Informatieveiligheid in Opsterland: Tussen ambitie en uitvoering

Rekenkameronderzoek naar beleid, uitvoering en bestuurlijke grip op digitale veiligheid

OPSTERLAND

Inhoudsopgave

Bestuurlijke nota

Samenvatting

Gemeenten zijn steeds afhankelijker geworden van digitalisering; elk gemeentelijk proces kent wel een digitaal component. Daarom neemt ook het belang van informatieveiligheid toe. De Rijksoverheid en Europa dringen met Richtlijnen en wetgeving aan op digitaal veilige gemeenten. De Europese ‘Network and Information Security-directive’ (NIS2 richtlijn) is bedoeld om de cyberbeveiliging en de weerbaarheid van ‘essentiële diensten’, waaronder lokale overheden, in de EU-lidstaten te verbeteren. Op dit moment wordt de richtlijn naar Nederlandse wetgeving vertaald. De bepalingen worden opgenomen in de Cyberbeveiligingswet. Dit houdt in dat digitale veiligheid een plicht wordt voor gemeenten. Vanwege het toegenomen belang van digitale veiligheid en de aanvullende verplichtingen voor gemeenten, hebben de rekenkamers van de gemeenten Opsterland, Weststellingwerf en Ooststellingwerf hier onderzoek naar gedaan. Dit onderzoek is uitgevoerd van september 2024 tot december 2025.

Het doel van het onderzoek is om in beeld te brengen of de informatiebeveiliging adequaat is georganiseerd en geborgd bij de OWO-gemeenten en in hoeverre de gemeenteraden in positie zijn om hun taken uit te voeren. De volgende vraag staat centraal in dit onderzoek:
Is de informatiebeveiliging van de OWO-gemeenten adequaat georganiseerd en geborgd?

Beleid en uitvoering in Opsterland

De gemeente Opsterland werkt op het gebied van ICT en informatiebeveiliging samen met Ooststellingwerf en Weststellingwerf in het samenwerkingsverband OWO. Binnen deze samenwerking is Team ICT verantwoordelijk voor de uitvoering van technische beveiligingsmaatregelen, zoals firewalls, monitoring, back-ups en het beheer van applicaties. Grote applicaties worden centraal beheerd, terwijl kleinere applicaties onder de verantwoordelijkheid van de afzonderlijke gemeenten vallen. Er is nog geen volledig overzicht van wie waarvoor verantwoordelijk is, maar hier wordt aan gewerkt.

Opsterland heeft een strategisch informatiebeveiligingsbeleid opgesteld op basis van het format van de Informatiebeveiligingsdienst (IBD).
Dit beleid is actueel, maar algemeen van aard en sluit onvoldoende aan op de specifieke situatie van de gemeente. De gemeente voldoet nog niet aan de BIO-normen en werkt aan een implementatieplan om de BIO2-norm te behalen. De uitvoering van maatregelen is versnipperd en een integrale aanpak ontbreekt.

De gemeente voert jaarlijks een ENSIA-audit uit en beschikt over een datalekregister. In het strategisch beleid is vastgelegd dat incidenten worden gebruikt om beleid te verbeteren, maar in de praktijk gebeurt dit nog onvoldoende. Medewerkers weten vaak niet goed hoe ze een datalek moeten herkennen of melden, ondanks het bestaan van een datalekprotocol.

De gemeente benoemt de PDCA-cyclus als uitgangspunt, maar deze wordt in de praktijk beperkt toegepast. Buiten de ENSIA-rapportage zijn er geen concrete verbeterplannen of structurele evaluaties. De opvolging van audits en risicoanalyses is beperkt en niet goed gedocumenteerd.

Binnen de organisatie zijn de rollen en verantwoordelijkheden formeel vastgelegd volgens het Three Lines of Defence-model. In de praktijk zijn veel taken belegd bij teamleiders, wat leidt tot werkdruk en onduidelijkheid. De CISO en FG zijn onafhankelijk gepositioneerd, maar onvoldoende zichtbaar binnen de organisatie.

Op het gebied van bewustwording worden activiteiten georganiseerd, zoals lezingen en de wekelijkse Digiheld-vraag. Deelname is echter niet verplicht en er is geen vaste planning. Nieuwe medewerkers krijgen een onboardingstraining, maar voor zittende medewerkers zijn er nauwelijks structurele trainingen. Het kennisniveau over informatieveiligheid is laag.

De crisisorganisatie is nog niet goed ingericht. Er is geen actueel crisisprotocol en er wordt niet periodiek geoefend.
In 2024 vond een OWO-brede crisisoefening plaats, maar het is onduidelijk wat Opsterland met de uitkomsten heeft gedaan. De PDCA-cyclus wordt op dit vlak niet toegepast.

Rol van de gemeenteraad

De gemeenteraad van Opsterland ontvangt jaarlijks rapportages over informatieveiligheid, zoals de ENSIA-audit. Toch is de betrokkenheid beperkt: er worden weinig vragen gesteld en de opkomst bij bijeenkomsten is laag. Raadsleden vinden het onderwerp vaak te technisch en missen inzicht in risico's en bestedingen. Er is behoefte aan duidelijke, periodieke informatie en aan opname van digitale veiligheid in het inwerkprogramma voor nieuwe raadsleden. Raadsleden nemen nog niet deel aan bewustwordingsactiviteiten, terwijl zij wel met vertrouwelijke informatie werken.

Belangrijkste bevindingen

- **Beleid:** Opsterland heeft een strategisch informatiebeveiligingsbeleid gebaseerd op het IBD-format, maar dit is algemeen en niet afgestemd op de eigen organisatie. De gemeente voldoet nog niet aan de BIO-normen en is onvoldoende voorbereid op de BIO2-standaarden.
- **Uitvoering:** Team ICT voert technische taken uit zoals monitoring, firewalls en back-ups. De verdeling van verantwoordelijkheden is onduidelijk en er is geen structureel overleg tussen Team ICT en de CISO's. De gemeente voert zelf geen pentesten uit.
- **Incidenten:** Er zijn procedures voor het melden van datalekken en een datalekregister. Medewerkers weten echter niet altijd hoe ze een datalek moeten herkennen of melden. Incidenten worden niet structureel gebruikt om beleid of processen te verbeteren.
- **PDCA-cyclus:** De PDCA-cyclus wordt in beleid genoemd, maar is in de praktijk nauwelijks zichtbaar. Alleen de ENSIA-audit wordt jaarlijks uitgevoerd. Er zijn geen concrete verbeterplannen of structurele evaluaties.
- **Bewustwording:** Er zijn activiteiten zoals lezingen en de Digiheld-vraag, maar deze zijn niet verplicht. Deelname wordt niet gemonitord en het kennisniveau is laag. Nieuwe medewerkers krijgen een onboardingstraining, maar voor zittende medewerkers zijn er nauwelijks structurele trainingen.
- **Crisisorganisatie:** Er is geen actueel crisisprotocol en er wordt niet periodiek geoefend. In 2024 vond een OWO-brede crisisoefening plaats, maar het is onduidelijk wat Opsterland met de uitkomsten heeft gedaan. De PDCA-cyclus wordt ook op dit vlak niet toegepast.
- **Rol van de raad:** De gemeenteraad ontvangt rapportages zoals de ENSIA-audit, maar stelt weinig vragen. Raadsleden vinden het onderwerp vaak te technisch en missen inzicht in risico's en bestedingen. Er is behoefte aan duidelijke, periodieke informatie en training.

Conclusies en aanbevelingen

Hieronder presenteren wij de conclusies en aanbevelingen van dit onderzoek in de gemeente Opsterland.

Conclusies

De gemeente Opsterland is verantwoordelijk voor het informatiebeveiligingsbeleid, maar de uitvoering daarvan vindt sinds 2012 voor een belangrijk deel plaats in OWO verband. Deze samenwerking levert belangrijke schaalvoordelen op, maar de taakverdeling tussen het samenwerkingsverband en de gemeente Opsterland is niet op alle onderdelen duidelijk. Zo ontbreekt de structurele afstemming tussen de CISO's van de drie OWO gemeenten en het samenwerkingsverband. Ook hebben de drie OWO gemeenten los van elkaar trainings- en bewustwordingsactiviteiten ingekocht en uitgevoerd. Dit komt de effectiviteit van de samenwerking niet ten goede. Na de onderzoeksperiode zijn plannen voor uitbreiding van de samenwerking gepresenteerd om de doelmatigheid en doeltreffendheid van beleid en uitvoering te vergroten.

In Opsterland is het format van de Informatie Beveiligings Dienst (IBD) van de VNG gebruikt voor het strategisch informatiebeveiligingsbeleid. Hierdoor ontbreekt de koppeling met de werkpraktijk. Het beleid is in algemene termen beschreven en niet toegespitst op de eigen gemeentelijke organisatie. Wel sluit het beleid aan op de gangbare normen voor de gemeentelijke overheid. Zo wordt de Baseline Informatieveiligheid Overheid (BIO) als uitgangspunt van het beleid genomen. Opsterland voldoet echter niet aan deze norm, maar dit is wel een belangrijke doelstelling. De BIO norm wordt onder de Cyberbeveiligingswet vervangen door de BIO2 en verplicht gesteld.

De gemeente heeft het afgelopen jaar de ENSIA-verklaring gekregen. Dit betekent dat een externe auditor heeft vastgesteld dat de gemeente voldoet aan de veiligheidseisen van stelselhouders bij de Rijksoverheid voor het gebruik van hun applicaties. Hier voldoet Opsterland aan de gestelde norm.

Uit het onderzoek komt naar voren dat de gesproken medewerkers van de gemeente Opsterland het belang van digitale veiligheid onderkennen, maar dat er verbetering mogelijk is. Zo geven deze medewerkers aan dat de CISO en FG niet goed zichtbaar zijn in de organisatie en is er in het lijnmanagement te weinig aandacht voor digitale veiligheid, waardoor het onvoldoende is geborgd in de werkprocessen.

Opsterland is zelf verantwoordelijk voor de digitale weerbaarheid van de eigen medewerkers door middel van trainings- en bewustwordingsactiviteiten. Er worden wel diverse activiteiten aangeboden, maar deelname is vrijblijvend. Een gestructureerde aanpak van activiteiten en opleiding, voor zowel nieuwe als zittende medewerkers zal de digitale veiligheid in de gemeente versterken. Als de drie OWO gemeenten dit gezamenlijk oppakken, zijn ook hier schaalvoordelen te halen.
In het beleid wordt risicomanagement genoemd als uitgangspunt voor sturing op digitale veiligheid door het gemeentebestuur. Maar in de praktijk stuurt het college van b. en w. onvoldoende op veiligheidsrisico's. Ook de gemeenteraad stuurt onvoldoende op digitale veiligheid. De gemeenteraad wordt via de P&C cyclus op hoofdlijnen op de hoogte gebracht van ontwikkelingen op dit gebied, maar wordt door het college van b. en w. onvoldoende in stelling gebracht om de controlerende en kaderstellende rol in te vullen. Maar de raad kan zichzelf ook actiever opstellen; de afgelopen jaren heeft de raad van Opsterland geen vragen gesteld over dit onderwerp.

Aanbevelingen

Beleid en Uitvoering:

1. ***Intensiveer de samenwerking in OWO verband en breid deze uit door niet alleen de uitvoering gezamenlijk op te pakken, maar ook gezamenlijk beleid te formuleren.***
   Maak hiermee een einde aan onduidelijkheid in taakverdeling tussen de OWO samenwerking en de gemeente Opsterland en draag zorg voor een duidelijke aansturing.

2. ***Vertaal de uitgevoerde GAP-analyse structureel naar een concreet verbeterplan met meetbare mijlpalen, versnel de implementatie van de BIO2-norm en zorg voor een integrale aanpak voor informatieveiligheid om het volwassenheidsniveau te verhogen.***
   De gemeente Opsterland heeft onvoldoende stappen gezet in de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Hierdoor voldoet de gemeente niet aan de BIO. Dat betekent dat de gemeente kwetsbaar blijft en digitale veiligheidsrisico's loopt. Een forse extra inspanning is nodig om volledig aan de BIO te voldoen. Om aan de verplichtingen van de Cyberbeveiligingswet te voldoen moet de gemeente doorgroeien naar volwassenheidsniveau vier (voorspelbaar en geoptimaliseerd). Dit niveau kan worden bereikt door een systematische monitoring van beveiligingsmaatregelen, het verbeteren van de interne evaluatieprocessen en sturing.

Incidenten(afhandeling):

3. ***Verhoog de aandacht voor risicobeheersing en zorg voor een duidelijke opvolging van incidenten****.*
   Hoewel er procedures zijn voor het melden van datalekken, is de risicobeheersing in processen waarin veel persoonsgegevens worden verwerkt nog niet optimaal omdat incidenten nog onvoldoende worden gebruikt bij het verbeteren en actualiseren van processen en beleid. Een betere opvolging van incidenten helpt om herhaling te voorkomen en de algehele veiligheid te verbeteren.

PDCA-cyclus:

4. ***Versterk de PDCA-cyclus door de opvolging van audits en adviezen te verbeteren en te documenteren***.
   In het strategisch beleidsplan van de gemeente Opsterland is in paragraaf 2.6.2 Belangrijkste uitgangspunten aangegeven dat: 'Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging. Dit uitgangspunt is onvoldoende aangetroffen. Er wordt over het algemeen planmatig gewerkt, maar de laatste twee fasen van de PDCA cyclus moeten beter worden ingevuld. Audits en incidenten moeten vertaald worden in verbeterplannen die vervolgens geïmplementeerd en periodiek geëvalueerd moeten worden.

Weerbaarheid:

5. ***Maak bewustwordingsactiviteiten verplicht voor medewerkers, bestuurders en raadsleden en zorg voor een gestructureerde aanpak voor opleiding en training.*** De medewerkers van de gemeente Opsterland zijn erg betrokken bij digitale veiligheid maar kennis en vaardigheden kunnen verbeterd worden. Vrijblijvende activiteiten kunnen leiden tot lage deelname en vervolgens tot onvoldoende kennis en vaardigheden ten aanzien van digitale veiligheid. Verplichte, gestructureerde en periodieke trainingen zorgen voor een structureel hoger kennisniveau en betere naleving van veiligheidsprotocollen.

Crisisorganisatie:

6. ***Organiseer periodieke crisisoefeningen en borg de effectiviteit ervan binnen een PDCA-cyclus.***
   Hierbij is het van belang de betrokken rollen en verantwoordelijkheden helder vast te leggen en te evalueren. Ontwikkel een duidelijk crisisprotocol en oefen periodiek met crisissituaties, ook in OWO samenwerkingsverband. Zonder een duidelijk crisisprotocol en regelmatige oefeningen is de gemeente niet goed voorbereid op daadwerkelijke crisissituaties. Periodieke oefeningen helpen om de respons te verbeteren en de effectiviteit van het crisismanagement te verhogen.

Rol van de Gemeenteraad:

7. ***Informeer de gemeenteraad zodanig dat zij haar controlerende en kaderstellende rol op het gebied van digitale veiligheid kan vervullen.***
   Geef de raad periodiek inzicht in de voortgang van het digitaal veiligheidsbeleid. Hierbij dient minimaal aandacht besteed te worden aan:
   - De mate waarin de gemeente voldoet aan de BIO norm;
   - Ontwikkeling in het volwassenheidsniveau;
   - Risicomanagement en crisisbeheersing.

Bestuurlijke reactie

Aan de Rekenkamer
T.a.v. Mevrouw H. Vervoort

Uw kenmerk:	Uw brief van:	Ons kenmerk:	Behandeld door:	Telefoon:	Bijlagen:
		0086219638	Marnik Jan Slagman	(0512) 386 222	

Onderwerp:
Bestuurlijke reactie Rekenkameronderzoek naar informatiebeveiliging

Beetsterzwaag, 9 juli 2025
Verzonden op:

Geachte leden van de Rekenkamer,

Aanleiding
U heeft onderzoek gedaan naar de huidige stand van informatiebeveiliging binnen de gemeente Opsterland, en de andere OWO-gemeenten. Een goede zaak, gezien alle ontwikkelingen rondom dit onderwerp op digitaal vlak, in wet- en regelgeving en in de fysieke wereld.

Kritisch, en grotendeels waardevol
Uw rapport geeft een kritische blik op de huidige stand van zaken rondom informatiebeveiliging. Het onderzoek richt zich vooral op beleid, het naleven ervan in de praktijk en de controle erop door de gemeenteraad. Hierbij staan enkele onderwerpen centraal. Denk aan: incidentenafhandeling, de PDCA-cyclus, de rol van de gemeenteraad en bewustwording onder medewerkers, bestuurders en raadsleden.

Deels zijn de bevindingen en aanbevelingen terecht en worden deze verwelkomt door het college. Het college verbetert zichzelf immers graag waar nodig. Echter, deels zijn de bevindingen naar mening van het college ongegrond of onjuist en de aanbevelingen daardoor niet relevant.

Reactie op aanbevelingen
Het college kan zich vinden in aanbevelingen 1, 2, 4, 6 en 7 uit het onderzoeksrapport. Het college geeft aan dat deze aanbevelingen van toegevoegde waarde zijn en tot verbetering van de informatiebeveiliging leiden. Dit wordt hieronder verder toegelicht.

- Beleid en uitvoering
  <u>Aanbeveling 1:</u> Intensiveer de samenwerking in OWO verband en breid deze uit door niet alleen de uitvoering gezamenlijk op te pakken, maar ook gezamenlijk beleid te formuleren.

  Intern zijn de drie OWO-gemeenten al sinds halverwege 2024 bezig met het opstellen van geharmoniseerd OWO-informatiebeveiligingsbeleid. Hierover is de raad op 27 februari dit jaar geïnformeerd. De verwachting is dat het geharmoniseerde beleid in Q3 van dit jaar wordt

opgeleverd. Het college juicht het opstellen van geharmoniseerd beleid in OWO-verband toe en ziet deze ontwikkeling als een benodigde versterking voor een veilige digitale toekomst.

<u>Aanbeveling 2:</u> Vertaal de uitgevoerde GAP-analyse structureel naar een concreet verbeterplan met meetbare mijlpalen, versnel de implementatie van de BIO2-norm en zorg voor een integrale aanpak voor informatieveiligheid om het volwassenheidsniveau te verhogen

Het college erkent dat de BIO nog niet volledig is geïmplementeerd binnen de gemeente en dat het erg belangrijk is dat hiervoor op korte termijn stappen worden gezet. Ook landelijk blijkt de implementatie van de BIO een uitdaging bij gemeenten.

De CISO's van de drie gemeenten werken samen met OWO-I&A sinds Q4 2024 aan het opstellen van een BIO-implementatieplan, gezien de implementatie deels bij de eigen gemeente, maar deels ook bij OWO-I&A uitgevoerd dient te worden. Het implementatieplan wordt naar verwachting in Q3 van 2025 opgeleverd.

- PDCA-cyclus
  <u>Aanbeveling 4:</u> Versterk de PDCA-cyclus door de opvolging van audits en adviezen te verbeteren en te documenteren.

  De gemeente werkt op dit moment met de Audit & Control rapportage. In deze rapportages wordt de voortgang op bevindingen en aanbevelingen o.a. op het gebied van privacy en informatiebeveiliging bijgehouden en gestuurd op risico's (PDCA-cyclus). Deze rapportage wordt periodiek ingebracht bij het directieteam en gedeeld met het MT. Deze rapportage wordt al enkele jaren succesvol ingezet voor de Verbijzonderde Interne Controle. Sinds eind 2024 is de rapportage uitgebreid met punten voor privacy en informatiebeveiliging.

  Het college kan zich vinden in de bevinding van de Rekenkamer dat laatste twee fasen van de PDCA-cyclus verbeterd kunnen worden.

  Echter, de rode beoordelingen van de stoplichten in H5.2.2 van het onderzoeksrapport met betrekking tot de PDCA-cyclus en het inzicht hebben in verbeterplannen en -maatregelen zouden naar de mening van het college, aanpassing behoeven, aangezien er wel een volledige PDCA-cyclus aanwezig is, en de conclusie van de Rekenkamer is dat enkel de werking van de laatste twee fasen verbeterd moet worden.

- Crisisorganisatie
  <u>Aanbeveling 6:</u> Organiseer periodieke crisisoefeningen en borg de effectiviteit ervan binnen een PDCA-cyclus.

  Op dit moment beschikt OWO-I&A over een actueel en werkend plan over hoe om te gaan met technische verstoringen. Het is echter ook belangrijk om de organisatorische kant ervan vast te leggen. Het college is daarom voorstander voor het ontwikkelen van een crisisprotocol en het periodiek oefenen daarmee. In OWO-verband wordt op dit moment onderzoek gedaan naar het gezamenlijk invulling geven aan crisismanagement, als onderdeel van het afwegingskader (opstellen geharmoniseerd informatiebeveiligingsbeleid).

- Rol van de gemeenteraad
  Aanbeveling 7: Informeer de gemeenteraad zodanig dat zij haar controlerende en kaderstellende rol op het gebied van digitale veiligheid kan vervullen.

  Het college kan zich vinden in deze aanbeveling. Het college werkt graag mee aan het intensiveren van de samenwerking met de gemeenteraad op het gebied van informatiebeveiliging. Tot op heden wordt de gemeenteraad geïnformeerd over informatiebeveiliging via de jaarstukken. Intern wordt al sinds het einde van 2024 gewerkt aan het beter informeren van de gemeenteraad. Het college gaat graag het gesprek aan met de gemeenteraad over hoe hier effectief invulling aan te geven, en is benieuwd naar de visie van de gemeenteraad hierop.

Het college kan zich niet vinden in aanbevelingen 3 en 5. Voorop staat dat de onderwerpen die deze aanbevelingen behelzen (incidentenafhandeling en weerbaarheid) erg belangrijk zijn. Echter, het college is van mening dat de invulling van deze onderwerpen op dit moment al goed is ingericht. Dit wordt hieronder verder toegelicht.

- Incidenten(afhandeling)
  Aanbeveling 3: Verhoog de aandacht voor risicobeheersing en zorg voor een duidelijke opvolging van incidenten.

  De datalekprocedure van onze eigen gemeente voorziet in een adequate afhandeling van datalekken en voorziet ook in het nemen van maatregelen om in de toekomst soortgelijke incidenten te voorkomen. De Audit & Controle-rapportage zorgt voor de opvolging van eventuele maatregelen. Ook brengen we met het datalekkenregister trends in kaart. Daarnaast worden beveiligingsincidenten afgehandeld door OWO-I&A.

- Weerbaarheid
  Aanbeveling 5: Maak bewustwordingsactiviteiten verplicht voor medewerkers, bestuurders en raadsleden en zorg voor een gestructureerde aanpak voor opleiding en training.

  De gemeente past een uitgebreide bewustwordingsstrategie toe die vrijwillige en verplichte onderdelen bevat. Denk hierbij aan: klassikale onboardingstraining voor alle medewerkers, lezingen, VR-game en phishing-tests.

  Naar mening van het college zijn meer verplichte bewustwordingsactiviteiten niet een waardevolle toevoeging. Verplichte deelname verhoogt de deelname, niet per definitie ook het kennisniveau. Daarnaast doet verplichte deelname ook afbreuk aan het draagvlak en de positieve associatie met het onderwerp. Privacy en informatiebeveiliging moeten gewaarborgd worden omdat we dat binnen de gemeente belangrijk vinden, niet enkel omdat het moet.

Kritische kanttekening van het college
In het rapport worden enkele kritische bevindingen gedaan op basis van het gesprek met de focusgroep, in het bijzonder met betrekking tot bewustwording en de organisatiecultuur. Naar mening van het college missen de bevindingen voldoende grondslag om van toepassing te worden verklaard voor de gehele organisatie. De reden hiervoor is dat de focusgroep enkel bestond uit vier medewerkers uit één team, het gebiedsteam (sociaal domein) en daarom een niet-representatief beeld geeft.

Daarnaast heeft de *Privacy Company*, een gerenommeerd privacy advieskantoor, onafhankelijk onderzoek gedaan naar de inbedding van privacy binnen de gemeente, waaronder het

bewustwordingsniveau. Het resultaat: volwassenheidsniveau 4 (schaal 1-5), een goed kennisniveau bij medewerkers, complimenten voor de creatieve aanpak en aantoonbare vooruitgang van het kennisniveau ten opzichte van voorgaande jaren. Dit onderzoek, dat op verzoek van onze gemeente is uitgevoerd, betreft dezelfde onderzoeksperiode, waarbij gesproken is met medewerkers uit 2 teams (Openbare Orde en Veiligheid en het gebiedsteam).

Het rapport van de Privacy Company is weliswaar opgeleverd kort na de onderzoeksperiode van het onderzoek dat de Rekenkamer heeft uitgevoerd. Echter, omdat beide onderzoeken dezelfde onderzoeksperioden betreffen, roept het college de Rekenkamer op om de resultaten van de Privacy Company tóch mee te nemen. Aangezien de resultaten van de Privacy Company de bevindingen van de Rekenkamer ter discussie stellen, waaronder ook de beoordelingen van de stoplichten in H5.2.3 van het onderzoeksrapport.

Verder is het verschil in beoordelingen van de stoplichten in H5.2.2 tussen de gemeente Opsterland en de andere OWO-gemeenten in onze optiek grotendeels toe te rekenen aan het feit dat het behalen van de ambities in het informatiebeveiligingsbeleid bij de drie OWO-gemeenten anders is geformuleerd. Daarbij heeft Opsterland geen tijdspad in het beleid opgenomen om de gewenste ambities te bereiken.

Tot slot
Het college verwelkomt in algemene zin de kritische blik van de Rekenkamer op het onderwerp informatiebeveiliging. Diverse bevindingen en aanbevelingen helpen de gemeente om richting te geven aan de reeds ingezette verbeteracties en bieden daarnaast bevestiging dat de juiste weg is ingeslagen. De gemeenteraad wordt geïnformeerd over de voortgang met betrekking tot de overgenomen maatregelen.

Met vriendelijke groet,

burgemeester en wethouders,

de gemeentesecretaris de burgemeester,

Sandra van ’t Hooge Andries Bouwman

Nawoord

De Rekenkamer bedankt het college voor de uitgebreide bestuurlijke reactie de daarin opgenomen onderkenning van het belang van dit onderzoek. We zijn blij te lezen dat een aantal van de aanbevelingen die we doen, al in meer of mindere mate uitvoering krijgen in de praktijk of dat er stappen genomen worden om te onderzoeken wat er met de aanbevelingen gedaan kan worden. Het doel van het onderzoek is altijd geweest om positief kritisch te zijn en aanbevelingen te doen die zowel de raad als de organisatie voor de toekomst op weg kunnen helpen.

Voor een aantal van de aanbevelingen die we geven, willen we naar aanleiding van de bestuurlijke reactie nogmaals het belang benadrukken en de raad sterk adviseren deze aanbevelingen wel over te nemen.

- **Aanbeveling 3:** In de bestuurlijke reactie schrijft het college dat de datalekprocedure voorziet in een adequate afhandeling van datalekken en in het nemen van maatregelen om in de toekomst soortgelijke incidenten te voorkomen. Daarnaast worden beveiligingsincidenten afgehandeld door OWO-I&A. Deze argumentatie is volgens de rekenkamer onvoldoende aanleiding om de aanbeveling te herzien. Risicobeheersing gaat immers verder dan het melden van datalekken. Deze aanbeveling komt voort uit de bevinding dat de risicobeheersing in processen waar veel persoonsgegevens verwerkt worden geoptimaliseerd kan worden door het gebruiken van incidenten bij het verbeteren en actualiseren van zowel processen als beleid. De gemeente geeft zelf in het strategisch beleid ook aan dat incidenten hiervoor gebruikt moeten worden. Een betere opvolging van incidenten helpt om herhaling te voorkomen en de algehele veiligheid te verbeteren. Dit is ook belangrijk in het licht van het doorlerend vermogen voor een volwassen organisatie met het oog op Cbw/BIO2. Gezien het belang van de bescherming van persoonsgegevens en de mogelijkheden tot optimalisatie van die processen die er binnen de gemeente zijn, blijft dit ons inziens een belangrijke aanbeveling waarvan we de raad adviseren deze over te nemen.

- **Aanbeveling 4:** In de bestuurlijke reactie schrijft het college dat de rode beoordeling van de stoplichten in H5.2.2 in relatie tot de PDCA-cyclus aangepast moeten worden aangezien er een volledige cyclus aanwezig is en enkel de werking van de laatste twee fasen verbeterd moet worden. Echter, het onderzoek laat zien dat er geen concrete verbeterplannen of andere documenten beschikbaar zijn die wijzen op een vastgelegde en volledige PDCA-cyclus. Dit is in tegenspraak met het strategisch beleid waarin de PDCA-cyclus als één van de belangrijke uitgangspunten is genoemd. Daarnaast is het zo dat de audit en controle rapportages waar wij uiteindelijk inzicht in hebben gekregen bijvoorbeeld niets benoemen over incidentafhandeling, wat wel een belangrijk onderdeel is van een complete PDCA-cyclus. Hierdoor zijn wij van mening dat de rode beoordeling correct is..

- **Aanbeveling 5:** In de bestuurlijke reactie schrijft het college dat de gemeente een uitgebreide bewustwordingsstrategie toepast die zowel uit verplichte als vrijwillige onderdelen bestaat. Het uitbreiden van verplichte onderdelen wordt niet als een waardevolle toevoeging gezien door het college en zou afbreuk doen aan het draagvlak en de positieve associatie met het onderwerp. Het onderzoek heeft echter laten zien dat kennis en vaardigheden van medewerkers, bestuurders en raadsleden nog verbetering nodig hebben. Daarom doen wij hier een aanbeveling over en we vinden het ook van belang dat daar opvolging aan gegeven wordt. We hebben daarin een verplichtend karakter opgenomen juist omdat de ervaring leert dat vrijblijvende activiteiten kunnen leiden tot lage deelname en vervolgens tot onvoldoende kennis en vaardigheden ten aanzien van digitale veiligheid. Verplichte, gestructureerde en periodieke trainingen zorgen uiteindelijk voor een structureel hoger kennisniveau en betere naleving van veiligheidsprotocollen.

Naar aanleiding van de opmerking van het college over de focusgroep en het van toepassing verklaren van de uitkomsten voor de gehele organisatie willen we herhalen wat we in het rapport ook al hebben opgenomen. We hebben gekozen voor een focusgroep met medewerkers uit het sociaal domein omdat juist hier veel persoonsgegevens worden verwerkt en dus ook een verhoogde kans is op risico's op het terrein van informatiebeveiliging. De focusgroep bestond uit vier deelnemers van verschillende teams binnen het sociaal domein. Vier deelnemers mag misschien weinig lijken in verhouding tot de grootte van de gehele organisatie maar toch kunnen de resultaten wel meegenomen worden in het onderzoek. We wegen namelijk elke bijdrage van elke respondent, los van functie, even zwaar in het onderzoek. Dit betekent dat de interviews, de opbrengst uit de focusgroep en de documenten die zijn bestudeerd een gelijke weging krijgen in het vergaren van informatie. Als rekenkamer staan we nog steeds achter deze onderzoeksmethodiek, waarbij we nogmaals willen benadrukken dat het beeld wat in het rapport geschetst wordt gebaseerd is op analyse van alle vergaarde informatie en niet uitsluitend op wat in de focusgroep naar voren is gekomen.

Voor wat betreft het onderzoek van de Privacy Company waarnaar het college verwijst, merken wij op dat de onderzoeksresultaten daarvan na de onderzoeksperiode van de rekenkamer zijn opgeleverd en wij dit dus ook niet mee hebben kunnen nemen in ons onderzoek en onze afwegingen. Het college geeft mee dat de Privacy Company een gerenommeerd privacy advieskantoor is. Wij wijzen er op onze beurt op dat het onderzoeksbureau dat voor de Rekenkamer het onderzoek heeft uitgevoerd, ruime ervaring heeft met onderzoeken naar informatiebeveiliging bij gemeenten en dat ze de benodigde kennis en kunde ruimschoots in huis hebben om op dit onderwerp goed onderzoek te doen. We hebben dan ook geen enkele twijfel dat de aanbevelingen die wij aan de gemeenteraad doen de juiste aanbevelingen zijn op basis van de uitkomsten van het voorliggende onderzoek.

Nota van bevindingen

1. Inleiding

1.1 Aanleiding

Gemeenten zijn steeds afhankelijker geworden van digitalisering; elk gemeentelijk proces kent wel een digitale component. Daarom neemt ook het belang van informatieveiligheid toe. Dit belang wordt onderkend door de VNG die met en voor haar leden de Agenda Digitale Veiligheid heeft opgesteld. In deze agenda wordt gepleit voor meer bestuurlijke aandacht voor dit thema. Deze aandacht behelst niet alleen die van de burgemeester of het college van b. en w. , maar ook van de gemeenteraad. De VNG adviseert de colleges dan ook om periodiek het gesprek met de raad aan te gaan over digitale veiligheid.[1]

Ook de Rijksoverheid en Europa dringen met Richtlijnen en wetgeving aan op digitaal veilige gemeenten. De Europese 'Network and Information Security-directive' ofwel de NIS2 richtlijn is bedoeld om de cyberbeveiliging en de weerbaarheid van 'essentiële diensten', waaronder lokale overheden, in de EU lidstaten te verbeteren. Op dit moment wordt de richtlijn naar Nederlandse wetgeving vertaald. De bepalingen worden opgenomen in de Cyberbeveiligingswet. Dit houdt in dat digitale veiligheid een plicht wordt voor gemeenten; de vrijblijvendheid gaat er vanaf. De Cyberbeveiligingswet treedt naar verwachting in oktober 2025 in werking.

Het gemeentelijk beleidsdomein van informatieveiligheid is dus, ook in de OWO-gemeenten, volop in beweging. Gelet op de toegenomen cyberdreigingen en de (op handen zijnde) wettelijke verplichting op het gebied van informatieveiligheid is het van belang dat de gemeenteraad zijn kaderstellende en controlerende rol op dit domein goed kan invullen. De Rekenkamer van de OWO-gemeenten (Ooststellingwerf, Weststellingwerf en Opsterland) hebben daarom een onderzoek uitgevoerd naar de informatieveiligheid bij deze gemeenten.

1.2 Doel- en vraagstelling

Het doel van het onderzoek is het in beeld brengen of de informatiebeveiliging adequaat is georganiseerd en geborgd bij de OWO-gemeenten en in hoeverre de gemeenteraden in hun positie zijn om hun taken uit te voeren.

De centrale vraag van dit onderzoek luidt als volgt:
Is de informatiebeveiliging van de OWO-gemeenten adequaat georganiseerd en geborgd?

Deze centrale vraag is opgesplitst in de volgende deelvragen:

1. Wat is het beleid op het gebied van informatieveiligheid; voldoet dit aan actuele standaarden (als de BIO en ENSIA) en zijn de gemeenten voorbereid op de BIO2 en ENSIA?
2. Hoe wordt het Informatieveiligheidsbeleid uitgevoerd op bestuurlijk, organisatorisch, technisch, proces- en medewerkersniveau? Worden hierbij pentesten ingezet, zo ja, welke?
3. Zijn gegevens voldoende beschermd tegen toegang door onbevoegden? In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging en welke instrumenten worden hierbij gebruikt?
4. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident, hoe ziet het incidentmanagementproces eruit en wordt dit in de praktijk geoefend?

[1] Digitale veiligheid en privacy | VNG

5. Hoe wordt omgegaan met risico's en incidenten op het gebied van informatieveiligheid en in hoeverre toont de organisatie lerend vermogen (PDCA cyclus)?
6. Hoe wordt gezorgd voor bewustwording voor informatiebeveiliging bij medewerkers, bestuur, raad en samenwerkingspartners?
7. Zijn de rollen en taken op het gebied van informatiebeveiliging voor medewerkers en het management duidelijk en hoe wordt er gestuurd in de gemeentelijke organisatie?
8. Hoe is de raad betrokken bij het informatieveiligheidsbeleid en is dit voldoende om de kaderstellende en controlerende rol te kunnen vervullen?

1.3 Normenkader

Op basis van bovenstaande vragen is een normenkader uitgewerkt. Onderstaand normenkader, dat normen bevat over het gemeentelijk beleid, de uitvoeringspraktijk en de cultuur is toegepast in dit onderzoek.

Normen ten aanzien van het gemeentelijk beleid

- De gemeente heeft BIO- conform informatiebeveiligingsbeleid.
- De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad.
- In het beleid wordt o.a. ingegaan op:
  - Strategische uitgangspunten
  - Risicomanagement
  - Governance (waaronder rollen en verantwoordelijkheden)
  - De PDCA-cyclus van de gemeente
- In (voortgangs)rapportages wordt ingegaan op informatiebeveiliging.
- In programma's en projecten wordt expliciet aandacht besteed aan informatiebeveiliging.
- Er is een procedure hoe wordt omgegaan met informatiebeveiligingsincidenten (waaronder cyberaanvallen) en een crisisprotocol.
- De gemeente heeft beleid voor informatiebeveiliging ten aanzien van samenwerkingspartners, gemeenschappelijke regelingen en leveranciers.

Normen ten aanzien van de uitvoeringspraktijk

- In de praktijk wordt gehandeld conform de wijze waarop informatie wordt beveiligd, waaronder in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.
- De gemeente heeft een leer- en verbetercyclus (PDCA-cyclus).
- De gemeente heeft inzicht in de belangrijkste verbeterplannen en –maatregelen.
- Er wordt in het geval van incidenten, calamiteiten en crisis volgens de vastgelegde procedures gehandeld.
- De vastgelegde controles en rapportages worden in de praktijk uitgevoerd.
- De gemeente test en toetst procedures regelmatig om de effectiviteit en werking te toetsen.
- De gemeente houdt toezicht op de afspraken ten aanzien van informatiebeveiliging met (samenwerkings)partners, regelingen en leveranciers.
- De raad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.

Normen ten aanzien van de organisatiecultuur

- De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging en worden van aanpassingen op de hoogte gehouden.
- In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven.
- In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente op het gebied van informatiebeveiliging.

1.4 Werkwijze

Het onderzoek is gedaan in de periode september 2024-december 2024. Voorafgaand aan dit onderzoek heeft de rekenkamer een vooronderzoek gedaan bij de drie gemeenten, waarin gesprekken zijn gevoerd en documentatie is verzameld. Het rekenkameronderzoek is vervolgens gestart met een startbijeenkomst voor betrokken medewerkers van de drie gemeenten

Tijdens het onderzoek zijn verschillende onderzoeksmethoden ingezet, waaronder een documentenstudie en interviews met diverse functionarissen (zie bijlage 1)..Om te onderzoeken hoe in de gemeente het beleid in praktijk wordt gebracht, is voor elke gemeente een bijeenkomstemet een focusgroep uit het sociaal domein[2] en een raadsbijeenkomst georganiseerd. Vervolgens is een zogenaamde convergentiesessie een gesprek gevoerd met ambtelijk betrokkenen om nadere informatie op te halen. Op basis van al dezeverkregen informatie is onze analyse uitgevoerd en deze rapportage geschreven.

Het onderzoeksrapport is conform het onderzoeksprotocol van de rekenkamer voorgelegd aan de ambtelijke organisatie van de gemeente om na te gaan of de feiten zoals beschreven in die nota in het licht van de onderzoeksdoelstelling en –vraagstelling, juist en volledig zijn. Op- of aanmerkingen als gevolg van dit ambtelijk hoor en wederhoor zijn, na zorgvuldige afweging van de rekenkamer, verwerkt. De wijze waarop de rekenkamer dit gedaan heeft is middels een memorie van antwoord teruggekoppeld aan de gemeentelijke organisatie. Vervolgens zijn de conclusies en aanbevelingen geschreven.

Het onderzoeksrapport is daarna voor bestuurlijk wederhoor voorgelegd aan het college van B&W (conform artikel 9 lid d, onderzoeksprotocol van de rekenkamer d.d. 23 april 2024). Vervolgens is op verzoek van het college een gesprek gevoerd over de conclusies en aanbevelingen in het onderzoeksrapport. Daarbij werd duidelijk dat na afronding van het onderzoek de gemeente Opsterland verschillende documenten heeft opgesteld en zaken in gang heeft gezet die de digitale veiligheid van de gemeente gaan versterken. Tien van de 25 nagestuurde documenten zijn echter opgesteld na afsluiting van het onderzoek. Deze documenten vallen hiermee buiten scope van het onderzoek. Daar waar relevant wordt hiervan wel in voetnoten melding gemaakt.
Vijftien documenten zijn gepubliceerd voor of in de onderzoeksperiode. Tien van deze documenten had de rekenkamer niet eerder ontvangen maar zijn alsnog meegenomen in een aanvullende documentenanalyse. Vijf documenten waren (deels) bekend en waren al meegenomen in de bevindingen.

[2] Gekozen is voor het sociaal domein omdat hier veel persoonsgegevens worden verwerkt en dus ook een verhoogde kans is op risico's. De focusgroep bestond uit vier deelnemers van verschillende teams binnen het sociaal domein. Deze opkomst had hoger kunnen zijn, maar twee deelnemers zijn op het laatste moment niet komen opdagen. Toch kunnen de resultaten wel meegenomen worden in het onderzoek. We wegen iedere bijdrage van respondenten, los van functie, even zwaar in het onderzoek. Dit betekent dat de interviews en de opbrengst uit de focusgroep een gelijke weging krijgen in het vergaren van informatie.

De bestuurlijke reactie van het college is opgenomen in het onderzoeksrapport, evenals het nawoord van de rekenkamer.

1.5 Leeswijzer

Het rapport begint met een uitleg over de wettelijke- en overige kaders voor het gemeentelijk digitale veiligheidsbeleid. In dit hoofdstuk wordt dieper ingegaan op (veranderingen in) de wet- en regelgeving zoals de NIS2 richtlijn, de Cyberbeveiligingswet, de BIO2 en ENSIA.

Vervolgens behandelen wij in hoofdstuk drie de OWO-samenwerking en het beleid en de uitvoering in Opsterland. Dit hoofdstuk bevat een belangrijk deel van de bevindingen van ons onderzoek. In hoofdstuk vier zetten we de rol van de raad uiteen, door eerst te benoemen welke informatievoorziening zij ontvangen en daarna in te gaan op het perspectief van de raad.

De beantwoording van de onderzoeksvragen en de toetsing aan het normenkader is opgenomen in hoofdstuk 5.

In de bijlagen treft u ten slotte een overzicht van de functionarissen waarmee in het kader van dit onderzoek is gesproken plus een overzicht van de documenten die zijn geraadpleegd. Ook is hier een overzicht opgenomen van de gebruikte afkortingen.

2. Speelveld digitale veiligheid

Dit hoofdstuk is een algemene beschrijving van de context en organisatie van digitale veiligheid in gemeentelijke organisaties en de sturing daarop door college en gemeenteraad.

2.1 Belangrijke elementen digitale veiligheid

Digitale veiligheid gaat over veel meer dan bedrijfsvoering. De gemeentelijke dienstverlening is van digitalisering afhankelijk. Bovendien beschikken gemeenten over steeds meer persoonsgegevens van hun inwoners. Deze inwoners mogen van hun gemeente verwachten dat deze gegevens veilig zijn en dus niet op straat komen te liggen. Als dat toch gebeurt, dan schaadt dit het vertrouwen in de gemeentelijke overheid, en brengt mogelijk zelfs (directe) schade toe aan de getroffen inwoners.

Elke gemeente moet maatregelen nemen om ervoor te zorgen dat persoonsgegevens veilig zijn en de continuïteit van dienstverlening wordt geborgd. 100% Veilig bestaat echter niet; er is altijd een risico dat er iets misgaat, bijvoorbeeld dat een hacker inbreekt in een gemeentelijk informatiesysteem. Deze dreiging komt niet alleen van buiten, ook een slordigheidje van een van de eigen medewerkers kan leiden tot bijvoorbeeld een datalek (zie ook de voorbeelden uit de fictieve gemeente Fonkelveen in de kaders).

Daarnaast is informatiebeveiliging ook vaak in het belang van de gemeente zelf, denk bijvoorbeeld aan informatie over voorbereidingen op strategische aankopen. Dergelijke informatie is niet per se door wetgeving beschermd, echter iedere gemeente realiseert zich dat dergelijke informatie niet moet lekken.

Een hack met gevolgen

Fractievoorzitter Jouke Drenth van oppositiepartij ***Voorwaarts Fonkelveen*** *was net thuis van een crisisberaad met het presidium. Dit was zijn derde raadsperiode, maar zo zout had hij het nog niet eerder gegeten. De burgemeester vertelde dat hackers hadden ingebroken in de gemeentelijke informatiesystemen. Er was vertrouwelijke informatie buitgemaakt; persoonsgegevens van inwoners die bij de gemeente vanwege de jeugdzorg geregistreerd waren. Het ging hierbij niet alleen om namen, adressen en BSN nummers, maar ook om behandeldossiers van jongeren. De hackers eisten 5 Bitcoin losgeld van de gemeente, dan zou de gemeente weer toegang krijgen tot de eigen bestanden. Dat kwam neer op € 450.000,-! Waar moest je als kleine gemeente dat geld vandaan halen? Niet ingaan op deze eis ging misschien nog wel meer kosten. De hackers dreigden om de buitgemaakte informatie op het dark web te plaatsen en, zo gaf de burgemeester aan, Fonkelveen zou de hele IT-omgeving opnieuw moeten opbouwen. Dat kon wel een paar miljoen kosten. Het was een duivels dilemma; zakendoen met criminelen of een financiële strop die de gemeente wel eens de kop kon kosten. Binnen twee dagen moest de burgemeester beslissen. Tot die tijd werd er nog naar een oplossing gezocht. Als de back-up bestanden niet aangetast waren, kon de (financiële) schade nog beperkt worden. Maar wat zouden de inwoners van hun gemeente vinden als hun persoonsgegevens op het web gepubliceerd zouden worden? Drenth had er geen goed gevoel bij. Digitale veiligheid was altijd een hamerstuk geweest op de raadsagenda, maar na deze wake-up call vast niet meer.*

In het algemeen leggen gemeenten hun doelstellingen, processen en rolverdeling vast in een beleidsdocument. Hierbij maken veel gemeenten gebruik van het format van de Informatiebeveiligingsdienst (IBD) van de VNG. Dit format gaat ervan uit dat een beleidsplan voor een periode van meestal vier jaar wordt vastgesteld. Op tactisch niveau wordt het beleid uitgewerkt in jaarplannen. Die plannen worden aan de hand van de Plan-Do-Check-Act (PDCA) cyclus gemonitord met als doel om permanente verbetering door te voeren.

2.2 Wetten & regels

Bij de uitvoering van het informatieveiligheidsbeleid moeten gemeenten voldoen aan verschillende wetten en regels. De belangrijkste zijn de Europese Network- and Information Security 2 directive (NIS2), de Cyberbeveiligingswet (Cbw), de Algemene Verordening Gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en de Eenduidige Normatiek Single Information Audit (ENSIA).

De NIS2 richtlijn van de Europese Unie heeft als doel om de informatiebeveiliging van essentiële diensten, waaronder die van gemeenten, in de EU-lidstaten te verbeteren. In de richtlijn is hiertoe onder meer een zorgplicht en een meldplicht opgenomen, en wordt ook het toezicht op informatiebeveiliging geregeld. De NIS2 richtlijn is niet rechtstreeks van toepassing op gemeenten, maar wordt uitgewerkt in de Cyberbeveiligingswet, waar gemeenten wel aan moeten voldoen. Naar verwachting wordt de wet in het derde kwartaal van 2025 ingevoerd. Vanaf het moment dat de wet ingaat, moet de gemeentelijke digitale veiligheid voldoen aan de eisen die in deze wet staan. De invoering van de Cyberbeveiligingswet leidt tot een taakverzwaring en extra kosten voor gemeenten. De VNG heeft in een reactie op deze wet gevraagd om compensatie van het Rijk voor deze kosten.[3]

De maatregelen die de Cyberbeveiligingswet voorschrijft om de informatiebeveiliging te verbeteren, de zorgplicht, zijn grotendeels opgenomen in de BIO2. In de Cyberbeveiligingswet gaat het naast de beveiliging van kantoorautomatisering (KA) ook over de beveiliging van operationele technologie (OT). Deze OT betreft bijvoorbeeld gemeentelijke bruggen en sluizen die op afstand worden bediend, en camera's in de openbare ruimte. Nieuw met de komst van de Cyberbeveiligingswet is ook dat er naast ad hoc toezicht (achteraf, via rapportage aan de raad en de stelselhouders bij het Rijk) ook proactief toezicht zal worden gehouden op de informatiebeveiliging van gemeenten. De Rijksinspectie Digitale Infrastructuur (RDI) is daarvoor aangewezen als toezichthouder voor de gemeenten en andere overheidsorganisaties.

IT leverancier vliegt uit de bocht
Eind november krijgt raadslid Elke Schrijver van coalitiepartij ***Fonkelveen Vooruit*** *een telefoontje van een alleenstaande ouder die in haar straat woont. Haar bijstandsuitkering was niet op haar rekening gestort, misschien zou Elke eens navraag kunnen doen of er iets aan de hand was. Schrijver besluit op onderzoek uit te gaan en neemt contact op met de verantwoordelijk wethouder. Het blijkt om een serieus probleem te gaan: geen enkele uitkeringsgerechtigde in Fonkelveen heeft zijn of haar uitkering gekregen en de telefoon van het klantcontactcentrum staat roodgloeiend. Sommige bellers zijn acuut in de problemen gekomen en moeten geld lenen om boodschappen te doen.*
Sinds jaar en dag neemt de gemeente Fonkelveen het ICT-systeem van de firma Rik de Zand IT Solutions af voor de uitkeringsadministratie. Uit onderzoek van de beheerders van Fonkelveen bleek dat er enkele dagen geleden een nieuwe versie van deze cloudapplicatie draait die een fout betaalbestand genereert. Geen enkele uitkeringen is daarom betaald. Fonkelveen lijkt overvallen door de nieuwe versie en heeft deze, omdat het om een cloudapplicatie gaat, zelf niet getest. De leverancier probeert de fout op te lossen, maar weet nog niet wanneer dat gaat lukken. Ondertussen is het advies om de betaaltape van vorige maand te gebruiken. Maar die is niet accuraat. De portefeuillehouder weet nog even niet hoe dit op te lossen. Ondertussen stromen de klachten binnen bij het KCC en vraagt Schrijver zich af wat zij haar buurvrouw kan melden.

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening betreft een uitwerking van Europese regelgeving die bedoeld is om de privacy van alle

[3] zie VNG-reactie consultatie Cyberbeveiligingswet (NIS2) | VNG voor meer informatie

inwoners (beter) te beschermen. De Autoriteit Persoonsgegevens houdt toezicht op de uitvoering van de AVG in Nederland. Wanneer gemeenten de bescherming van persoonsgegevens niet op orde hebben, riskeren zij een boete van de Autoriteit Persoonsgegevens. Het maatschappelijk en financieel belang van een adequaat privacybeleid is groot. Gemeenten hebben echter niet alleen een goed privacybeleid nodig, maar ook een goede uitvoering daarvan. Beiden zijn verplicht op grond van de AVG. Omdat de beveiliging van persoonsgegevens veel raakvlak heeft met de beveiliging van informatie in het algemeen, zijn de verplichtingen die voortvloeien uit de AVG ook meegenomen in dit onderzoek.

De BIO is sinds 2019 het verplichte basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (en dus ook gemeenten). De BIO is gebaseerd op de informatiebeveiligingsstandaarden ISO 27001 en ISO 27002 en omvat een minimum aan maatregelen die getroffen moeten worden op het gebied van informatiebeveiliging. Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk in belangrijke mate op deze BIO. De BIO wordt op dit moment doorontwikkeld naar de BIO2 en wordt wettelijk verplicht onder de Cyberbeveiligingswet. In de BIO2 is mede naar aanleiding van de komst van de Cyberbeveiligingswet de verantwoordelijkheid van het hogere management in de gemeentelijke informatiebeveiliging vastgelegd. Ook het toewijzen van benodigde middelen, het verhogen van veiligheidsbewustzijn en het uitvoeren van controles maken onderdeel uit van de BIO2.

ENSIA is ontstaan uit een gezamenlijk initiatief van een aantal departementen en de VNG. Het doel van ENSIA is om tot een effectief en efficiënt ingericht verantwoordingsstelsel voor informatieveiligheid te komen. De ENSIA is een jaarlijkse audit die gebaseerd is op de BIO. Uitgangspunt voor ENSIA is het horizontale verantwoordingsproces waarin het college van b. en w. zich over de informatieveiligheid verantwoordt aan de gemeenteraad. Deze verantwoording vormt de basis voor de verantwoording aan de stelselhouder (bijvoorbeeld het ministerie van BZK of SZW). Er wordt dus jaarlijks één audit uitgevoerd waarvan (een deel van) de resultaten zowel naar de gemeenteraad als de stelselhouder gaan. Net als de BIO, wordt ook de ENSIA op dit moment doorontwikkeld naar een nieuwe versie. Deze moet vooral gebruikersvriendelijker worden, zowel voor de ambtelijke organisatie als het gemeentebestuur.

2.3 Bestuur & organisatie

Informatieveiligheid is van de hele gemeentelijke organisatie. Vaak is in beleidsdocumenten vastgelegd dat het lijnmanagement hier verantwoordelijkheid voor draagt. Managers moeten erop toezien dat richtlijnen bij medewerkers bekend zijn en worden nageleefd. Vanuit wet- en regelgeving is een aantal functies verplicht gesteld. Zo verplicht de AVG gemeenten om een Functionaris Gegevensbescherming (FG) in dienst te hebben en dient de Chief Information Security Officer (CISO) volgens de BIO2 zo gepositioneerd te zijn binnen de organisatie dat hij onafhankelijk van de lijn kan adviseren over informatieveiligheid[4].

[4] CISO (Chief Information Security Officer): Verantwoordelijk voor het ontwikkelen en implementeren van het informatiebeveiligingsbeleid binnen een organisatie. Houdt toezicht op de beveiliging van informatie en zorgt ervoor dat de organisatie voldoet aan relevante wet- en regelgeving. Heeft kennis van informatiebeveiliging, risicoanalyse en beveiligingstechnieken.
FG (Functionaris Gegevensbescherming) of DPO (Data Protection Officer): Houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) binnen een organisatie. Adviseert en rapporteert aan het hoogste managementniveau over privacykwesties. Is verplicht voor overheidsinstanties en organisaties die op grote schaal bijzondere persoonsgegevens verwerken.
PO (Privacy Officer): Ontwikkelt en voert het privacybeleid uit binnen een organisatie. Ondersteunt de FG en fungeert als juridisch adviseur op het gebied van privacy. Is niet verplicht zoals de FG, maar speelt een belangrijke rol in het waarborgen van privacy binnen de organisatie.

Het college is eindverantwoordelijk voor de informatieveiligheid van de organisatie. Het college stelt beleid vast en ziet erop toe dat onbevoegden zich geen toegang kunnen verschaffen tot gemeentelijke informatiesystemen. Mocht dit toch gebeuren, dan kan het nodig zijn om een crisisorganisatie in te richten.

De gemeenteraad is bevoegd de kaders te stellen en het college te controleren. Allereerst wordt van de gemeenteraad verwacht dat hij voldoende middelen beschikbaar stelt, zodat de gemeente aan wet- en regelgeving kan voldoen. In de praktijk blijkt vaak dat raden het lastig vinden om hun controlerende rol goed in te vullen omdat informatieveiligheid als een technisch onderwerp wordt beschouwd. Maar net als bij andere beleidsterreinen is ook hier het de rol van de gemeenteraad om kaders te stellen en te controleren of de gemeente recht- en doelmatig handelt. Zo is het belangrijk dat de raad controleert of de gemeente voldoet aan de BIO. Maar ook over de andere vlakken van het speelveld kan de raad het college bevragen.

2.4 Weerbaarheid

Weerbaarheid is het vierde belangrijke onderdeel van digitale veiligheid. Elke gemeente neemt maatregelen om onbevoegd gebruik van data en informatiesystemen tegen te gaan. Maar 100% veilig bestaat niet; er is altijd een kans dat het mis gaat. Het gaat hierbij niet alleen om het risico op een hack, maar ook onbedoeld verlies van geclassificeerde informatie, of een IT- leverancier van de gemeente die een fout maakt, waardoor de continuïteit van de gemeentelijke dienstverlening in gevaar komt.

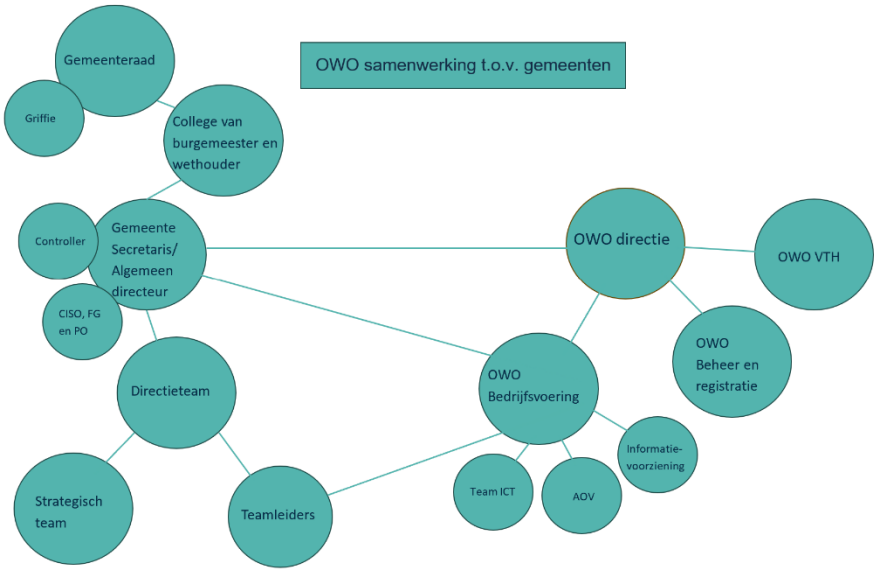
Bij weerbaarheid gaat het in eerste instantie om preventieve maatregelen die worden genomen om digitale verstoringen te voorkomen. Voorbeelden van deze maatregelen zijn het autorisatiebeleid en de toegang van medewerkers tot de verschillende informatiesystemen. Ook bewustwordingsactiviteiten als (online) opleidingen en pentesten zijn belangrijke preventieve maatregelen om verstoringen te voorkomen. Bij opleidingen gaat het niet alleen over de vraag of er voldoende wordt aangeboden, maar ook over de mate waarin opleidingen, al dan niet verplicht worden gevolgd en de wijze waarop hierop wordt gemonitord en gestuurd. Pentesten kunnen zowel betrekking hebben op de technische beveiliging van informatiesystemen als op de medewerkers (human factor pentesten). Voorbeelden van deze laatste categorie zijn ‘phishing mails’ en mystery guests, die proberen om fysiek het gemeentehuis binnen te komen en toegang te krijgen tot informatiesystemen.

Weerbaarheid gaat ook over de respons van de gemeente als een digitale verstoring zich voordoet. Reageert de gemeente adequaat? Wordt er tijdig een crisisorganisatie ingericht en worden hier de juiste beslissingen genomen? Met oefeningen en simulaties van digitale ordeverstoringen kan de gemeente inzicht krijgen in de respons van de organisatie op een digitale verstoring. Zeker als gemeenten samenwerken op het gebied van digitalisering en informatieveiligheid is het van belang om periodiek te oefenen met een digitale verstoring, zodat duidelijk wordt of de juiste afspraken zijn gemaakt ten aanzien van mandaten en bevoegdheden.

3. Beleid en uitvoering

3.1 OWO-samenwerking

De colleges van b. en w. van de gemeente Ooststellingwerf, Weststellingwerf en Opsterland zijn in 2011 een intergemeentelijke samenwerking aangegaan voor verschillende diensten, waaronder bedrijfsvoering, de OWO-samenwerking. Ter aanvulling is er tussen de drie samenwerkende gemeenten de regeling 'gezamenlijke verantwoordelijkheid' opgesteld in 2015 en door de afzonderlijke colleges vastgesteld[5]. De OWO samenwerking beslaat verschillende onderdelen, waaronder een afdeling die verantwoordelijk is voor de bedrijfsvoering van de drie gemeenten (OWO bedrijfsvoering). OWO bedrijfsvoering bestaat uit verschillende teams. Een van de teams die onderdeel zijn van OWO bedrijfsvoering is Team ICT. De schematische weergave van de OWO-samenwerking biedt een globaal overzicht van de onderlinge verbanden tussen individuele OWO gemeenten en de OWO organisatie. Deze weergave is gebaseerd op de PowerPoint-presentatie van de themabijeenkomst ICT voor raadsleden van de OWO-gemeenten en op informatie verkregen uit interviews.



De operationele taken en verantwoordelijkheden met betrekking tot de ICT-informatiebeveiliging liggen bij Team ICT van de afdeling OWO-Bedrijfsvoering. De medewerkers van het team ICT dragen zorg voor de uitvoering van alle beveiligingsmaatregelen die in het Informatiebeveiligingsplan ICT 2020 zijn benoemd. Team ICT is verantwoordelijk voor de centrale ICT-infrastructuur van de drie OWO gemeenten, waaronder data, applicaties en telefonievoorzieningen. Daarnaast is Team ICT verantwoordelijk voor de operationele activiteiten op gebied van informatieveiligheid, dit omvat bijvoorbeeld tooling, logging, firewalls en monitoring. Het leveranciersmanagement voor de drie gemeenten wordt deels door Team ICT uitgevoerd. Leveranciersmanagement is belegd bij team ICT van OWO-bedrijfsvoering en bij de afdeling Inkoop, de toetsing of leveranciers voldoen aan contractuele eisen is niet duidelijk belegd. Daarnaast is Team ICT ook verantwoordelijk voor de uitvoering van de back-ups en restores. Ook is Team ICT betrokken bij een monitoring- en responsproject van de VNG, daar is verder geen aanvullende informatie over opgevraagd.

Alle grotere applicaties staan onder verantwoordelijkheid van Team ICT, kleinere applicaties staan onder verantwoordelijkheid van de individuele OWO-gemeenten zelf. Grote applicaties zijn applicaties die in OWO-verband worden gebruikt, te denken valt aan VTH (Vergunning, Toezicht en Handhaving), I-zaak (archivering), Teams, I-Babs, csam en isam. Tijdens het onderzoek is gebleken dat iedere applicatie een eigenaar behoort te hebben en hieraan wordt gewerkt, maar dit nog niet bij elke applicatie al het geval is. Er is geen documentatie ontvangen over de precieze verdeling van

[5] Deze Regeling Gezamenlijke verantwoordelijkheid is onder de herziende bestuursovereenkomst OWO-samenwerking in 2024 vernieuwd. Deze zijn tijdens de onderzoeksperiode niet ontvangen.

verantwoordelijkheden rondom applicaties. Medewerkers vertelden in het kader van het onderzoek dat de CISO's van de individuele gemeenten in samenwerking met Team ICT op dit moment bezig zijn hun applicaties en de bijbehorende taken, rollen en verantwoordelijkheden in kaart te brengen.

De OWO-gemeenten hebben een gezamenlijke aanpak voor de levering en het beheer van ICT-voorzieningen. Apparatuur en applicaties worden door Team ICT centraal verstrekt aan de medewerkers van de gemeente. Medewerkers hebben op laptops geen mogelijkheid om zelf applicaties te downloaden. Dat geeft enige mate van controle over de gebruikte software. Voor mobiele telefoons ontbreekt echter een vergelijkbare mate van beleid; zo blijkt uit de focusgroepen dat er geen richtlijnen zijn voor wachtwoordbeheer en het downloaden van applicaties op mobiele werktelefoons, afgezien van de standaard wachtwoordvereisten, en het downloaden van applicaties op mobiele werktelefoons.

Het proces van in- en uitdiensttreding op gebied van apparatuur start en eindigt bij voor medewerkers bij de eigen teamleider. Zo leveren medewerkers hun apparatuur in bij de teamleider in het geval van een uitdiensttreding. Het verdere proces is belegd bij Team ICT. Dit proces omvat bijvoorbeeld het resetten van apparatuur, tijdig afmelden van medewerkers bij systemen en het toekennen van toegang van nieuwe werknemers tot systemen. Team ICT kent de juiste toegangsrechten tot het systeem toe aan de juiste medewerkers van de individuele OWO gemeenten. De informatie over de juiste toegangsrechten per medewerker ontvangt Team ICT van de drie HR afdelingen van de OWO gemeenten zelf. Het HR-beleid is de verantwoordelijkheid van de drie individuele OWO-gemeenten zelf. Uit interviews blijkt dat het beheer op de juiste toegangsrechten tot systemenvolgens Team ICT nog niet sluitend is geregeld binnen de gemeenten. Hier zit een risico dat onbevoegden toegang kunnen krijgen tot gevoelige informatie en systemen.

De colleges van b. en w. van de drie individuele gemeenten zijn eindverantwoordelijk voor het informatiebeveiligingsbeleid. De drie OWO-gemeenten hebben daarom tot nu toe eigen strategisch informatieveiligheidsbeleid. Dit beleid is gebaseerd op de ISO 27001- en ISO 27002-standaarden. Uit gesprekken met medewerkers is gebleken dat Team ICT van OWO-bedrijfsvoering niet structureel bij het opstellen van het strategisch informatieveiligheidsbeleid van alle gemeenten betrokken is. De CISO van de gemeente Weststellingwerf heeft advies gevraagd aan Team ICT over het strategisch informatieveiligheidsbeleid, de CISO van gemeente Ooststellingwerf heeft het strategisch informatieveiligheidsbeleid ter informatie opgestuurd en de CISO van gemeente Opsterland heeft enkel gesprekken gehad met OWO ICT over het strategisch informatieveiligheidsbeleid. De drie gemeenten zijn momenteel met elkaar in gesprek om gezamenlijk informatiebeveiligingsbeleid op te stellen. Ten tijde van de onderzoeksactiviteiten was dit echter nog niet uitgewerkt.

Naast het strategisch informatieveiligheidsbeleid van de drie OWO gemeenten zelf zijn door Team ICT de veiligheidsstandaarden van het informatieveiligheidsbeleid aangevuld met richtlijnen die voor alle OWO-gemeenten gelden. Een van de documenten waar veiligheidsstandaarden voor de drie OWO- gemeenten zijn beschreven, is het Informatiebeveiligingsplan ICT 2020. Hiermee wordt nadere invulling gegeven aan het strategisch informatiebeveiligingsbeleid van de OWO-gemeenten. Het informatiebeveiligingsplan ICT 2020 benoemt de beveiligingsobjecten op het gebied van de ICT en de getroffen maatregelen ten behoeve van het gevraagde beveiligingsniveau.

Team ICT heeft daarnaast een werkinstructie opgesteld voor het omgaan met ernstige verstoringen die voor alle drie de OWO-gemeenten geldt en de verschillende directies van de gemeenten hebben hier op kunnen reageren. De werkinstructie 'procedure ernstige verstoring ICT' is in 2024 vernieuwd naar aanleiding van de gezamenlijke crisisoefening van de drie OWO gemeenten in april 2024 hebben uitgevoerd. Dit blijkt uit de memo "terugkoppeling OWO colleges bijeenkomst 2 april."

De werkinstructie ernstige verstoring ICT bevat een standaardprocedure die gevolgd moet worden zodat er op toegezien kan worden dat de verstoring met de juiste aandacht en op een gestructureerde wijze wordt behandeld. Een ernstige ICT verstoring wordt in deze werkinstructie beschreven als een incident waarbij meerdere personen niet verder kunnen werken omdat het kritische werkproces niet beschikbaar is of ernstig beïnvloed wordt door het probleem. Het doel van de procedure ernstige verstoringen is het gestructureerd oplossen van het probleem en een juiste prioritering bepalen om de dienstverlening te kunnen herstellen.

In de werkinstructie ‘ernstige verstoring ICT’ staat beschreven wie de crisiscoördinatoren zijn, wat een ernstige verstoring is, hoe prioriteiten aan verstoringen worden toebedeeld en een stappenplan om een ernstige ICT verstoring op te lossen. In het stappenplan staat beschreven wat er gedaan moet worden door de verschillende actoren en in welke volgorde. Het proces start met een melding van een verstoring die wordt beoordeeld door een securitymedewerker van Team ICT. Vervolgens beoordeelt de crisiscoördinator of er sprake is van een ernstig of major incident. Als dit het geval is dan stelt de crisiscoördinator een oplosteam samen en wordt er naar aanleiding van een eerste analyse een oplossingsrichting bepaald. Het oplosteam geeft prioriteit aan de herstelwerkzaamheden. Vervolgens wordt gestart met het herstellen van de dienstverlening en vindt er indien nodig regelmatig contact plaats met de CISO van de desbetreffende gemeente. Als laatste stap wordt onder verantwoordelijkheid van de crisiscoördinator een major incident rapport opgesteld dat naar de CISO’s van de OWO gemeenten wordt gestuurd. De betreffende medewerkers coördineren waar mogelijk de verbetervoorstellen.

Oefenen met crisissituaties is cruciaal om adequaat te kunnen handelen in het geval van een crisis. In april 2024 vond een oefening plaats met de colleges en gemeentesecretarissen van de drie gemeenten. Uit gesprekken met medewerkers bleek dat er binnen de OWO-samenwerking redelijk veel afspraken duidelijk zijn door de procedure ernstige verstoringen, maar dat er ook onderdelen zijn waar aanvullende afspraken over gemaakt moeten worden, zoals een gezamenlijk standpunt op ransomware[6].

De PDCA-cyclus op informatiebeveiliging is voor een groot deel bij de individuele gemeenten zelf belegd. Zo worden jaarlijks audits uitgevoerd volgens de ENSIA systematiek. Hiervoor levert Weststellingwerf voor Ooststellingwerf en Opsterland de gegevens op gebied van ICT aan. Ooststellingwerf levert de gegevens aan voor BAG en BGT rapportage. Op operationeel gebied worden technische verbeterplannen uitgevoerd door Team ICT van OWO bedrijfsvoering. Uit interviews is gebleken dat niet bij alle acties duidelijk is waar de verantwoordelijkheid ligt op het vervolg. Team ICT wordt daarnaast niet structureel betrokken bij de opstart en uitvoering van risicoanalyses door de individuele gemeenten.

Er is geen structureel overleg tussen de CISO’s van de drie gemeenten en Team ICT van OWO bedrijfsvoering. Uit gesprekken met medewerkers blijkt dat Team ICT niet altijd op de hoogte is van informatiebeveiligingsplannen van de gemeenten en dat de effectiviteit van advies en samenwerking daardoor beperkt wordt. Deze medewerkers geven aan dat er wel regelmatig contact is met de CISO van de gemeente Weststellingwerf en enig contact met de CISO van Opsterland. De CISO van Weststellingwerf treedt op als contactpersoon bij de ISO’s van de drie gemeenten. Echter, met de CISO van de gemeente Ooststellingwerf is minder vaak contact. De CISO's hebben onderlinge werkafspraken gemaakt. Eén van de werkafspraken is dat de CISO van West als contactpersoon optreedt bij I&A aangelegenheden (waaronder de ICT gerelateerde vragen vanuit ENSIA) en van daaruit doorschakelt naar de CISO's van Oost en Opsterland. De CISO van Oost is contactpersoon

[6] Informatiebeveiligingsdienst (IBD) De IBD is het Computer Emergency Response Team, of Computer Security Incident Response Team (CERT/CSIRT) voor alle Nederlandse gemeenten, en onderdeel van de Vereniging van Nederlandse Gemeenten.

voor wat betreft de OWO-onderdelen BVI en Backoffice Sociaal Domein. Uit gesprekken is ook gebleken dat enige tijd terug een CITSO (Chief Information Technical Security Officer) is aangenomen door OWO bedrijfsvoering. Deze CITSO dient als tussenpersoon tussen Team ICT van OWO bedrijfsvoering en de drie CISO's van de individuele OWO-gemeenten en adviseert op de technische infrastructuur. Ook blijkt uit de interviews dat de CITSO vanuit team ICT het nieuwe gezamenlijke strategische informatieveiligheidsbeleid coördineert en voor de drie OWO-gemeenten technische vraagstukken afstemt.

3.2 Opsterland

Het strategisch beleid voor informatiebeveiliging is bij de gemeente Opsterland vastgelegd in het document 'Strategisch Gemeentelijk informatiebeveiligingsbeleid Gemeente Opsterland'. Hiervoor heeft de gemeente het format van de Informatiebeveiligsdienst (IBD[7]) overgenomen. Dit heeft als voordeel dat het een actueel document is, waarin alle aspecten van het strategisch informatiebeveiligingsbeleid beschreven zijn. Het nadeel is dat in het document cruciale verbindingen met de situatie in Opsterland buiten beschouwing zijn gelaten omdat het format enkel algemeenheden beschrijft. Het document gaat niet in op de specifieke verbeter- of aandachtspunten van de gemeentelijke organisatie Opsterland. Het beleidsdocument is hierdoor een algemene beschrijving van voorbeeldbeleid en is geen richtinggevend document voor de gemeente Opsterland.[8]

Hieronder gaan we nader in op de uitwerking van de aspecten van het strategische informatieveiligheidsbeleid, waarbij we kijken naar de documenten die onder het strategisch beleid hangen. Hierbij zullen we telkens de verbinding maken tussen die documenten en het strategische beleid dat als basis dient.

3.2.1 BIO

De BIO wordt getoetst door middel van een zelfevaluatie. Uit de evaluatie van 2023 kwam een aantal verbeterpunten naar voren, waaronder het toegangsbeheer. De autorisaties worden nog te vaak niet op de juiste manier toegewezen, waardoor de ambtelijke organisatie risico's loopt. Er wordt ten tijde van dit onderzoek gewerkt aan een tool om dit te verbeteren.

Het BIO-normenkader beschrijft dat met alle leveranciers die, als verwerker voor of namens de organisatie persoonsgegevens verwerken, verwerkersovereenkomsten gesloten moeten worden waarin alle wettelijk vereiste afspraken zijn vastgesteld. De gemeente Opsterland heeft met de leveranciers van belangrijke applicaties verwerkersovereenkomsten gesloten. Op dit moment is de gemeentelijke organisatie de resterende applicaties in kaart aan het brengen en aan het onderzoeken of er verwerkersovereenkomsten gesloten dienen te worden.

Uit gesprekken met diverse medewerkers blijkt dat er momenteel wordt gewerkt aan een implementatieplan, door een werkgroep, voor de nog in te regelen maatregelen uit de BIO, aangezien deze nog niet allemaal aanwezig zijn in de ambtelijke organisatie. Zo mist momenteel een integrale aanpak voor het normenkader van de BIO, veel verschillende onderdelen zijn nog gescheiden.

De ambtelijke organisatie is, volgens gesprekken met functionarissen, op weg om te voldoen aan de BIO2 die in het kader van de Cyberbeveiligingswet verplicht wordt opgesteld. Maar voordat aan de BIO norm voldaan wordt, moet de ambtelijke organisatie nog wel een ontwikkeling doormaken. Momenteel worden werkzaamheden binnen informatiebeveiligingsprocesssen op verwerkingsniveau informeel uitgevoerd. Te weinig processen en procedures zijn vastgelegd of bekend en de PDCA-

[7] Informatiebeveiligingsdienst (IBD) De IBD is het Computer Emergency Response Team, of Computer Security Incident Response Team (CERT/CSIRT) voor alle Nederlandse gemeenten, en onderdeel van de Vereniging van Nederlandse Gemeenten.

[8] De gemeente is momenteel bezig het beleid te herzien. We hebben hier geen conceptdocumenten van ontvangen.

cyclus is onvoldoende aanwezig. Het aantoonbare cyclische doorlopende verbeterproces ontbreekt in de gemeente Opsterland. Om te voldoen aan de Cyberbeveiligingswet moet de gemeente een hoger volwassenheidsniveau realiseren waarbij prestaties worden gemeten, vergeleken en worden gebruikt voor een geoptimaliseerd leervermogen.

3.2.2 Incidenten(afhandeling)

De gemeente Opsterland heeft een actueel geldend privacy beleid waarin het juridisch kader, de toezichthoudende autoriteit, governance, beginselen, rechten van betrokkenen, website (cookies) en bewustwording uiteen wordt gezet. Daarnaast werkt de Privacy Officer van Opsterland op dit moment aan het inzichtelijk maken hoe in elk domein van de gemeentelijke organisatie het met privacy gesteld is. De volgorde waarin domeinen op gebied van privacy worden geanalyseerd, is gekozen op basis van een risico inschatting. Adviezen vanuit DPIA's (Data Protection Impact Assessments) worden opgenomen in audit- en controlerapportages, en er wordt gestreefd naar het verhogen van de rapportagefrequentie naar elk kwartaal.[9][10]

De gemeente Opsterland beschrijft het volgende in het strategisch beleid over incidenten(afhandeling):

- De gemeente kent een eigen systeem waarin incidenten worden vastgelegd.
- Dit systeem geeft waardevolle informatie om van te leren.

Incidenten worden gebruikt voor input bij het actualiseren van het beleid.

De gemeentelijke organisatie van Opsterland heeft een *Datalekprotocol*[11] waarin de te doorlopen stappen worden beschreven in het geval van een datalek, geschreven door de Chief Information Security Officer (CISO), die het document heeft geschreven toen hij de rol van Privacy Officer (PO) had. Ook worden de taken en verantwoordelijkheden van verschillende functies beschreven die een rol spelen bij een datalek, zoals de Privacy Officer (PO), CISO en de teammanager. Bijbehorend is er een *datalekregister* waar alle datalekken worden geregistreerd. De PO en CISO actualiseren het protocol en het register.

Uit interviews met de CISO en FG komt naar voren dat men in de veronderstelling is dat medewerkers het niet als een probleem ervaren om een datalek te melden. Medewerkers weten bij wie ze moeten zijn en wat de procedure is om te volgen. Het strategisch beleid wordt deels nageleefd door het 'eigen systeem' in de vorm van een datalekkenregister. Er staat niet gedocumenteerd wanneer het register herzien wordt en welke rol de incidenten hebben in de actualisatie van het beleid.

Uit het gesprek met de focusgroep met medewerkers in het sociaal domein komt echter een ander beeld naar voren. Door de deelnemers werd aangegeven dat de gemiddelde medewerker onvoldoende over kennis en kunde beschikt om een datalek te identificeren en vervolgens geen weet heeft waar ze die zouden moeten melden.

[9] Rapportages zijn niet aan ons beschikbaar gesteld tijdens de onderzoeksperiode. We kunnen het bestaan van de documenten bevestigen, aangezien er een enkele audit & controle rapportage bij het ambtelijk wederhoor is nagestuurd. Er valt dus nog steeds geen uitspraken te doen over de frequentie van de rapportage, enkel de uitgesproken ambitie.
[10] Dit geldt ook voor de uitgevoerde privacyscan door The Privacy Company. Document is pas beschikbaar gesteld na de onderzoeksperiode na het ambtelijk wederhoor.
[11] Op 28 maart 2025 (na de onderzoeksperiode) is een nieuwe versie van het datalekprotocol vastgesteld

3.2.3 PDCA-cyclus[12]

Volgens het strategisch beleid is informatiebeveiliging een continue verbeterproces. Dit krijgt vorm in de ‘Plan, do, check en act’-cyclus van het managementsysteem van informatiebeveiliging. In de ENSIA-rapportage worden ook de eventuele verbetermaatregelen opgenomen.

De ENSIA rapportage is onderdeel van de jaarlijkse cyclus en omvat ook het informatiebeveiligingsbeleid. Buiten de ENSIA-rapportage wordt de PDCA-cyclus onvoldoende in de praktijk gebracht bij de gemeente Opsterland. Uit het toegezonden ENSIA rapport van 2023 blijkt dat de gemeente Opsterland voldoet aan de eisen van de audit. ENSIA omvat echter niet de hele organisatie en het beleid. Het blijkt dat er niet periodiek niet aantoonbaar wordt gedocumenteerd en cyclisch verbeterd. In het jaarplan staat enkel dat bevindingen van de ENSIA rapportage zijn gebruikt om verbeteringen door te voeren en dat er maatregelen zijn getroffen voor de normen waar de gemeente Opsterland niet aan voldeed. Er zijn daarmee ook geen concrete verbeterplannen of andere documentatie gevonden die wijst op een vastgelegde PDCA-cyclus.
Dit is in tegenspraak met het strategisch beleid waarin de PDCA-cyclus als één van de belangrijke uitgangspunten is genoemd.

Ook de CISO en FG geven aan dat er elementen van de PDCA-cyclus aanwezig zijn, maar nog niet zijn geïntegreerd tot één geheel. Er is, voor zover wij konden onderzoeken, geen PDCA-cyclus, afgezien van de jaarlijkse ENSIA rapportages, aanwezig in de gemeente Opsterland.

3.2.4 Bestuur & organisatie

Het strategisch beleid van de gemeente Opsterland voorschrijft het Three Lines of Defence model voor de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging. In dit model is het lijnmanagement verantwoordelijk voor de eigen processen in de eerste lijn. De tweede lijn, waaronder de CISO, ondersteunt, adviseert en coördineert en bewaakt of het management zijn verantwoordelijkheden neemt. In de derde lijn wordt het geheel door een auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering, waaronder de FG.

De directie van gemeente Opsterland is volgens het beleid aangewezen voor de aansturing van het strategisch beleid. Zij zorgen dat alle processen en systemen zijn ondergebracht bij een afdelingsmanager. Daarnaast stelt de directie het gewenste niveau van continuïteit en vertrouwelijkheid vast en werkt de tactische informatiebeveiligingsonderwerpen uit. De uitvoering van informatiebeveiliging is belegd bij de teamleiders en zij vullen hun eigen rol in. Zij hebben een aantal taken, zoals het uitdragen van het informatiebeveiligingsbeleid en het vroegtijdig signaleren van de voornaamste bedreigingen.

[12] Nagezonden documenten versterken het beeld dat de PDCA cyclus nog onvoldoende in praktijk wordt gebracht. Een extra onderbouwing hiervan is de GAP-analyse uit 2023. In deze analyse worden 11 risico’s gesignaleerd, waarvan een aantal zeer ernstig. In het BIO-implementatieplan, waarvan wij in mei 2025 een ongedateerde conceptversie ontvingen, zijn dezelfde risico’s uit 2023 integraal overgenomen. Er is geen indicatie dat de risico’s zijn opgenomen in een werkproces en stellen wederom vast dat de PDCA cyclus niet tot uitvoer wordt gebracht. In aanvulling op ons onderzoeksrapport stellen wij wel ernstige tekortkomingen in (de uitvoering van) het digitale veiligheidsbeleid vast.

Bovendien staat in het document ‘Directieadvies audit en controle rapportage’ dat ‘aanbevelingen blijven lang liggen’. Dit wordt bevestigd door het feit dat de audit en control rapportages van 2023 en 2024 bijna exacte kopieën zijn op het gebied van informatiebeveiliging.

Uit het eerdergenoemde BIO-implementatieplan blijkt vervolgens dat gemeente twee jaar nodig heeft om aan de BIO te voldoen en door te groeien naar een volwassenheidsniveau 3. De BIO is al 8 jaar een verplichtend normenkader voor gemeenten en wordt wettelijk verplicht onder de Cyberbeveiligingswet.

De rol van het lijnmanagement wordt in de gemeentelijke organisatie Opsterland ingevuld door de gemeentesecretaris. De overige directieleden hebben geen formele rol als het gaat om informatieveiligheid, afgezien van het beleid. Veel taken zijn immers belegd bij de teamleiders. Deze laatste groep heeft de verantwoordelijkheid over de medewerkers en het informatiebeveiligingsbeleid. De FG en CISO zijn in de gemeente Opsterland onafhankelijk in positie gezet in de organisatie, waardoor ze onafhankelijk advies kunnen geven. Deze functionarissen geven aan dat ze contact hebben met de portefeuillehouder. Er is vertrouwen in de functionarissen vanuit het bestuur.

In de praktijk zijn veel taken bij de teamleiders belegd, zoals het toekennen van rollen in applicaties bij nieuwe medewerkers (gebruikersrechten), onboarding en bewustwording. Daarnaast zijn zij ervoor verantwoordelijk dat hun medewerkers de (gedrag)sregels voor digitale veiligheid in acht nemen. In interviews gaven zowel teamleiders als medewerkers aan dat dit voor extra werkdruk zorgde en niet altijd de aandacht kreeg die nodig was. Daarnaast geven medewerkers aan dat de FG, CISO en PO vaak onvoldoende op de hoogte zijn hoe de afdelingen werken en de daarbij behorende werkprocessen.

3.2.5 Weerbaarheid

Een van de strategische doelen van de gemeente Opsterland op gebied van informatieveiligheid is het minimaliseren van de risico's van menselijk gedrag. Dit wordt ingevuld door alle medewerkers te trainen in het gebruik van beveiligingsprocedures en in het verantwoord omgaan met persoonsgegevens en andere informatie.

Om de weerbaarheid van de hele gemeentelijke organisatie, mens en systeem, te kunnen garanderen, moet aan preventie worden gewerkt. Om nieuwe medewerkers te informeren en op te leiden betreffende informatieveiligheid, is er een onboardingstraining. De Privacy Officer is ten tijde van dit rekenkameronderzoek bezig met het herzien van deze onboarding. Zo is een nieuwe training ontwikkeld die in 2025 van start zal gaan voor alle nieuwe medewerkers.[13]

Uit gesprekken met verschillende medewerkers is gebleken dat er diverse activiteiten worden georganiseerd om de bewustwording rond informatieveiligheid te vergroten, zoals lezingen en de wekelijkse Digiheld-vraag. Deze activiteiten zijn echter niet verplicht en medewerkers kunnen makkelijk niet deelnemen. Ook lijken er geen informatiebeveiligingsopleidingen en/of trainingen te zijn voor zittende medewerkers, naast de vrijblijvende activiteiten. Daarnaast is informatieveiligheid geen onderwerp van gesprek in afdelingsoverleggen en het lijkt verder in de organisatie ook niet op de agenda te staan. De fysieke veiligheid van medewerkers wordt wel besproken tijdens dit soort overleggen.

In Opsterland wijst de praktijk uit dat het kennisniveau van de meeste medewerkers onvoldoende is om informatieveiligheid goed te borgen in de werkprocessen. In het gesprek met de focusgroep is aangegeven dat men de CISO en FGonvoldoende zichtbaar vindt met als gevolg dat medewerkers onwetend zijn. Dit bemoeilijkt het werken met persoonsgegevens omdat onvoldoende duidelijk is hoe medewerkers hiermee om moeten gaan en welke kaders en richtlijnen zij in hun werk moeten meenemen om digitaal veilig te zijn. Daarmee wordt niet voldaan aan de uitgangspunten van het strategisch beleid.[14]

3.2.6 Crisisorganisatie

Het adequaat reageren op incidenten wordt benoemd als strategisch doel van het informatieveiligheidsbeleid. Hieronder valt het oefenen met (cyber)crisissituaties. Het oefenen met crisissituaties staat echter niet als specifiek uitgangspunt genoemd in het strategisch beleid.

[13] Inmiddels is de nieuwe onboardingstraining begin 2025 van start gegaan. Dit was na de onderzoeksperiode.
[14] In het rapport van de Privacy Company wordt benoemd dat het niveau op bewustwording 4 is.

Er wordt momenteel gewerkt aan een cybercrisisoefening binnen de gemeente Opsterland, zo is gebleken uit gesprekken met functionarissen. Er is een oefening begin 2024 geweest om een cyberaanval OWO-breed te stimuleren. We hebben niet kunnen verifiëren dat de verbeterpunten binnen de gemeentelijke organisatie Opsterland zijn doorgevoerd aan de hand van een PDCA-cyclus. Daarnaast werd gemeld dat er in OWO-verband geoefend wordt, naast de gemelde oefening van begin 2024 al hebben we hier ook geen documentatie van ontvangen van de gemeente Opsterland. Er is aangegeven dat momenteel in OWO-verband wordt gewerkt aan een verdere invulling van de crisisstructuur.[15]

Oefenen met (cyber)crisisoefeningen is cruciaal in deze tijd om adequaat te kunnen handelen bij een soortgelijk incident, zoals het strategisch beleid voorschrijft. Dit is in de gemeente Opsterland nog niet geformaliseerd en geprofessionaliseerd. Het onderdeel crisisoefening ontbreekt in het strategisch beleid. Er wordt niet periodiek geoefend en het is onduidelijk wat er met de bevindingen en verbeterpunten uit de genoemde sessie van april 2024 is gebeurd. De PDCA-cyclus ontbreekt op dit vlak.

[15] De OWO directie heeft na de onderzoeksperiode een continuïteitsplan vastgesteld om dit te verbeteren.

4 Rol van de Raad

De gemeenteraad speelt een belangrijke rol bij de digitale veiligheid van de gemeente. De raad controleert immers het college of de veiligheid voldoet aan de daaraan gestelde eisen. Ook stelt de raad de beleids- en financiële kaders vast. Deze belangrijke rol van de raad is expliciet meegenomen in dit onderzoek. In elk van de OWO-gemeenten is gesproken met een vertegenwoordiging van de gemeenteraad. Na een korte introductie over de status van het onderzoek is met de aanwezige raadsleden een casus over digitale veiligheid besproken. Deze casus speelde zich af in een fictieve gemeente die in karakteristiek vergelijkbaar is met de eigen gemeente. Na de behandeling van deze casus is het gesprek gevoerd over de wijze waarop de raad thans de controlerende en kaderstellende rol ten aanzien van digitale veiligheid vervult. Vervolgens is gesproken over mogelijke verbeteringen van deze rol.

4.1 Informatievoorziening

Er zijn verschillende manieren waarop de raad geïnformeerd kan worden over informatieveiligheid. Allereerst zijn er raadsstukken die de situatie rondom informatieveiligheid uiteenzetten. Dit zijn bijvoorbeeld jaarrapportages en ENSIA evaluaties. Raadsleden kunnen daarnaast zelf ook vragen stellen over de actualiteiten rondom informatieveiligheid.

De CISO van Opsterland stelt gezamenlijk met de FG een jaarlijkse rapportage op, deze wordt door het college van b. en w. aan de gemeenteraad aangeboden. Deze jaarrapportage biedt een overzicht van de stand van zaken rondom informatieveiligheid. Daarnaast krijgen de gemeenteraadsleden informatie over de ENSIA-audit. Ook wordt de gemeenteraad geïnformeerd over nieuwe ontwikkelingen binnen de OWO-samenwerking.

Er zijn door de raad geen schriftelijke vragen ingediend over het onderwerp informatieveiligheid. Functionarissen vertellen dat de opkomst bij raadsbijeenkomsten op dit onderwerp over het algemeen ook laag is, al zijn alle fracties vaak wel vertegenwoordigd. Er lijkt weinig belangstelling voor het onderwerp. Wanneer de gemeenteraad mondelinge vragen stelt, gaan deze vooral over het technische deel in plaats van het menselijke en organisatorische deel van informatieveiligheid.

4.2 Perspectief raadsleden in Opsterland

In de raadsbijeenkomst in Opsterland leidt de casus tot veel herkenning. Sommige raadsleden geven aan dat het gebruik van jargon en afkortingen in documenten over digitale veiligheid niet bijdraagt aan een raadsbreed begrip van het onderwerp digitale veiligheid. Raadsleden die beter ingevoerd zijn in de materie geven aan dat het voor de gemeenteraad niet relevant is om te focussen op de techniek. Die is immers snel achterhaald. Ook de BIO en ENSIA rapportages bieden volgens hen te weinig aanknopingspunten voor de raad om te sturen.

Raadsleden zijn van mening dat digitale veiligheid meer aandacht en sturing van de gemeenteraad nodig heeft. De gemeente besteedt geld aan preventie, maar de raad krijgt geen inzicht in de besteding van deze middelen of in de incidenten die daarmee zijn voorkomen. Raadsleden hebben er onvoldoende zicht op of het college daadwerkelijk ‘in control’ is bij een cyberincident.

Een deel van de raadsleden wil periodiek worden bijgepraat over digitale veiligheid. Ook zou het onderwerp verankerd moeten worden in het inwerkprogramma van (nieuwe) raadsleden.[16]

[16] Er liggen plannen om privacy en informatiebeveiliging onderdeel te maken van het inwerkprogramma voor de raad. Deze ontwikkeling is niet ter sprake gekomen tijdens het onderzoek.

Niet alleen de kaderstellende en controlerende rol van de raad komt aan bod in deze bijeenkomst. Raadsleden zijn immers ook gebruikers van digitale voorzieningen. Er is aandacht voor digitale veiligheid bij ambtenaren en ook het college van b. en w. doet mee als het gaat om bewustwordingsactiviteiten als ‘phishing mails’. Dat geldt (nog) niet voor de raad terwijl ook raadsleden werken met vertrouwelijke informatie.

5. Beantwoording onderzoeksvragen en toetsing aan het normenkader

5.1 Beantwoording onderzoeksvragen

1. **Wat is het beleid op het gebied van informatieveiligheid; voldoet dit aan actuele standaarden (als de BIO en ENSIA) en zijn de gemeenten voorbereid op de BIO2 en ENSIA?**

De drie OWO-gemeenten stellen op dit moment hun eigen strategisch informatiebeveiligingsbeleid op. Team ICT werkt samen met de individuele OWO-gemeenten aan een gezamenlijk nieuw strategisch informatiebeveiligingsbeleid dat voor alle drie de gemeenten geldt. Individuele gemeenten bereiden zich voor op de BIO2, team ICT is hier via de CITSO bij betrokken. Voor de drie individuele gemeenten geldt wel dat ze verschillen in volwassenheid en de mate waarin ze aan de BIO en ENSIA standaarden voldoen. Het niveau van de gemeente Opsterland (en daarmee het voldoen aan de BIO en ENSIA) ligt lager dan de gemeenten Ooststellingwerf en Weststellingwerf.

Het beleid van de gemeente Opsterland is algemeen beschreven en niet toegespitst op de gemeente zelf. De BIO is niet volledig geïmplementeerd, er wordt momenteel gewerkt aan een plan met maatregelen. De verbeterpunten van de BIO uit 2020 zijn nog niet doorgevoerd. De gemeente is nog onvoldoende voorbereid op de BIO2 en ENSIA.

2. **Hoe wordt het Informatieveiligheidsbeleid uitgevoerd op bestuurlijk, organisatorisch, technisch, proces- en medewerkersniveau? Worden hierbij pentesten ingezet, zo ja, welke?**

Team ICT is verantwoordelijk voor de operationele activiteiten op gebied van informatieveiligheid. Op bestuurlijk niveau wordt Team ICT betrokken bij het nieuwe strategisch informatieveiligheidsbeleid dat door de drie gemeenten opgesteld wordt. Er is echter geen structureel bestuurlijk overleg tussen OWO en de portefeuillehouders van de individuele gemeenten. Daarnaast worden er periodiek pentesten en ENSIA audits uitgevoerd door Team ICT. De verantwoordelijkheid voor het vervolg op bevindingen van pentesten, interne audits en evaluaties zijn bij de desbetreffende OWO-gemeenten belegd. De opvolging daarvan is verschillend in uitvoering. Team ICT voert de technische en praktische bevindingen uit.

Het informatieveiligheidsbeleid van de gemeente Opsterland is algemeen en wordt niet structureel getoetst op uitvoering. Er worden vanuit Team ICTpentesten uitgevoerd. De uitvoering op het beleid laat verschillende witte vlekken zien. De gemeente Opsterland voert zelf geen (human) pentesten uit. De gemeente is bezig met het verhogen van de frequentie van de audit- en controlerapportages, maar het is momenteel onduidelijk wat de huidige frequentie is en wat er met de uitkomsten van de rapportages gebeurt.

3. **Zijn gegevens voldoende beschermd tegen toegang door onbevoegden? In hoeverre wordt getoetst of de organisatie ‘in control’ is op het gebied van informatiebeveiliging en welke instrumenten worden hierbij gebruikt?**

Team ICT voert het leveranciersmanagement uit voor de drie OWO-gemeenten. Alle grotere applicaties staan onder verantwoordelijkheid van team ICT van OWO, kleinere applicaties staan onder verantwoordelijkheid van de gemeenten zelf. De drie OWO-gemeenten werken gezamenlijk aan een overzicht van alle kernapplicaties en de bijbehorende regie verantwoordelijkheden. Het beheer op de juiste toegangsrechten voor applicaties is volgens team ICT van OWO nog niet sluitend geregeld binnen de gemeenten, waardoor onbevoegden mogelijk toegang kunnen krijgen tot gevoelige informatie en systemen. Team ICT van OWO maakt gebruik van tooling, logging, firewalls

en monitoring. Daarnaast is team ICT ook verantwoordelijk voor de uitvoering van de back-ups en restores van de OWO gemeenten.

In de gemeente Opsterland is momenteel nog onvoldoende controle op toegangsbeheer, zoals ook eerder geconstateerd in de BIO audit van 2020. Opsterland is momenteel bezig met het in kaart brengen van de resterende applicaties die de eigen gemeente heeft aangeschaft. Niet met alle leveranciers en externe partijen zijn er al verwerkersovereenkomsten gesloten en de gemeente heeft deze partijen nog niet volledig in beeld. Het risico bestaat dat gegevens in handen van onbevoegden vallen. De gemeente hanteert voor applicaties een twee-factor-authenticatie, al is er voor apparatuur geen beleid hierop. Er is geen overzicht op de gebruikersrechten en het is onduidelijk of dit periodiek wordt onderzocht.

4. **Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident, hoe ziet het incidentmanagementproces eruit en wordt dit in de praktijk geoefend?**

In OWO-verband is een procedure ernstige verstoringen waarin de volgorde en prioriteit van handelen tijdens een ernstige verstoring beschreven staat. Er wordt echter niet structureel geoefend met een uitgebreide verstoring zoals een cybercrisis. Ook zijn de taken en verantwoordelijkheden tijdens een cybercrisis tussen de individuele gemeenten en Team ICT momenteel niet geheel duidelijk.

In Opsterland is een procedure voor het melden van datalekken aanwezig en er wordt een jaarlijks overzicht gemaakt van de incidenten in de gemeente Opsterland. Er is geen crisisprotocol aanwezig en er wordt niet periodiek geoefend. Er is een enkele oefening op OWO niveau geweest, al heeft Opsterland hier geen documentatie over aangeleverd en is het niet benoemd in gesprekken. De uitkomsten en opvolging van deze oefening zijn onduidelijk. Team ICT van OWO bedrijfsvoering volgt een incidentenprotocol waardoor de dienstverlening in zekere mate geborgd lijkt.

5. **Hoe wordt omgegaan met risico’s en incidenten op het gebied van informatieveiligheid en in hoeverre toont de organisatie lerend vermogen (PDCA cyclus)?**

Er is geen gezamenlijke verbetercyclus voor de drie OWO-gemeenten. De risicoanalyses en incidentenprocedures worden bij de verschillende gemeenten verschillend uitgevoerd. Wel wordt binnen team ICT gewerkt aan monitoring en verbetering van zwakke punten in de informatiebeveiliging van de applicaties die op OWO niveau zijn belegd. Het verlenen en beheren van de juiste toegangsrechten voor gebruikers wordt door team ICT genoemd als een van die verbeterpunten. Een incident wordt vastgesteld bij de servicedesk van OWO door een gebruikersmelding van een medewerker van een van de OWO gemeenten of vanuit een van de monitoringstools. Team ICT monitort vervolgens of een incident een ernstige verstoring is en start de bijbehorende oplossingsmaatregel.

Er is in Opsterland geen volledige PDCA-cyclus. Er zijn wel elementen aanwezig, zoals een datalekprocedure en incidentenregister, maar er mist een sluitende systematiek waarin periodiek geleerd en verbeterd wordt op informatieveiligheid. Zo is het onduidelijk hoe er op de bevindingen van de ENSIA rapportages opvolging plaatsvindt. Incidenten worden bijgehouden, maar het is onduidelijk hoe risico’s worden gemonitord.

6. **Hoe wordt gezorgd voor bewustwording voor informatiebeveiliging bij medewerkers, bestuur, raad en samenwerkingspartners?**

Team ICT van OWO heeft geen rol in de bewustwording over informatiebeveiliging onder medewerkers van de individuele OWO-gemeenten. Er is geen gezamenlijke aanpak. De individuele gemeenten hebben hun eigen bewustwordingsprogramma. De intensiteit van dat programma verschilt per gemeente.

Opsterland heeft een verplichte onboarding voor nieuwe medewerkers, die in 2025 wordt herzien. Daarnaast organiseert de gemeente Opsterland bewustwordingsactiviteiten. Deze activiteiten zijn echter niet verplicht en medewerkers onttrekken zich er makkelijk aan. De monitoring van de activiteiten is onduidelijk en eventuele opvolging en verbeterplannen zijn er niet. Het kennisniveau op informatieveiligheid lijkt onvoldoende onder de medewerkers van de ambtelijke organisatie.

Er worden verwerkersovereenkomsten gesloten met samenwerkingspartners om de bewustwording te borgen. Binnen het bestuur is informatieveiligheid tijdens functioneringsgesprekken een onderwerp van gesprek. Onder de raadsleden is het geen onderwerp van gesprek, al is die wens er wel. De raad doet daarbij niet mee aan de wekelijkse bewustwordingsvraag.

7. **Zijn de rollen en taken op het gebied van informatiebeveiliging voor medewerkers en het management duidelijk en hoe wordt er gestuurd in de gemeentelijke organisatie?**

Er is geen structureel bestuurlijk overleg tussen Team ICT van OWO en de CISO's van de individuele gemeenten. Er is hierdoor nog geen eenduidige afstemming over het informatieveiligheidsbeleid en uitvoering tussen de gemeenten en Team ICT van OWO. De taken en verantwoordelijkheden binnen Team ICT liggen vooral op de technische en praktische uitvoering van ICT zoals het leveranciersmanagement en het beheer van de grotere applicaties. De drie OWO-gemeenten werken op dit moment gezamenlijk met Team ICT aan een overzicht autorisaties, rollen en taken van de kernapplicaties. Een CITSO dient als tussenpersoon tussen Team ICT van OWO bedrijfsvoering en de drie CISO's van de individuele OWO gemeenten en adviseert op de techniek.

De rollen en verantwoordelijkheden zijn in het beleid van Opsterland duidelijk uiteengezet. In de praktijk hebben teammanagers in de gemeente Opsterland echter meer taken en lijken de verantwoordelijkheden voor de informatiebeveiliging naar de achtergrond te verdwijnen. De FG en CISO zijn echter wel onafhankelijk binnen de ambtelijke organisatie en hebben een eigen budget. Ze staan sterk in hun positie naar het bestuur toe. Echter dit is niet het geval naar de medewerkers van de ambtelijke organisatie toe. Medewerkers zijn minder bekend met de FG en CISO en het is hen onduidelijk wat hun taken en verantwoordelijkheden zijn in de praktische uitvoering.

8. **Hoe is de raad betrokken bij het informatieveiligheidsbeleid en is dit voldoende om de kaderstellende en controlerende rol te kunnen vervullen?**

Raadsleden ontvangen een jaarlijkse rapportage en de resultaten van de ENSIA audit. Raadsleden geven aan onvoldoende kennis en informatie te hebben om hun taken uit te voeren. Dit wordt mede veroorzaakt door het gebrek aan informatievoorziening afgezien van het jaarlijkse rapport van de FG en CISO en de ENSIA rapportage.

5.2 Toetsing aan het normenkader

5.2.1 Normen ten aanzien van het beleid

Norm	Ooststellingwerf	Weststellingwerf	Opsterland	OWO
De gemeente heeft BIO- conform informatiebeveiligingsbeleid.				nvt
De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad.				
In het beleid wordt o.a. ingegaan op: • Strategische uitgangspunten • Risicomanagement • Governance (waaronder rollen en verantwoordelijkheden) • De PDCA-cyclus van de gemeente				nvt
In (voortgangs)rapportages wordt ingegaan op informatiebeveiliging.				nvt
In programma's en projecten wordt expliciet aandacht besteed aan informatiebeveiliging.				nvt
Er is een procedure hoe wordt omgegaan met informatiebeveiligingsincidenten (waaronder cyberaanvallen) en een crisisprotocol.				
De gemeente heeft beleid voor informatiebeveiliging ten aanzien van samenwerkingspartners, gemeenschappelijke regelingen en leveranciers.				

5.2.2 Normen ten aanzien van digitale veiligheid in de praktijk

Norm	Ooststellingwerf	Weststellingwerf	Opsterland	OWO
In de praktijk wordt gehandeld conform de wijze waarop informatie wordt beveiligd, waaronder in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren				

van burgers en het vragen van toestemming.				
De gemeente heeft een leer- en verbetercyclus (PDCA-cyclus).				nvt
De gemeente heeft inzicht in de belangrijkste verbeterplannen en –maatregelen.				
Er wordt in het geval van incidenten, calamiteiten en crisis volgens de vastgelegde procedures gehandeld.				
De vastgelegde controles en rapportages worden in de praktijk uitgevoerd.				
De gemeente test en toetst procedures regelmatig om de effectiviteit en werking te toetsen.				
De gemeente houdt toezicht op de afspraken ten aanzien van informatiebeveiliging met (samenwerkings)partners, regelingen en leveranciers.				
De gemeenteraad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.				nvt

5.2.3 Normen ten aanzien van de organisatiecultuur

Norm	Ooststellingwerf	Weststellingwerf	Opsterland	OWO
De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging en worden van aanpassingen op de hoogte gehouden.				
In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven.				
In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente op het gebied van informatiebeveiliging.				

Bijlage 1- Geïnterviewde personen

Afdelingshoofd OWO bedrijfsvoering
CISO Opsterland
FG Opsterland
Gemeentesecretaris Opsterland
Inkoopstrateeg OWO bedrijfsvoering
Privacy Officer Opsterland
Teamleider ICT OWO bedrijfsvoering
Wethouder Opsterland

Bijlage 2 - Documentatie

Documentnaam	Versie	Datum
Verwerkingsregister Opsterland		2024
Model verwerkersovereenkomst gemeente Opsterland		
Assurance rapport ENSIA audit 2023		25-04-2024
b. en w. -advies Collegeverklaring ENSIA 2023		16-04-2024
DPIA privacyprotocol ondermijning	1.0	12-2023
Datalekprotocol gemeente Opsterland		
Datalekregister AVG-gegevens		
Gemeentelijke informatiebeveiligingsplan ICT OWO[17]	4.0	18-12-2019
Informatiebeveiligingsplan Werk en Inkomen 2016	4.0	01-09-2016
Onboardingstraining privacy 2025		
Privacybeleid 2022-2026	1.0	
Rechten van betrokkenen protocol		
Strategisch Gemeentelijk Informatiebeveiligingsbeleid Gemeente Opsterland 2020		2020
Werkinstructie Procedure Ernstige Verstoring ICT[18]	1.9	04-2024

Nagestuurde documenten:

Documentnaam	Datum document	Document na onderzoeksperiode?
AC rapportage 2024 Q3	2024 Q3	Nee
Jaarplan Audit & Control 2024	2024	Nee
Actielijst OWO-afdeling Bedrijfsvoering	12-5-2025	Ja
Audit & Control rapportage interim 2023	2023	Nee
BIO vragenlijst Opsterland template 2025	2025	Ja
Concept OWO-informatiebeveiligingsbeleid	datum niet ingevuld (maar beleid voor 2026-2030)	Ja
Datalekprotocol - gemeente Opsterland v1.1	27-mrt	Ja
Datalekregister AVG-gegevens	2025	Deels
Directie advies Audit & Control rapportage interim 2023	1-7-2024	Nee
DT akkoord audit& control rapportage	17-7-2024	Nee
DT akkoord audit & control rapportage	22-1-2025	Ja

[17] Geldig voor alle OWO gemeenten. Aangeleverd door Opsterland.
[18] Geldig voor alle OWO gemeenten. Aangeleverd door Opsterland.

Gemeente Opsterland ENSIA 2023	25-4-2024	Nee
GAP analyse BIO: top 11 risico's	24-5-2023	Nee
Veilig werken bij Opsterland, dat doe je zo!	1-11-2024	Nee
Verslag overleg MT-breed	6-4-2023	Nee
Voortgangsrapportage interm 2022	2022	Nee
Werkinstructie Procedure Ernstige Verstoringen ICT	jun-24	Nee
Jaarplan Audit & control 2025	2025	Ja
Meldingen in TOPdesk OWO-gemeenten	9-10-2023	Nee
Privacybeleid 2022-2026	2022	Nee
Projectplan - implementatie BIO	geen datum, maar naar schatting begin 2025 (streefdoel 2 jaar en 2027 wordt genoemd als jaartal)	Ja
Gemeentelijk Informatiebeveiligingsplan ICT	18-12-2019	Nee
Incident Managment Proces	29-1-2025	Ja
Actielijst OWO-afdeling Bedrijfsvoering	26-5-2025	Ja
TO DO lijst printscreens	Q2 2025	Ja

Bijlage 3 - Lijst met afkortingen

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
Wpg	Wet politiegegevens
DPIA	Data Protection Impact Assessment
ENSIA	Eenduidige Normatiek Single Information Audit
IBP	Informatiebeveiliging en Privacy
FG	Functionaris Gegevensbescherming
CISO	Chief Information Security Officer
CITSO	Chief Information Technical Security Officer
PO	Privacy Officer
OWO	Ooststellingwerf, Weststellingwerf en Opsterland (samenwerkingsverband gemeenten)
PDCA	Plan-Do-Check-Act (kwaliteitscyclus)
BIO	Baseline Informatiebeveiliging Overheid
VNG	Vereniging van Nederlandse Gemeenten
KCC	Klant Contact Centrum
AP	Autoriteit Persoonsgegevens
b. en w.	Burgemeester en Wethouders
ICT	Informatie- en Communicatietechnologie
VTH	Vergunning Toezicht en Handhaving
I&A	Informatie en Automatisering
IBD	Informatie beveiligingsdienst