Informatieveiligheid in Ooststellingwerf: tussen ambitie en uitvoering

Rekenkameronderzoek naar beleid, uitvoering en bestuurlijke grip op digitale veiligheid

OOSTSTELLINGWERF

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 oktober 2024 tot januari 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 Ooststellingwerf

De gemeente Ooststellingwerf werkt op het gebied van ICT en informatiebeveiliging samen met Weststellingwerf en Opsterland 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.

Ooststellingwerf heeft een eigen strategisch informatiebeveiligingsbeleid dat in november 2023 is vastgesteld. Dit beleid is gebaseerd op de BIO-normen en richt zich op het verhogen van de informatieveiligheid en het verbeteren van de organisatie. De gemeente heeft een GAP-analyse uitgevoerd om te bepalen welke maatregelen nog nodig zijn om aan de BIO2 te voldoen. De uitvoering van deze maatregelen gebeurt stapsgewijs en wordt jaarlijks geëvalueerd.

De gemeente voert jaarlijks een ENSIA-audit uit en stelt een jaarrapport op over informatieveiligheid en privacy. Hierin worden ook de resultaten van zelfevaluaties en risicoanalyses besproken. In 2023 zijn er elf datalekken gemeld, vooral veroorzaakt door verkeerd geadresseerde e-mails. De Functionaris Gegevensbescherming (FG) houdt een register bij van deze incidenten en is het aanspreekpunt voor de Autoriteit Persoonsgegevens.

De gemeente gebruikt de PDCA-cyclus (Plan-Do-Check-Act) om continu te verbeteren. De CISO en FG coördineren deze cyclus en geven adviezen aan teamleiders op basis van audits en controles. Er worden ook technische en menselijke pentesten uitgevoerd, zoals phishingtests en mystery guests. De opvolging van de resultaten is echter niet altijd goed vastgelegd.

Binnen de organisatie zijn de rollen en verantwoordelijkheden verdeeld over het college van B&W, de directie, het lijnmanagement en de teamleiders. De CISO en FG vervullen een dubbele rol. Op het gebied van bewustwording worden er verschillende activiteiten georganiseerd, zoals wekelijkse kennisvragen, informatie op intranet en presentaties. Deelname is echter niet verplicht en er is geen vaste planning. Nieuwe medewerkers krijgen bij hun start uitleg over informatieveiligheid en moeten een VOG overleggen. Voor specifieke functies zijn er nauwelijks gerichte trainingen.

Rol van de gemeenteraad

De gemeenteraad van Ooststellingwerf ontvangt rapportages over informatieveiligheid, zoals de ENSIA-audit en het jaarrapport van de CISO en FG. In 2023 is er een themabijeenkomst georganiseerd over digitale veiligheid. Toch blijkt uit gesprekken dat raadsleden weinig vragen stellen over dit onderwerp en dat het thema weinig prioriteit krijgt. Sommige raadsleden hebben wel kennis van digitale veiligheid, maar anderen vinden het onderwerp te technisch en vertrouwen op collega's. De raad geeft aan behoefte te hebben aan betere informatie en ondersteuning om haar controlerende en kaderstellende rol goed te kunnen vervullen.

Belangrijkste bevindingen

- **Beleid**: Ooststellingwerf heeft een strategisch informatiebeveiligingsbeleid dat voldoet aan de BIO-normen, maar is nog niet volledig voorbereid op de nieuwe BIO2-standaarden.
- **Uitvoering**: Team ICT voert technische taken uit zoals beveiliging van systemen, pentesten en back-ups. Er is nog geen duidelijke verdeling van verantwoordelijkheden bij incidenten.
- **Incidenten**: Er zijn procedures voor het melden van datalekken. In 2023 waren er 11 datalekken, vooral veroorzaakt door verkeerd geadresseerde e-mails.
- **PDCA-cyclus**: De gemeente werkt met een jaarlijkse cyclus van plannen, uitvoeren, controleren en verbeteren. Resultaten worden gedeeld met de gemeenteraad.
- **Bewustwording**: Nieuwe medewerkers krijgen uitleg over informatieveiligheid. Er zijn wekelijkse kennisvragen en presentaties, maar deelname is niet verplicht en wordt niet goed gemonitord.
- **Crisisorganisatie**: Er is een crisisteam, maar er wordt weinig geoefend. De laatste oefening in 2024 verliep chaotisch.
- **Rol van de raad**: De gemeenteraad krijgt rapportages, maar stelt weinig vragen. Veel raadsleden vinden het onderwerp te technisch en geven aan onvoldoende kennis te hebben.

Conclusies en aanbevelingen

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

Conclusies

De gemeente Ooststellingwerf 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 Ooststellingwerf 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. Direct na afloop van dit onderzoek zijn plannen voor uitbreiding van de samenwerking gepresenteerd om de doelmatigheid en doeltreffendheid van beleid en uitvoering te vergroten.

In Ooststellingwerf is het strategisch informatiebeveiligingsbeleid vastgesteld door de gemeenteraad. Dit beleid sluit aan op de gangbare normen voor de gemeentelijke overheid. Zo wordt de Baseline Informatieveiligheid Overheid (BIO) als uitgangspunt van het beleid genomen. Ooststellingwerf voldoet nog niet helemaal aan deze norm, maar dit is wel een belangrijke doelstelling. 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 Ooststellingwerf volledig aan de gestelde norm.

Uit het onderzoek komt ook naar voren dat de medewerkers van de gemeente Ooststellingwerf het belang van digitale veiligheid onderkennen. Het bewustzijn hiervoor is toegenomen. Maar ook op dit vlak is verbetering mogelijk. Op dit moment is de gemeente Ooststellingwerf zelf verantwoordelijk voor de digitale weerbaarheid van de eigen medewerkers door middel van trainings- en bewustwordingsactiviteiten. Er worden incidenteel wel trainingen aangeboden, maar deelname is vrijblijvend. Een gestructureerde aanpak van training 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. niet 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 Ooststellingwerf geen vraag gesteld over dit onderwerp.

Een laatste conclusie betreft de crisisorganisatie. Als er, ondanks alle preventieve maatregelen die de gemeente Ooststellingwerf (individueel of in OWO samenwerkingsverband) genomen heeft, toch een digitale verstoring plaatsvindt, moet er snel gehandeld worden om de schade te beperken. Bij majeure verstoringen wordt dan een crisisorganisatie ingericht. Dat gebeurt ook in Ooststellingwerf. Er is een crisisprotocol en een crisisteam, maar er wordt niet structureel geoefend.

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 op korte termijn gezamenlijk beleid te formuleren.***
   Maak hiermee een einde aan onduidelijkheid in taakverdeling tussen de OWO samenwerking en de gemeente Ooststellingwerf 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 Ooststellingwerf heeft stappen gezet in de implementatie van de Baseline Informatiebeveiliging Overheid (BIO). Maar de gemeente voldoet niet op alle onderdelen aan de BIO. Dat betekent dat de gemeente kwetsbaar blijft en digitale veiligheidsrisico's loopt. Een 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 4 (voorspelbaar en geoptimaliseerd). Dit niveau kan worden bereikt door een systematische monitoring van beveiligingsmaatregelen en het verbeteren van de interne evaluatieprocessen.

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.
   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.***
   Op het terrein van digitale veiligheid 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 worden uitgevoerd.

Weerbaarheid:

5. ***Maak bewustwordingsactiviteiten verplicht voor medewerkers, bestuurders en raadsleden en zorg voor een gestructureerde aanpak voor opleiding en training.***
   Vrijblijvende activiteiten kunnen leiden tot lage deelname en onvoldoende kennis en vaardigheden ten aanzien van digitale veiligheid. Verplichte 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

gemeente ooststellingwerf

Contactpersoon:
Telefoonnummer:
Zaaknummer:
Documentnummer:

Rekenkamercommissie Ooststellingwerf
t.a.v. mevrouw H. Vervoort

Onderwerp: Bestuurlijke reactie rapport onderzoek informatieveiligheid

Oosterwolde, 3 juni 2025

Beste mevrouw Vervoort,

Het rapport van uw rekenkamercommissie over het onderzoek naar informatieveiligheid in de gemeente Ooststellingwerf hebben wij met belangstelling gelezen. Hierbij geven we graag onze reactie op het onderzoek.

Algemene reactie
Binnen de gemeenten maken we steeds meer en steeds vaker gebruik van geautomatiseerde systemen. Ook is er sprake van toenemende (digitale) informatie-uitwisseling tussen overheidsorganisaties onderling en met burgers en bedrijven door ontwikkelingen zoals internet en telewerken. We moeten hierbij rekening houden met de privacyregels. Burgers, bedrijven, instellingen moeten de overheid kunnen vertrouwen en hebben er recht op te weten wie welke gegevens verzamelt en waarvoor deze gebruikt worden. Het is daarom van groot belang dat gegevens alleen onder strikte voorwaarden gebruikt worden en goed beveiligd zijn tegen onbevoegd gebruik. De gemeente Ooststellingwerf onderkent het voldoen aan de eisen van informatiebeveiliging en privacy.

Inhoudelijke reactie
Hieronder leest u een puntsgewijze opsomming van uw aanbevelingen aan de gemeenteraad en onze reactie hierop

Algemeen:
Onafhankelijke positie CISO/FG
In uw rapport stelt u dat de CISO en FG nog niet volledig in hun onafhankelijke positie zijn gezet. Hier kunnen wij ons niet in vinden. De gecombineerde rol van CISO/FG binnen de gemeente Ooststellingwerf is organisatorisch belegd, volledig onafhankelijk buiten de lijn. De FG ontvangt geen instructies, adviseert, signaleert en rapporteert gevraagd en ongevraagd zoals ook in het Reglement voor de FG is opgenomen en als zodanig is vastgesteld. Er is geen sprake van belangenverstrengeling tussen de FG-taken en die van de rol van CISO. In de rol van CISO wordt niet het doel en de middelen van de gegevensverwerking bepaald. Vanuit die onafhankelijke positie beschikt de CISO/FG derhalve niet over eigen budget, dat is ook niet nodig. Het aanwenden van budget voor het treffen van beveiligingsmaatregelen is een verantwoordelijkheid van directie en lijnmanagement. De CISO/FG houdt onafhankelijk toezicht of de implementatie van de maatregelen in voldoende mate is geborgd, waaronder het aanwenden van budget voor het inzetten van instrumenten om het informatiebeveiligings- en privacy bewustzijn binnen de organisatie op peil te houden.

Wanneer directie en lijnmanagement niet zichtbaar voldoen aan het inzetten van instrumenten (en daarvoor geen budget beschikbaar stellen) rapporteert de CISO vanuit zijn

onafhankelijke rol aan directie dat aan deze maatregel niet wordt voldaan. Wanneer de CISO zelf zou beschikken over een budget om aan te wenden voor dit doel dan is de CISO op dit punt de beheersmaatregel van de organisatie, hij draagt dan immers direct zorg voor implementatie van de norm, daar waar de CISO juist toezicht houdt of genoemde maatregel in voldoende mate binnen de organisatie is geborgd. Wanneer de CISO zou beschikken over budget en dit budget niet voor dit doel zou inzetten, dan wordt daarmee niet aan deze maatregel voldaan en zou de CISO zichzelf tot de orde moeten roepen (slager keurt daarmee zijn eigen vlees).

In artikel 38, Lid 6 van de AVG is opgenomen dat de functionaris voor gegevensbescherming andere taken en plichten kan vervullen en dat de verwerkingsverantwoordelijke ervoor zorgt dat deze taken of plichten niet tot een belangenconflict leiden. Deze splitsing in de inhoudelijk rol van CISO (organisatorisch of technisch uitvoerend) wordt echter niet als zodanig in de berichtgeving op de website van de AP gemaakt. De wijze waarop de gemeente hieraan invulling heeft gegeven voldoet volledig aan de AVG.

***Beleid en Uitvoering**:*
Aanbeveling 1. Intensiveer de samenwerking in OWO verband en breid deze uit door niet alleen de uitvoering gezamenlijk op te pakken, maar ook op korte termijn gezamenlijk beleid te formuleren.
Op 9 december 2024 is op basis van een afwegingskader door de OWO-directie besloten om de beleidsmatige kant van informatiebeveiliging gezamenlijk op te pakken. Daarmee volgen wij deze aanbeveling al op.

Aanbeveling 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.
In de OWO-samenwerking wordt inmiddels gewerkt aan een projectmatige (meerjaren-)aanpak waarin een keuze is gemaakt de BIO2 risicogericht te implementeren. Het volwassenheidsniveau voor informatiebeveiliging wat hierbij wordt nagestreefd is minimaal niveau 3.

De verwachting is dat de projectgroep ongeveer twee jaar nodig heeft om de BIO2 voor de bepaalde scope te implementeren. Naar verwachting is het project rond 1 juli 2027 afgerond om daarmee aan te sluiten op het afleggen van bestuurlijke verantwoording in het kader van ENSIA.

Incidenten(afhandeling):
Aanbeveling 3. Verhoog de aandacht voor risicobeheersing en zorg voor een duidelijke opvolging van incidenten.
Er is reeds voldoende aandacht voor risicobeheersing en zorg voor duidelijke opvolging van beveiligingsincidenten. De wijze waarop, is duidelijk verwerkt in de procedure. In de situatie van een beveiligingsincident, waarbij persoonsgegevens betrokken zijn, is er sprake van een datalek. Uit het rapport onder 3.2.2. lijkt het alsof wij hebben verzuimd deze datalekken te melden aan de AP, echter indien er geen gevoelige of bijzondere persoonsgegevens zijn gelekt en er geen ernstige nadelige gevolgen van de persoonlijke levenssfeer van betrokkenen zijn, is een melding aan de AP niet verplicht, maar is registratie van het datalek en terugkoppeling aan de verantwoordelijken voldoende.

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

Deze aanbeveling kunnen wij niet plaatsen, omdat wij dat ons inziens al doen. In de rapportage aan de gemeenteraad staat een overzicht van ondernomen acties om tot het gewenste niveau van informatiebeveiliging te komen en staan de overige actiepunten in een verbeterplan beschreven. De opvolging van de audits op informatieveiligheid en privacy worden gemonitord en gecoördineerd door de CISO en FG. De gemeente voldoet zichtbaar aan alle normen binnen de ENSIA-audit. Aanbevelingen, niet dwingend van aard, worden niet verwerkt in een verbeterplan maar worden teruggekoppeld aan de verantwoordelijken om na te gaan of er eventueel quick wins mogelijk zijn. De gemeente hanteert hierin een risicogerichte aanpak. De PDCA-cyclus is daarmee voldoende geborgd.

Weerbaarheid:
Aanbeveling 5. Maak bewustwordingsactiviteiten verplicht voor medewerkers, bestuurders en raadsleden en zorg voor een gestructureerde aanpak voor opleiding en training.
Alle nieuwe medewerkers en contractanten worden conform de BIO binnen 3 maanden na indiensttreding geïnstrueerd over informatiebeveiliging en privacy via de onboardingsapp als onderdeel van het inwerkprogramma. Door de directie is in het verleden besloten de kwaliteitsleercirkel informatieveiligheid toe te passen en jaarlijks instrumenten voor zittend personeel in te zetten in het kader van bewustwording. Dit doet Ooststellingwerf ook. Dit heeft echter geen verplicht karakter, het volgen van medewerkers past niet binnen de cultuur van de gemeente Ooststellingwerf. In de praktijk is ook gebleken dat deelname aan de verschillende bewustwordingsactiviteiten hoog is. Het volgen en monitoren van deelname door medewerkers, bestuurders en raadsleden is privacygevoelig. We zullen HRM en de OR betrekken om te onderzoeken of het gewenst is aan bewustwordingsactiviteiten een verplicht karakter mee te geven en van daaruit te komen tot een gestructureerde aanpak.

Crisisorganisatie:
Aanbeveling 6. Organiseer periodieke crisisoefeningen en borg de effectiviteit ervan binnen een PDCA-cyclus.
De gemeente Ooststellingwerf onderschrijft het belang van het periodiek oefenen met crisissituaties. In de OWO-samenwerking ligt het voornemen de rollen en verantwoordelijkheden helder vast te leggen in een bedrijfscontinuïteitsplan en aan te sluiten op de bestaande crisisorganisatie.

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.

Over de voortgang van het digitaal veiligheidsbeleid wordt de raad geïnformeerd in de paragraaf Bedrijfsvoering en in een separate rapportage informatieveiligheid en privacy. De mate waarin de gemeente voldoet aan de BIO norm maakt hiervan op hoofdlijnen onderdeel uit. De gemeente Ooststellingwerf zal bezien op welke wijze hierin verbeteringen kunnen worden doorgevoerd. We gaan in gesprek met de raad over wat nodig is om de controlerende en kader stellende rol op dit gebied te vervullen en daarbij de raad in zijn kracht te zetten.

Met vriendelijke groet,
het College van burgemeester en wethouders

E.H.C. van der Laan
gemeentesecretaris

J. Werkman
burgemeester

Bijlage(n):
Mandaatregeling:

Nawoord

De Rekenkamer bedankt het college voor de uitgebreide bestuurlijke reactie en de daarin opgenomen expliciete onderkenning van het belang van het voldoen aan de eisen van informatiebeveiliging en privacy. 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.

Voor twee 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 er al voldoende aandacht is voor risicobeheersing en het opvolgen van beveiligingsincidenten. Dit wordt vervolgens gekoppeld aan het melden van datalekken waarbij wordt aangegeven dat het rekenkamerrapport zegt dat de gemeente daar verzuimd heeft. Dit is niet het geval en dat hebben we ook in de memorie van antwoord op het ambtelijk wederhoor teruggekoppeld - in het rapport geven we aan dat niet alle datalekken gemeld hoeven te worden bij de AP. Dit is in lijn met wat het college aangeeft. Maar, risicobeheersing gaat immers verder dan alleen het melden van datalekken indien dat noodzakelijk is. Deze aanbeveling komt voort uit de bevinding dat de risicobeheersing in processen waar veel persoonsgegevens verwerkt worden geoptimaliseerd kan worden. 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 deze aanbeveling niet te kunnen plaatsen omdat ze audits en adviezen al opvolgen en documenteren. In ons onderzoek komt naar voren dat er inderdaad over het algemeen planmatig wordt gewerkt binnen de gemeente, zoals we in de toelichting op de aanbeveling ook schrijven. Het is heel goed dat de gemeente al grotendeels op deze manier werkt. In het onderzoek hebben we echter ook aanknopingspunten voor optimalisatie gevonden. Die optimalisatie ligt hem voornamelijk in het goed documenteren en vervolgens structureel opvolgen van de (uitvoering van) de verbeterplannen. Het college geeft in het bestuurlijk wederhoor aan dat aanbevelingen (uit de audits) die niet dwingend van aard zijn, worden teruggekoppeld aan de verantwoordelijken en niet worden vastgelegd. Dat is wat ons betreft juist een voorbeeld waarvan we zeggen: leg het wel vast, zodat ook deze aanbevelingen in beeld blijven en opvolging gewaarborgd is. Als dat gedaan wordt dan is de invulling van de PDCA-cyclus nog steviger dan deze nu is.

Naar aanleiding van de toelichting van het college op de positie van de CISO en de FG willen we extra toelichten waarom de dubbelrol van de CISO en FG ons inziens problematisch is. De dubbelrol brengt de onafhankelijkheid in het geding, omdat het kan resulteren in een FG die zijn eigen werk moet controleren, omdat dezelfde functionaris ook de CISO-functie heeft. Een CISO ontwikkelt beleid en geeft advies en de FG moet vervolgens dat beleid controleren. In hoeverre is die controle goed mogelijk als je zelf ook de ontwikkelaar of adviseur kunt zijn geweest? Daarnaast kan het belangenverstrengeling veroorzaken wanneer beveiligingsmaatregelen botsen met privacybescherming. Als laatste moet de FG kunnen opereren zonder instructies te ontvangen over de uitvoering van de eigen taken. Wanneer de FG en CISO dezelfde persoon zijn, kan dit leiden tot een situatie waarin de FG instructies moet opvolgen die in strijd zijn met de vereiste onafhankelijkheid. De Autoriteit Persoonsgegevens draagt ook deze onwenselijkheid van het combineren van CISO en FG rollen uit[1].

[1] https://www.binnenlandsbestuur.nl/digitaal/brabants-privacytoezicht-gebeurt-vaak-met-een-dubbele-pet

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.[2]

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) heeft 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?

[2] 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

Voorafgaand aan dit onderzoek heeft de rekenkamer een vooronderzoek gedaan bij de drie gemeenten, waarin gesprekken zijn gevoerd en documentatie is verzameld. Het onderzoek bestond uit verschillende fasen. Het onderzoek is gestart met een startbijeenkomst voor betrokken medewerkers van de drie gemeenten. Vervolgens is een documentstudie uitgevoerd en zijn verdiepende interviews gehouden. Om te onderzoeken hoe in de OWO-gemeenten het beleid in praktijk wordt gebracht, zijn voor elke gemeente bijeenkomsten met een focusgroep en raadsbijeenkomst georganiseerd. Om te toetsen of de onderzoeksbevindingen correct waren, is voor aanvang van het schrijven van het rapport een convergentiesessie uitgevoerd met ambtelijk betrokkenen van de drie OWO-gemeenten. Op basis van de verkregen informatie is onze analyse uitgevoerd en deze rapportage geschreven.

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 Ooststellingwerf. 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.

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

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 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.

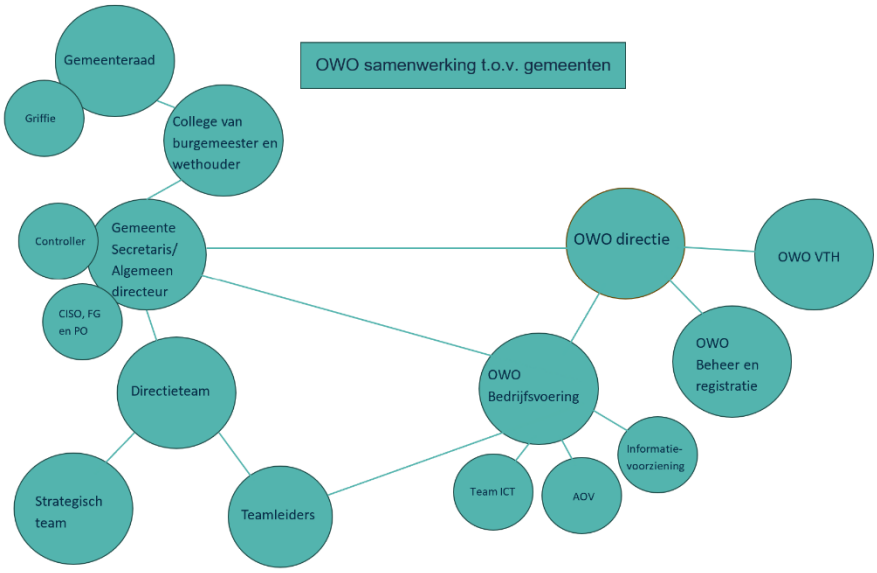
Bij weerbaarheid gaat het in eerste instantie om preventieve maatregelen die worden genomen om digitale verstoringen te voorkomen. Voorbeelden van deze maatregelen zijn het autorisatiebeleid en de toegang van medewerkers tot de verschillende informatiesystemen. Ook bewustwordingsactiviteiten als (online) 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 (penetratietesten) 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.

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

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 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. Echter, met de CISO van de gemeente Ooststellingwerf is minder vaak contact. De CISO's hebben onderlinge werkafspraken gemaakt.

[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.

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 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 Ooststellingwerf

Het strategisch beleid voor informatiebeveiliging en privacy is bij de gemeente Ooststellingwerf vastgelegd in het document 'Informatiebeveiligingsbeleid Ooststellingwerf'. Deze is vastgesteld op 7 november 2023 door het college van b. en w. In dit strategische informatiebeveiligingsbeleid staan de belangrijkste prioriteiten voor de komende jaren vermeld. Dit zijn het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. In het document wordt gesteld dat een betrouwbare informatievoorziening noodzakelijk is voor het goed functioneren van de gemeente en is de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist volgens de gemeente Ooststellingwerf een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn.

De gemeente Ooststellingwerf werkt op dit moment aan de vernieuwing van het strategisch informatiebeveiligingsbeleid op basis van het BIO normenkader. Zo is er een GAP analyse uitgevoerd om te bezien welke maatregelen nog uitgevoerd moeten worden in het kader van de BIO. De implementatie van die maatregelen vindt gefaseerd plaats. De volgorde van implementatie wordt in de jaarrapportage beschreven.

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

In het gemeentelijk informatiebeveiligingsbeleid van Ooststellingwerf is de BIO als normenkader opgenomen. Het BIO normenkader bevat het totaalpakket aan informatiebeveiligingsmaatregelen die gelden voor iedere gemeente, zo ook Ooststellingwerf. Het BIO normenkader wordt jaarlijks met een zelfevaluatie getoetst. De CISO speelt hierbij een coördinerende rol.

In het jaarrapport Informatieveiligheid en Privacy van 2023 van Ooststellingwerf wordt een aantal zaken genoemd die uit de zelfevaluatie en de GAP-analyse zijn gekomen, en nog (deels) geïmplementeerd moeten worden met oog op de BIO2. Risicobeheersing is hierbij het belangrijkste doel. Allereerst wordt er prioriteit gegeven aan gemeente brede informatiebeveiliging, waaronder ook HRM en dienstverlening. Daarna ligt de focus voornamelijk op informatiesystemen, die persoonlijke en andere gevoelige gegevens bevatten van inwoners en de eigen medewerkers van de ambtelijke organisatie.

Om te kunnen voldoen aan het BIO normenkader is een aantal acties ondernomen. Hierover wordt gerapporteerd in het jaarrapport over Informatieveiligheid en Privacy 2023.

Zo wordt gestreefd naar een meer planmatige aanpak waarbij periodiek over de voortgang van de implementatie wordt gerapporteerd. Hieronder valt de GAP-analyse en zelfevaluatie van de BIO. De gemeente stelt dat dit een jaarlijks terugkerend proces is.

Het BIO normenkader stelt dat met alle leveranciers die, als verwerker voor of namens de gemeentelijke organisatie persoonsgegevens verwerken, verwerkersovereenkomsten gesloten moeten worden waarin alle wettelijk vereiste afspraken zijn vastgesteld. De onderzoekers hebben geen inzicht verkregen in het verwerkingsregister en verwerkersovereenkomsten van de ambtelijke organisatie.

Uit gesprekken komt naar voren dat de BIO rapportage in de gemeente Ooststellingwerf ter besluitvorming wordt voorgelegd aan de directie. De gemeentelijke organisatie bereidt zich momenteel voor om te voldoen aan de BIO2 in het kader van de Cyberbeveiligingswet. Uit gesprekken met medewerkers blijkt dat het daarin nog stappen kan zetten op het gebied van het volwassenheidsniveau van digitale veiligheid. Momenteel bevindt de gemeentelijke organisatie van Ooststellingwerf zich op niveau 2; het beheersd en herhaalbaar processen uitvoeren. Om te kunnen voldoen aan de Cyberbeveiligingswet moet de gemeentelijke organisatie echter groeien naar niveau 4 (voorspelbaar). Op dit niveau worden prestaties gemeten, vergeleken en gebruikt voor een geoptimaliseerd leervermogen. De ambtelijke organisatie van de gemeente Ooststellingwerf heeft wel de ambitie om door te groeien, zo blijkt uit interviews, maar de concrete plannen zijn er nog niet.

3.2.2 Incidenten(afhandeling)

De gemeente Ooststellingwerf beschrijft in het strategisch informatieveiligheidsbeleid dat incidenten mogelijk negatieve gevolgen kunnen hebben voor burgers, bedrijven, partners en de eigen organisatie met mogelijk politieke consequenties. Daarnaast stelt het strategisch informatieveiligheidsbeleid dat een van de strategische doelen het adequaat reageren op incidenten is. De gemeentelijke organisatie van Ooststellingwerf rapporteert jaarlijks door middel van de ENSIA systematiek over de incidenten en risico’s met betrekking tot informatieveiligheid.

Er worden binnen de ambtelijke organisatie van Ooststellingwerf DPIA’s (Data Protection Impact Assessment) uitgevoerd aan de hand van een stroomschema. De FG adviseert in dit traject en de Privacy medewerker voert de DPIA uit.

Het college van b. en w. heeft in 2017 de procedure meldplicht datalekken vastgesteld met daarin een stroomschema voor het melden en afhandelen van een datalek. Deze procedure is in 2019 geactualiseerd in het kader van de AVG en in 2023 geactualiseerd in het kader van de Wpg. De FGvan Ooststellingwerf is de contactpersoon richting de Autoriteit Persoonsgegevens en houdt centraal een register bij van beveiligingsincidenten en datalekken die binnen de gemeentelijke organisatie van Ooststellingwerf hebben plaatsgevonden. In het jaarrapport van 2023 zijn er 11 datalekken geregistreerd. Deze voldeden echter niet allemaal aan de verplichtingen voor een melding bij de AP.

Uit gesprekken met medewerkers blijkt dat de FG en CISO van Ooststellingwerf goed benaderbaar zijn in de organisatie. Medewerkers weten ze te vinden zodra iets een datalek zou kunnen zijn en er wordt dan ook direct contact gezocht. Dit wordt gezien als basisprincipe op de afdelingen van de gemeente Ooststellingwerf. De meest voorkomende datalekken gaan voornamelijk over verkeerd geadresseerde mails of contactgegevens. Medewerkers zijn zich ervan bewust dat het om een datalek gaat en zijn bekend met de procedure.

3.2.3 PDCA-cyclus

Het college van b. en w. van Ooststellingwerf verantwoordt zich over informatiebeveiliging met de ENSIA-rapportage. Zo legt het College van b. en w. jaarlijks verantwoording af aan de gemeenteraad met een door een externe auditor ondertekende verklaring. Uit de ENSIA rapportage blijkt dat de ambtelijke organisatie voldoet aan alle normen die gesteld worden. Zo blijkt bijvoorbeeld uit de BRP audit dat de gemeente Ooststellingwerf in 2023 een score heeft behaald van 97%, waarmee voldaan wordt aan de gestelde veiligheidseisen. De gemeente toont daarmee aan goede resultaten te hebben behaald op gebied van informatiebeveiliging. In de rapportage aan de gemeenteraad staat een overzicht van ondernomen acties om tot het niveau van informatiebeveiliging te komen en staan de overige actiepunten in een verbeterplan beschreven.

Daarnaast publiceren de CISO en de FG van Ooststellingwerf gezamenlijk een jaarrapport waarin de behaalde resultaten, ontwikkelingen, activiteiten, incidenten en risico's met betrekking tot informatieveiligheid en privacy worden beschreven. De jaarrapportage wordt ter kennisname naar de gemeenteraad van Ooststellingwerf verstuurd. De beide functionarissen geven aan dat naast het jaarrapport ook adviezen aan de lijnorganisatie meegegeven worden. Deze adviezen zijn gekoppeld aan de bevindingen uit het jaarrapport.

De opvolging van de audits op informatieveiligheid en privacy worden gemonitord en gecoördineerd door de CISO en FG. Specifieke adviezen voor teams worden gekoppeld aan de betreffende teamleiders. De FG en CISO voeren daarnaast jaarlijkse controles op gebruikersrechten, op basis van de verkregen overzichten vanuit HR. Op basis van deze controles worden verbeterplannen opgesteld met bevindingen die ook worden gerapporteerd aan de teamleiders. Het opvolgen van deze verbeterplannen valt onder verantwoordelijkheid van de teamleiders.

Periodiek worden er pentesten en phishing-testen uitgevoerd vanuit team ICT van OWO-bedrijfsvoering. De FG en CISO van Ooststellingwerf hebben een mystery guest geïnitieerd. Uit de interviews is duidelijk geworden dat opvolging van de bevindingen door de beveiligingsfunctionarissen CISO en FG van Ooststellingwerf wordt gecoördineerd. De resultaten of bevindingen zijn gerapporteerd, maar de opvolging hiervan is niet terug te vinden in de documentatie. Naar aanleiding van het inzetten van de mystery guest zijn adviezen opgesteld en wordt bijgehouden welke maatregelen op basis van deze adviezen ondernomen zijn.

3.2.4 Bestuur & organisatie

Het strategisch beleid onderscheidt vier rollen met betrekking tot informatiebeveiliging: het College van b. en w. van Ooststellingwerf in de beslissende rol, de directie in de sturende rol, het lijnmanagement in de vragende rol en als laatst de teammanagers in de uitvoerende rol.
Het college van b. en w. stelt het informatiebeveiligingsbeleid formeel vast en controleert de uitvoering van dit beleid. De directie adviseert over het vaststellen van dit beleid, stuurt op risico's en is verantwoordelijk voor de kaderstelling. Het lijnmanagement is verantwoordelijk voor het opstellen van beveiligingseisen en plannen. Teammanagers van de verschillende domeinen rapporteren aan de beveiligingsfunctionaris (CISO). De rol van College van b. en w., de directie en het lijnmanagement van Ooststellingwerf zijn beschreven in het beleidsdocument "Verantwoordelijkheden voor de informatiebeveiliging."

In het strategisch informatieveiligheidsbeleid is de rol van de beveiligingsfunctionaris (CISO) beschreven. De CISO coördineert, houdt toezicht, adviseert gevraagd en ongevraagd en rapporteert aan de directie van gemeente Ooststellingwerf. De CISO is daarnaast secretaris van de beveiligingsadviescommissie die periodiek afstemming heeft over het informatiebeveiligingsbeleid. Deze commissie bestaat uit vakinhoudelijke specialisten of teamleiders van de gemeente Ooststellingwerf op gebied van I&A, Beheer en Onderhoud, burgerzaken en sociaal domein.

De rol van de FG en de privacy officer worden niet verder uitgewerkt in het strategisch informatiebeveiligingsbeleid.

Volgens het normenkader van de BIO2 dient de CISO zo gepositioneerd te zijn binnen de organisatie dat hij onafhankelijk van de lijn kan adviseren over informatieveiligheid. De CISO en FG functie zijn beiden in een duo rol belegd. Twee functionarissen vervullen daarmee dus zowel de CISO als de FG rol. Zij zijn onafhankelijk gepositioneerd binnen de organisatie om te rapporteren en signaleren, maar hebben geen budgetten om de adviezen op te stellen. Op die manier zijn zij wel volledig afhankelijk van de budgetten van de lijnorganisatie voor de uitvoering van deze adviezen en zijn daarmee dus nog niet volledig in hun onafhankelijke positie gezet. Het is daarbij wettelijk vastgelegd dat de FG geen taken mag uitvoeren die buiten het takenpakket van een FG vallen, zoals een CISO.

De FG en CISO van Ooststellingwerf zijn wel goed te vinden en worden ook door de andere medewerkers als onafhankelijk gezien. Verschillende medewerkers vertellen dat er een open cultuur heerst op het gebied van informatieveiligheid. Teamleiders agenderen het onderwerp in team overleggen, maar agendering kan ook vanuit de teams zelf komen. Men stelt dat het gesprek op verschillende momenten vanzelf op gang komt. Bij de gesproken medewerkers is duidelijk bij wie de expertise ligt in de ambtelijke organisatie om de lastige informatiebeveiligingsvraagstukken op te pakken, namelijk bij de FG en de CISO.

3.2.5 Weerbaarheid

Een van de strategische doelen van de ambtelijke organisatie Ooststellingwerf op gebied van informatieveiligheid is het minimaliseren van de risico's van menselijk gedrag. Om de weerbaarheid van de gemeentelijke organisatie te kunnen garanderen, moet er aan preventie gewerkt worden. Dit kan door verschillende bewustwordingsacties onder medewerkers uit te zetten. Bij de gemeente Ooststellingwerf komt tijdens de onboarding van nieuwe medewerkers informatieveiligheid aan bod en hebben nieuwe medewerkers een Verklaring Omtrent het Gedrag (VOG) nodig om te kunnen werken bij de gemeentelijke organisatie. Daarnaast werkt de gemeentelijke organisatie Ooststellingwerf aan bewustwording door wekelijkse korte kennisvragen over informatieveiligheid en privacy uit te zetten naar alle zittende medewerkers via Digiheld en maandelijkse informatie over informatieveiligheid en privacy op intranet te delen. Daarnaast worden er activiteiten rondom bewustwording georganiseerd, zoals een lezing en een presentatie aan de gemeenteraad. Voor specifieke functiegroepen zijn geen aparte opleidingen over informatieveiligheid, met uitzondering van een training omtrent het veilig gebruik van Suwinet. Zo hebben teammanagers verschillende uitvoerende taken rondom informatieveiligheid, maar is er geen verplichte opleiding die hen daarvoor voorbereid.

Weerbaarheid wordt onder meer ook getest door middel van een phishingtest, periodieke pentesten en de inzet van een mystery guest. In 2024 is zowel een phishingtest als een pentest uitgezet. De uitvoering en opvolging van bevindingen uit pentesten ligt op technisch vlak bij de Team ICT van OWO bedrijfsvoering, tenzij bevindingen binnen de scope van de gemeentelijke organisatie van Ooststellingwerf vallen. De coördinatie van het behandelen van deze bevindingen ligt bij de beveiligingsfunctionarissen, de CISO en FG, van de gemeente Ooststellingwerf.

Medewerkers van de gemeente Ooststellingwerf zijn niet verplicht om deel te nemen aan deze bewustwordingsactiviteiten. De opkomst bij evenementen en het deelnemerspercentage van de trainingen en de Digiheld vragen worden wel gemonitord en teruggekoppeld aan teammanagers door de beveiligingsfunctionarissen. De onderzoekers hebben geen inzichten en inhoudelijke gegevens ontvangen vanuit deze monitoring. De bewustwordingsactiviteiten kennen daarnaast geen vaste cyclus of jaarplanning en worden incidenteel ingepland. In het bestuur is informatieveiligheid geen onderwerp van gesprek.

3.2.6 Crisisorganisatie

In het strategisch informatieveiligheidsbeleid van de gemeente Ooststellingwerf staat beschreven dat er een crisisteam is geïnstalleerd voor het interne crisisbeheer. Dit team staat onder leiding van de gemeentesecretaris van Ooststellingwerf. De onderzoekers hebben geen documenten over de werkwijze van dit crisisteam ontvangen. Daarnaast staat in het strategisch beleid beschreven dat de gemeente participeert in landelijke platforms en contacten met de Informatiebeveiligingsdienst (IBD) onderhoudt.

Er is op 2 april 2024 voor het laatst geoefend met een cybercrisis in OWO-verband, al is dit volgens betrokken en gesproken medewerkers chaotisch verlopen omdat de doelstellingen als onrealistisch werden ervaren. Het was namelijk onduidelijk wat met de oefening bereikt moest worden. De ambitie is om in de toekomst vaker gezamenlijk te oefenen met de ambtenaren openbare orde en veiligheid en dat in OWO-verband. In ieder geval is uit gesprekken met functionarissen duidelijk geworden dat het essentieel is om een goed afgesproken crisisstructuur te hebben waarbij goede informatie uitwisseling van belang is. Hierbij is de wens uitgesproken om met deze structuur in de praktijk te gaan oefenen. Tijdens de onderzoeksperiode was dit nog niet gebeurd.

In het strategisch beleid van gemeente Ooststellingwerf wordt het belang van oefenen met (cyber)crisissituaties onderschreven, maar er lijkt na de laatste oefening verder geen invulling aan het onderwerp gegeven. Er wordt nog niet periodiek geoefend en het is onduidelijk wat er met eventuele bevindingen en verbeterpunten van de oefening van april 2024 gebeurt. Een PDCA-cyclus ontbreekt op dit vlak.

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 gemeenteraad geïnformeerd wordt over informatieveiligheid. Allereerst zijn er raadsstukken die de situatie rondom informatieveiligheid uiteenzetten. Dit zijn bijvoorbeeld jaarrapportages en ENSIA-rapportages. Raadsleden kunnen daarnaast zelf ook vragen stellen over de actualiteiten rondom informatieveiligheid.

De CISO van Ooststellingwerf 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 raadsleden informatie over de ENSIA-audit. Ook wordt de gemeenteraad geïnformeerd over nieuwe informatiebeveiliging ontwikkelingen binnen de OWO samenwerking.

In 2023 is er een themabijeenkomst georganiseerd voor de gemeenteraad van Ooststellingwerf over privacy en informatieveiligheid.

De gemeenteraad heeft sinds 2018 geen schriftelijke vragen gesteld over het onderwerp informatieveiligheid of digitale veiligheid. Op de website van de gemeenteraad zijn afgezien van de jaarrapportages over informatieveiligheid en privacy geen stukken te vinden. Over de jaarrapportages zijn geen schriftelijke vragen gesteld. Medewerkers geven aan dat zij het jammer vinden dat de gemeenteraad weinig interesse lijkt te hebben in het onderwerp informatieveiligheid.

4.2 Perspectief raadsleden in Ooststellingwerf

Uit de raadsbijeenkomst kwam naar voren dat de raadsleden van Ooststellingwerf een wisselend kennisniveau hebben ten aanzien van digitale veiligheid. Een deel van de raadsleden heeft in het dagelijks werk te maken met IT en digitale veiligheid en is daarom bekend met de ‘techniek’. Deze raadsleden kunnen uit de voeten met het jargon en willen in algemene zin meer informatie. Het deel van de raadsleden dat aangeeft minder verstand te hebben van digitalisering, weet op basis van de verkregen informatie de controlerende en kaderstellende rol niet goed in te vullen. Zij vertrouwen op het oordeel van collega-raadsleden die beter in de materie zitten.

Raadsleden van Ooststellingwerf onderkennen over het algemeen het toegenomen belang van digitale veiligheid, maar geven aan hier nog onvoldoende op te sturen. Dat heeft enerzijds te maken met de informatie die de raad ontvangt en anderzijds met het feit dat de gemeenteraad zelf zegt te weinig prioriteit toe te kennen aan dit thema.
Zo is er onlangs op het niveau van de OWO-samenwerking een raadsbijeenkomst georganiseerd, maar was de opkomst vanuit de gemeenteraden laag. Ook geeft men aan dat zij niet weten of in de andere OWO-gemeenten raadsvragen over dit onderwerp worden gesteld.

De raadsleden van Ooststellingwerf vinden over het algemeen dat het geen zin heeft om te sturen op ‘techniek’. Dat vraagt volgens hen om veel detailkennis en is bovendien snel achterhaald. Maar ook de jaarlijkse ENSIA rapportage, waarin is aangegeven of de gemeente voldoet aan de veiligheidseisen die door stelselhouders zijn gesteld aan kernapplicaties (bijvoorbeeld Digid, Suwinet, BRP) en de informatie die de raad ontvangt in het kader van de P&C cyclus, bieden voor raadsleden onvoldoende aanknopingspunten om de sturende rol waar te maken.

De gemeenteraadsleden van Ooststellingwerf hebben geen eenduidig beeld over de wijze waarop ze hun sturende rol in kunnen vullen en welke informatie daarvoor nodig is. Wel geeft een aantal raadsleden aan in gesprek te willen over de positie van en informatievoorziening aan de raad, met name voor wat betreft incidenten.

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 in Ooststellingwerf is hierbij hoger dan in Opsterland en relatief gelijk aan Weststellingwerf. Geen van de drie gemeenten voldoen volledig aan de BIO.

Het lokale beleid voldoet deels aan de actuele standaarden. De gemeente Ooststellingwerf scoort voldoende op de ENSIA vragenlijst. De BIO is echter nog onvoldoende geïmplementeerd. Dit wil de gemeente door middel van de GAP-analyse gaan verbeteren. Momenteel heeft de gemeente Ooststellingwerf nog niet de volwassenheid op het gebied van informatieveiligheid om te voldoen aan BIO2 en ENSIA en zijn dus onvoldoende voorbereid.

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. Dit zijn technische testen op de apparatuur en applicaties die vanuit OWO ICT worden uitgegeven. 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 beleid in Ooststellingwerf wordt uitgevoerd met behulp van de verbeterplannen die voortkomen uit de jaarrapporten over de behaalde resultaten. Hiervoor worden periodiek de uitkomsten van OWO ICT pentesten gebruikt. Daarnaast voert de gemeente Ooststellingwerf ook human pentesten uit, in de vorm van mystery guests en phishing testen.

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. Dit resulteert erin dat de organisatie niet volledig ‘in control’ is, omdat het toegangsbeheer niet sluitend en overzichtelijk ingeregeld is. 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.

De gebruikersrechten zijn nog niet goed genoeg geregeld bij de gemeente Ooststellingwerf. OWO ICT is verantwoordelijk voor het toekennen van gebruikersrechten aan medewerkers, maar de informatie voor het toekennen van deze rechten komt van gemeenten zelf. De teammanagers zijn verantwoordelijk voor het doorgeven van gebruikersrechten en aanpassingen daarop aan OWO ICT. Er wordt jaarlijks een check gedaan op de gebruikersrechten van medewerkers.

Het toegangsbeheer is goed geregeld is bij de gemeente Ooststellingwerf, waardoor de gemeente beschermd is tegen toegang door onbevoegden. De gemeente werkt met twee-factor-authentificatie voor toegang tot applicaties. De gemeentelijke organisatie is op dit vlak ‘in control’, maar mist op andere gebieden de controle op informatieveiligheid, zoals te zien is aan het nog bescheiden volwassenheidsniveau.

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.

Ooststellingwerf heeft een procedure aanwezig voor incidenten en datalekken. De ambtelijke organisatie maakt jaarrapporten met een overzicht van alle incidenten. Er is geen crisisprotocol aanwezig en er wordt niet periodiek geoefend. Er is een enkele oefening in OWO verband geweest, maar de uitkomsten en opvolging van deze eenmalige oefening is onduidelijk. De verdeling van taken en verantwoordelijkheden tijdens een cybercrisis zijn momenteel ook onduidelijk.

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 zaken die op OWO niveau zijn geregeld. 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 Ooststellingwerf een jaarlijkse PDCA-cyclus door middel van de ENSIA rapportages. De behaalde resultaten van de ENSIA rapportage worden gezamenlijk met informatie over incidenten, risico’s en uitgevoerde plannen rondom informatieveiligheid in een jaarlijkse rapportages beschreven. Deze rapportages zijn organisatiebreed beschikbaar en worden gedeeld met de gemeenteraad. De jaarrapporten worden ook gebruikt door de CISO om adviezen naar betreffende teams te sturen, om zo gerichte verbeteringen door te voeren.

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.

Er is een verplichte onboarding voor nieuwe medewerkers in Ooststellingwerf. Er worden bewustwordingsactiviteiten georganiseerd en er is een wekelijkse vraag voor alle medewerkers. Alle activiteiten zijn echter vrijblijvend en medewerkers kunnen zich hier makkelijk aan onttrekken. De monitoring van de activiteiten en eventuele opvolging is ook niet altijd duidelijk.
Daarmee kan niet met zekerheid iets gezegd worden over het bewustwordingsniveau van medewerkers binnen de ambtelijke organisatie op het gebied van informatieveiligheid. Binnen het bestuur is informatieveiligheid geen onderwerp van gesprek en bewustwording kan verbeterd worden.

Het is onduidelijk of er verwerkersovereenkomsten worden gesloten met samenwerkingspartners en of hier bewust met informatieveiligheid wordt omgegaan. Daarnaast is het onduidelijk of de gemeenteraad betrokken wordt bij de bewustwordingsactiviteiten. Er is een verschillend kennisniveau binnen de gemeenteraad.

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 verantwoordelijkheden worden voor alle rollen op het gebied van informatiebeveiliging in de gemeentelijke organisatie van Ooststellingwerf staan beschreven. De CISO en FG hebben echter een dubbelrol en hebben geen eigen budget en zijn daarmee niet volledig onafhankelijk in hun positie gesteld. Dit is problematisch aangezien het vanuit de AVG verplicht is dat de FG geen andere taken uitvoert dan die voor de FG zijn vastgesteld om de onafhankelijkheid van de FG te waarborgen. Er wordt gestuurd op informatieveiligheid vanuit de FG, CISO en PO.

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

De raadsleden ontvangen rapportages, maar niet frequent. Raadsleden ontvangen enkel de ENSIA rapportages en het jaarrapport van de CISO dacht ik, dit is te weinig informatie om te kunnen sturen op informatieveiligheid. Daarnaast stellen ze weinig vragen en stellen ze zelf het kennisniveau te missen. De raad geeft aan te weinig prioriteit te geven aan op het thema. Raadsleden komen bij een bijeenkomst over dit thema maar in lage getalen opdagen. Het kennisniveau is onvoldoende voor de raadsleden om hun kaderstellende en controlerende rol uit te voeren.

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
Burgemeester Ooststellingwerf
FG/CISO Ooststellingwerf
FG/CISO Ooststellingwerf
Gemeentesecretaris Ooststellingwerf
HR Ooststellingwerf
Inkoopstrateeg OWO bedrijfsvoering
Privacy Officer Ooststellingwerf
Teamleider ICT OWO bedrijfsvoering

Bijlage 2 - Documentatie

Documentnaam	Versie	Datum
Presentatie iBewustzijn Bestuur en Management		30-11-2026
Advies b. en w. – Informatiebeveiligingsbeleid gemeente Ooststellingwerf		05-12-2023
Advies b. en w. – plan van aanpak ENSIA 2023		07-11-2023
Advies b. en w. – rapport mystery guest		12-01-2018
Advies b. en w. – Verantwoording informatieveiligheid ENSIA 2023		02-04-2024
Advies college proces Data Protection Impact Assessment AVG Wpg		05-12-2023
Advies directie informatiebeveiligingsbewustzijn		28-09-2016
Advies directie procedure rechten van betrokkene AVG Wpg		07-11-2023
Advies directie proces meldplicht datalekken		30-11-2023
Beleidsuitgangspunten IB Sociaal Domein Ooststellingwerf	8.0	20-12-2023
Beleidsuitgangspunten informatiebeveiliging BRP en waardedocumenten		
Beleidsuitgangspunten informatiebeveiliging webapplicaties DigiD	2.0	
Besluit b. en w. informatiebeveiligingsbeleid		05-12-2023
Besluit b. en w. rapportage informatieveiligheid en privacy 2022		16-05-2023
Besluit b. en w. verantwoording informatieveiligheid ENSIA		02-04-2024
Besluit MT Plan van aanpak ENSIA 2023		11-11-2023
Directie-advies: Afwegingskader opstellen informatieveiligheidsbeleid		09-12-2024
Evaluatie phishingtest		26-02-2024
Formulier melding datalek Ooststellingwerf AVG Wpg		
Handreiking DPIA Ooststellingwerf 2023		10-2023
Informatiebeveiligingsbeleid Gemeente Ooststellingwerf	5.0	07-11-2023
Mededeling aan de raad – rapportage informatieveiligheid en privacy 2022		16-05-2023
Mededeling aan de raad – rapportage informatieveiligheid en privacy 2023		21-05-2024
Overzicht aanbevelingen, acties en advies tot aanvullende maatregelen – rapport Mystery guest		16-07-2020
Plan van aanpak ENSIA 2024		
Privacybeleid extern AVG Wpg		02-2023
Privacybeleid intern AVG Wpg		11-2022

Privacyverklaring AVG Wpg		02-2023
Presentatie: Kick-off Sociaal domein		07-01-2025
Presentatie Themabijeenkomst ICT Voor raadsleden van de OWO gemeenten		
Raadsbrief: afwegingskader informatieveiligheidsbeleid		
Rapportage Informatieveiligheid en Privacy periode 2022		02-05-2023
Registratie beveiligingsincidenten – datalekken		16-09-2024
Reglement Functionaris Gegevensbescherming AVG Wpg		
Samenvatting behaalde resultaten informatieveiligheid en privacy		2022
Stroomschema DPIA		2023
Stroomschema meldplicht datalekken AVG Wpg		
Terugkoppeling OWO-colleges bijeenkomst cyberaanval oefening		01-10-2024
Verantwoordelijkheden voor de informatiebeveiliging		

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