en rechtmatig zijn de gemeenten de Wolden en Hoogeveen om de informatieveiligheid te waarborgen?” De hoofdconclusie die de rekenkamercommissies trekken is dat de SWO zijn best doet, maar dat dat niet voldoende is. Er is te weinig capaciteit in de organisatie en er worden te weinig middelen ter beschikking gesteld om informatieveiligheid op het vereiste niveau te brengen. Er worden de nodige onderzoeken en analyses op informatieveiligheid door of in opdracht van de SWO uitgevoerd, maar de aanpak van veel van de geconstateerde risico’s laat vaak op zich wachten. Het risicobewustzijn bij medewerkers en het urgentiegevoel bij leidinggevenden, management en bestuur om hierop te sturen behoeft verbetering. De rekenkamercommissies constateren risico’s dat de uitvoering van het beleid op onderdelen niet effectief is en dat gemeenten, en daarmee inwoners en instellingen risico’s lopen.

Naar aanleiding van de testen van de ethische hackers, die in opdracht van de rekenkamercommissies zijn uitgevoerd, zijn risico’s aangetroffen. De SWO is van de kwetsbaarheden die aangetroffen zijn op de hoogte gesteld en heeft maatregelen getroffen deze aan te pakken.

Aanbevelingen

De rekenkamercommissies hebben, naar aanleiding van de bevindingen, conclusies en aanbevelingen geformuleerd ter verbetering van de uitvoering van het beleid op informatiebeveiliging en privacy. Dat zijn aanbevelingen in de richting van de colleges van B&W ten aanzien van de uitvoering van het beleid, mede met de SWO op de achtergrond. Ook zijn aanbevelingen gericht aan colleges en gemeenteraden om gezamenlijk ambities op informatieveiligheid vast te stellen en de informatiepositie van de raad op dit onderwerp bespreekbaar te maken en te verbeteren. En tot slot aanbevelingen aan de gemeenteraden om de kaderstellende en controlerende rol die zij hebben beter in te kunnen vullen. De ervaringen met hacks in gemeenteland is dat informatieveiligheid niet meer beperkt is tot een technische uitvoeringszaak, maar een plek op de bestuurlijke agenda’s van colleges en gemeenteraden verdient.

Conclusies

Hieronder gaan we in op de conclusies naar aanleiding van de bevindingen uit het rekenkameronderzoek medio 2023 is uitgevoerd bij de gemeenten De Wolden en Hoogeveen. In deze paragraaf geven we de conclusies op basis van de driedeling Techniek, Organisatie en beleid en Mens en gedrag. Afgesloten wordt met aanbevelingen aan de colleges van B&W en de gemeenteraden van beide gemeenten.

Techniek

De onderzoeksvragen over de techniek betreffen de daadwerkelijke veiligheid van de systemen en de aandacht daarvoor.

De Samenwerkingsorganisatie De Wolden Hoogeveen (hierna: SWO) heeft in de afgelopen vijf jaar verschillende kwetsbaarheidsanalyses en een enkele pentest laten uitvoeren op de systemen. Daaruit bleken kritieke en ernstige kwetsbaarheden die niet altijd met de benodigde urgentie zijn opgepakt. Voor inwoners kan dit ernstige gevolgen hebben. Zoals BSN-nummers of persoonsgegevens van kwetsbare groepen die door een kwaadwillende hacker buit worden gemaakt en mogelijk op straat komen te liggen. Dat is geen denkbeeldig risico, zoals bijvoorbeeld blijkt in geval van Hof van Twente. Daarnaast lopen de gemeenten grote financiële risico's en is er sprake van grote schade op het vlak van bestuur en reputatie.

Organisatie en beleid

Hieronder vallen de onderzoeksvragen over de risicoanalyses, het informatiebeveiligingsbeleid, concrete activiteiten in het kader van het informatiebeveiligingsbeleid, de rollen en verantwoordelijkheden, informatie aan de raad en data-ethiek.

Risicoanalyses

Het informatiebeveiligingsbeleid moet volgens de Baseline Informatiebeveiliging Overheid (BIO) gebaseerd zijn op risicomanagement. Overheden moeten op basis van onder andere risicoanalyses controleren waarop ze nog niet voldoen aan de basiseisen van de BIO, welke risico's ze daardoor lopen, welke maatregelen ze treffen en welke risico's ze accepteren.
De laatste analyses dateren uit 2021. In 2021 is naar aanleiding van de reguliere actualisatie een Actieplan opgesteld. Die laatste is omgevormd tot een Risicobehandelplan, waarop nog een bestuurlijk besluit moet worden genomen. Ondertussen wachten risico's die in een pentest uit 2018 en de verschillende analyses zijn geconstateerd op verbetermaatregelen. Daarbij wordt verwezen naar ontbrekende middelen en capaciteit.

Informatiebeveiligingsbeleid

Het strategisch informatiebeveiligingsbeleid is geformuleerd in 2022, waarbij het privacybeleid uit 2018 als bijlage is toegevoegd. Een nieuw privacybeleid is in ontwikkeling.

In het strategische beleid zijn de rollen beschreven en verantwoordelijkheden op informatiebeveiliging belegd. Het tactische beleid bestaat uit protocollen en leidraden op de diverse beleidsterreinen van informatiebeveiliging en privacy. Een deel daarvan is vastgesteld, maar een deel is ook nog in ontwikkeling. De meeste protocollen en leidraden zijn op 2 datums vastgesteld in 2022 en 2023. Daarmee voldoen de gemeenten weliswaar voor een deel aan de eisen van de BIO, maar de protocollen zijn nog niet volledig doorvertaald naar het niveau van werkprocessen. Daardoor worden aspecten op informatiebeveiliging en privacy te weinig of te laat in de uitvoering betrokken. Dat blijkt onder meer ook uit de casestudie die in het rapport is opgenomen. De functionarissen op informatiebeveiliging en privacy worden niet altijd of niet tijdig betrokken door lijnmanagement. Deels komt dat ook door gebrek aan capaciteit op de functies op informatiebeveiliging en privacy. Dat zorgt voor risico's op ineffectiviteit en inefficiëntie bij de uitvoering van werkprocessen.

Rollen en verantwoordelijkheden

In een bijlage bij het strategische beleid zijn de rollen en verantwoordelijkheden beschreven. Daarin zijn de verantwoordelijkheden beschreven van bestuur, directie, (lijn)management, medewerkers en de functionarissen op informatiebeveiliging en privacy. En die van de functionarissen op informatiebeveiliging en privacy. De Chief Information Security Officer (CISO) is voor 0,5 fte aangesteld en combineert de functie met de functie van Chief Information Officer (CIO). De cruciale functie van CISO is bij I&A gepositioneerd, wat niet in overeenstemming is met een van de lijn onafhankelijke positionering zoals door de IBD wordt geadviseerd. Dat kan een risico op ineffectiviteit met betrekking tot de strategische functie van de CISO inhouden.

De Functionaris Gegevensbescherming wordt extern met een overeenkomst van opdracht ingevuld. De (Chief) Privacy Officer (CPO en PO) is intern voor in totaal 1 fte ingevuld. Naast deze functionarissen is er plek voor een Controller informatieveiligheid, vier I-adviseurs op deelgebieden en enkele beveiligingsbeheerders (onder andere BRP, BAG-BGT-BRO, ICT, HRM en Archief). Ter ondersteuning van de CPO en PO zijn medewerkers gepolst om privacy-ambassadeur in de teams te worden. Deze neventaken worden vanaf het najaar van 2023 ingevuld. Als deze invulling van de privacy ambassadeurs zo wordt gerealiseerd is er met betrekking tot de functies voldoende aandacht voor gegevensbescherming in de teams aanwezig. Geconstateerd wordt dat er voldoende momenten zijn voor overleg tussen de professionals op informatiebeveiliging en privacy om de tactische en operationele zaken te bespreken.

Er zijn bij de SWO twee tijdelijke Information Security Officers (ISO) voor in totaal 0,4 fte werkzaam. Er is behoefte aan uitbreiding en structurele invulling van deze functies. Mede daardoor stagneert de doorvertaling van de protocollen op informatieveiligheid naar werkprocessen.

Activiteiten

Het tekort aan capaciteit, onder andere vanwege de krapte op de arbeidsmarkt, zorgt voor vertraging in de realisatie van de benodigde activiteiten. Dat zijn ontwikkelactiviteiten in verband met de stormachtige ontwikkelingen in het veld en verbeteractiviteiten naar aanleiding van de uitgevoerde assessments en testen. Zo zijn verbetermaatregelen uit de pentest uit 2018 en latere risico- en kwetsbaarheidsanalyses pas in 2022 gerealiseerd of wachten nog op realisatie. Dit komt door gebrek aan structurele middelen en gebrek aan capaciteit. Ook wordt vooralsnog een managementinformatiesysteem voor informatieveiligheid (ISMS) gemist om rapportages op te leveren, activiteiten te beleggen en te volgen. Het ligt in de bedoeling deze systematiek op korte termijn uit te proberen en te laten ondersteunen door een ISMS-applicatie.

Informatie aan de raad

In de BIO is opgenomen dat de raden jaarlijks in het kader van de planning- en control-cyclus over informatieveiligheid worden geïnformeerd. In de jaarstukken van de gemeenten wordt op hoofdlijnen hierover gerapporteerd. De raden krijgen via de jaarlijkse ENSIA rapportages een update over de stand van zaken. De ENSIA rapportage bevatten de

verplichte collegeverklaringen over DigiD en Suwinet, of en in hoeverre de gemeente voldoet aan de BIO-maatregelen en resultaten van de assessments op applicaties als de Basisregistratie Personen (BRP), Basisregistratie Adressen en Gebouwen (BAG) en Waardering Onroerende Zaken (WOZ).

`

In 2022 hebben de functionarissen op informatiebeveiliging en privacy een presentatie voor een van de gemeenteraden verzorgd. Voorts zoomt de accountant in op de beveiligingsaspecten van een beperkt aantal applicaties in, met een nadruk op de financiële rechtmatigheid. En tot slot heeft de raad van Hoogeveen antwoord gekregen op vragen van een fractie over informatiebeveiliging en privacy.

De conclusie is dat de informatievoorziening over de stand van zaken met betrekking tot informatieveiligheid aan de gemeenteraden voldoet aan de basiseisen. Gezien de risico's die gemeenten hiermee lopen, kan geconcludeerd worden dat de raden zeer summier en alleen op hoofdlijnen worden geïnformeerd.

Data-ethiek

In het Informatiebeleid 2022-2022 wordt gewag gemaakt van data-ethiek binnen het kader van privacywetgeving. Het thema is niet verder uitgewerkt, bijvoorbeeld niet naar digitale inclusie zodat niemand wordt buitengesloten om mee te doen aan het digitale tijdperk. Ook is het beleid niet uitgewerkt naar controleerbaarheid, zodat op een democratisch verantwoorde wijze de digitale en fysieke ruimte wordt ingericht. Geconstateerd kan worden dat data-ethiek bij de gemeenten nog in de kinderschoenen staat en verdere bewustwording en uitwerking op dit thema gewenst is.

Mens en gedrag

Bewustwording

Een van de belangrijkste aspecten in het kader van informatieveiligheid is het risicobewustzijn van medewerkers. Gevraagd naar wat er goed gaat op het gebied van informatiebeveiliging en privacy antwoorden de respondenten dat bewustwording toeneemt, maar dat dat nog lang niet op het gewenste niveau is. Deze conclusie wordt ondersteund door de bevindingen uit de verschillende assessments en kwetsbaarheidsanalyses. Het gemiddelde volwassenheidsniveau van de medewerkers is relatief laag en medewerkers zijn nauwelijks op de hoogte van de verantwoordelijk-heden, regels en verplichtingen met betrekking tot informatieveiligheid. Er is nog geen structurele plek voor informatiebeveiliging en privacy in het inwerkprogramma en het management draagt het belang van deelname aan opleiding of training niet uit.

De phishingmail test in het kader van dit rekenkameronderzoek, onder medewerkers van SWO en raadsleden van de twee gemeenten, wees uit dat op het herkennen van phishing mails en risicobewustzijn ingezet moet blijven worden. Positief signaal is dat medewerkers bereid zijn om ambassadeur op informatiebeveiliging en privacy te worden, inclusief een wethouder en burgemeester.

Op informatiebeveiliging lopen de gemeenten een groot risico op het onderwerp bewustwording, een thema dat continue aandacht vergt.

Betrokkenheid bestuur en management

Issues op informatiebeveiliging en privacy komen op de directie- en bestuurlijke tafels aan bod. Veel signalen worden afgegeven in de assessments en rapportages die op deze tafels terecht komen, met de boodschap dat het nodige gedaan en geïnvesteerd moet worden om informatieveiligheid op het basisniveau te krijgen die de BIO voorschrijft. De urgentie wordt wel gevoeld, maar de indruk is dat de doorzettingskracht er niet is om structurele middelen ervoor beschikbaar te stellen. Daardoor ontstaat vertraging bij de uitvoering van benodigde maatregelen op informatieveiligheid en lopen de gemeenten een groot risico op ineffectiviteit.

De ervaring van de afgelopen jaren met de risico's op incidenten en hacks in gemeenteland is dat informatieveiligheid 'chefsache' is. Geconstateerd wordt dat informatieveiligheid geen onderdeel uitmaakt van de collegeambities van de gemeenten en dat geen van de collegeleden verantwoordelijk is voor deze portefeuille.

Hoofdvraag

De SWO doet zijn best, maar dat is niet voldoende: er is te weinig capaciteit en er wordt te weinig geld ingezet voor informatieveiligheid. Daardoor lopen de gemeenten, en bijgevolg de inwoners, grote risico's. Zij voldoen nog niet aan de BIO, de algemene basiseisen die gemeenten zichzelf stellen om de informatiebeveiliging op orde te hebben. De aanbevelingen vloeien dan ook uit deze algemene constatering voort.

De aanbevelingen zijn onderverdeeld in aanbevelingen gericht aan de colleges van B&W, aan de gemeenteraden van De Wolden en Hoogeveen en aan colleges en raden samen.

Aanbevelingen

Aanbevelingen aan de colleges van B&W

1. **Beleg informatieveiligheid als aandachtsgebied bij een van de collegeleden, bij voorkeur de burgemeester, en organiseer bestuurlijke doorzettingskracht op informatiebeveiliging en privacy.**
2. **Zorg dat procedure en richtlijnen op informatiebeveiliging en privacy in de werkprocessen worden ingebed.**
   Daarmee wordt niet alleen op papier aan de BIO en AVG voldaan, maar ook de daadwerkelijke werking van de maatregelen in de praktijk.
3. **Positioneer de cruciale positie CISO onafhankelijk van de lijn.**
   De Informatiebeveiligingsdienst (IBD) heeft hiervoor richtlijnen opgesteld.
4. **Zorg voor voldoende kwalitatieve en kwantitatieve capaciteit op informatiebeveiliging en privacy om de ambities (zie hierna) te realiseren.**

Mogelijk is samenwerking hierop met omliggende gemeenten en/of provincie nodig om voldoende capaciteit of schaalgrootte te realiseren.

5. **Ga verder met implementatie van een Informatiemanagementsysteem voor informatieveiligheid (ISMS).**
   Daarmee worden activiteiten op informatiebeveiliging en privacy meer plan- en volgbaar, rapportages voor ENSIA makkelijker op te stellen en kan de PDCA-cyclus op informatiebeveiliging en privacy ingericht worden.
6. **Investeer in activiteiten om het risicobewustzijn van medewerkers te bevorderen en zorg dat het management de noodzaak hiervan inziet en dat uitdraagt.**
7. **Maak tempo met het vervolledigen van het (tactisch) informatieveiligheidsbeleid, door de nog ontbrekende protocollen en richtlijnen vast te stellen.**

   Aanbevelingen aan colleges en raden

8. **Formuleer samen ambities op informatiebeveiliging en privacy.**
   Bijvoorbeeld over welke periode de gemiddelde taakvolwassenheid van de medewerkers op een bepaald niveau moet zijn, wanneer de gemeenten aan de BIO moeten voldoen enz.
9. **Spreek samen af op welke wijze de raad geïnformeerd wordt over informatiebeveiliging en privacy.**
   Bijvoorbeeld halfjaarlijks in een aparte raadscommissie of een commissie onder een bestaande commissie.[1]
10. **Formuleer samen beleid op data-ethiek, hoe gemeenten verantwoord omgaan met data van inwoners.**
    De Agenda Digitale Grondrechten en Ethiek 2022-2026 van de VNG kan hierbij behulpzaam zijn. [2]

    Aan de raden

11. **Zorg dat er in overeenstemming met de ambities structureel middelen ter beschikking worden gesteld om de activiteiten op informatiebeveiliging en privacy te financieren.**
    Onder andere het Risicobehandelplan 2023-2026 biedt daarvoor de financiële kaders. De IBD geeft hier richtlijnen voor, zoals 10% van het budget voor ICT.
12. **Zorg ervoor dat je als raad voldoende geïnformeerd wordt op informatiebeveiliging en privacy.**
    Bijvoorbeeld door externe expertise te raadplegen, zoals de accountant of een beveiligingsexpert.

---

[1] Zo heeft bijvoorbeeld de gemeente Hof van Twente een commissie op ICT onder de auditcommissie die regelmatig wordt gebriefd over de voortgang op de beveiligingsmaatregelen.

[2] https://vng.nl/sites/default/files/2022-02/agenda_digitale_grondrechten_en_ethiek_2022-2026.pdf

1 Inleiding

Gemeenten zijn kwetsbaar

Onder andere door de toegenomen taken in het sociaal domein beheren en verwerken gemeenten meer en meer persoonsgegevens en gevoelige data. Dat doen gemeenten in toenemende mate met digitale hulpmiddelen. Gemeenten zijn kwetsbaar, zoals onder andere blijkt uit datalekken en hacks. Wat gebeurt er bijvoorbeeld als gevoelige informatie op straat komt te liggen of op het dark web wordt aangeboden? Of als de gegevens worden gegijzeld en de digitale dienstverlening aan burgers niet meer mogelijk is? Naast ernstige financiële, juridische en technische gevolgen kunnen deze crises de privacy van burgers en het imago van de gemeente aantasten.[3] Dit zijn redenen voor de rekenkamercommissies De Wolden en Hoogeveen geweest om een onderzoek te doen naar opzet, bestaan en werking van het informatiebeveiliging- en privacybeleid in de gemeenten en de ambtelijke samenwerkingsorganisatie SWO.

1.1 Leeswijzer

Samenvatting, conclusies en aanbevelingen zijn in het hieraan voorafgaande hoofdstuk opgenomen. In hoofdstuk 2 behandelen we de doelstelling, onderzoeksvragen en de aanpak van het onderzoek. Hoofdstuk 3 bevat de bevindingen, geordend aan de hand van de onderzoeksvragen. Deze bevindingen zijn getoetst bij de in dit onderzoek betrokken respondenten (inclusief de feitencheck door middel van ambtelijke hoor en wederhoor).

In bijlage 1 is de casestudie naar een Wmo-aanvraag die bij de gemeente binnenkomt opgenomen. Een korte samenvatting van de casestudie is in §3.2.4 opgenomen. In de bijlage 2 staan veel gebruikte termen en afkortingen die gebruikt worden bij informatieveiligheid en privacy. Daarna volgt in bijlage 3 de lijst met geraadpleegde stukken en de lijst met functies van de respondenten. Vervolgens komen in bijlage 4 de normen aan bod, gekoppeld aan de onderzoeksvragen. In §3.2.5 wordt verwezen naar het volwassenheidsniveau zoals gehanteerd door de beroepsorganisatie van IT-auditors in Nederland (de Nederlandse Organisatie van Register EDP-Auditors, NOREA.). Daarom is deze in een tabel in bijlage 5 opgenomen

[3] Gemeenten hebben in 2013 in verband van de Vereniging van Nederlandse Gemeenten (VNG) afgesproken te voldoen aan de maatregelen van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De baseline is gebaseerd op de ISO-normering (NEN-ISO 27002) met richtlijnen voor informatiebeveiligingsnormen. In 2021 hebben gemeenten in VNG-verband afgesproken structureel voldoende middelen voor de weerbaarheid tegen digitale bedreigingen vrij te maken.
Vanaf 25 mei 2016 schrijft de Algemene Verordening Gegevensbescherming (AVG of GDPR) voor de gehele Europese Unie voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger, overheden en bedrijven/instellingen. Vanwege een overgangstermijn van 2 jaar wordt de AVG vanaf 25 mei 2018 gehandhaafd.

2 Doelstelling, onderzoeksvragen en aanpak

2.1 Doelstelling en onderzoeksvragen

Doelstelling en hoofdvraag

De Rekenkamercommissies De Wolden en Hoogeveen willen de gemeenteraden inzicht geven in de stand van zaken in de gemeenten, en SWO, met betrekking tot beleid en uitvoering van informatiebeveiliging en privacy. Deze doelstelling is vertaald naar de volgende hoofdvraag:

"Hoe doelmatig, doeltreffend en rechtmatig zijn de gemeenten de Wolden en Hoogeveen om de informatieveiligheid te waarborgen?"

Onderzoeksvragen

De doelstelling en hoofdvraag worden uitgewerkt aan de hand van de onderzoeksvragen zoals opgenomen in onderstaande tabel 2.1. Zoals bij informatieveiligheid gebruikelijk is zijn de vragen door middel van de trits Techniek > Organisatie en beleid > Mens en gedrag opgedeeld.

Tabel 2.1. Onderzoeksvragen
1. Techniek
1.1. Zijn het netwerk en de bedrijfskritische systemen voldoende technisch beveiligd om ongeautoriseerde toegang te voorkomen?
1.2. Is er extra aandacht voor de technische beveiliging van gevoelige informatie, zoals persoonlijke gegevens?
2. Organisatie en beleid
2.1. Worden er systematische en actuele risicoanalyses gemaakt rond informatiebeveiliging en worden er op basis daarvan passende beheersmaatregelen genomen?
2.2. Biedt het informatiebeveiligingsbeleid voldoende basis voor de bescherming van gegevens?
2.3. Zijn binnen de organisatie de rollen en verantwoordelijkheden voor informatiebeveiliging helder belegd? En is de organisatie qua formatie toegerust om het informatiebeveiligingsbeleid uit te voeren?
2.4. Is het informatiebeveiligingsbeleid vertaald naar concrete activiteiten en zijn hiervoor voldoende middelen beschikbaar gesteld?
2.5. Wordt de raad periodiek geïnformeerd over de status van de informatiebeveiliging?
2.6. Is er sprake van data-ethiek: wordt er gereflecteerd op dat wat er met data gebeurt? Is er sprake van een bewuste, reflectieve omgang met data, waarin de wenselijkheid van het datagebruik en de doelen ervan wordt bevraagd?
3. Mens en Gedrag
3.1. Zijn medewerkers zich bewust van informatiebeveiligingsrisico's en is voor medewerkers duidelijk wat van hen verwacht wordt ten aanzien van informatiebeveiliging?
3.2. Is het hogere management actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen de organisatie?

Voor de normen bij deze onderzoeksvragen verwijzen we naar bijlage 4.

2.2 Korte inleiding op informatiebeveiliging en privacy

Informatiebeveiliging

Informatiebeveiliging gaat over het geheel aan preventieve, detectieve en correctieve maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de informatie binnen een organisatie garanderen. Doel is de continuïteit van de informatie en de informatievoorziening of dienstverlening te waarborgen en eventuele gevolgen van (beveiligings)incidenten te beperken. Het beleid dat gemeenten hierop hebben afgesproken is neergelegd in de Baseline Informatiebeveiliging Overheid (BIO).[4] De BIO bevat maatregelen die gemeenten op basis van een risicoanalyse kunnen nemen om aan het basisniveau voor informatiebeveiliging te voldoen.

Gegevensbescherming

Gegevensbescherming betreft de regels voor de verwerking van persoonsgegevens door bedrijven, instellingen en overheden. Doel is de privacy van burgers op een adequate manier te beschermen. De Europese General Data Protection Regulation (GDPR), in Nederland bekend als de Algemene Verordening Gegevensbescherming (AVG), is sinds mei 2018 van kracht.

Informatieveiligheid

De AVG schrijft onder andere voor dat passende maatregelen getroffen moeten worden om persoonsgegevens te beveiligen, in het belang van de burger en de gemeenten zelf. De twee onderwerpen informatiebeveiliging en gegevensbescherming (privacy) hebben dus onderling een grote overlap. Een deel van de protocollen en procedures op beide terreinen komen met elkaar overeen. Overkoepelend wordt vaak de term informatieveiligheid gebruikt, zie onderstaand afbeelding 2.1.

[4] Gemeenten hebben in 2013 in VNG-verband afgesproken te voldoen aan de maatregelen van de Baseline Informatie-beveiliging Gemeenten (BIG). De BIG is vanaf 2020 vervangen door de Baseline Informatiebeveiliging Overheid (BIO). De baseline is gebaseerd op de kwaliteitsnormen NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017.

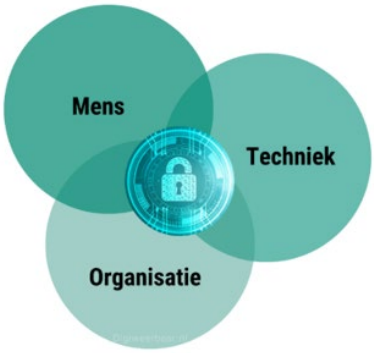
Afbeelding 2.1. Informatieveiligheid met privacy en informatiebeveiliging.

Bron: Rekenkamer Utrecht, 2021.

In dit onderzoek worden de beide onderwerpen, informatiebeveiliging en privacy, geadresseerd.

Mens, techniek, organisatie

Informatieveiligheid wordt vaak nog enkel vanuit een technische invalshoek benaderd. De ervaring leert evenwel dat technische oplossingen te organiseren zijn, hoewel deze natuurlijk ook de praktische (pen)testen moeten doorstaan ("the proof of the pudding is in the eating"). Naast techniek zijn mens en organisatie essentieel bij informatiebeveiliging en privacy. Cruciale factoren die de informatieveiligheid bepalen zijn houding en gedrag van de menselijke actor, kortom bewustwording op risico's bij medewerkers en lijnmanagement. Ook moeten de organisatorische randvoorwaarden gecreëerd zijn om techniek en mens te ondersteunen. Beleid en protocollen moeten daarvoor opgesteld en vastgesteld zijn (voor een gedeeltelijk overzicht van de protocollen op informatiebeveiliging en privacy zie afbeelding 3.1) en in de praktijk worden toegepast. Om dat optimaal te laten slagen moet beleid op informatie-beveiliging en privacy gedragen en uitgedragen worden door bestuur en management van de gemeente.



2.3 Aanpak

Methoden

De onderzoeksvragen worden beantwoord door middel van een analyse van documenten in deskresearch, interviewverslagen, casestudie en pentesten (zie volgende alinea's.) De documenten bevatten beleid en rapportages van de gemeente. De documenten die zijn bestudeerd zijn in bijlage 3 opgenomen, evenals de functies van de bestuurders en functionarissen van SWO die zijn geïnterviewd. De deskresearch vond plaats in de periode mei-juli 2023. De interviews zijn in juni-juli 2023 afgenomen.

Casestudie

Voor de casestudie is de (klant)reis weergegeven van informatie door de gemeentelijke organisatie naar aanleiding van een Wmo-aanvraag. De casestudie gaat in op de vraag welke gegevens worden verwerkt als een inwoner een Wmo-voorziening aanvraagt. Welke gegevens worden opgevraagd, in welke systemen worden de gegevens opgeslagen, wie heeft toegang tot de informatie en met welke externe partijen worden deze gedeeld. Op basis van flowchart, uitvraag bij de teamleider Zorg en mailwisseling is deze gegevensreis in kaart gebracht. De bevindingen uit de casestudie over hoe de gemeente omgaat met (bijzondere) persoonsgegevens zijn meegenomen in de paragrafen 3.1-3.3.

Pentesten

In mei en juni 2023 zijn in het kader van het rekenkameronderzoek verschillende pentesten uitgevoerd op de systemen. Ook zijn phishing mails verstuurd naar medewerkers van SWO en raadsleden van de gemeenten De Wolden en Hoogeveen.[5] Door SWO is aangegeven dat pentesten uitgevoerd zijn op de systemen. De laatste is in 2018 uitgevoerd.

In 2022 zou de SWO opnieuw een pentest laten uitvoeren. Omdat het rekenkameronderzoek werd uitgevoerd én om dubbelingen te voorkomen, hebben de rekenkamercommissies in overleg met de Chief Information Security Officer (CISO) besloten een externe netwerk test, een interne netwerk test, Active Directory (AD) audit, phishing test uit te voeren. [6] Voor een nadere uitleg van de testen en de resultaten zie §3.1.1 en §3.3.1.

De nota van bevindingen is in september 2023 voor de ambtelijke hoor en wederhoor (feitencheck) aangeboden.

---

5 Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken.

6 Phishing is een vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens.

3 Bevindingen

In dit hoofdstuk worden de bevindingen per onderzoeksvraag weergegeven.

3.1 Techniek

In deze paragraaf presenteren de rekenkamercommissies de bevindingen met betrekking tot onderzoeksvraag 1.1 en 1.2 op techniek:

1.1 Zijn het netwerk en de bedrijfskritische systemen voldoende technisch beveiligd om ongeautoriseerde toegang te voorkomen?
1.2 Is er extra aandacht voor de technische beveiliging van gevoelige informatie, zoals persoonlijke gegevens?

Hieronder gaan we in op de technische beveiliging, daarna volgen organisatie en beleid in §3.2. We gaan in §3.1.1.1 in op de technische pentesten die in het kader van het rekenkameronderzoek zijn uitgevoerd, in overleg met SWO.

3.1.1 Technische beveiliging netwerk en bedrijfskritische systemen

Beveiliging

Op de technische kant van informatiebeveiliging kan veel georganiseerd en ingesteld worden om kwaadwillenden buiten te houden. Zoals firewalls, spamfilters en virusscanners. Of, als de kwaadwillenden onverhoopt tot het netwerk en de systemen zijn doorgedrongen, dat tijdig te detecteren en te blokkeren. En ervoor te zorgen dat er in het interne netwerk drempels worden opgeworpen, zodat men niet (makkelijk) bij de informatie in de kritieke systemen kan geraken. Ook moet de software voorzien zijn van de nieuwste updates en patches, waardoor kwetsbaarheden in de software zijn verholpen.

Assessments en scans

Om de technische beveiliging te testen laat SWO assessments en testen uitvoeren op de systemen.[7] De laatste pentest in opdracht van SWO dateert uit 2018. In 2022 zou opnieuw een pentest uitgevoerd worden, maar deze is (in overleg met de rekenkamercommissie) uitgesteld en opgenomen in het rekenkameronderzoek. Verder is begin 2021 een assessment op de systemen uitgevoerd, medio 2021 een externe netwerkscan en een forensisch onderzoek begin 2022 naar aanleiding van de Log4J-kwetsbaarheid. [8]

---

[7] In de Baseline Informatiebeveiliging Overheid (BIO) is opgenomen dat gemeenten jaarlijks pentesten of kwetsbaarheidsanalyses (laten) uitvoeren.

[8] (Apache) Log4J is een stuk software dat gebruikt wordt in webapplicaties en systemen die gebruik maken van Java. December 2021 beoordeelde het Nationaal Cyber Security Centrum (NCSC) de impact van de kwetsbaarheid als uiterst hoog.

In het assessment van begin 2021 is een hoog risico aangetroffen vanwege ‘outdated software on server’. Uit de interviews blijkt dat niet altijd de meest recente updates van software werd geïnstalleerd. Er wordt nog lang met bepaalde 'outdated' apparatuur en software doorgewerkt door het ontbreken van prioritering in relatie tot onvoldoende menskracht voor tijdige vervanging en soms vanuit kostenoverwegingen. Door de externe partij die het assessment uitvoerde is aanbevolen dat op korte termijn te verhelpen. Daarnaast zijn 2 kwetsbaarheden met medium en 2 met lage risico’s aangetroffen. Deze kwetsbaarheden zijn inmiddels verholpen.

Medio 2021 bleek uit een externe netwerkscan 3 kritieke en 38 ernstige risico’s. Begin 2022 zijn bij een forensisch onderzoek naar aanleiding van de Log4J-kwetsbaarheid een aantal risico’s geconstateerd die op korte termijn opgepakt moesten worden. Deze hadden te maken met het (beter) configureren van beheer- en informatiebeveiligingsinstellingen op systemen en apparaten. De kritieke kwetsbaarheden en ernstigste risico's zijn toen aangepakt. De hiervoor genoemde assessments en onderzoeken hebben vaak een beperktere scope dan penetratietesten of pentesten door ethische hackers.

Pentest 2018

In 2018 heeft SWO voor het laatst een pentest op het netwerk uitgevoerd. Naar aanleiding van deze pentest is onder andere op beveiligingsgebied geadviseerd monitoring met behulp van een SIEM/SOC [9] te implementeren, Multi Factor Authenticatie (MFA)[10] te implementeren en de netwerk-segmentatie te optimaliseren. Hieronder gaan we op de implementatie van deze verbetermaatregelen uit 2018 in.

SIEM/SOC

De netwerken van de gemeenten De Wolden en Hoogeveen en SWO zijn tegen externe inbreuken beschermd door firewalls en virusscanners. Aanvullend hebben zij geparticipeerd in een tender van de VNG voor de aanschaf van een zogenoemde SIEM/SOC-applicatie, net als veel andere gemeenten.[11] Deze tender is uiteindelijk mislukt, vanwege het stopzetten van de samenwerking tussen VNG en KPN. Daardoor moesten gemeenten op zoek naar een andere oplossing. Op basis van de software die nu wordt gebruikt kan het netwerkverkeer van buiten naar binnen op de systemen gemonitord worden en verdacht verkeer gedetecteerd worden. Analyseren, controleren en met name opvolgen van de meldingen kost veel capaciteit van medewerkers. Deze capaciteit is er momenteel onvoldoende.

---

9 SIEM/SOC: Security Information & Event Management (SIEM) en Security Operations Center (SOC) is een tool die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.

10 Multi factor authenticatie (MFA of 2FA) is een authenticatie of verificatie methode waarbij twee of meer stappen succesvol doorlopen moeten zijn om ergens toegang tot te krijgen, zoals naast het gebruik van een wachtwoord het gebruik van een token of biometrisch gegeven.

11 SIEM/SOC: Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.

MFA

Over Multi Factor Authenticatie (MFA) werd in 2021 in de ENSIA-rapportage[12] geconstateerd dat deze maatregel nog geïmplementeerd moest worden. In het Actieplan Informatieveiligheid uit 2021 is de implementatie van MFA opgenomen (zie voor het Actieplan §3.2.1-3.2.2). Op 11-7-2022 is dit als onderdeel van het wachtwoordbeleid vastgelegd.[13]

Segmentatie

Om ervoor te zorgen dat indringers die eenmaal binnen zijn niet meteen tot de meest gevoelige informatie in de kritische systemen toegang kunnen krijgen, worden in het netwerk drempels opgeworpen. Dat heet netwerksegmentatie. Deze verbeteractie, naar aanleiding van de pentest van 2018, is in 2021 opgenomen in het Actieplan Informatieveiligheid en grotendeels uitgevoerd in 2021. Bedoeling is dat de netwerksegmentatie in de eerste helft 2023 is gerealiseerd. In de interviews, gehouden in juni 2023, werd aangegeven dat ongeveer 90% van het netwerk gesegmenteerd was. Er vindt een overgang plaats naar de cloud en SAAS-omgeving, daarbij wordt met betrekking tot segmentatie uitgegaan van het zogenoemde Zero Trust principe.[14] Dat betekent dat verdere voortgang op segmentatie mede afhangt van de snelheid van deze overgang.

Mobile devices

Uit de interviews blijkt SWO op de technische kant achter te lopen op noodzakelijke ontwikkelingen, zie ook §3.2.1 en de ENSIA-rapportages. Ook blijkt uit de interviews dat er hard wordt gewerkt aan de beveiliging van de systemen en het netwerk. Zo is SWO op een aantal prioriteiten bezig, zoals het beheer van de laptops en smartphones (Mobile Device Management, MDM). Respondenten melden dat SWO op de goede weg is, maar dat er nog veel moet gebeuren. En gemeld wordt dat de capaciteit ontbreekt om alle benodigde activiteiten, ook al zijn ze geprioriteerd, meteen op te pakken.

Pentesten

Pentesten

De rekenkamercommissies hebben in het kader van het rekenkameronderzoek besloten een externe netwerk pentest, een interne netwerk pentest, een wifi-netwerk pentest, een Active Directory audit en een phishing mail test uit te voeren. Door ethisch hackers is getest op een beperkt aantal doelen, dat wil zeggen dat de reikwijdte of scope van het

---

12 ENSIA: Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders).

13 Zie: Wachtwoordbeleid – Informatieveiligheid en privacy 2022 – SWO v 1.0, 11-7-2022.

14 Zero trust is een veiligheidsstrategie met betrekking tot design en implementatie van software, hardware en systemen. Meestal gebruikt in verband met de strategie dat alle verkeer geverifieerd moet worden en zo min mogelijk wordt gewerkt met geprivilegieerde toegang tot gegevens en systemen.
De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan.
SAAS betekent Software-as-a-Service en is een model waarbij softwaretoepassingen via internet worden aangeleverd.

onderzoek beperkt is.[15] Daarvoor is in samenspraak tussen SWO en de onderzoekers een testplan opgesteld. De pentesten zijn in mei 2023 uitgevoerd. Getest is op doelen met een zekere risicoclassificatie. Deze risicoclassificatie is in de onderstaande tabel 3.1 weergegeven.

Disclaimer

Algemene disclaimer is dat pentesten een momentopname zijn van de stand van zaken van de beveiligingsmaatregelen. De ontwikkelingen aan de kant van de bedreigingen gaan snel. Kwaadwillende hackers hebben de tijd om diep te graven in mogelijkheden om schade aan te richten. Terwijl middelen en tijd voor ethische hackers beperkt zijn en de scope van de pentesten navenant beperkt is. Daardoor bieden de resultaten van de pentesten geen garantie voor de toekomst. Ze kunnen wel zicht geven op de risico's die de organisatie op dat moment loopt.

Tabel 3.1. Risicoclassificatie pentesten.

Risicoclassificatie	Toelichting
Kritisch (9-10)	Extreem hoge kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg catastrofale financiële verliezen.
Hoog (7. 0-8.9)	Hoge kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg enorme financiële verliezen.
Gemiddeld (4.0-6.9)	Aannemelijke kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg financiële verliezen.
Laag (0.1-3.9)	Mogelijke kans dat beveiligingsmaatregelen niet voldoende zijn of omzeild kunnen worden en dat hierdoor de kwetsbaarheid misbruikt kan worden met als gevolg gelimiteerde financiële verliezen.
Best Practice	Deze bevinding omvat geen direct aanvalsscenario met negatieve gevolgen. Echter duidt een bevinding met deze classificatie wel aan dat er een beveiligingsmaatregel niet voldoet aan security best practices. Het ontbreken van deze beveiligingsmaatregel kan het uitvoeren van andere aanvallen vergemakkelijken.

Afgesproken is dat kritieke risico's meteen gemeld zouden worden aan de CISO. Dat is op 2 punten gebeurd tijdens de pentesten. Daarop heeft de organisatie meteen geacteerd en de benodigde verbetermaatregelen geïmplementeerd. Daarnaast heeft de CISO na de testen vertrouwelijk de technische rapportages van de pentesten gekregen en deze in bijzijn van de ethisch hacker intern besproken. Daarbij zijn de verbetermaatregelen die de ethisch hacker aanraadt aan de orde gekomen.

[15] Een ethisch hacker is een computerspecialist die beveiligingssystemen en netwerken test op een positieve manier. Zijn doel is om door middel van hacken fouten en veiligheidslekken op te sporen in de systemen en netwerken om deze daarna te melden aan de bedrijven of instanties waarmee ze samenwerken.

Hieronder gaan we nader in op de technische pentesten zelf en op hoofdlijnen de daarbij gesignaleerde risico's. De test met phishing mails wordt in §3.3.1 behandeld, omdat deze test met name gericht is op de ‘awareness’ en niet zozeer op de techniek.

Externe netwerk pentest

Om de staat van de beveiliging van het externe netwerk te testen zijn in het kader van het rekenkameronderzoek de kwetsbaarheden in kaart gebracht. Daarmee wordt de effectiviteit van de genomen beveiligingsmaatregelen geverifieerd, met name om de bedreigingen van buitenaf tegen te gaan. De aanvalsscenario’s van de externe pentest betroffen vier mogelijke risico’s, waarvan 1 van kritisch, 2 hoog en 1 gemiddeld niveau.

Deze 4 doelen zijn niet behaald, dat wil zeggen dat het de ethisch hackers niet gelukt is de geplande aanvalsscenario’s succesvol uit te voeren. Wel zijn gedurende de pentest 3 kwetsbaarheden op gemiddeld niveau aangetroffen. Daarnaast zijn 6 bevindingen met een classificatie ‘best practice’ gedaan. Deze bevindingen betreffen niet zozeer kwetsbaarheden, maar behoeven wel verbetering om aan geldende veiligheidsstandaarden te voldoen. Op basis van de resultaten van de uitgevoerde pentest en de en de uitvoerbaarheid van de aangetroffen kwetsbaarheden (van medium en best practice niveau) wordt het risiconiveau van het externe netwerk van de gemeenten De Wolden en Hoogeveen op laag ingeschat. Dat betekent een lager risiconiveau dan bij de externe netwerkscan in 2021 is aangetroffen.[16]

Interne en wifi-netwerk pentest

Deze pentest is bedoeld om de kwetsbaarheden van het interne en wifi-netwerk in kaart te brengen. Hiermee wordt de effectiviteit van de genomen beveiligingsmaatregelen getest die ervoor moeten zorgen dat de schade die een kwaadwillende in het netwerk kan aanrichten zoveel mogelijk beperkt wordt. Die kwaadwillende kan iemand zijn die van buiten in het netwerk is doorgedrongen of over inloggegevens op het netwerk beschikt.

Het eerste onderdeel van deze pentest was de exploitatie van de wifi-netwerken:

- SSID: Medewerkers
- SSID: Hoogeveen-Gasten

Tijdens de pentest is het de ethisch hacker niet gelukt het wifi-netwerk te exploiteren.

[16] Gelet op de continue risico-ontwikkeling is de constatering dat er een laag niveau is nog geen reden om de aandacht te laten verslappen, zoals bij de disclaimer is aangegeven.

Een ander onderdeel van deze pentest betrof het interne netwerk op basis van "white box" test.[17] Hierbij wordt bewust aan de ethisch hacker een netwerkaccount verstrekt door de organisatie, zodat ook het netwerk "van binnenuit" getest kan worden op eventuele kwetsbaarheden. De scope van deze test betrof risico's waarvan 1 kritisch, 2 hoog en 1 gemiddeld niveau. De ethische hacker slaagde erin alle doelen van de aanvalsscenario's te behalen. Daarbij zijn de volgende kwetsbaarheden aangetroffen: 2 van kritiek niveau, 2 van hoog niveau, 6 van medium niveau en 4 van 'best practice' niveau. Deze bevindingen uit de pentest waren niet aangetroffen bij eerdere assessments of testen. Op basis van de interne en wifi-netwerk pentest wordt het risico dat de gemeenten ten tijde van de test liepen als hoog ingeschat. Dat wil zeggen dat de gemeenten kwetsbaar zijn voor een ransomware aanval zoals bij Hof van Twente heeft plaatsgevonden, met grote financiële en andere nadelige effecten tot gevolg.

Zoals eerder aangegeven zijn de twee risico's van kritiek niveau meteen gedeeld met de CISO en zijn deze door de organisatie meteen aangepakt en gemitigeerd. De overige kwetsbaarheden zijn vertrouwelijk met de CISO gedeeld en met de afdeling I&A besproken.[18]

AD audit

De Active Directory (AD) audit is op 22 mei 2023 uitgevoerd. Een AD staat beheerders toe om het beleid met betrekking tot rechten van medewerkers en instellingen in het netwerk van een organisatie te beheren. De AD-audit test met name op risico's in verband met de uitvoering van het wachtwoordenbeleid, kwetsbaarheden met betrekking tot de inrichting van de Active Directory en op accounts en wachtwoorden die bekend zijn op internet.[19]

De AD-audit checkt op kwetsbare en zwakke wachtwoorden. Deze worden gecheckt op de vereiste complexiteitsgraad en vergeleken met een lijst op internet met wachtwoorden die in relatie gebracht kunnen worden met de gemeente. In totaal zijn 1.446 gebruiker accounts gescand, van SWO en de 2 gemeenten.

Van de 1.446 gebruikersaccounts zijn er 209 aangetroffen met een wachtwoord van een jaar of ouder, 108 accounts waarvan het wachtwoord nooit verloopt, 194 wachtwoorden die vaker worden gebruikt (niet uniek zijn) en 35 accounts met de optie 'password not required'. Verder zijn er 60

---

17 Een white box test is een teststrategie waarbij de ethische hackers kennis hebben van de technische infrastructuur en systemen en met behulp van die kennis technische zwakheden trachten op te sporen. Dit in tegenstelling tot black- of greybox testen, waarbij de hackers vooraf respectievelijk geen of beperkte kennis hebben van de systemen

18 Uit de ambtelijke hoor en wederhoor blijkt dat de afdeling I&A inmiddels is begonnen met de top-10 van deze kwetsbaarheden te mitigeren. Acht hiervan zijn gemitigeerd. De andere twee bestaan uit kwetsbare applicaties waarvoor inmiddels een vervangingstraject loopt voor het uitfaseren.

19 Accounts en wachtwoorden die bekend zijn op internet betekent dat deze bij eerdere hacks of phishing mails zijn buitgemaakt en gepubliceerd worden op het dark web.

accounts zonder versleuteling (missende AES-sleutels)[20] en 60 accounts die van een verouderde beveiliging (LM hash)[21] gebruik maken. Een zeer groot aantal van deze accounts worden gebruikt voor functionele postbussen, MS Teams-objecten en service accounts ten behoeve van functionele applicaties. Bij de functionele postbussen zijn de accounts inmiddels uitgeschakeld. Veel van de overige accounts zijn "systeemaccounts" waarbij het wachtwoord niet periodiek veranderd kan worden, omdat dat bepaalde services onder een applicatie of een koppeling met andere systemen niet meer werken.

Er zijn 6 wachtwoorden in combinatie met gebruikersnamen van de gemeenten gevonden die publiekelijk bekend zijn (bij eerdere hacks of phishing mails buitgemaakt) en mogelijk nog in gebruik zijn.

Van de administrator accounts valt op dat de accounts van de beheerders ook lid zijn van een groep met algemene service accounts. Dat is onwenselijk, zeker omdat het zo ingeregeld is dat deze accounts op 2 manieren rechten kunnen verkrijgen. Andersom is een algemeen service account lid van het beheerdersdomein. Een van de ingeschakelde administrator accounts is gedurende een jaar niet gebruikt. 36 administrator accounts hebben een wachtwoord ouder dan een jaar en met 16 accounts zijn al meer dan een jaar geen autorisaties uitgevoerd.

Van de ingeschakelde admin accounts hebben er 7 langer dan 90 dagen niet meer ingelogd, en zijn hoewel ingeschakeld dus feitelijk inactief. In totaal hebben 71 accounts niet alleen geprivilegieerde rechten op het domein, maar ook in andere geprivilegieerde groepen. En het domein beheerder account heeft een wachtwoord ouder dan 180 dagen. Voorts zijn er risico's aangetroffen bij niet standaard accounts met rechten, een beveiligings-protocol en de infrastructuur van de AD-beveiliging.

Er zijn bij deze AD audit kwetsbaarheden gevonden. Een deel kan verklaard worden door systeemaccounts waarvan de wachtwoorden niet aangepast hoeven te worde, maar een deel lijkt voort te komen uit het niet consequent toepassen van het wachtwoordbeleid. Dat kan onder andere verklaren waarom er accounts zijn met verouderde of niet unieke wachtwoorden, of accounts met missende veiligheidssleutels. In interviews werd ook opgemerkt dat het wachtwoordenbeleid niet consequent uitgevoerd wordt.

3.1.2 Aandacht voor technische beveiliging van gevoelige informatie

De verwerking door of namens de gemeente van gevoelige informatie, zoals bijzondere persoonsgegevens, moet in het kader van de AVG met de nodige

[20] Advanced Encryption Standard (AES) is een (cryptografische) versleutelingstechniek.
[21] LM hash is een versleutelingsmethode gebaseerd op een verouderd algoritme.

waarborgen en veiligheidseisen geschieden.[22] Zoals we in de vorige paragraaf hebben gezien is er wel aandacht voor de technische beveiliging van het netwerk, de systemen en informatie. Er worden door de organisatie assessments en audits op de systemen uitgevoerd om te weten te komen waar kwetsbaarheden aanwezig zijn. Tegelijkertijd kan geconstateerd worden dat dringende maatregelen die naar aanleiding van deze testen en audits genomen zouden moeten worden, niet altijd worden opgepakt en doorgevoerd.

DPIA, IRPA

Onderdeel van de implementatie van de AVG is de uitvoering van data protection impact assessments (dpia's) op verwerkingsprocessen met persoonsgegevens met een hoog privacyrisico. Dat geldt ook voor nieuwe aanbestedingen waarin sprake is van gegevensverwerking. Die taak ligt bij het lijnmanagement, omdat deze de risico's in de werkprocessen het best kan beoordelen. Om te controleren of een volledige dpia op een verwerkingsproces nodig is en mogelijk overbodige administratieve last voor lijnmanagement te voorkomen, wordt eerst een zogenoemde pre-dpia uitgevoerd.

Als de dpia afgerond is moet de FG deze fiatteren. Op moment van onderzoek waren 2 dpia's gefiatteerd:

- Cameratoezicht in de gemeentelijke gebouwen
- Sociale teams

Andere dpia's worden opgesteld, maar waren nog niet voor een fiat voorgelegd aan de FG. De SWO maakt gebruik van de integrale risico- en privacy-analyse tool (IRPA, voorheen PIA-tool) van de IBD.[23] Daarmee kunnen de risico's bij de verwerking van gegevens op de aspecten informatiebeveiliging en privacy integraal in één instrument worden onderzocht. Uit de interviews blijkt dat dat de impact assessments, daar waar ze nodig zijn, nog niet altijd uitgevoerd worden. Een dergelijke stap is wel vastgelegd in beleid en procedures, maar in de praktijk onvoldoende geborgd waardoor functionarissen op informatiebeveiliging en privacy niet altijd op tijd worden aangehaakt.

Lijnmanagement

Uit de interviews en de casestudie (zie bijlage 1) blijkt dat het lijnmanagement zich niet altijd bewust is van het feit dat zij het best bekend zijn met de werkprocessen en zo het best de risico's op informatiebeveiliging en privacy kunnen inschatten. In het strategisch informatiebeveiligingsbeleid (zie §3.2.2) is vastgelegd dat de lijn proceshouder is op informatiebeveiliging en privacy. De lijn kan het best inschatten welke risico's met

---

[22] Bijzondere persoonsgegevens zijn gegevens die zo privacygevoelig zijn dat het grote impact op iemand kan hebben als deze gegevens worden verwerkt. Het zijn gevoelige gegevens, zoals informatie over iemands godsdienst, ras, gezondheid of strafrechtelijke verleden. Daarom krijgen bijzondere persoonsgegevens extra bescherming in de AVG.

[23] Informatiebeveiligingsdienst (IBD) is onderdeel van de VNG en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.

maatregelen aangepakt moeten worden en welke risico's geaccepteerd kunnen worden. Ondersteund door de functionarissen op informatiebeveiliging en privacy. Niet iedereen in de organisatie blijkt van dit beleid en deze werkwijze doordrongen of op de hoogte.

Verwerkersovereenkomsten

In de verwerkersovereenkomsten, die onder de contracten met derde partijen liggen, waarin sprake is van verwerking van persoonsgegevens namens de gemeenten en SWO, zijn eisen op technische veiligheid en privacy opgenomen. Zo wordt bijvoorbeeld in het sociaal domein samengewerkt met veel verschillende partijen in de keten van maatschappelijke dienstverlening en zorg, waarbij sprake is van uitwisseling en verwerking van persoonsgegevens (zie ook de casestudie in bijlage 1). De verwerkersovereenkomsten die door de organisatie gebruikt worden zijn gebaseerd op de standaard van de IBD.

De verwerkersovereenkomsten worden door de Privacyofficer gecontroleerd op de privacyaspecten en de veilige verwerking van persoonsgegevens. Maar de opstart van een verwerkersovereenkomst wordt niet geïnitieerd door de privacyofficer, dat is de verantwoordelijkheid van het lijnmanagement. Uit de interviews blijkt dat de privacyofficer niet bij elk contract of verwerkersovereenkomst is aangehaakt. Zie §3.2.4 voor hoe de verwerkersovereenkomsten in de praktijk worden ingeregeld.

WPG

De Wet politiegegevens (Wpg), vanaf 2019 geldig, regelt onder andere hoe gemeenten om moeten gaan met gegevens die door en met de politie worden gedeeld. In het kader van de Wpg is elke 4 jaar een interne en externe privacy audit over de stand van zaken verplicht. De audits moeten ter controle aan de Autoriteit Persoonsgegevens worden gestuurd. In het door een externe partij opgestelde Assurance rapport Privacy audit van begin 2023, is geconstateerd dat SWO niet geheel voldoet aan de eisen die de Wpg stelt. Ook wordt geconstateerd dat SWO niet over de capaciteit met afdoende deskundigheid beschikt om de interne audits uit te voeren. Aangeraden wordt ook deze door een externe partij te laten uitvoeren.[24]

[24] Uit de ambtelijke hoor en wederhoor blijkt dat SWO dit zelf ook al had geconstateerd en daarom is voor de komende jaren in de begroting een bedrag opgenomen voor het laten uitvoeren van een interne audit door een externe partij.

3.2 Organisatie en beleid

In deze paragraaf presenteren de rekenkamercommissies de bevindingen met betrekking tot onderzoeksvraag 2.1 tot en met 2.6 op organisatie en beleid:

2.1. *Worden er systematische en actuele risicoanalyses gemaakt rond informatiebeveiliging en worden er op basis daarvan passende beheersmaatregelen genomen?*
2.2. *Biedt het informatiebeveiligingsbeleid voldoende basis voor de bescherming van gegevens?*
2.3. *Is het informatiebeveiligingsbeleid vertaald naar concrete activiteiten en zijn hiervoor voldoende middelen beschikbaar gesteld?*
2.4. *Zijn binnen de organisatie de rollen en verantwoordelijkheden voor informatiebeveiliging helder belegd? En is de organisatie qua formatie toegerust om het informatiebeveiligingsbeleid uit te voeren?*
2.5. *Wordt de raad periodiek geïnformeerd over de status van de informatiebeveiliging?*
2.6. *Is er sprake van data-ethiek: wordt er gereflecteerd op dat wat er met data gebeurt? Is er sprake van een bewuste, reflectieve omgang met data, waarin de wenselijkheid van het datagebruik en de doelen ervan wordt bevraagd?*

3.2.1 Risicoanalyses op informatiebeveiliging en beheersmaatregelen

Risicoanalyse

De BIG was tot en met 2019 de baseline met beheersmaatregelen op informatiebeveiliging voor gemeenten. De BIO, vanaf 2020 de geldende baseline voor de gehele overheid, is meer dan de BIG gebaseerd op risicomanagement. Daarvoor worden GAP-analyses gehouden om te bepalen in hoeverre de gemeente voldoet aan de maatregelen in de BIO.[25] Als er maatregelen ontbreken dient een risicoanalyse te worden uitgevoerd om te bepalen welke maatregelen met prioriteit worden opgepakt en welke risico's vooralsnog geaccepteerd worden.

Beleid

In het tactisch informatiebeveiligingsbeleid, vastgesteld in juli 2022 (zie ook §3.2.2), is een jaarplanning opgenomen om jaarlijks de GAP- en risicoanalyses uit te voeren.[26] Bij nieuwe of gewijzigde processen moeten risicoanalyse of impact assessments worden uitgevoerd. Uit de interviews blijkt dat onvoldoende structuur in de processen aanwezig is om elk jaar de GAP-analyse en (wanneer nodig) de risicoanalyse uit te voeren. Daarvoor

[25] GAP is de Engelse term voor 'kloof'. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie. GAP-analyse is de check of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn.

[26] Er is in informatiebeveiligingsbeleid sprake van drie niveaus, strategisch-tactisch-operationeel. In het strategische informatiebeveiligingsbeleid worden de uitgangspunten en verantwoordelijkheden op informatiebeveiliging beschreven. In het tactische beleid zijn er de protocollen en richtlijnen die voor de organisatie nodig zijn om het beleid te implementeren. Op operationeel niveau zijn er de werkprocessen die de strategische en tactische vereisten naar de werkvloer vertalen.

wordt een informatiemanagement systeem op informatiebeveiliging of ISMS gemist (zie §3.2.4).[27]

GAP- en risicoanalyse

Een GAP-analyse is in 2021 uitgevoerd op de BIO-maatregelen die gemeenten op informatieveiligheid moeten implementeren. Op basis van die analyse is een risicoanalyse opgesteld. In 2021, 2022 en 2023 is in het kader van de jaarlijkse ENSIA-rapportages over het voorafgaande jaar geconstateerd dat de organisatie nog niet volledig aan de eisen van de BIO voldoet.[28] Gemeld wordt dat gelet op de capaciteit en de beschikbare middelen niet alle risico's meteen kunnen worden opgepakt. De risico's die geprioriteerd aangepakt dienen te worden, worden met beheers- of veiligheidsmaatregelen getackeld in een jaarplan.

Naar aanleiding van de driejaarlijkse actualisatie van het beleid is in 2021 de visie op informatieveiligheid en privacy geactualiseerd.[29] Zie hiervoor §3.2.2.

Actieplan

Naast de GAP- en risicoanalyse van 2021 bleek uit een rondgang door de gemeentelijke gebouwen dat de organisatie ook op andere kritieke onderdelen niet voldeed aan de veiligheidseisen. Een hoog risico werd geconstateerd met betrekking tot veiligheid van (persoons)gegevens, privacy en bedrijfscontinuïteit. Naar aanleiding daarvan is in 2021 een Actieplan geformuleerd. De activiteiten die daarin zijn opgenomen betroffen onder andere het verhogen van het risicobewustzijn, aanscherpen en actualiseren van beleid en procedures, ontwikkelen van risicomanagement en implementeren van aanvullende technische beveiligingsmaatregelen.

Onder de aanvullende maatregelen zaten onder andere de verbeter-maatregelen naar aanleiding van de pentest van 2018, zoals de implementatie van SIEM/SOC, back-up en recovery en MFA. De voortgang op deze maatregelen in 2021 was beperkt, zodat veel van de maatregelen en de middelen daarvoor naar 2022 werden overgeheveld. In de update van het Actieplan van eind 2022 wordt geconstateerd dat veel van de maatregelen in 2023 zullen worden uitgevoerd. Gewezen wordt op gebrek aan capaciteit als de belangrijkste drempel voor de realisatie van de maatregelen uit het Actieplan.

Bestuurlijk gesprek

5 december 2022 hebben bestuur, directie en ambtenaren van de gemeenten en SWO een bestuurlijk gesprek met een delegatie van de VNG en de gemeente Overbetuwe over digitale veiligheid. Dat gesprek stond onder leiding van cyberburgemeester Van Rooij van Meierijstad. In het

---

27 Information Security Management System (ISMS).

28 Eenduidige Normatiek Single Information Audit (ENSIA). Audits en rapportage in verband met de horizontale verantwoording (richting gemeenteraad) en verticale verantwoording (richting landelijke toezichthouders) over de stand van zaken met betrekking tot informatiebeveiliging en privacy. Zie ook §3.2.5.

29 Visie op Informatieveiligheid & Privacy 2022-2025.

gesprek is geconstateerd dat veel zaken nog in ontwikkeling zijn en er nog geen integrale vorm van risicomanagement wordt uitgevoerd door de gemeenten en SWO. Veel van de punten uit het actieplan die nog uitgevoerd zouden moeten worden, worden aangehaald in het gespreksverslag. Ook worden een aantal zaken benoemd waar de 'punten op de i' gezet moeten worden. Zoals de omzetting van budget en menskracht van incidenteel naar structureel, monitoring en response in toezicht op het netwerkverkeer en het 'oefenen en oefenen' van de crisisorganisatie.

Risicobehandelplan

Mede op basis van het dreigingsbeeld is in 2023 het actieplan uit 2021 omgevormd tot een Risicobehandelplan 2023-2025. Dat plan is in maart 2023 opgesteld, maar nog niet vastgesteld door directie.[30] In het risicobehandelplan wordt gemeld dat door externe ontwikkelingen het huidige kritieke veiligheidsniveau een groeiende dreiging inhoudt. Aanvallers zouden succesvol kunnen zijn vanwege het ontbreken van basismaatregelen. Geconstateerd wordt dat organisatorische en technische maatregelen nodig zijn om het risiconiveau van kritisch naar medium te verlagen. Daarbij zijn prioriteiten voorgesteld op de maatregelen die uit de pentest uit 2018 en het actieplan van 2021 naar voren zijn gekomen. Daarnaast zijn ook nieuwe maatregelen voorgesteld. Zoals hard- en software update, logische toegangsbeveiliging, testen ICT-herstelplannen, security testen en beveiliging op mobiele devices. Met extra aanvullende maatregelen zou het risiconiveau naar acceptabel kunnen worden teruggebracht.

Accountant

Risico's worden ook geconstateerd bij de accountantscontroles die in opdracht van de raad worden uitgevoerd. Zie daarvoor uitgebreider §3.2.5. In 2022 zijn controllers met de accountant bij de audit meegelopen en hebben een tool voor de koppeling van systemen met Civision Samenlevingszaken bekeken, het systeem voor het sociale domein. Daar zijn risico's geconstateerd, zo blijkt uit de interviews. Uit de interviews blijk dat daar nog onvoldoende aandacht aan geschonken is, vanwege de ontoereikende capaciteit.

3.2.2 Beleid voldoende basis voor de bescherming van gegevens?

Beleid afgestemd

Het beleid van de beide gemeenten De Wolden en Hoogeveen op informatiebeveiliging en privacy is op elkaar afgestemd, omdat ze samenwerken in SWO. Vanuit SWO in 2019 is een visie op Informatie-voorziening en IT-strategie uitgewerkt. In 2020 heeft SWO een visie uitgewerkt op Dienstverlening 2021-2025 en op basis daarvan in 2022 een visie op informatiebeveiliging en privacy. Tot begin 2022 gold het informatiebeveiligingsbeleid uit 2018 dat gebaseerd was op de BIG. Het

[30] Uit de ambtelijke hoor en wederhoor blijkt dat het plan nog niet is vastgesteld in afwachting van de uitkomst van de scan op de I&A-organisatie die door M&I/Partners wordt uitgevoerd.

nieuwe Strategisch en tactisch informatiebeveiligingsbeleid, in 2022 geformuleerd, is gebaseerd op de BIO. In dat beleid zijn de uitgangspunten en de rollen op informatiebeveiliging en privacy beschreven. Het beleid moest al eerder dan 2022 aangepast worden, maar uit de interviews blijkt dat voorrang werd gegeven aan de implementatie van noodzakelijke beveiligingsmaatregelen.

Privacybeleid

Het privacybeleid uit 2018 is momenteel als bijlage bij informatie-beveiligingsbeleid opgenomen. De elementen die vanuit de AVG benodigd zijn, zoals verwerkingsregister, datalekprocedure en gepubliceerde privacyverklaring, zijn aanwezig. Het verwerkingsregister dient nog geactualiseerd te worden. Ook de rollen op strategisch en tactisch niveau zijn beschreven in het privacybeleid. Uit de interviews blijkt dat er een nieuw en organisatiebreed privacybeleid is opgesteld dat nog vastgesteld moet worden.[31]

Protocollen en procedures

Onder, of wellicht beter gesteld 'naast' het strategische informatie-beveiligings- en privacy beleid ligt het tactische en operationele beleidsdeel. Dat bestaat op tactisch niveau uit protocollen en leidraden op meer dan 40 deelterreinen op informatieveiligheid (zie onder andere afbeelding 3.1). Deze moeten op operationeel niveau uitgewerkt worden in procedures en werkprocessen (zie daarvoor §3.2.3 'Vertaling van beleid naar concrete activiteiten').

11-7-2022 en 21-4-2023

Op tactisch gebied zijn onder andere de volgende beleidsstukken geformuleerd, zoals een gedragscode, Regeling gebruik elektronische middelen, Regeling voor gebruik sociale media, Veiligheidsincidenten, beslisboom voor datalekken en een Procedure afhandeling AVG-verzoek recht op inzage. De meeste protocollen en richtlijnen op informatie-beveiliging en privacy op tactisch niveau zijn op 2 datums vastgesteld. Zo zijn op 11 juli 2022 het Anti-malwarebeleid, Back-up en recovery beleid, Logische toegangsbeveiliging beleid, E-mail- en chatbeleid, Hardening beleid, Patchmanagement beleid, Internet- en wifi-beleid, Wachtwoorden-beleid en Handboek Informatiebeveiliging en privacy en wijzigingen vastgesteld. Op 21 april 2023 zijn de Procedure autorisaties, Beveiligd ontwikkelen beleid, Websites, webapplicaties en e-mailbeveiligingsbeleid, Mobile Devices en Application Management, Classificatiebeleid, Loggingbeleid, Mobiele gegevensdragersbeleid vastgesteld. Veel van de stukken dragen een tentatief karakter, dat wil zeggen dat het de bedoeling is dat het beleid aldus geformuleerd uitgevoerd moet gaan worden en zijn neerslag nog moet krijgen in werkprocessen. In de interviews wordt

[31] Uit de ambtelijke hoor en wederhoor blijkt dat het de intentie is dit beleid in dit najaar 2023 voor te leggen ter vaststelling.

gewezen op het tekort aan capaciteit waardoor de doorvertaling van tactisch naar operationeel niveau nog grotendeels moet plaatsvinden. De

Afbeelding 3.1. Protocollen en richtlijnen op Informatiebeveiliging en privacy

Bron: IBD.

vacature voor een processpecialist op ICT staat al ruim een half jaar open. Het blijkt lastig specialisten uit de huidige arbeidsmarkt binnen te halen en te binden, met name op dit soort technische functies.

Geconstateerd wordt dat er beleidsdocumenten ontbreken die in de BIO verplicht zijn, waaronder Encryptiebeleid, Bewustwordingsprogramma en Procesautomatisering. Een Integraal bedrijfscontinuïteitsplan is in een basisversie aanwezig. Dit plan moet echter nog wel geactualiseerd en aangevuld worden om essentiële dienstverlening te kunnen garanderen. En daar wordt niet op geoefend, zo blijkt uit het verslag van het bestuurlijk gesprek (zie hiervoor §3.2.1) en wat respondenten in de interviews aangeven.

Middelen

Voor de activiteiten in het Actieplan is in 2021 eenmalig €127.000 ter beschikking gesteld. Daarvan is €119.740 overgeheveld naar boekjaar 2022, vanwege de achterblijvende voortgang. Niet alles daarvan is uitgegeven is 2022.

Voor de geprioriteerde maatregelen uit het Risicobehandelplan informatiebeveiliging en privacy 2023-2026 is becijferd dat de incidentele kosten voor 2023 €137.000 zijn en structurele kosten €209.000 bedragen. Daarvan is voor incidenteel €68.000 dekking en voor structureel €78.000. De meerkosten voor de maatregelen om het risiconiveau van kritisch naar medium te brengen bedragen voor 2023 €68.000 incidenteel en €78.000 structureel. De incidentele en structurele meerkosten voor 2024 zijn respectievelijk €32.000 en €560.000. Daarover is nog geen besluit genomen.[32]

3.2.3 Rollen en verantwoordelijkheden voldoende belegd?

Rollen en verantwoordelijkheden op informatiebeveiliging en privacy zijn uitgebreid beschreven in een bijlage bij het Strategisch Informatie-beveiligingsbeleid, mede op basis van de RASCI-tabel.[33] Daarin is vastgelegd wie verantwoordelijk is (Responsible), eindverantwoordelijk (Accountable), ondersteunend (Supportive), re raadplegen (Consultated) of te informeren (Informable). De rollen van raad, college, management, FG, CISO, ISO, PO, Controller Informatieveiligheid, en beveiligingsbeheerders op de diverse werkterreinenzijn beschreven.[34]

---

[32] Uit de ambtelijke hoor en wederhoor blijkt dat er nog geen besluit is genomen in afwachting van de in afwachting van de scan op de I&A-organisatie door M&I/Partners.

[33] Zie bij het Strategisch Beleid Informatieveiligheid & Privacy 2022-2025 - Gemeente Hoogeveen v1.0def: Bijlage 1d - Organisatie Informatieveiligheid & Privacy 2022 - SWO v6.0d; Bijlage 1e - RASCI-tabel BIO-controls Informatieveiligheid & Privacy 2022 - SWO v1.0d.

[34] Dat zijn de beveiligingsbeheerder op de applicaties voor DigID, Suwinet, BRP, BAG, BRO, BGT, WOZ, HRM, ICT en Waardedocumenten.

Bezetting informatie-beveiliging	Op informatiebeveiliging is de CISO met 0,5 fte werkzaam. De CISO is verantwoordelijk voor het opstellen en implementeren van, en toezicht houden op het informatiebeveiligingsbeleid. Hij combineert deze functie met de CIO-functie, de Chief Information Officer. De CISO valt momenteel onder de leidinggevende op bedrijfsvoering en I&A. Dat is niet de positie die de CISO volgens de IBD zou moeten hebben om onafhankelijk zijn strategische rol richting organisatie, bestuur en management goed te kunnen pakken.
Privacy	De FG-functie heeft geen vaste formatieplaats, maar is extern ingevuld met een overeenkomst van opdracht. De formatie van de Privacy Officer is in 2022-2023 uitgebreid tot 1,0 fte, namelijk 0,2 fte voor Chief Privacy Officer (CPO) en 0,8 fte voor de PO. Uit de interviews blijkt dat behoefte is aan uitbreiding op de functie van Privacy Officer.
Privacy ambassadeurs	Ter ondersteuning van de functies op privacy zijn bij een enquête medewerkers gepolst om privacy ambassadeur in de teams te worden. De ambassadeurs krijgen een training en gaan dan aan de slag onder andere als een eerste lijns-vraagbaak voor medewerkers in de teams (zie ook §3.3.2). Er was al langer sprake van om deze ondersteunende taken op informatiebeveiliging en privacy bij medewerkers in de teams te beleggen. Het ligt in de bedoeling dit in het derde kwartaal van 2023 te realiseren, melden respondenten.
Automatisering	In het team I&A is informatiebeveiliging verdeeld over meerdere rollen (1e-2e-3e lijn). Met name de netwerkbeheerders proberen zo goed mogelijk verbetermaatregelen te implementeren naar aanleiding van het actieplan, projecten, audits en opvolging vanuit monitoringssystemen. Uit de interviews en de taken die er liggen blijkt dat er genoeg werk is voor aanvullende structurele formatie van 2 fte TISO. Uit het risicobehandelplan blijkt dat die wens bij de afdeling al langer bestond.
Informatiemanagement	De ISO is recent vertrokken. In afwachting van invulling van deze vacature zijn twee ISO's tot eind 2023 ingehuurd (totaal 0,5 fte). Deze richten zich vooral op bewustwording, het opzetten en vertalen van beleid naar de concrete praktijk, vormgeving van de Business Impact Analyse (BIA) en proces op data protection impact assessments (DPIA), handhaving webbeleid en spilfunctie richting Automatisering.
I-adviseurs	Naast de CIO zijn er als aanspreekpunt op informatievoorziening momenteel drie I-adviseurs werkzaam, onder andere op het sociaal domein en het fysieke domein. Zij geven niet alleen advies over de informatie-voorziening, maar kijken ook naar aspecten als informatieveiligheid en privacy. De I-adviseur sociaal domein combineert dat met de functie

Security Officer Suwinet.[35] Er is plek voor in totaal vier I-adviseurs. Een van de voormalig I-adviseurs is aangesteld als Information Security Officer (ISO). Deze is recent vertrokken. De bezetting bij de I-adviseurs is vervolgens aangepast.

Controller Informatie-veiligheid

Vanuit het team Control heeft een medewerker Interne Audit momenteel de rol van 'controller informatieveiligheid'. Deze functionaris toetst regelmatig bij de CISO of het raamwerk van control goed functioneert en ondersteunt bij de uitvoering van audits (met name die van de accountant).[36]

Overleggen op Informatieveiligheid en privacy

De aandacht voor informatiebeveiliging en privacy is over verschillende afdelingen en functionarissen verdeeld. Er zijn verschillende overleggen waar de lijnen bijeenkomen.

Team informatiebeveiliging en privacy

Een van de interne overleggen op de betreffende terreinen is het Team Informatieveiligheid en privacy dat elk kwartaal plaatsvindt. Dat is een organisatiebreed overleg dat vier keer per jaar bijeenkomt. Daar nemen de CISO, FG, PO, I-adviseurs, Controller Informatieveiligheid en beveiligingsbeheerders aan deel. Hierin worden de belangrijkste zaken en recente ontwikkelingen op informatiebeveiliging en privacy organisatie-breed besproken.

CISO

In het beleid is opgenomen dat de CISO eenmaal per maand met de directie een overleg heeft. Uit de interviews blijkt dat dat niet gebeurt. In de praktijk staat de lijn van de CISO met directie en bestuur open, vanwege de onafhankelijke en strategische adviesfunctie van de CISO. Daar wordt door de CISO ook gebruik van gemaakt, bijvoorbeeld bij calamiteiten als het eerder genoemde Log4J-incident. Daarnaast zijn er contactmomenten zoals bij de jaarlijkse ENSIA-rapportages. Maar een maandelijks regulier overleg is er niet.

De CISO heeft structureel elke 2 weken met de PO/CPO/ISO en elke week met de tijdelijk aangestelde ISO's overleg. Een ISO overlegt elke week met medewerkers van Automatisering. Hierbij worden onder andere de incidenten besproken die medewerkers via Topdesk melden, afhankelijk van de aard van het incident. Ook aanbestedingen van applicaties op informatieveiligheid worden daar behandeld. Onderling hebben de CISO, CPO, PO, ISO en FG veel en regelmatig contact om lopende zaken te bespreken. De CISO is tevens lid van het Netwerk Cyberveiligheid Noord-Nederland.

---

35 Suwinet: Gemeenschappelijke elektronische Voorziening Suwi (Wet structuur uitvoering werk en inkomen), of GeVS, ook wel Suwinet genoemd, is een digitale infrastructuur die is ontwikkeld om ervoor te zorgen dat de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen

36 Uit de ambtelijke hoor en wederhoor blijkt dat deze medewerker inmiddels de organisatie verlaten heeft.

FG, PO, I-adviseurs

De FG heeft geen regulier overleg met de directie. Wel heeft de FG regelmatig overleg met de CISO, CPO en PO. Met de I-adviseur sociaal domein heeft de PO een driewekelijks overleg. En een tweemaandelijks overleg met alle I-adviseurs, onder andere over wijzigingsverzoeken van verwerkingsprocessen die mogelijk leiden tot een (pre-)dpia of een nieuwe verwerkersovereenkomst met een externe partij. Leiders van projecten waarin privacy een rol speelt nemen ook deel aan dat overleg.

De I-adviseurs hebben elke week onderling een overleg. Daarin worden uiteenlopend zaken besproken zoals problemen en zaken die relevant zijn voor de andere domeinen De I-adviseurs hebben maandelijks een overleg met de PO en wekelijks met de ISO. Indien nodig wordt opgeschaald naar de CISO.

Drents overleg FG

Verder nemen de FG en PO deel aan een Drents privacyoverleg. Daaraan nemen per kwartaal alle Drentse FG-en en privacyofficers van gemeenten en provincie aan deel. Dit overleg is voor kennisuitwisseling en advies op privacyaspecten in provincie brede projecten.

3.2.4 Vertaling van beleid naar concrete activiteiten

Informatieveiligheid en privacy is van alle medewerkers, niet alleen van de functionarissen zoals de CISO, FG of PO. Zo staat het beschreven in het strategisch informatiebeveiligingsbeleid. Informatiebeveiliging en privacy moeten integraal onderdeel worden van concrete activiteiten en opgenomen en op operationeel niveau beschreven worden in werk-processen. Daar gaan we hieronder op in.

Werkprocessen

Zoals hiervoor beschreven is het strategische en grotendeels het tactische beleid op informatiebeveiliging en privacy geformuleerd. Uit de interviews blijkt dat daarvan nog maar weinig is ingebed in werkprocessen. Een aantal teams is zich van deze noodzaak meer bewust dan andere teams. Deze teams zien zichzelf eigenaar van de onderdelen informatiebeveiliging en privacy binnen het werkproces. Zij zijn degenen die de risico's het best kunnen inschatten. Zo staat het ook beschreven in het beleid.

Daarbij kunnen de teams advies gebruiken van de functionarissen op informatiebeveiliging en privacy. De functionarissen zaten volgens de respondenten tot voor kort dichter op de processen in de teams. Maar door capaciteitsgebrek is dat niet meer vanzelfsprekend. Wat volgens de respondenten goed gaat is dat de medewerkers de functionarissen op informatiebeveiliging en privacy steeds beter weten te vinden.

De ervaring van een aantal respondenten is dat er ruis op de lijn is omdat de werkprocessen niet volledig op orde zijn, in ieder geval wat informatie-beveiliging en privacy betreft. Vaak wordt er te laat of helemaal niet aan gedacht om veiligheids- of privacyaspecten mee te nemen bij contract-vorming. Dan moet op het eind van een aanbesteding of wijziging van een

verwerkingsproces toch respectievelijk een verwerkersovereenkomst afgesloten worden of een dpia worden uitgevoerd. Dat werkt vertragend en is, volgens de respondenten, frustrerend voor alle betrokken partijen. Soms gaat het wel goed, zoals bij de aanschaf van het nieuwe HRM-systeem.

Verwerkingen

Bij nieuwe overeenkomsten is de verwerkingsovereenkomst vaak wel een punt van aandacht. Onder de oude overeenkomsten (voor 2018) ligt soms nog geen verwerkersovereenkomst met afspraken over informatiebeveiliging en privacy. De verwerkingen van persoonsgegevens moeten opgenomen worden in het verwerkingsregister. Dat is in 2018 samen met een externe partij opgezet en is, volgens respondenten, sindsdien niet meer goed bijgehouden.

Samenvatting casus aanvraag Wmo-voorziening (voor de volledige beschrijving zie bijlage 1)

Aanvragen voor een Wmo-voorziening (zoals huishoudelijk hulp, scootmobiel of aanpassingen aan huis) kunnen inwoners via de website doen. Via de post/telefoon of op spreekuur bij het Wmo-team (ma-do 9-17 uur, vr 9-13 uur) kan de melding ook binnen komen. De aanvraag wordt doorgestuurd naar het Wmo-team. De contact- en persoonsgegevens van de aanvrager worden geregistreerd, eventueel aangevuld met gegevens uit de gemeentelijke systemen. Dat betreft onder andere naam, BSN, geslacht, nationaliteit en burgerlijke stand. De registratie wordt in Civision Samenlevingszaken gedaan.

Daarna volgt een gesprek bij de aanvrager thuis door de Wmo-consulent. In dat gesprek komt onder andere aan bod welk probleem ervaren wordt, wat de aanvrager nog zelf kan eventueel met behulp van familie of omgeving, de woon- en financiële situatie enz. Medische gegevens worden alleen opgenomen als dat voor de verstrekking van de voorziening nodig is. Een verslag van het gesprek, met de indicatie welke voorziening nodig is, wordt gedaan in de applicatie Montr of in een Word-bestand dat in Civision Samenlevingszaken wordt opgenomen. De aanvrager kan het verslag inzien en ondertekenen. Als de aanvrager niet ondertekent volgt soms een aanpassing. Bij een afwijzing kan de aanvrager bezwaar maken.

Het ondertekende verslag en de daarop gebaseerde beschikking wordt opgeslagen in Civision Samenlevingszaken. De medewerkers zijn op basis van hun functie geautoriseerd voor toegang tot een deel van de gegevens. De autorisatiebeheerder moet 2x per jaar de autorisaties controleren en krijgt hiervoor een signaal vanuit een aparte autorisatietool (niet vanuit de applicatie CiVision Samenlevingszaken). Na afronding van de melding wordt de map met cliëntgegevens overgebracht naar het digitale zaaksysteem Decos Join.

De gegevens van de aanvrager wordt gedeeld met de externe partijen die de Wmo-voorziening verzorgen. Dat zijn onder andere Argonaut als adviseur met betrekking tot (medische) vragen, leveranciers van hulpmiddelen, zoals Meyra en Handicare en aanbieders van huishoudelijke hulp en vervoer. Het berichtenverkeer met gegevens van de aanvrager verloopt meestal via beveiligde portals. Die gegevens zijn over het algemeen de contactgegevens van de aanvrager en de voorziening die verstrekt moet worden. Medische gegevens worden alleen gedeeld als dat nodig is voor de verstrekking van de voorziening.

Als de eigen bijdrage van toepassing is, wordt dit in Civision Samenlevingszaken geregistreerd. Eens in de week worden alle wijzigingen (start of stop berichten) via het berichtenverkeer doorgestuurd naar het CAK. De medewerker verstrekt dan de naam van de cliënt, BSN en wijzigingsdatum.

Er is geen data protection impact assessment gedaan (dpia) op het proces van de Wmo-aanvraag.

'Security by design' [37]

Als de functionarissen op informatiebeveiliging en privacy en de afdeling I&A worden betrokken bij aanschaf van systemen en software gaan ze uit van 'security by design' en 'zero trust'.[38] In ieder geval bij de nieuwe contracten, maar de functionarissen zijn niet altijd in de lead of soms zelfs in het geheel niet betrokken bij de aanschaf. Bestaande contracten, waarin sprake is van toegang tot data, worden geïnventariseerd om bij verlenging aanvullend afspraken over informatiebeveiliging en privacy op te nemen. Daar is onder andere een van de ingehuurde ISO's mee bezig, in overleg de PO, I-adviseurs en CISO.

ISMS en PDCA-cyclus [39]

Het Information Security Management Systeem (ISMS) is opgenomen in het risicobehandelplan, maar is er nog niet. In een ISMS kunnen taken worden belegd, de Plan-Do-Check-Act-cyclus (PDCA) op informatiebeveiliging ingeregeld worden en kan managementinformatie gegenereerd worden. Daardoor kan onder andere de informatie die nodig is voor ENSIA makkelijk gegenereerd worden. Makkelijker dan bijvoorbeeld informatie uit verschillende systemen verzamelen. Volgens respondenten zal een ISMS voldoende structuur kunnen bieden om jaarlijks een risicoanalyse uit te kunnen voeren. De structuur op basis van ENSIA helpt daarbij, maar is onvoldoende geborgd om vaker per jaar te rapporteren over informatie-veiligheid aan management en bestuur.

Een opzet voor de systematiek van een ISMS is in concept gereed. De intentie is eerst hiermee te gaan werken om te kijken of de PDCA-cyclus goed op te zetten en te doorlopen is. Daarna zal een geschikt ISMS-systeem worden verworven, wat in de planning staat voor 2024. De CISO is in de lead bij de aanschaf ervan, ondersteund door advies van medewerkers van de afdeling I&A en de controller informatieveiligheid.

Logging [40]

Logging betekent de monitoring van een systeem waarin wordt vastgelegd wie wanneer tot welke (persoons)gegevens toegang had. In de AVG staat dit niet expliciet vermeld, maar het is meestal een noodzakelijke maatregel

---

37 Security by design betekent dat vanaf de ontwerpfase, van bijvoorbeeld software, rekening wordt gehouden met informatieveiligheid.

38 Zero trust is een veiligheidsstrategie met betrekking tot design en implementatie van software, hardware en systemen. Meestal gebruikt in verband met de strategie dat alle verkeer geverifieerd moet worden en zo min mogelijk wordt gewerkt met geprivilegieerde toegang tot gegevens en systemen.

39 Plan-do-check-act cyclus (PDCA) is de zogenoemde beleidsleercyclus.

40 Logging is een vorm van monitoring waarbij (inlog)gegevens geautomatiseerd worden geregistreerd, bedoeld om bij te houden welke gebeurtenissen/ handelingen binnen een systeem of applicatie hebben plaatsgevonden.

om bewijslast te hebben bij oneigenlijke toegang tot gegevens. Na opmerkingen in ENSIA over benodigde verbetering van de logging is in april 2023 het loggingbeleid vastgesteld.

Niet op alle systemen is logging ingesteld. Uit de interviews blijkt dat de capaciteit ontbreekt om de loggingbestanden standaard te controleren op misbruik van toegang tot gegevens en systemen. Op het moment dat oneigenlijk gebruik is geconstateerd kan wel op basis van de logbestanden vastgesteld worden wat er is gebeurd.

In het kader van ENSIA wordt voor de landelijke toezichthouder op Suwinet een zware controle uitgevoerd. Omdat in de zogenoemde Suwinet-Inkijk, veel bijzondere persoonsgegevens van inwoners worden verwerkt. Per kwartaal wordt op basis van loggingbestanden vanuit de applicatie een rapportage opgesteld met aantal raadplegingen in Suwinet-Inkijk, aantal geraadpleegde Burger Service Nummers, aantal raadplegingen binnen/buiten kantooruren en aantal inlogpogingen.[41] Als daaruit bijzonderheden uit naar voren komen kan de Security Officer Suwinet in de logbestanden mogelijk bewijsmateriaal zoeken.

Autorisaties [42]

In 2022 is het Logische Toegangsbeveiligingsbeleid vastgesteld, waarin is opgenomen dat over de autorisatieprocedure afspraken gemaakt moesten worden. In april 2023 zijn deze opgenomen in de Procedure autorisaties. Daarin is onder andere vastgelegd hoe autorisaties tot het netwerk, toegang tot de gebouwen en ruimtes, het informatiesysteem en de beveiligde mappen worden toegekend. Voor de grotere, bedrijfskritische applicaties is een autorisatietool aanwezig, die het proces van aanvragen, toekennen en controleren ondersteunt. Nog niet alle applicaties zijn in deze tool opgenomen.

Medewerkers kunnen via de tool de meeste autorisaties aanvragen op basis van de functie/rol die de medewerker heeft. Beheer van de autorisaties wordt uitgevoerd door de autorisatiebeheerder. Deze kunnen de autorisaties al dan niet toekennen naar aanleiding van de functie van de medewerker. Sommige autorisaties moeten door een leidinggevende worden aangevraagd, dat kan de medewerker niet zelf doen. De applicatie-beheerder zorgt dat de autorisaties worden ingeregeld.

Bij in- en uitdiensttreding gaat het toekennen of wegnemen van autorisaties meestal goed. Het punt is vaak of autorisaties snel worden bijgewerkt bij een functiewisseling. De autorisatietool is gekoppeld aan de personeelsadministratie, maar de huidige koppeling werkt niet optimaal.

---

41 Aantal raadplegingen binnen/buiten kantooruren was tot voor kort een sterke indicator voor een mogelijke onrechtmatigheid. Onder andere door het meer thuiswerken vanwege corona, waardoor de kantooruren minder leidend zijn, is die indicator minder sterk.

42 Autorisatiebeheer is het proces waarin een medewerker rechten krijgt op het benaderen van een bedrijfsmiddel (systeem, applicatie, gegevens of locatie).

Interne rol- of functiewijziging worden daardoor niet gesignaleerd in relatie tot de juiste autorisaties. Dat vormt nog een zwakke schakel. Respondenten geven aan dat het mis kan gaan als op basis van persoon en niet op basis van functie autorisaties worden toegekend en als een duidelijke omschrijving van de functie ontbreekt. Zo wordt nog wel eens ‘nodig voor de uitvoering van werkzaamheden’ gebruikt voor de aanvraag van de autorisatie en dat biedt te weinig houvast.

In het beleid is afgesproken dat autorisatiebeheerders twee keer per jaar de autorisaties controleren op juistheid. Zij krijgen van applicatiebeheer een lijst met gebruikers op de systemen. Als de applicatie en rollen/autorisaties binnen die applicatie opgenomen zijn in de autorisatietool, dan krijgen zowel de applicatiebeheerder als autorisatiebeheerder automatisch een signaal (1x/2x per jaar) om de autorisaties te controleren. Uit de casestudie blijkt dat autorisatiebeheerders niet altijd tijdig een signaal krijgen of op een signaal reageren (zie bijlage 1).

3.2.5 Informatievoorziening aan de raden

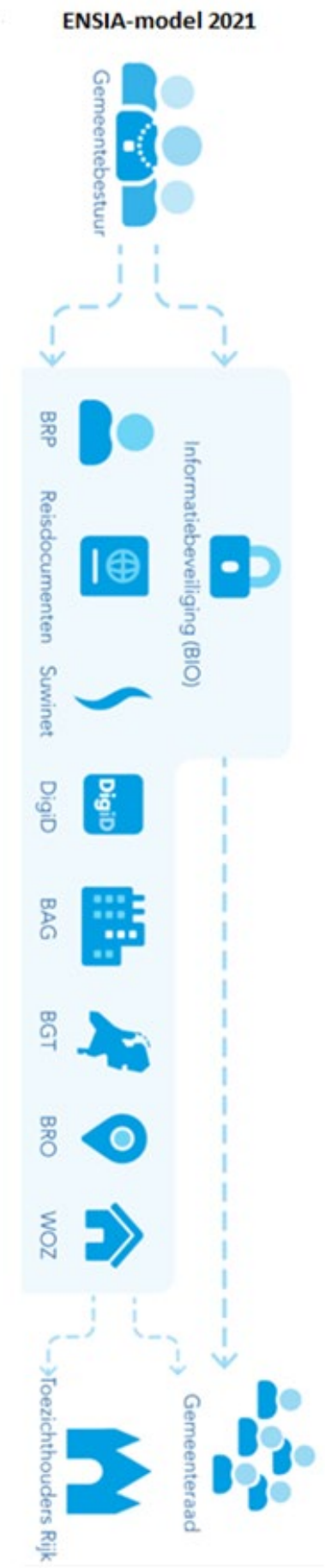
In de BIO is opgenomen dat de gemeenteraden minimaal 1x per jaar in het kader van de P&C-cyclus over de stand van zaken op informatieveiligheid geïnformeerd worden. Daarvoor is de ENSIA-rapportage bedoeld. De FG en CISO doen verslag in de jaarrekening over de stand van zaken op privacy en informatie-beveiliging. Op de rol staat een eigen-standige jaarlijkse rapportage op privacy door de FG.

ENSIA

De jaarlijkse ENSIA-rapportage ziet toe op interne en externe audits op applicaties zoals Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Over deze applicaties moet de gemeente door middel van ENSIA verant-woording afleggen richting landelijke toezichthouders. Met name aan DigiD en Suwinet worden hoge eisen met betrekking tot veiligheid gesteld. Het college moet hierover rapporteren met een assurance-statement van een extern bureau.

ENSIA-rapportage 2020

Daarnaast wordt via ENSIA aan de gemeenteraad gerapporteerd over de vorderingen op informatiebeveiliging. Zo stond in de collegeverklaring ENSIA over 2020 aan de raad dat de informatie-beveiliging DigiD en Suwinet positief was, maar dat nog niet volledig werd voldaan werd aan de eisen van de BIO. De raad is op de hoogte gesteld van elementen uit een verbeterplan, zoals structureel programma vergroten bewustzijn, aanscherping processen en procedures, toepassen MFA en verbetering logging en controle op autorisaties. Ook gaf het



college aan dat enkele zaken al werden opgepakt, zoals voorbereiding en aanschaf van een Monitoring & Respons-systeem, back-up/recovery en implementatie MFA. Extra middelen vanuit het Actieplan werden aangekondigd om te gaan voldoen aan de BIO.

ENSIA-rapportage 2021

In de aanbiedingsbrief van de ENSIA-rapportage over 2021 aan de raad, gaf het college aan te voldoen aan de normen van Suwinet en DigiD. En nog niet werd voldaan aan de eisen van de BIO en dat de basis nog niet op orde was. Het college constateerde een gestage maar onvoldoende ontwikkeling in de realisatie van het Actieplan. Een risicobehandelplan werd opgezet met onder andere activiteiten op de structurele training van bewustwording, governance (beleid en organisatie), implementeren aanvullende technische beveiligingsmaatregelen en aanscherpen diverse processen en procedures. De doelstelling werd geformuleerd om eind 2023 te voldoen aan BIO en AVG en dat informatiebeveiliging en privacy op adequaat niveau zijn geborgd.

ENSIA-rapportage 2022

In de aanbiedingsbrief over 2022, in 2023 aan de raad aangeboden, wordt summier maar wederom geconstateerd dat voldaan wordt aan de normen van Suwinet en DigiD, maar dat de basis nog niet op orde is zoals voorgeschreven door de BIO. Dezelfde verbetermaatregelen als in 2022 worden in de aanbiedingsbrief richting raad opgenomen.

Presentatie aan de raden

In oktober 2022 hebben CISO, ISO, FG en PO een presentatie verzorgd voor de raad van Hoogeveen over de risico's en succesfactoren op informatiebeveiliging en privacy, de maatregelen die intern worden genomen en het Actieplan. De presentatie aan de raad De Wolden is, in overleg met de griffier, uitgesteld in verband met de rapportage vanuit het onderhavige rekenkameronderzoek. De maatregelen zijn die de functionarissen benoemen zijn grosso modo gericht op verbeterpunten die uit de assessments, testen en audits voortkomen. Zoals bewustwording, technische beveiligingsmaatregelen, toegangsbeveiliging back-up/recovery, monitoring dataverkeer, contractafspraken met leveranciers en ketenpartners, actualisatie beleid, aanscherpen procedures en vrijmaken van mensen en middelen.

Accountant

Een andere bron van informatie voor de raad over de stand van zaken op informatiebeveiliging en privacy zijn de verslagen van de accountants-controles. Meestal geven accountants geen diepgaande analyse van de systemen en zijn de controles beperkt tot veiligheidsaspecten die met de financiële rechtmatigheid te maken hebben. Maar meer en meer reiken de controles verder, afhankelijk van de opdracht die de raden verstrekken. De accountant heeft zich over 2022 gefocust op het pakket voor het sociaal domein, financieel pakket en personeelsinformatiesysteem. Daaruit komen verbeterpunten die ook breder voor de organisatie gelden, zoals de autorisaties. Specifiek voor het financiële pakket constateert de accountant een nieuwe bevinding en twee al eerder gecommuniceerde bevindingen,

die blijkbaar niet tot verbetering hebben geleid.[43] Een daarvan is dat er geen vastgelegde controle is op de toegang door gebruikers van het financiële systeem. Dat wil zeggen dat niet te controleren is of een check op de autorisaties op het financiële systeem is uitgevoerd.

Vragen vanuit de raad

Voor zover bij de rekenkamercommissies bekend is één keer door een fractie uit de gemeenteraden vragen gesteld over informatiebeveiliging en privacy. Dat was de Christen Unie uit de gemeenteraad Hoogeveen met vijf vragen over digitale risico's. De vragen zijn oktober 2022 beantwoord.

3.2.6 Data-ethiek

Over informatiebeleid en digitale dienstverlening zijn beleidsstukken opgesteld, zoals het Informatiebeleid 2020-2022. Dat beleid kent vier strategische doelen: modern, integraal, informatiegedreven werken en flexibel & schaalbaar. En het beleid heeft vijf sporen:

1. Doorontwikkelingen dienstverlening
2. Informatiegedreven werken
3. Informatievoorzieningen op orde
4. 21e -eeuwse organisatie (digivaardig, digibewust, datavaardig en flexibel)
5. Positionering informatiemanagement en automatisering

Ethiek komt voor in het beleid, namelijk dat 'het verzamelen, combineren en ontsluiten van data […] binnen de kaders van privacywetgeving en ethiek [wordt] gedaan'. Er is geen apart geformuleerd beleid met betrekking tot de ethische kwesties die op dit onderwerp spelen.

Sociaal domein

Voor de medewerkers in het sociaal domein is door een jurist een training over de privacywet- en regelgeving gegeven. De ketenpartners van de gemeente zijn ook daarin meegenomen. Uitgangspunt is dat gegevens met derden uitgewisseld mogen worden, zolang de afweging gemaakt wordt of dat proportioneel is. Bijvoorbeeld, in het kader van de veiligheid van een kind is er meer toegestaan. Bovendien geldt dat goed moet worden vastgelegd op welke gronden die afweging is gemaakt.

Binnen het sociaal domein worden grote hoeveelheden bijzondere persoonsgegevens van kwetsbare groepen burgers door of namens de gemeenten verwerkt (zie hiervoor ook de casestudie naar de verwerking van gegevens in het kader van een Wmo-aanvraag, bijlage 1). Daar spelen prominent dilemma's rond de vergaring, verwerking en uitwisseling van gegevens.

WAMS

Deze problemen zijn bij de rijksoverheid bekend. Dat heeft geleid tot het opstellen van de Wet aanpak meervoudige problematiek sociaal domein

[43] In 1e instantie constateerde de accountant twee nieuwe bevindingen en drie eerder gecommuniceerde bevindingen die blijkbaar niet tot verbetering hebben geleid. In een later gesprek is dat gecorrigeerd en bijgesteld naar een nieuwe bevinding en twee eerder gecommuniceerde bevindingen.

(Wams). Daarin gaat geregeld worden dat informatie tussen ketenpartners gedeeld mag worden in het belang van inwoners met meervoudige problematiek. De ingang van Wams is vooralsnog gesteld op medio 2024.

Achteraf betrokken

Ook op het werkterrein van andere afdelingen en teams spelen vraagstukken op het gebied van het verzamelen, combineren en ontsluiten van data. Data-ethiek staat nog in de kinderschoenen in het beleid en de verwerking in werkprocessen, zo blijkt uit de interviews. Medewerkers weten dat ze met gevoelige informatie werken, maar uit niet iedere medewerker is daar even taakvolwassen op. Er is een data-analist bij SWO aanwezig. Als het gaat om privacyaspecten met betrekking tot informatievoorziening en -planning is met name de PO het aanspreekpunt, en op de achtergrond de FG. Aandachtspunten op privacy, maar ook informatiebeveiliging, worden nog vaak te laat bij processen betrokken. Dat vergt dan herstel- en reparatiewerk dat mogelijk voorkomen had kunnen worden.

Ook de informatieplanning in processen, dat antwoord geeft op de vraag welke informatie wanneer nodig is, staat volgens geïnterviewden in de kinderschoenen.

Drents FG-overleg

In het provinciaal overleg van FG’en is gesproken over een dataverzameling over vakantieparken in Drenthe. Daarover hebben de Drentse FG’en een negatief advies afgegeven, omdat er geen sprake was van dataminimalisatie. Dat is een van de uitgangspunten in de AVG, die voorschrijft dat er niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.

3.3 Mens en gedrag

In deze paragraaf presenteren de rekenkamercommissies de bevindingen met betrekking tot onderzoeksvraag 3.1 en 3.2 op mens en gedrag:

3.2. Zijn medewerkers zich bewust van informatiebeveiligingsrisico's en is voor medewerkers duidelijk wat van hen verwacht wordt ten aanzien van informatiebeveiliging?

3.1. Is het hogere management actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen de organisatie?

3.3.1 Bewustwording bij medewerkers van informatiebeveiligingsrisico's

Risicobewustzijn

Bewustwording van medewerkers op de risico van informatiebeveiliging is uitermate belangrijk. Respondenten melden op de vraag wat er goed gaat op het gebied van informatiebeveiliging en privacy dat de bewustwording van medewerkers de laatste jaren is toegenomen. Bekend uit onderzoek bij gemeenten in het algemeen is dat bij afdelingen en teams die al langer met (bijzondere) persoonsgegevens werken, zoals burgerzaken, sociaal domein, archief en de salarisadministratie, zijn medewerkers redelijk risicobewust. Maar er zijn ook medewerkers van afdelingen die daar minder bij stil staan. Voor een aantal medewerkers is aandacht voor informatieveiligheid iets dat afleidt en naast het dagelijkse werk erbij komt. Als de systemen of software drempels opwerpen of niet makkelijk meewerken zoeken medewerkers geitenpaadjes er omheen. En, zoals eerder aangegeven is stil staan bij de risico's op informatiebeveiliging en privacy niet overal in de werkprocessen ingebed (zie §3.2.4.)

Bijeenkomsten

De afgelopen jaren zijn enkele bijeenkomsten voor medewerkers gehouden om de bewustwording op risico's op informatiebeveiliging en privacy te vergroten. Door de FG is bijvoorbeeld een keer een cursus Juridische begrippen in het kader van privacy georganiseerd. Voor de medewerkers die met Suwinet werken komt een verplichte e-learning over het veilig gebruik ervan. Maar er is nog geen sprake van een structureel programma voor alle medewerkers. Ook komen de CISO, PO of FG niet regelmatig langs bij de afdelingsoverleggen om de onderwerpen op informatiebeveiliging en privacy te bespreken, zo blijkt onder andere uit de casestudie (zie bijlage 1).

Continu aandacht

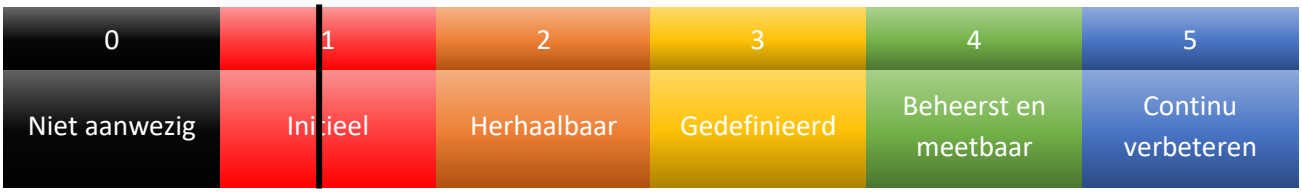
Met een frequentie van gemiddeld vijf keer per jaar worden berichten over informatiebeveiliging en privacy op intranet gepubliceerd. Respondenten geven aan dat medewerkers meer en meer met vragen komen bij de functionarissen op informatiebeveiliging en privacy. Tegelijk melden de meesten ook dat het risicobewustzijn nog niet op het gewenste niveau is, en dat er continu aandacht aan besteed moet worden.

Taakvolwassenheid op Informatieveiligheid

Zoals eerder opgemerkt moet informatiebeveiliging en privacy niet iets van de gespecialiseerde functionarissen zijn, maar een verantwoordelijkheid van de medewerkers en het lijnmanagement. De taakvolwassenheid op informatieveiligheid, dat wil zeggen de mate waarin zij bekend zijn met de protocollen en procedures en deze in de praktijk brengen, wordt vaak op een 5 puntsschaal weergegeven. NOREA, de beroepsvereniging voor IT auditors, onderdeel van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA), gebruikt de schaal zoals in bijlage 5 is opgenomen.

Uit de interviews blijkt dat de gemiddelde volwassenheid van de organisatie op informatiebeveiliging tegen 1,5 scoort. Dat wil zeggen dat er wel procedures zijn, maar onvolledig. En dat deze inconsistent en ad hoc worden uitgevoerd. Eenzelfde niveau van taakvolwassenheid wordt door respondenten op gebied van privacy ingeschat. Er zijn geen landelijke benchmarks op volwassenheidsniveau van medewerkers bij gemeenten.

Figuur 3.1. Volwassenheidsniveau informatieveiligheid.



Algemeen gesteld wordt dat een organisatie vanaf niveau 3 ‘in control’ is. Vanaf dat niveau zijn beheersingsmaatregelen gedocumenteerd en worden ze gestructureerd, geformaliseerd en aanwijsbaar uitgevoerd.

Plannen

In audits en plannen wordt eraan gerefereerd dat de gemeenten en SWO aandacht moeten besteden aan bewustwording van medewerkers. In de ENSIA rapportage over 2020 wordt gemeld dat een van de belangrijkste verbeterpunten bewustwording is, waar extra middelen voor ingezet moeten worden. In het Actieplan 2021 staat het onderwerp ook opgenomen. Bij een update van het Actieplan eind 2021 is bewustwording doorgeschoven naar 2022. In de update eind 2022 wordt gemeld dat een bewustwordingsprogramma voor het 1e kwartaal 2023 op de planning staat.

In het risicobehandelplan staat dat aandacht besteed moet worden aan structurele training van medewerkers op bewustwording. Daar wordt in de ENSIA rapportage 2022 ook aan gerefereerd. Eind 2022 in het bestuurlijk gesprek in het kader van de visitatie op informatiebeveiliging van de VNG wordt geconstateerd dat ingezet moet worden op bewustwording. Daarbij wordt gemeld dat dat breed opgevat moet worden, waaronder oefening op een cyberaanval, test phishing, mystery guest en eigenaarschap van informatieveiligheid bij directie en management. In het 2e kwartaal van 2023 was daarvoor een nulmeting en concept bewustwordingsprogramma beschikbaar, opgesteld door een extern adviesbureau. In het

Risicobehandelplan, dat voorjaar 2023 aan de directie werd voorgelegd, is bewustwording wederom als activiteit opgenomen. Uit de interviews blijkt dat het bewustwordingsprogramma in najaar 2023 zou worden opgepakt.

Belang van training

Uit de aanvullende vragenlijst bij ENSIA over 2022 blijkt dat het management niet het belang uitdraagt van deelname aan opleiding en training op het gebied van informatieveiligheid.[44] Bij 87% van de deelnemende gemeenten wordt dat belang wel uitgedragen en benadrukt door het management. Net als bij 11% van de deelnemende gemeenten zijn medewerkers niet op de hoogte van de regels en verplichtingen mbt informatiebeveiliging en de verantwoordelijkheid voor hun functie van toepassing is.

Cyberbarometer

Begin 2023 is door een extern bureau een meting gedaan naar het bewustzijn van medewerkers en leidinggevenden van SWO op informatiebeveiliging en privacy. Met 491 respondenten geeft dat een goed beeld van de beleving. Ten opzichte van de benchmark zijn er bij medewerkers lage scores met betrekking tot bewustzijn over beleid en processen op informatiebeveiliging en privacy, zelfvertrouwen in de eigen vaardigheden hierop, een veilige meldcultuur, de tijd nemen om veilig te werken en actie ondernemen bij verdachte situaties. Leidinggevenden scoren iets hoger, maar ook beneden de benchmark op 9 van de 16 onderwerpen. De helft van de leidinggevenden geeft aan onvoldoende kennis te hebben van informatiebeveiliging en privacy. Daarmee geven ze volgens de conclusies uit het rapport aan geen duidelijke voorbeeldrol te hebben. Een groot deel van de leidinggevenden geeft aan dat het team niet over voldoende vaardigheden of middelen beschikt om gedrag op informatiebeveiliging en privacy te veranderen of te stimuleren.

Activiteiten

Uit de interviews blijkt dat er wel middelen zijn gereserveerd voor bevordering van awareness bij medewerkers. Een van de extern ingehuurde ISO's gaat samen met de PO aan de slag met beleid en risicobewustzijn. Ook gaan in de teams ambassadeurs de eerstelijns vraagbaak vormen voor de medewerkers. Respondenten melden dat in het derde kwartaal voor de ambassadeurs een awareness training en twee netwerkbijeenkomsten gepland staan om de rol nader in te vullen. Ook een wethouder en een burgemeester hebben zich opgegeven.

Inwerkprogramma

Er was nog geen structurele plek voor informatiebeveiliging en privacy in het inwerkprogramma voor nieuwe medewerkers. Het ligt in de bedoeling dat deze aspecten vanaf najaar 2023 door team HRM in het inwerk-programma worden opgenomen.

Phishing mail

Een phishing mail test is erop gericht de awareness op risico's te testen. De resultaten van een phishing mail test uit 2019 was dat 41% van de mede-werkers de phishing mail heeft bekeken, dus op de mail heeft geklikt om te

[44] Zie: https://www.waarstaatjegemeente.nl/ onder het lemma Informatieveiligheid.

openen. 30% heeft op de link in de mail geklikt en heeft daarmee al een risicovolle actie uitgevoerd. Tenslotte heeft 17% het formulier met inloggegevens ingevuld. Dat is een iets hogere score dan de benchmark.

Phishing test juni 2023

In het kader van het rekenkameronderzoek is in de laatste week van juni 2023 een phishingmail-test uitgevoerd op de accounts die bij SWO en de gemeenten aanwezig zijn. In eerste instantie zou de test eerder uitgevoerd worden, maar deze is 2 weken uitgesteld. Vanwege een 'echte' phishingmail begin juni, waar medewerkers van SWO mee te maken kregen en waar een deel slachtoffer van werd.

De test betreft 1.188 mailaccounts, onderscheiden naar afdeling binnen SWO en de twee gemeenten. Naast de medewerkers zijn ook raadsleden en bestuurders van de twee gemeenten in de test meegenomen.

De mail die verstuurd werd lijkt van Microsoft te komen en lijkt een bijlage te bevatten met instructies voor een nieuw Intranet. De mail is onpersoonlijk, heeft geen aanhef en komt onaangekondigd. Als de medewerkers op de link klikken komen ze op een fake inlogpagina, met de logo's van de gemeenten De Wolden en Hoogeveen. Daar worden ze verzocht inlognaam en wachtwoord in te voeren. Doen ze dat, dan komen ze op een landingspagina waarop wordt uitgelegd dat ze 'gephisht' zijn. Ze krijgen uitleg over de test en waar ze meer informatie kunnen krijgen om phishingmails te herkennen.

In totaal heeft 12,9% van de geadresseerden op de link in de phishingmail geklikt. Van de klikkers op de link in de phishing mail heeft iets meer dan de helft, namelijk 51,6%, inloggegevens ingevoerd op de fake inlogpagina. Het resultaat van de test is lager dan de benchmark en levert een gematigd risico op. Dat resultaat is geflatteerd, omdat SWO twee weken eerder met een echte phishingmail aanval te maken kreeg. Daar is in de organisatie aandacht aan besteed, wat de alertheid bij medewerkers op phishingmails zou hebben moeten vergroten. Ook heeft een medewerker al redelijk snel na begin van de test op Intranet een waarschuwing geplaatst. Dit soort verdedigingsmechanismen werken, maar in dat licht kan 12,9% aan klikkers op de test phishingmail alsnog als redelijk veel geïnterpreteerd worden.

We kunnen overigens wel constateren dat het risicobewustzijn bij de medewerkers door de 'echte' phishingmail van begin juni is toegenomen. Zoals gezegd zijn ook de mailadressen van raadsleden van De Wolden en Hoogeveen in de test meegenomen. Van hen heeft respectievelijk 19% en 18% op de link geklikt. Dat is een hogere score dan die van de medewerkers van SWO. De raadsleden waren niet betrokken bij 'echte' phishingmail aanval van 2 weken eerder en hebben daar dus ook niet van kunnen leren.

Actie naar aanleiding van phishing

De echte phishing mail, 2 weken voor de test, heeft geleid tot actie van SWO. Er zijn aanscherpingen geweest met betrekking tot de toegangseisen via MFA.

3.3.2 Betrokkenheid bestuur en hoger management bij informatiebeveiliging

Informatiebeveiliging is een lastig bestuurlijk onderwerp. Op informatie-veiligheid worden risico's geschetst en het besef is aanwezig dat er iets mis kan gaan. Alleen weet niemand wanneer. Er moet dan geïnvesteerd worden in iets dat niet direct tastbaar is en niet direct als resultaat zichtbaar is. Uiteraard zijn er ook voorbeelden waarbij een gemeente slachtoffer van een hack is geworden en fors in de problemen is geraakt, zoals Hof van Twente.

Betrokkenheid

Urgente issues op informatiebeveiliging en privacy komen ook op de directie- en bestuurlijke tafels, bij SWO en de gemeenten. Uit de interviews blijkt dat de urgentie bestuurlijk wordt gevoeld. De CISO heeft in 2021 met de bestuurders van gemeenten en SWO een interactieve sessie gehouden over informatiebeveiliging. Ook blijkt uit de interviews dat directie en bestuur wat betreft intentie om informatiebeveiliging en privacy goed in te richten en te implementeren op één lijn zitten met de betreffende functionarissen. Het bestuur en management worden ervaren als betrokken en welwillend. Zij geven volgens respondenten aan dat ze er vertrouwen in hebben dat de functionarissen met de juiste kennis ermee bezig zijn. Een belangrijk teken van betrokkenheid is dat een burgemeester en een wethouder zich hebben aangemeld als privacy ambassadeur (zie §3.3.1). Daarmee toont de hoogste leiding dat het belang van informatiebeveiliging en privacy wordt onderkend en dragen ze het beleid actief uit.

Daarentegen blijkt uit de aanvullende vragenlijst bij ENSIA over 2022 dat de beide colleges informatieveiligheid niet opgenomen hebben als onderdeel van de collegeambities. 71% van de colleges van de deelnemende gemeenten heeft wel ambities daarop geformuleerd. De vraag of een lid van het college verantwoordelijk is voor informatieveiligheid is door beide gemeenten met 'nee' beantwoord. 98% van de gemeenten heeft wel een collegelid daarop aangewezen.

Middelen

Uit de interviews blijkt dat als een kwestie bestuurlijk geadresseerd wordt, de urgentie bestuurlijk wel gevoeld en geuit wordt. Op de bestuurstafels is dan ook de bereidheid aanwezig om extra middelen in te zetten, zij het voornamelijk incidenteel. Zoals bij de dreiging van het Log4J datalek eind 2021 of bij de aanbesteding van SIEM/SOC van de VNG. In het actieplan is voorzien in eenmalige middelen voor informatiebeveiliging. Het risicobehandelplan, met incidentele en structurele middelen ligt vanaf maart 2023 ter besluitvorming voor.

Meerdere tafels

Uit de gesprekken blijkt dat informatiebeveiliging en privacy op verschillende bestuurlijke tafels wordt besproken. Meerdere op elkaar volgende rapporten over informatiebeveiliging, waarin veel seinen op rood staan, hebben nog niet geleid tot de benodigde structurele investering ter verbetering van de situatie. In interviews wordt het beeld geschetst dat in de huidige constellatie van gemeenten en SWO de doorzettingsmacht of -kracht niet in die mate aanwezig is dat de gevoelde urgentie altijd wordt of kan worden omgezet in het vrijmaken van de benodigde middelen. Het probleemeigenaarschap van lijkt niet daardoor niet bestuurlijk gevoeld te worden. Los van de vraag of, mochten de middelen toegekend worden, de capaciteit aanwezig is deze om te zetten in de benodigde activiteiten.

Bestuurlijke reactie

Onderwerp:	Reactie op de rapportage Informatiebeveiliging en Privacy in het kader van bestuurlijke wederhoor
Datum:	26 oktober 2023

Geachte leden van de rekenkamercommissie,

De rekenkamercommissies van gemeente De Wolden en gemeente Hoogeveen hebben in gezamenlijkheid een onderzoek laten uitvoeren naar de opzet, bestaan en werking van het informatiebeveiligings- en privacybeleid in de gemeenten en de ambtelijke samenwerkingsorganisatie Samenwerkingsorganisatie De Wolden Hoogeveen (SWO). Hieronder treft u onze bestuurlijke reactie aan.

Het bestuur wil allereerst zijn waardering uitspreken voor het uitgevoerde onderzoek. Het rapport bevestigt voor een groot deel het beeld dat wij hebben van de kwetsbaarheden en uitdagingen rondom informatiebeveiliging en privacy binnen onze organisatie. Vanuit het onderzoek zijn enkele onderwerpen uitgelicht, die volgens de rekenkamercommissie specifiek aandacht behoeven voor het borgen van informatieveiligheid en privacy. Het rapport is daarmee een waardevol instrument dat ons in staat stelt de reeds ingezette acties aan te scherpen en verbeteren.

We zijn ons bewust dat er nog veel moet gebeuren. Het extreme tempo van digitalisering en dreigingen in de cyberwereld maken het enorm uitdagend én lastig voor de gemeentelijke organisatie bij te blijven en tijdig passende maatregelen te nemen. Voortdurend bewaken en bijschakelen is een vereiste.

Graag willen we benoemen dat we zowel de afgelopen jaren als op dit moment goede stappen zetten om de informatiebeveiliging en privacy te verbeteren. Vanaf 2021 zijn aanvullende incidentele en structurele middelen beschikbaar gesteld voor het vergroten van de personele bezetting, de implementatie van diverse beveiligingssystemen en ondersteuning door externe experts. Hierbij moesten we bij de ingezette acties echter wel prioriteiten stellen binnen de beschikbare capaciteit. Bovendien is in de rapporten over de organisatieontwikkeling geconstateerd dat op het gebied van digitalisering en informatisering sprake is van grote achterstanden. In de reeds in gang gezette aanpak hierop wordt momenteel een onafhankelijke scan uitgevoerd, die moet leiden tot tot een integrale aanpak.

Hieronder een toelichting op diverse acties die momenteel uitgevoerd worden.

Bij de opzet en uitvoering van het rekenkameronderzoek kon mooi aangehaakt worden bij een beveiligingstest van het netwerk door een ingehuurde ethisch hacker (een "pentest", penetratietest) die voor dit jaar bij de SWO al in de planning stond.De goede samenwerking tijdens het onderzoek heeft ervoor gezorgd dat een aantal geconstateerde risico’s direct kon worden verholpen. De meest kritische punten vanuit eerdere onderzoeken die de SWO heeft laten uitvoeren zijn inmiddels ook

opgelost. Verder heeft de SWO een risicobehandelplan opgesteld als basis voor een gestructureerde uitvoering van de vereiste maatregelen. Een belangrijke, geprioriteerde maatregel hieruit is een Monitoring & Responssysteem voor het controleren op verdachte handelingen binnen het netwerk (bijvoorbeeld door hackers). Dit systeem is opgenomen in de begroting 2024-2027. Overige elementen uit het risicobehandelplan zijn als input meegenomen in de scan op het gebied van informatievoorziening, ICT en informatieveiligheid die op dit moment wordt uitgevoerd door een extern bureau (als onderdeel van de pijler Processen & Informatie). De uitkomsten hiervan en van uw onderzoek zullen resulteren in één integraal voorstel voor verbeteringen en investeringen op het terrein van governance, organisatie, processen, houding & gedrag en techniek in een meerjarenperspectief. Daarnaast loopt een verkenning voor het extern plaatsen/outsourcen van (onderdelen van) de IT-omgeving. Het wordt namelijk steeds complexer binnen de eigen organisatie het onderhoud, beheer en de beveiliging van de eigen IT-omgeving op het gewenste niveau te houden. Het verplaatsen naar en afnemen van informatiesystemen "vanuit de cloud" is inmiddels een trend. Dit vereist echter ook andere competenties voor de eigen organisatie (van beheer naar regie).

Hieronder onze reactie op de concrete aanbevelingen van de rekenkamercommissie. We zijn hierbij niet ingegaan op aanbevelingen 11 en 12, omdat deze specifiek gericht zijn aan de raad. De reactie daarop laten wij aan de raad zelf.

1. *Beleg informatieveiligheid als aandachtsgebied bij een van de collegeleden, bij voorkeur de burgemeester, en organiseer bestuurlijke doorzettingskracht op informatiebeveiliging en privacy.*

   Dit thema is al belegd. Informatiebeveiliging en privacy maakt onderdeel uit van de portefeuille Bedrijfsvoering. De verschillende pijlers van de organisatie-ontwikkeling zijn regelmatig onderdeel van de gesprekken binnen het bestuur van de SWO, waardoor het thema informatiebeveiliging en privacy ook de komende tijd meer bestuurlijke aandacht gaat krijgen.

2. *Zorg dat procedures en richtlijnen op informatiebeveiliging en privacy in de werkprocessen worden ingebed. Daarmee wordt niet alleen op papier aan de BIO en AVG voldaan, maar ook de daadwerkelijke werking van de maatregelen in de praktijk.*

   Ook wij hebben geconstateerd dat borging binnen de werkprocessen noodzakelijk is. Naast het verankeren van informatieveiligheid en privacy moeten ook andere zaken geborgd worden, zoals rechtmatigheid. Dit is een langdurig proces vanwege de grote hoeveelheid processen en producten binnen een gemeentelijk organisatie. Dit vraagt een langjarige en gefaseerde aanpak.

3. *Positioneer de cruciale positie CISO onafhankelijk van de lijn. De Informatiebeveiligingsdienst (IBD) heeft hiervoor richtlijnen opgesteld.*

   De CISO valt functioneel al rechtstreeks onder de directie en heeft daarbij een onafhankelijke positie en rol (alleen voor HR-aspecten is deze rol gepositioneerd onder de leidinggevende

bedrijfsvoering). Bestuur en directie hebben weliswaar geen structureel overleg met de Functionaris Gegevensbescherming (FG) of Chief Information Security Officer (CISO), maar in de praktijk is er wel degelijk een directe, open lijn tussen bestuur, directie en de functionarissen van de beveiligingsorganisatie. Er wordt constructief geschakeld via korte lijnen, wat zich al heeft bewezen in crisissituaties, bijvoorbeeld tijdens de Citrix- en Log4j-incidenten[45]. Bij het anders inrichten van sturingslijnen van onze organisatie per 1 januari 2025 is nadrukkelijk oog voor de positionering van onafhankelijke posities van dergelijke functionarissen.

4. *Zorg voor voldoende kwalitatieve en kwantitatieve capaciteit op informatiebeveiliging en privacy om de ambities (zie hierna) te realiseren. Mogelijk is samenwerking hierop met omliggende gemeenten en/of provincie nodig om voldoende capaciteit of schaalgrootte te realiseren.*

   De afgelopen jaren is al geïnvesteerd in het vergroten van de capaciteit en verbetering van de rolinvulling van diverse beveiligingsfunctionarissen. Zo zijn inmiddels de capaciteit voor de CISO en (Chief) Privacy Officer verruimd naar 1 fte en is een fulltime ISO geworven, zodat regie, uitvoering en monitoring meer aandacht krijgen. De hierboven vermelde scan op het gebied van informatie-voorziening, ICT en informatieveiligheid moet input geven of en welke aanvullende capaciteit en competenties nodig zijn om verdere stappen kunnen zetten. Daarnaast wordt al nadrukkelijk samenwerking gezocht met andere gemeenten, provincies en veiligheidsregio's in Noord-Nederland, omdat alle overheidsinstanties voor dezelfde cyberuitdagingen staan.

5. *Ga verder met implementatie van een Informatiemanagementsysteem voor informatieveiligheid (ISMS). Daarmee worden activiteiten op informatiebeveiliging en privacy meer plan- en volgbaar, rapportages voor ENSIA makkelijker op te stellen en kan de PDCA-cyclus op informatiebeveiliging en privacy ingericht worden.*

   Een ISMS staat als een van de maatregelen vermeld in het risicobehandelplan. In 2024 gaan we allereerst de systematiek invoeren en daarna bekijken of er aanvullend behoefte is aan een ondersteunende applicatie om dit proces verder te ondersteunen. Eventueel volgt hierop een budgetaanvraag.

6. *Investeer in activiteiten om het risicobewustzijn van medewerkers te bevorderen en zorg dat het management de noodzaak hiervan inziet en dat uitdraagt.*

   Een belangrijke factor (zoals de rekenkamercommissie terecht aangeeft) is het vergroten van het bewustzijn met betrekking tot informatiebeveiliging en privacy bij zowel bestuur, directie en management als medewerkers. Hiervoor zijn al diverse interventies gedaan, maar we willen toewerken naar een structureel bewustwordingsprogramma. Uitdaging hierbij is de mens als risico- én succesfactor: houding en gedrag zijn niet gemakkelijk te beïnvloeden, maar het zijn wel de mensen die daadwerkelijk verbetering kunnen doorvoeren en waakzaam moeten zijn waarmee we de omstandigheden beter beheersbaar maken. Daarbij

[45] Respectievelijk in dec 2019 en dec 2021

hebben we te maken met een hoog verloop als gevolg van de huidige arbeidsmarkt, waardoor maatregelen aan de menskant lastig te borgen zijn.

7. *Maak tempo met het vervolledigen van het (tactisch) informatieveiligheidsbeleid, door de nog ontbrekende protocollen en richtlijnen vast te stellen.*

   De belangrijkste resterende tactische beleidsstukken (inclusief privacybeleid) worden binnenkort voorgelegd ter vaststelling. De afgelopen tijd hebben we bewust prioriteit gegeven aan het doorvoeren van concrete beveiligingsmaatregelen in de praktijk boven "papier". De komende periode zullen we de onderliggende protocollen en richtlijnen zo spoedig mogelijk opstellen op basis van toegevoegde waarde om de risico's te verkleinen.

Aanbevelingen aan colleges en raden

8. *Formuleer samen ambities op informatiebeveiliging en privacy. Bijvoorbeeld over welke periode de gemiddelde taakvolwassenheid van de medewerkers op een bepaald niveau moet zijn, wanneer de gemeenten aan de BIO moeten voldoen enz.*

   De komende periode staat in het teken van de basis op orde brengen. De uitkomst van de scan en het besluit hierop is van invloed op de eventuele ambities die hier bovenop gesteld kunnen worden. Te zijner tijd gaan we hierover graag met beide colleges en gemeenteraden in gesprek.

9. *Spreek samen af op welke wijze de raad geïnformeerd wordt over informatiebeveiliging en privacy. Bijvoorbeeld halfjaarlijks in een aparte raadscommissie of een commissie onder een bestaande commissie.*

   Het is gebruikelijk minimaal eenmaal per jaar de raden via een informele sessie bij te praten over de belangrijkste ontwikkelingen en stand van zaken op het gebied van informatieveiligheid & privacy. Daarnaast zijn informatiebeveiliging en privacy onderdeel van het organisatie ontwikkeltraject waarover de raad ook periodiek wordt bijgepraat. Wij gaan graag in gesprek met de raad of dit voldoende is of dat de raad voorkeur heeft voor een andere invulling.

10. *Formuleer samen beleid op data-ethiek, hoe gemeenten verantwoord omgaan met data van inwoners. De Agenda Digitale Grondrechten en Ethiek 2022-2026 van de VNG kan hierbij behulpzaam zijn.*

    We zien net als u het belang van data-ethiek. Als overheid zijn we ons bewust van zorgvuldig omgaan met en beschikbaar stellen van data. Wij geven hier al invulling aan, bijvoorbeeld door het borgen van privacy of beleggen van eigenaarschap van data bij contracten met leveranciers. Een volgende stap, na het op orde brengen van de basis, is het samen formuleren van gemeentelijk beleid.

Het is goed te beseffen dat er altijd risico's blijven bestaan. 100% veiligheid bestaat niet. Dat zullen we moeten accepteren. Wel moeten we de risico's terugbrengen tot een acceptabel niveau en ons zo goed mogelijk voorbereiden op mogelijke calamiteiten, binnen de beperkingen in capaciteit en middelen.

Tot slot:
We voelen steun met dit rapport van de rekenkamercommissie om de juiste stappen te zetten. Wij gaan verder op de ingeslagen weg en verbeteracties door eerst de basis op orde te brengen. De volwassenheid van de organisatie is nog laag, maar er worden diverse acties uitgezet om dit naar het gewenste niveau te brengen. Dit doen we aan de hand van de pijler Processen en Informatie, welke onderdeel uitmaakt van het lopende organisatie ontwikkeltraject.

Met vriendelijke groet,

het bestuur van de SWO

Nawoord

De rekenkamercommissie heeft met tevredenheid kennis genomen van de reactie van het bestuur van de SWO en het college De Wolden op de rapportage Informatiebeveiliging en Privacy in het kader van bestuurlijk wederhoor van 26 oktober 2023.

Wij lezen in de brief dat het bestuur van de SWO en het college zich grotendeels herkent in het rapport geschetste beeld van de kwetsbaarheden en uitdagingen rondom informatiebeveiliging en privacy binnen de SWO. Dit geldt voor de onderzoeksthema's techniek, de mens en organisatie & beleid.

De rekenkamercommissie waardeert het dat het bestuur per aanbeveling concreet aangeeft op welke wijze zij hier invulling aan geeft. De RKC wil hierbij enkele punten accentueren:

1. Wij vinden het uit veiligheidsoogpunt een goed idee om systemen naar de cloud te brengen. Wij willen benadrukken dat het realiseren van een goede regie- en controlefunctie een stevige uitdaging is en vragen hier aandacht voor. Het bestuur geeft aan dat het steeds complexer wordt om binnen de eigen organisatie het onderhoud, beheer en de beveiliging van de eigen IT-omgeving op het gewenste niveau te houden. Het verplaatsen naar en afnemen van informatiesystemen "vanuit de cloud" is inmiddels een trend. Dit vereist echter ook andere competenties voor de eigen organisatie (van beheer naar regie). Het bestuur geeft al aan dat men zich bewust is van het feit dat dit een andere rol vergt van gemeenten en de SWO.
2. Daarnaast vragen wij aandacht voor aanbeveling 1. Het bestuur geeft aan dat informatieveiligheid als aandachtsgebied reeds bij een van de collegeleden is belegd, terwijl uit de ENSIA-enquête van 2022 blijkt dat het niet zo was: De vraag of een lid van het college verantwoordelijk is voor informatieveiligheid is door beide gemeenten met 'nee' beantwoord. 98% van de gemeenten heeft wel een collegelid daarop aangewezen. Ook onderstrepen wij de conclusie dat er in de huidige werkwijze weinig bestuurlijke doorzettingskracht op informatiebeveiliging en privacy is.
3. Verder staat in de bestuurlijke reactie dat de onafhankelijke positie van de Chief Information Security Officer (CISO) geborgd is. De RKC denkt daar iets genuanceerder over. De CISO is voor 0,5 fte aangesteld en combineert de functie met de functie van Chief Information Officer (CIO). De cruciale functie van CISO is bij I&A gepositioneerd, wat niet in overeenstemming is met een van de lijn onafhankelijke positionering zoals door de Informatiebeveiligingsdienst (IBD) wordt geadviseerd. Dat kan een risico op ineffectiviteit met betrekking tot de strategische functie van de CISO inhouden. Het bestuur geeft aan dat hiermee rekening gehouden wordt met het anders inrichten van de sturingslijnen van de organisatie per 1-1-2025. De RKC juicht dat toe, maar pleit ervoor daar meer snelheid mee te maken.

De RKC spreekt waardering uit voor de uitstekende samenwerking met de ambtelijke organisatie, de samenwerking met de rekenkamercommissie van de Wolden en de medewerking met zowel bestuur als organisatie.

De rekenkamercommissie adviseert de gemeenteraad om over een periode van 6 maanden na behandeling van het rapport in de gemeenteraad het college te vragen naar een stand van zaken van de invulling.

Tot slot wil de rekenkamercommissie benadrukken dat iedereen een bijdrage kan leveren aan een betere informatiebeveiliging: *het grootste risico bevindt zich namelijk tussen het beeldscherm en de bureaustoel.*

Bijlage 1. Casestudie Wmo-aanvraag - concept

In deze casestudie in het kader van het rekenkameronderzoek informatie-beveiliging en privacy De Wolden en Hoogeveen gaan de rekenkamer-commissies na hoe een stuk informatie de organisatie binnenkomt, welke informatie verwerkt wordt, door wie benaderd kan worden en met welke derden wordt gedeeld. In dit geval gaat het om een aanvraag in het kader van de Wet maatschappelijke Ondersteuning (Wmo). De Wmo is bedoeld om mensen zo lang mogelijk thuis te laten wonen en maatschappelijke participatie te stimuleren. Een aanvraag kan onder andere gaan om huishoudelijke hulp, aanpassingen aan huis, een scootmobiel of vervoer in de regio.

Aanvraag

Aanvragen voor ondersteuning in het kader van de Wmo komen grotendeels bij de gemeenten binnen via de website. De inwoner kan via https://www.hoogeveen.nl/hulp-en-zorg/wmo-hulp-melden een aanvraag melden. Dan komt de aanvraag via de algemene mailbox van de gemeente binnen. De mail wordt door de afdeling DIV doorgestuurd naar de mailbox van het Wmo-team binnen de afdeling Zorg. Op de website wordt er ook naar verwezen dat de inwoner het Wmo-team telefonisch om informatie kan vragen of op het spreekuur kan binnenlopen. Het team is op maandag-donderdag van 9-17 uur en vrijdag van 9-13 uur bereikbaar. Een klein deel van de aanvragen komt via de post of via de balie van de gemeenten binnen.

De dagdienst van het Wmo-team pakt alles op wat die dag binnenkomt aan mail, telefoon, post en eventueel vragen die fysiek aan de balie binnenkomen. Nieuwe meldingen worden dezelfde dag gescreend en de melder wordt gebeld om de hulpvraag verder uit te vragen. Het kan zijn dat de melder wordt verwezen naar voorzieningen in het voorliggend veld of dat er gelijk wordt aangegeven dat de hulpvraag niet valt onder de Wmo.

Afdeling Zorg

De afdeling Zorg bestaat uit de volgende teams:

- Administratieve ondersteuning
- Backoffice (financiële administratie)
- Wmo consulenten
- Toezicht
- Contractmanagement
- Team Kinderopvang/Leerlingenvervoer

In de dagdienst zit roulerend een Wmo consulent. Momenteel loopt een pilot samen met het Klantcontactcentrum (KCC), waarbij twee medewerkers vanuit het KCC de dagdienst versterken. Zij zijn getraind op het gebied van de Wmo en draaien mee met alle voorkomende werkzaamheden binnen de dagdienst. Zij nemen echter geen besluiten, dat is de taak van de Wmo-consulenten.

Gesprek en registratie van (bijzondere) persoonsgegevens

De persoonsgegevens van de inwoner worden opgehaald uit de gemeentelijke bestanden, als die daar bekend is. Als de inwoner niet bekend is worden de gegevens van de melder/aanvrager uit Makelaar opgehaald. Makelaar is het systeem waar de afdeling Burgerzaken mee werkt. De consulenten en administratief ondersteuners kunnen in Makelaar. Civision Samenlevingszaken [46] en Makelaar zijn applicaties van Pink en aan elkaar gekoppeld.

Het gaat hierbij om de volledige persoonsgegevens, zoals naam, BSN, geslacht, nationaliteit, burgerlijke stand en adresgegevens. Deze gegevens worden aangevuld met de contactgegevens van de melder. Het BSN is een bijzonder persoonsgegeven.

Daarna volgt een gesprek bij de melder thuis met een medewerker van het Wmo-team. De volgende gespreksonderwerpen komen daar aan bod:

- Welk probleem u ervaart
- Wat u zelf kunt doen, eventueel met hulp van uw kinderen, vrienden, kennissen of anderen
- Uw woonsituatie en huishouden
- Of u zelfstandig kunt reizen
- Contacten met andere mensen
- Activiteiten buitenshuis, dagbesteding en vrijwilligerswerk
- Uw financiële situatie
- Of u al hulp ontvangt (vanuit andere wetgeving en/of organisaties)

Van het gesprek wordt door Wmo-consulenten een verslag gemaakt dat in de applicatie Montr wordt opgesteld. Sommige Wmo-medewerkers maken eerst een verslag in Word en plaatsen dat bestand in CiVision Samenlevingszaken. In het verslag heeft de consulent de indicatie opgenomen voor welke voorziening de cliënt in aanmerking komt. De cliënt tekent in principe het verslag voor gezien en gelezen. Als er haast is bij het afhandelen van de melding, kan er in overleg met de cliënt een aanvraagformulier ingevuld en ondertekend worden. Dan is een getekend gespreksverslag niet meer noodzakelijk. Als de cliënt niet ondertekent volgt

[46] Civision Samenlevingszaken is een backoffice systeem voor het sociaal domein.

er geen beschikking. Dit kan wel op verzoek van de cliënt, zodat de mogelijkheid op bezwaar tegen de afwijzing mogelijk is.

In het gespreksverslag kunnen de al geregistreerde gegevens aangevuld worden met gegevens over de woonsituatie, financiële en betaalgegevens en medische gegevens. Medische gegevens worden alleen opgenomen in het gesprekverslag als dat voor de aanvraag van toepassing is. Het gespreksverslag wordt in de applicatie Montr opgesteld. Het gespreksverslag wordt door de administratief ondersteuners (AO) vanuit Montr opgeslagen in de applicatie Civision Samenlevingszaken. AO boekt de voorziening op basis van de indicatie uit het gespreksverslag en stelt de beschikking op.

Alle documenten worden opgeslagen in een beveiligde map op de gezamenlijke Q-schijf. Binnen die map wordt voor elke nieuwe aanvraag een submap aangemaakt. Daarin worden de documenten verzameld die uiteindelijk gearchiveerd moeten worden. Op basis van de verschillende rollen kunnen medewerkers gegevens inzien.

Dat betreft het proces van de nieuwe meldingen. Als de casus is afgehandeld en de beschikking is verstuurd wordt de map met cliënt-gegevens van Civision overgebracht naar het digitale zaaksysteem Decos Join.[47] De gegevens zijn alleen toegankelijk voor de medewerkers van de afdeling Zorg.

Autorisaties

De autorisatiebeheerder, afdelings- of teamhoofd, bepaalt wie welke rol heeft en op basis daarvan worden autorisaties toegekend door de applicatiebeheerder. Binnen Civision Samenlevingszaken zijn de volgende rollen:

- Ondersteuning Zorg (Administratief ondersteuners en Wmo consulenten)
- Indicatiesteller Zorg (Wmo consulenten en administratief ondersteuners)
- Financiële administratie Zorg (backoffice)
- Toetser Zorg (toetsers binnen de afdeling)
- Post Zorg (administratief ondersteuners)

Binnen de verschillende rollen is de medewerker geautoriseerd om verschillende stappen af te handelen. Zo heeft de backoffice medewerker toegang tot betalingsgegevens, om betalingen te kunnen uitvoeren. Andere medewerkers kunnen dat niet. Dit zorgt ook voor de functiescheiding. Via procesbeheer is in te zien wie wat heeft gedaan.

De autorisatiebeheerder moet 2x per jaar de autorisaties controleren op juistheid. Deze moet dat op eigen initiatief doen, want er wordt vanuit het

[47] Decos JOIN is een applicatie voor gestructureerd opslaan, ontsluiten, bewerken en delen van (documentaire) digitale informatie.

systeem geen signaal gegenereerd wanneer het tijd is om de autorisaties te controleren.

Met welke 3e partijen wordt de informatie gedeeld

Met verschillende partijen wordt informatie gedeeld om de aanvraag te kunnen realiseren. Dat gebeurt door de administratief ondersteuners als onderdeel van de afhandeling. Zij geven de informatie van de cliënt door en hebben daarmee inzicht in de (medische) gegevens. Als financiën zijn betrokken bij de afhandeling, dan kunnen ook de backoffice medewerkers in verband met de facturen en dergelijke bij de betreffende portals, zoals bij de portal Publiek Vervoer (zie hieronder.)

De wetgever heeft een maximale bijdrage van €19 per maand gesteld voor de Wmo-voorziening. Het CAK int deze bijdrage bij de cliënt. Als de eigen bijdrage van toepassing is, wordt dit in Civision Samenlevingszaken geregistreerd. Eens in de week worden alle wijzigingen (start of stop berichten) via het berichtenverkeer doorgestuurd naar het CAK. De medewerker verstrekt dan de naam van de cliënt, BSN en wijzigingsdatum. De gegevens worden door de backoffice medewerkers beveiligd verstuurd. Als daarbij wordt aangevinkt dat de cliënt om wat voor reden dan ook de eigen bijdrage (waarschijnlijk) niet kan betalen, stelt het CAK de hoogte van de eigen bijdrage vast.

Argonaut is de partner die sociaal medisch advies geeft over de Wmo-aanvraag. Argonaut geeft advies naar aanleiding van (medische) vragen om de aanvraag/melding af te kunnen handelen. De communicatie tussen de medewerkers van de administratieve ondersteuning verloopt via de beveiligde webapplicatie Regas.[48]

Daarnaast worden gegevens gedeeld met de leveranciers van hulpmiddelen, zoals Meyra en Handicare. Met deze partijen worden de contactgegevens en het pakket van eisen gedeeld in verband met de in te zetten voorzieningen. Geen medische gegevens. Dezelfde informatie wordt gedeeld met de woningbouwcorporaties Domesta, Woonconcept en Actium. Met leveranciers, corporaties en huisartsenpraktijken wordt via de beveiligde mail Zivver gecommuniceerd.

Met aanbieders van huishoudelijke hulp en begeleiding wordt via het iWmo berichtenverkeer gegevens en de indicatie voor de beschikking gedeeld. Dat verkeer verloopt beveiligd via het Gemeentelijk Gegevensknooppunt (GGk). Via dat knooppunt verlopen ook ander verkeer, zoals in het kader van de Jeugdzorg, Wlz en Pgb. Het GGk is een beveiligde webportal waarvoor de gemeente een zogenoemd Collaboration Protocol Agreement (CPA) moet

[48] Regas is een cliëntvolgsysteem binnen zorg en welzijn.

aanvragen en eHerkenning[49] voor de medewerkers die daarop moeten werken.

Contactgegevens van de inwoner en de gestelde indicatie voor vervoer worden gemeld op de portal Publiek vervoer. Het taxibedrijf dat het vervoer regelt kan in de portal om adresgegevens op te halen en te controleren of degene een Wmo-pas heeft. En via de portal van HRC worden gegevens van de inwoners doorgegeven voor de aanmelding herstelgerichte hulp. Rapportages van HRC komen via de portal ook weer retour naar de gemeenten. Centrumgemeente voor beschermd wonen is Assen en daarmee wordt via Cryptshare beveiligd gemaild en gegevens uitgewisseld. De gemeente Assen werkte al langer met Cryptshare voor beveiligd mailverkeer en niet met Zivver. Die werkwijze is niet gewijzigd nadat SWO met Zivver is gaan. En tot slot hebben consulenten via Zivver beveiligd mailcontact met zorgaanbieders, maatschappelijk werk en collega's bij SWO voor gegevens naar aanleiding van casuïstiek (individuele gevallen).

Voor alle hiervoor genoemde portals wordt door iedere medewerker een inlognaam en wachtwoord gebruikt.

Dpia en verwerkersovereenkomst

Op processen waarin veel persoonsgegevens worden verwerkt moet in het kader van de AVG een data protection impact assessment worden gedaan Als persoonsgegevens met derden worden uitgewisseld moet er ook een verwerkersovereenkomst zijn, waarin de privacy- en beveiligingsaspecten worden geadresseerd. Er is nog geen dpia op de verwerkingsprocessen in het kader van de Wmo-meldingen uitgevoerd. Wel op de sociale teams, maar de Wmo-meldingen komen niet via dit kanaal bij de gemeenten binnen. De verwerkersovereenkomsten die bekend zijn, zijn die voor het gebruik van Zivver en de portal Publiek Vervoer.

Afdelingsoverleggen

De medewerkers van de afdeling Zorg zijn zich naar eigen zeggen bewust van de risico's op informatiebeveiliging en privacy. Voor de AVG is vanaf 2018 meerdere malen aandacht geweest. De medewerkers zijn twee jaar geleden op de AVG geschoold door Jolanda van Boven, directeur van Van Boven Juridisch Adviesbureau en gespecialiseerd in de privacywet. De bedoeling is dat er binnenkort een bewustwordingsprogramma voor informatiebeveiliging en privacy vanuit SWO wordt gestart.

[49] EHerkenning is beveiligd inlogmiddel waarmee bij verschillende dienstverleners, zoals UWV, GGk, Belastingdienst en verzekeraars ingelogd kan worden.

Privacy en informatiebeveiliging staan niet standaard op de agenda van teamoverleggen. De PO of CISO zijn nog niet langs geweest bij een teamoverleg.

Bijlage 2. Veel voorkomende termen en afkortingen

2FA	Zie MFA
Active Directory (AD)	Active Directory staat beheerders toe om het beleid (rechten en instellingen) in het netwerk van een organisatie te beheren
Applicatie	Softwareprogramma, zoals SUWInet
AVG (GDPR)	Algemene Verordening Gegevensbescherming, Europese regelgeving die de privacyregels in de Europese lidstaten harmoniseert
BIG	Baseline Informatiebeveiliging Gemeenten, maatregelen voor de informatiebeveiliging bij gemeenten, in 2013 als standaard afgesproken in VNG-verband. Deze is in 2019 vervangen door de Baseline Informatiebeveiliging Overheid (BIO)
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid. Termen waarop de beveiligingsrisico's van de informatie/applicaties zijn geënt
Blackbox pentest	Zie Pentest
CDO	Chief Data Officer
CERT	Computer Emergency Response Team, multidisciplinair samengesteld team dat kan acteren op incidenten en crises. Voor gemeenten fungeert de IBD als CERT voor de gehele sector
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cloud	De cloud staat voor een netwerk van computers die een soort 'wolk van computers' vormt, waarbij de eindgebruiker niet weet op hoeveel of welke computer(s) de software draait of waar die computers precies staan
Dataclassificatie	Betekent inzicht krijgen in de beschikbaarheid, de integriteit en de vertrouwelijkheid van de door of namens de organisatie beheerde en verwerkte informatie (BIV)
Dataminimalisatie	Is een van de uitgangspunten in de AVG, die voorschrijft dat er niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt
DigiD	Digitale Identiteit
DPIA, pre-dpia	Data protection impact assessment, analyse op risico's in verband met privacy en gegevensbescherming bij verwerkingsprocessen. Onder de AVG verplicht bij gegevensverwerking met waarschijnlijk een hoog privacy risico.
ENSIA	Eenduidige Normatiek Single Information Audit, eenmalige informatieverstrekking en eenmalige IT-audit voor de horizontale (richting gemeenteraad als toezichthouder) en verticale verantwoording (richting landelijke toezichthouders)
FG	Functionaris gegevensbescherming, verplicht voor overheden.
GAP	Is de Engelse term voor ‘kloof’. Dat betekent hier het verschil tussen de bestaande situatie en de gewenste situatie
GAP-analyse	Controle of en in welke mate de maatregelen uit de BIO geïmplementeerd zijn
GDPR	General Data Protection Regulation (zie ook AVG)
GRC	Tool om de Governance, Risk and Compliance (GRC) op informatie-beveiliging en privacy te monitoren
Greybox pentest	Zie Pentest
IAM	Zie Identity and Access management
IBD	Informatiebeveiligingsdienst voor gemeenten

ICT	Informatie- en communicatietechnologie
Identity and Access management (IAM)	IAM regelt dat de juiste medewerkers het juiste toegangsniveau hebben tot de netwerken en de daarin opgeslagen of verwerkte gegevens. Gebruikersrollen en toegangsrechten worden via een IAM-systeem gedefinieerd en beheerd.
ISMS	Information Security Management System
Logging	In bestanden vastleggen welk dataverkeer over een netwerk gaat. Zo wordt onder andere vastgelegd wie toegang had tot welke persoonsgegevens.
MFA	Multi factor authenticatie is een authenticatie of verificatie methode waarbij twee of meer stappen succesvol doorlopen moeten zijn om ergens toegang tot te krijgen, zoals naast het gebruik van een wachtwoord het gebruik van een token of biometrisch gegeven
NBA	De koninklijke Nederlandse Beroepsorganisatie van Accountants
NOREA	De Nederlandse Organisatie van Register EDP-Auditors
P&C-cyclus	Planning & Control cyclus
PDCA	Plan-Do-Check-Act beleidsleercyclus
Pentest	Een pentest of penetratietest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden gebruikt kunnen worden om in deze systemen in te breken. Een white box test is een teststrategie waarbij de ethische hackers kennis hebben van de technische infrastructuur en systemen en met behulp van die kennis technische zwakheden trachten op te sporen. Dit in tegenstelling tot black- of greybox testen, waarbij de hackers vooraf respectievelijk geen of beperkte kennis hebben van de systemen
Phishing mail	Vorm van internet oplichting en fraude, door middel van een vals e-mail bericht 'hengelen' naar inlog- of andere persoonsgegevens
PO	Privacy officer
Role based access control (Rbac)	Concept waarmee toegang tot gegevens en systemen geschiedt op basis van rollen en functies van de medewerkers. Dat is het concept waarmee Identity Access Management (IAM) wordt uitgevoerd.
SAAS	Software-as-a-Service, is een model waarbij softwaretoepassingen via internet worden aangeleverd.
SIEM/SOC	Security Information & Event Management (SIEM) en Security Operations Center (SOC) is software die computerdreigingen en verdacht verkeer op systemen detecteert en monitort.
Social engineering	Social engineering is een techniek waarbij een aanval op de computerbeveiliging via het verkrijgen van vertrouwelijke of geheime informatie (van personen).
SSO	Single Sign On, op 1 werkplek via 1 aanmelding toegang krijgen tot alle applicaties waar de gebruiker recht op heeft
Suwinet	Gemeenschappelijke elektronische Voorziening Suwi (Wet structuur uitvoering werk en inkomen), of GeVS, ook wel Suwinet genoemd. Is een digitale infrastructuur die is ontwikkeld om ervoor te zorgen dat de Suwipartijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen
TISO	Technical Information Security Officer
TPM	Third Party Memorandum. Verklaring dat de derde partij, die de gegevens voor de gemeente bewerkt voldoet aan de geldende richtlijnen over informatiebeveiliging
Verwerkingsregister	Register waarin de gemeente bijhoudt welke persoonsgegevens de gemeente en de verwerkers die deze inschakelt verwerkt

VNG	Vereniging Nederlandse Gemeenten
VNG Realisatie	Kwaliteitsinstituut van de VNG (voorheen KING)

Bijlage 3. Lijst geraadpleegde stukken en lijst respondenten

Geraadpleegde stukken

- 20210420 Collegeverklaring ENSIA 2020 - Informatiebeveiliging DigiD en Suwinet - Hoogeveen v1.0def – ondertekend
- 20210420 Voorstel B&W Hoogeveen - Collegeverklaring ENSIA 2020 en rapportages BAG-BGT-BRO-Reisdoc-BRP v1.0def
- 20210430 Voorstel BenW Hoogeveen - Collegeverklaring ENSIA 2020-Informatieveiligheid - brief raad v1.0def
- 20210518 Aanbiedingsbrief raad Hoogeveen - Informatieveiligheid-Collegeverklaring ENSIA 2020 v2.0def
- 20230411 Voorstel B&W Hoogeveen - Collegeverklaring ENSIA 2022 en verantwoordingsrapportages v1.0def
- 220405 Collegeverklaring ENSIA 2021 inzake Informatiebeveiliging DigiD en Suwinet - Hoogeveen – ondertekend
- 220405 Voorstel B&W Hoogeveen - Collegeverklaring ENSIA 2021 en rapportages BAG-BGT-BRO-WOZ-Reisdoc-BRP v1.0d
- Aanbiedingsbrief raad Hoogeveen - Beleid Informatieveiligheid & Privacy v1.0def
- Aanbiedingsbrief raad Hoogeveen - Informatieveiligheid-Collegeverklaring ENSIA 2021 v2.0d
- Aanbiedingsbrief raad Hoogeveen - Informatieveiligheid-Collegeverklaring ENSIA 2022 v1.0def
- Analyse BIO 2021
- Anti-malware beleid - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Assurance rapport - Privacy audit Wpg
- Back-up en recovery beleid - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Basis SLA - HGV-DWD-SWO met CE-matrix v1.0c
- Bedrijfscontinuïteitsplan Bijlage 1 - Contactgegevens Intern Crisisbeheerteam (ICBT) v1.0def
- Bedrijfscontinuïteitsplan Bijlage 2 - Overzicht kritische processen - SWO-HGV- DWD v1.0def
- Bedrijfscontinuïteitsplan Bijlage 3 - Contactgegevens derde partijen bij calamiteiten v1.0def
- Bedrijfscontinuïteitsplan Bijlage 4 - Overzicht vergaderlocaties crisisteams v1.0def
- Bedrijfscontinuïteitsplan Bijlage 5 - Vereiste voorzieningen bij calamiteit v1.0def
- Bedrijfscontinuïteitsplan Bijlage 6 - Uitwerking uitwijkscenarios v1.0def
- Bedrijfscontinuïteitsplan Bijlage 7 - Basis draaiboek Crisiscommunicatie v1.0def
- Bedrijfscontinuïteitsplan Samenwerkingsorganisatie De Wolden Hoogeveen v1.0def
- Begroting risicobehandelplan Informatieveiligheid & Privacy 2023-2026 v1.0c
- Beslisboom datalek v1.0d
- Bestuurlijk gesprek Digitale Veiligheid - Onderwerpen en toelichting v1.0c
- Beveiligd ontwikkelen beleid Informatieveiligheid & Privacy 2022 - SWO v1.0def
- Beveiligingsbeleid SUWI Informatieveiligheid & Privacy 2022 - SWO v1.0def
- Bijlage 1f - Toewijzing rollen organisatie Informatieveiligheid & Privacy 2022 - SWO v7.0def
- Classificatie bedrijfskritische systemen v1.0def
- Classificatie beleid Informatieveiligheid & Privacy 2022 - SWO v1.0def
- Collegeverklaring ENSIA 2022 - Informatiebeveiliging DigiD en Suwinet - Hoogeveen-getekend
- Contacten met overheidsinstanties - Informatieveiligheid & Privacy 2022 - SWO v1.0
- De Wolden Hoogeveen - MS Cloud Security Assessment v1.0

- Dreigingsbeeld - 2023 SWO 1.0def
- DW en HGV Rapportage Controle Suwinet
- E-mail en chat beleid (inclusief NTA 7516) - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Eyesight Report - Website gemeente Hoogeveen
- Gedragscode 2020 SWO – Personeelshandboek
- GIBIT 2020
- GIBIT 2020 Addendum GIBIT 2020 - SWO De Wolden Hoogeveen v2.0def
- GR regeling gebruik elektronische middelen – Personeelshandboek
- Handboek IBP in projecten en wijzigingen - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Hardening beleid - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Hoofdproces veiligheidsincidenten
- Informatiebeleid SWO 2020-2022 v1.0def
- Informatieveiligheidsanalyse 2021 De Wolden Hoogeveen 1.0def
- Internet en wifi beleid (incl. buitenlocaties) - Informatieveiligheid & Privacy 2022 - SWO v1.0
- ISMS SWO v0.9c
- Logging beleid Informatieveiligheid & Privacy 2022 - SWO v1.0def
- Logische toegangsbeveiliging beleid - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Mobiele gegevensdragers beleid Informatieveiligheid & Privacy 2022 - SWO v1.0def
- Mobile Device en Application Management - SWO v1.0def
- Observaties IT SWO - Deloitte v0.7c
- Organisatie Informatieveiligheid & Privacy 2022 - SWO v6.0d
- Overzicht verwerkte persoonsgegevens v0.1c
- Patchmanagement beleid - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Phishing campagneresultaten
- Presentatie Informatieveiligheid & Privacy - RKC HGV v0.1c
- Presentatie Informatieveiligheid & Privacy met toelichting - Gemeenteraad Hoogeveen v1.0def
- Presentatie Stand van zaken informatieveiligheid & Privacy - Colleges en Bestuur SWO v1.0def
- Privacybeleid 2023-2025 - SWO v1.0def
- Procedure afhandeling AVG-verzoek recht op inzage v0.6c
- Procedure autorisaties SWO v1.0def - v RKC
- Projectopdracht Actieplan Informatieveiligheid - PI-270 v2.0d
- Rapportage - Cyber Barometer 2023 - SWO De Wolden Hoogeveen (Brooklyn Partners 20230313)
- Rapportage Forensisch Onderzoek - SWO - Schippers IT
- RASCI-tabel BIO-controls Informatieveiligheid & Privacy 2022 - SWO v1.0d
- Reactie op schriftelijke vragen digitale risico's - ChristenUnie Hoogeveen v1.0def
- Regeling voor gebruik sociale media – Personeelshandboek
- Risicobehandelplan Informatieveiligheid & Privacy - SWO 2023-2025 v1.0def
- Samenwerkingsorganisatie De Wolden Hoogeveen - MSO-Scan-v1.1
- Strategisch Beleid Informatieveiligheid & Privacy 2022-2025 - Gemeente Hoogeveen v1.0def
- Tactisch Beleid Informatieveiligheid & Privacy 2022-2025 - SWO v1.0def
- Veiligheidsbeleid kantoorgebouwen en buitenlocaties SWO v1.1def
- Verwerkersovereenkomst Addendum - Basis Privacybepalingen voor contract v2.0c
- Verwerkersovereenkomst of Contractuele bepaling privacy 2.0c
- Visie op Informatieveiligheid & Privacy 2022-2025 - Gemeente Hoogeveen v1.0def
- Voortgangsrapportage Actieplan Informatieveiligheid

- Wachtwoord beleid - Informatieveiligheid & Privacy 2022 - SWO v1.0
- Websites, webapplicaties en e-mailbeveiliging beleid Informatieveiligheid & Privacy 2022 - SWO v2.0def

Functies respondenten

- Gemeentesecretaris De Wolden
- Gemeentesecretaris Hoogeveen
- CISO
- Privacy officer
- FG
- Controller Informatieveiligheid
- Medewerker afdeling I&A/ICT
- Hoofd Afdeling I&A/ICT
- I-adviseur sociaal domein, security officer Suwi
- Teamleider Zorg

Bijlage 4. Onderzoeksvragen en normen

De onderstaande normen zijn voornamelijk ontleend aan de BIO en de AVG.

Onderzoeksvragen	Normen
4. Techniek	
4.1. Zijn het netwerk en de bedrijfskritische systemen voldoende technisch beveiligd om ongeautoriseerde toegang te voorkomen?	- Er is een up-to-date overzicht van systemen, applicaties en dergelijke, waarin de gemeente informatie verwerkt - De gemeente heeft afdoende technische maatregelen getroffen om ongeautoriseerde interne en externe toegang te voorkomen. - De gemeente laat jaarlijks testen en audits uitvoeren om de beveiliging van de systemen te testen.
4.2. Is er extra aandacht voor de technische beveiliging van gevoelige informatie, zoals persoonlijke gegevens?	- De gemeente heeft voldoende aanvullende technische beheersmaatregelen genomen om risico's ten aanzien van de bescherming van gevoelige informatie (waaronder persoonsgegevens) te waarborgen.
5. Organisatie en beleid	
5.1. Worden er systematische en actuele risicoanalyses gemaakt rond informatiebeveiliging en worden er op basis daarvan passende beheersmaatregelen genomen?	- Er worden met voldoende frequentie risicoanalyses uitgevoerd. In de risicoanalyses zijn de belangrijkste risico's geïdentificeerd. De risicoanalyses geven ook inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens - Relevante beheersmaatregelen worden vastgesteld op basis van good practices, zoals de BIO. - Het totaal aan maatregelen geeft voldoende waarborgen voor een goede bescherming van de (bijzondere) persoonsgegevens die de gemeente in beheer heeft
5.2. Biedt het informatiebeveiligingsbeleid voldoende basis voor de bescherming van gegevens?	- De gemeente beschikt over een actueel overkoepelend informatiebeveiligingsbeleid dat op onderdelen is uitgewerkt in specifieke procedures en/of richtlijnen. - De inhoud van het informatiebeveiligingsbeleid sluit aan op good practices, zoals de BIO en relevante wet- en regelgeving (zoals de AVG). - In het informatiebeveiligingsbeleid is beschreven hoe invulling wordt gegeven aan de PDCA-cyclus rond informatiebeveiliging. - Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld. - De gemeente classificeert de informatie die zij verwerkt naar mate van beschikbaarheid, integriteit en vertrouwelijkheid
5.3. Is het informatiebeveiligingsbeleid vertaald naar concrete activiteiten en zijn hiervoor voldoende middelen beschikbaar gesteld?	- De gemeente beschikt over een actueel informatie-beveiligingsplan met concrete activiteiten om nader invulling te geven aan diverse onderdelen van het informatie-beveiligingsbeleid. Op basis van de activiteiten is er een urenraming en budget op. - De gemeente besteedt 10% van het ICT-budget aan maatregelen ter bevordering van informatieveiligheid. - De gemeente beschikt over procedures en of richtlijnen waarin diverse onderdelen van het informatiebeveiligingsbeleid nader invulling hebben gekregen.
5.4. Zijn binnen de organisatie de rollen en verantwoordelijkheden voor informatiebeveiliging helder belegd? En is de organisatie qua formatie toegerust om het informatiebeveiligingsbeleid uit te voeren?	- Taken en verantwoordelijkheden rond informatiebeveiliging en de bescherming van (bijzondere) persoonsgegevens zijn duidelijk belegd in de organisatie. - De functionarissen op informatiebeveiliging en privacy zijn goed gepositioneerd om hun rol te kunnen vervullen. - Loopt de formatie van de bij informatiebeveiliging betrokken afdeling(en) in de pas met organisaties van gelijke omvang?

5.5. Wordt de raad periodiek geïnformeerd over de status van de informatiebeveiliging?	- Het college legt verantwoording af over het informatiebeveiligingsbeleid, de gemaakte afspraken en geplande activiteiten, i de BIO. - De raad kan zijn kaderstellende en controlerende rol invullen.
5.6. Is er sprake van data-ethiek: wordt er gereflecteerd op dat wat er met data gebeurt? Is er sprake van een bewuste, reflectieve omgang met data, waarin de wenselijkheid van het datagebruik en de doelen ervan wordt bevraagd?	- In de organisatie is beleid op datagedreven werken geformuleerd. - In de organisatie en beleid is bij het gebruik van data aandacht voor drie vragen: Kan het? (technisch) Mag het? (juridisch) Wil ik het? (ethisch)
6. Mens en Gedrag	
6.1. Zijn medewerkers zich bewust van informatiebeveiligingsrisico's en is voor medewerkers duidelijk wat van hen verwacht wordt ten aanzien van informatiebeveiliging?	- Alle medewerkers gaan bewust en veilig om met vertrouwelijke informatie. De regels wat betreft vertrouwelijkheid, integriteit, beschikbaarheid en privacybescherming worden nageleefd. - De gemeente zorgt ervoor dat iedere medewerker goed op de hoogte is van de regels, de risico's en de plicht om incidenten en datalekken te melden.
6.2. Is het hogere management actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen de organisatie?	- Directie en bestuur stellen zich duidelijk achter het informatiebeveiligingsbeleid, vervullen een voorbeeldfunctie en informeren en motiveren medewerkers om het beleid actief gestalte te geven.

Bijlage 5. Volwassenheidsniveau NOREA

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

Niveau	Naam	Omschrijving	Indicatieve criteria
1	Initieel	Beheersingsmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersingsmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersingsmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersingsmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersingsmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersingsmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersingsmaatregelen worden gebenchmarkt en zijn 'Best Practice' in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.