Gemeente Midden-Delfland

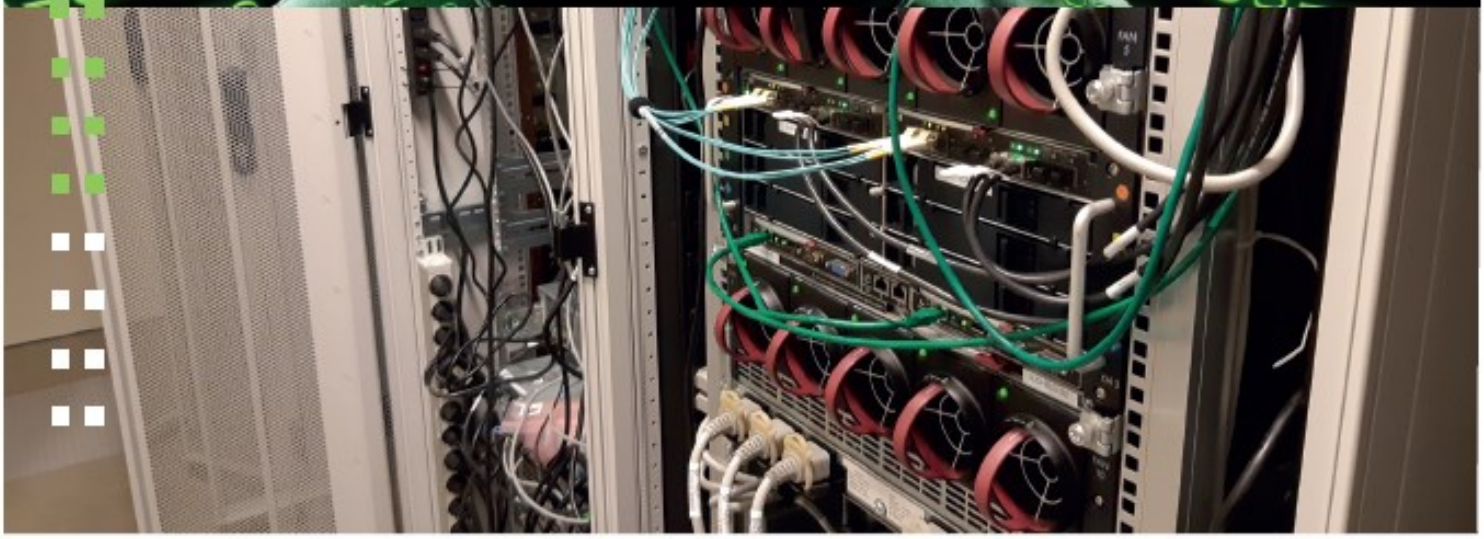
cittaslow

Jaarverslag Informatiebeveiliging Midden-Delfland

2023







Inhoud

Managementsamenvatting 3
Activiteiten in 2023 3
Beveiligingsincidenten 4
Zelfevaluaties 4
Vooruitblik 2024 op het gebied van de informatiebeveiliging 5
1. Inleiding 6
2. IB-beleid, doelstellingen en ambities 7
Wat is informatiebeveiliging? 7
Baseline Informatiebeveiliging Overheid (BIO) 7
Uitgangpunten en doelen van ons informatiebeveiligingsbeleid 8
Relatie met privacy 8
3. Horizontale en verticale verantwoording op basis van ENSIA 10
Verantwoordingsrapportages zelfevaluatie 2023 12
Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet 16
4. Samenvattend beeld en resultaten informatiebeveiliging 2023 17
Resultaat meting BIO 18
5. Disclaimer 21
6. Realisatie doelstellingen IB-beleid 22
Controls & beheersmaatregelen IB 23
Verbeterpunten op basis van meting BIO 24
7. Incidenten en ontdekte kwetsbaarheden 27
8. Meerjarenperspectief 30
Grootste risico’s voor gemeenten 30

Managementsamenvatting

Het college van B&W van gemeente Midden-Delfland legt jaarlijks verantwoording af over de uitvoering van het informatiebeveiligingsbeleid.
Dit jaarverslag Informatiebeveiliging Midden-Delfland 2023 bevat die verantwoording.

Het jaarverslag is gebaseerd op een actuele meting vanuit ons ISMS[1]. Deze meting is uitgevoerd op basis van de 112 normen zoals opgenomen in de Baseline Informatiebeveiliging Overheid (BIO). Hierin zijn ook de resultaten uit de Eenduidige Normatiek Single Information Audit (ENSIA[2]) 2023 opgenomen. Deze meting heeft het karakter van een zelfevaluatie waarbij is nagegaan in hoeverre de gemeente voldoet aan de 112 normen uit de BIO.

De normen uit de BIO zijn vooral vanuit een generiek beeld beoordeeld en niet specifiek toegespitst op applicaties. In het jaarverslag houden we rekening met verbeterpunten die voortkomen uit de meting over de BIO, ENSIA 2023 en de DigiD/Suwi-audit. De verbeterpunten met de hoogste risico's vormen het jaarplan 2024.

Het college van B&W wordt verzocht het jaarverslag informatiebeveiliging 2023 vast te stellen en de CISO het mandaat te geven het jaarplan met verbeteracties uit te (laten) voeren.

Activiteiten in 2023

In 2023 is op het gebied van informatiebeveiliging het volgende gerealiseerd:

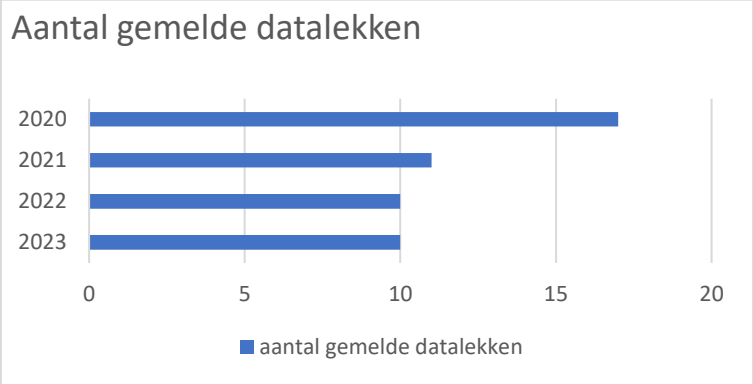
- We stelden in 2023 een nieuw geactualiseerd strategisch informatiebeveiligingsbeleid op, het vorige was 3 jaar oud en verloopt daarmee.
- We zijn gestart met het opstellen van bedrijfscontinuïteitsbeleid en crisisplannen voor onze meest kritieke processen op om voorbereid te zijn op crisissituaties dit loopt door in 2024.
- Ons Responsible Disclosure beleid[3] is vastgesteld en gepubliceerd op onze website.
- We zijn in 2022 gestart met de overgang naar Microsoft Office 365 als cloud-oplossing waarbij we belangrijke beveiligingsaspecten integreren in de verbeterde toegankelijkheid, dit gefaseerde project loopt door in 2024.
- We zijn in 2022 gestart met vernieuwing van onze WiFi-omgeving in het gemeentehuis die sterkverouderd was en niet meer aan alle informatiebeveiligingseisen voldeed. Dit project is afgerond in 2023.
- We zijn in 2023 samen met de gemeente Westland gestart met het opstellen van een pakket van eisen voor een gezamenlijke aanbesteding van een SIEM/SOC[4]. De daadwerkelijke aanbesteding hiervan gaat in 2024 plaatsvinden. Met een SIEM/SOC kunnen we 24/7 beveiligingsinformatie verzamelen, combineren en analyseren uit onze bronnen, zoals firewalls, IDS/IPS-systemen[5], antivirussoftware en logboeken van servers en netwerkapparaten. Het identificeert potentiële beveiligingsincidenten en genereert waarschuwingen die kunnen worden onderzocht door een medewerkers in een SOC.
- Het verouderde Thuiswerkbeleid is geactualiseerd naar het beleid voor hybride werken.
- Er zijn verschillende ad-hoc maatregelen genomen om geconstateerde kwetsbaarheden in gebruikte software op te lossen.
- Het is een verplichting vanuit de BIO om structureel aandacht aan training en bewustwording te geven over informatiebeveiliging en privacy. Aan deze verplichting voldoen we door medewerkers structureel te informeren over informatiebeveiliging en privacy. In 2023 is er een nieuwe meting gedaan onder de medewerkers op de mate van bewustzijn op informatiebeveiliging en privacy. Hierop is een strategisch jaarplan voor de bewustwordingsactiviteiten opgesteld.

[1] ISMS staat is een Engelse afkorting en staat voor Information Security Management System. In het Nederlands wordt dit aangeduid als een managementsysteem voor informatiebeveiliging.
[2] ENSIA staat voor Eenduidige Normatiek Single Information Audit
[3] Responsible disclosure is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden. Iedereen kan een responsible disclosure-melding doen onze gemeente.
[4] SIEM / SOC zijn afkortingen en staan voor 'Security Information & Event Management' en 'Security Operations Center. Het is kort samengevat een zeer proactieve bewaker van jde IT-omgeving, die in staat is kleine verdachte veranderingen, met mogelijk grote gevolgen, al in een vroeg stadium te herkennen en de kop in te drukken.
[5] Inbraakdetectiesystemen (IDS) en inbraakpreventiesystemen (IPS) houden ons netwerk constant in de gaten. Ze identificeren mogelijke incidenten en loggen informatie daarover, waarop gehandeld kan worden.

Beveiligingsincidenten

In 2023 zijn 22 spammails, 6 incidenten en 197 geconstateerde kwetsbaarheden gemeld bij de CISO en adviseurs informatiebeveiliging. Het gaat hierbij ook om ontdekte kwetsbaarheden die met updates van software en zijn opgelost. De gemelde kwetsbaarheden kwamen voornamelijk van de Informatie Beveiligingsdienst (IBD) en betroffen geconstateerde kwetsbaarheden in software met advies over hoe deze te verhelpen.

In 2023 zijn 10 datalekken gemeld bij de privacy officer. In 2020 was dit nog 17 keer.



Het lijkt hier om een trend te gaan die aandacht verdient. Van een organisatie met de omvang van de gemeente Midden-Delfland kan verwacht worden dat elk jaar enkele tientallen datalekken plaatsvinden, waar gewerkt wordt worden immers ook fouten gemaakt. In geen van de in 2023 geconstateerde datalekken bleek het nodig om de Autoriteit Persoonsgegevens en betrokkenen te informeren. Geconstateerd wordt dat het datalekkenregister adequaat wordt bijgehouden.

Zelfevaluaties

Gemeenten moeten richting de Rijksoverheid verantwoording afleggen over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI):

- De BRP en reisdocumenten (PUN) scoren met een 100% score goed op de norm.
- De gemeente Midden-Delfland is DigiD aansluithouder voor de Persoonlijke Internetpagina en web-formulieren van ons zaaksysteem. Door een externe IT-auditor is vastgesteld dat wordt voldaan aan het gestelde normenkader.
- Over het gebruik van Suwinet is door een externe IT-auditor vastgesteld dat op alle onderdelen wordt voldaan aan het gestelde normenkader.
- BAG scoort met 92% ruim voldoende, derhalve worden nog verbeteracties voorgesteld.
- BGT scoort met 100% goed op de norm.
- BRO scoort met 84% goed op de norm.

De zelfevaluatie van de WOZ is vanaf 2023 niet meer in de ENSIA verantwoording opgenomen en heeft weer een eigen verantwoordingsystematiek via de Waarderingskamer.

Vooruitblik 2024 op het gebied van de informatiebeveiliging

Activiteiten voor 2024:

- We stellen ons beleid op bedrijfscontinuïtet (BCM) vast, stellen een crisisplan op en breiden het aantal noodprocessen voor kritieke dienstverleningsprocessen uit.
- Het Information Security Management System (ISMS) wordt met taken verder uitgerold naar andere beheerder van applicaties om de plan-do-check-act cyclus voor informatiebeveiliging op een breder vlak structureel vorm te geven. Dit doen we gefaseerd en moet voor lastenverlichting zorgen bij de zelfverantwoordingstaken met betrekking tot ENSIA.
- We stemmen de eisen uit de BIO die gerelateerd zijn aan het ICT beheer door Westland af met Westland. Het gaat vooral om de bedieningsprocedures, het monitoren van ons datanetwerkverkeer, hoe zij omgaan met (controle op) logging, het installeren van software en het beheer van technische kwetsbaarheden. Het wordt in de praktijk goed uitgevoerd maar uitgangspunt is om dit ook helder vastgelegd te hebben voor de veranderde systemen die ingericht worden vanuit de projecten rond de verSAASing en de nieuwe cloud-technologie.
- In combinatie met voorlichting over privacy zal informatiebeveiliging continu onder de aandacht van de medewerkers worden gebracht. Dit doen we door middel van een e-learning oplossing. Hiermee krijgen we door monitoring meer inzicht in de kennis en vaardigheden van onze medewerkers waarop we vervolgens gerichter kunnen sturen.
- Het is een verplichting vanuit de BIO om structureel aandacht aan training en bewustwording te geven over informatiebeveiliging en privacy. In 2024 worden afdelingen die met gevoelige persoonsgegevens omgaan gericht getraind over social engineering en hacken.
- We voeren (samen met Westland) een aanbesteding uit voor een SIEM/SOC systeem op basis van de in 2023 opgestelde pakket ven eisen. Het identificeert potentiële beveiligingsincidenten en genereert waarschuwingen die kunnen worden onderzocht door medewerkers in een SOC.
- We maken organisatorische aanpassingen op de zelfevaluatie informatiebeveiliging om te voldoen aan de Europese wetgeving NIS2 en de nieuwe BOI 2.0.
- In 2024 actualiseren we ons dataclassificatie-overzicht en maken we procedures om onze informatie te labelen in de vak-applicaties (dit is wel georganiseerd in ons zaaksysteem).
- We hebben het beleid op hybride (tele) werken vastgesteld, we moeten echter nog verscherpen en regels opstellen over de fysieke beveiliging en de communicatieverbinding van de telewerklocaties.
- Er behoort een overzicht te zijn en te onderhouden van contacten met relevante overheidsinstanties die zich met informatiebeveiliging bezoig houden.
  We maken in 2024 een overzicht wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden. (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.

1. Inleiding

Met de VNG resolutie "Informatieveiligheid, randvoorwaarde voor de professionele gemeente" van 2013 hebben de gemeenten afgesproken de Baseline Informatieveiligheid Gemeenten (BIG) te implementeren. Deze baseline is vanaf 2020 overgegaan in de Baseline Informatiebeveiliging Overheid (BIO) en is nu de kern van de verantwoording over informatieveiligheid aan de gemeenteraad.

Gemeenten verantwoorden zich daarom elk jaar over de kwaliteit van de beveiliging van de informatievoorziening. Sinds 2018 gebeurd dit met de Eenduidige Normatiek Single Information Audit (ENSIA).
Gemeenten voeren nu over 2023 opnieuw een zelfevaluatie informatiebeveiliging uit. Deze is onder meer gericht op beveiligingsnormen van de BIO, AVG, BRP, PUN, BAG, BGT, DigiD en Suwinet. Het college van B&W rapporteert aan de gemeenteraad over de stand van zaken van de informatievoorziening met een jaarverslag.

Dit jaarverslag informatiebeveiliging bevat naast informatie over de informatiebeveiliging in brede zin ook een verwijzing naar de verplichte 'Collegeverklaring ENSIA'. Deze gaat over over twee specifiek geselecteerde beveiligingsnormenkaders (DigiD en Suwinet). Een gecertificeerd IT-auditor heeft de Collegeverklaring getoetst en een Assurancerapport opgeleverd dat nodig is voor de verticale verantwoording.

Met dit zesde jaarverslag over onze informatiebeveiliging geven we uitvoering aan de verantwoordingsplicht naar de gemeenteraad.



2. IB-beleid, doelstellingen en ambities

Met de vaststelling van het integraal informatiebeveiligingsbeleid in 2015 zette de gemeente Midden-Delfland een belangrijke stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente op orde te houden. Het beleid is gebaseerd op de Baseline Informatiebeveiliging Overheid die per 2020 de Baseline Informatiebeveiliging Gemeenten opvolgde.

Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie. Het informatiebeveiligingsbeleid geldt voor het complete proces van informatievoorziening en de hele levenscyclus van informatiesystemen. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het politiek bestuur, alle medewerkers, burgers, Midden-Delfland, bezoekers en externe relaties.

Baseline Informatiebeveiliging Overheid (BIO)

In november 2013 is tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de Vereniging van Nederlandse Gemeenten (VNG) de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' bekrachtigd. Deze Resolutie is opgesteld door de Vereniging van Nederlandse Gemeenten (VNG) in samenwerking met de Informatiebeveiligingsdienst voor gemeenten (IBD) en de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). De resolutie houdt in dat iedere gemeente het informatiebeveiligingsbeleid vaststelt aan de hand van de Baseline Informatiebeveiliging.

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten (BIG) uit 2013, Rijk, Waterschappen en Provincies. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek (NEN-ISO 27002).

Gericht op risicomanagement

De BIO legt de nadruk op risicomanagement. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter geworden. Om daaraan invulling te geven is tegelijkertijd met de BIO een handreiking '10 bestuurlijke principes voor informatiebeveiliging' van kracht geworden. Deze principes ondersteunen bestuurders bij de invulling van hun verantwoordelijkheid.

Informatieveiligheid is geborgd in de organisatie
Ons doel is om 'in control' te zijn op het gebied van informatiebeveiliging. 'In control' zijn betekent dat we weten welke passende technische en organisatorische maatregelen genomen moeten worden, welke maatregelen er al zijn en controleren op de werking ervan.

Het belang van informatieveiligheid is voor alle doelgroepen duidelijk
Mensen zijn de sleutel tot informatiebeveiliging. Voor een beveiligingsincident dat uitmondt in een datalek is vaak niet meer nodig dan een klik op een verkeerd linkje, een verkeerd geadresseerde e-mail met gegevens over een burger, een verloren laptop of het uitlenen van een toegangspas. Dit risico kan alleen beheerst worden als dag-in-dag-uit gewerkt wordt aan bewustzijn van medewerkers, als medewerkers veilige tools en procedures ter beschikking hebben om hun werk te doen en als bestuurders zelf het goede voorbeeld geven.

De P&C-cyclus voor informatieveiligheid is ingericht
De implementatie en borging van informatiebeveiliging is een continu proces. Omgevingsfactoren en navenante bedreigingen en kwetsbaarheden die deze met zich mee kunnen brengen, veranderen voortdurend.

Informatiebeveiligingsplan
Op basis van het informatiebeveiligingsbeleid stellen we jaarlijks een informatiebeveiligingsplan op. Hierin geven we aan op welke wijze de informatiebeveiliging wordt verbeterd en welke tijdsplanning hierbij gehanteerd gaat worden.

Uitgangpunten en doelen van ons informatiebeveiligingsbeleid

De belangrijkste globale uitgangspunten van het informatiebeveiligingsbeleid zijn:

- Het college van B&W is eindverantwoordelijk voor informatiebeveiliging en stelt het informatiebeveiligingsbeleid vast.
- De gemeentesecretaris is als Chief Information Officer (CIO) verantwoordelijk voor de uitvoering van het Informatiebeveiligingsbeleid.
- De Chief Information Security Officer (CISO) is gepositioneerd in een lijnfunctie.
- De CISO rapporteert jaarlijks over de informatiebeveiliging aan het college van burgemeester en wethouders.
- In het kader van de signaalfunctie rapporteert de CISO in bijzondere gevallen waarbij de veiligheid van de organisatie in het gedrang komt of dreigt te raken rechtstreeks aan de gemeentesecretaris.
- Aan de hand van een GAP-analyse uit ons ISMS en het actuele dreigingsbeeld (van NCSC en IBD) wordt periodiek een top 10 van te nemen maatregelen opgesteld.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de Gemeente Midden-Delfland worden bevorderd en geborgd.

De strategische doelen van het informatiebeveiligingsbeleid:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid

De 10 principes voor informatiebeveiliging voor de bestuurder

De hieronder aangegeven 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO. Zij gaan over de waarden die de bestuurder zichzelf oplegt.

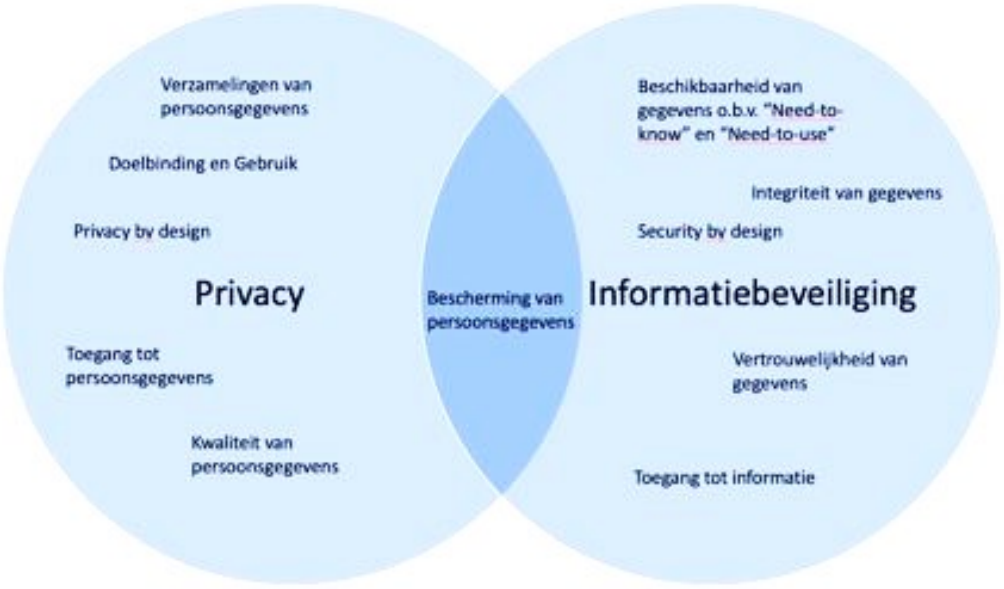
1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid calculeren we in.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Bij een incident met onze informatiebeveiliging binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor onze inwoners, ondernemers en partners. Daarmee moet informatiebeveiliging beslist een belangrijk onderwerp zijn voor de bestuurders.

Relatie met privacy

Met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 is privacy volop in de schijnwerpers komen te staan. Privacy heeft alleen betrekking op persoonsgegevens, waarbij dat begrip overigens ook heel ruim is. Zo kan het kenteken van een auto beschouwd worden als een persoonsgegeven als het herleidbaar is tot een individueel persoon. Informatiebeveiliging heeft een breder aandachtsgebied. De beveiliging is bijvoorbeeld ook gericht op de bedrijfscontinuïteit en beperkt zich niet tot uitsluitend persoonsgegevens.
Toch is het niet vreemd dat privacy en informatiebeveiliging vaak in één adem worden genoemd. Een aantal beveiligingsmaatregelen is van directe invloed op het waarborgen van de privacy.

Omgekeerd dragen privacy vereisten zoals het afsluiten van verwerkersovereenkomsten, bij aan verhoging van de informatiebeveiliging. Informatiebeveiliging en privacy worden binnen gemeente Midden-Delfland daarom in samenhang opgepakt.



3. Horizontale en verticale verantwoording op basis van ENSIA

ENSIA (Eenduidige Normatiek Single Information Audit)

Aanleiding
Sinds 1 juli 2017 is ENSIA (Eénduidige Normatiek Single Information Audit) een verplichte verantwoordingmethodiek voor gemeenten. ENSIA is gezamenlijke methodiek van het ministerie van Binnenlandse Zaken (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het ministerie van Infrastructuur en Milieu (I&M) en de Vereniging Nederlandse Gemeenten (VNG). Het heeft tot doel invulling te geven aan de verantwoordelijkheid van gemeenten rond informatieveiligheid.
De invoering van ENSIA betekent dat alle gemeenten sinds 2017 werken met één verantwoordingsstelsel voor informatieveiligheid. Daarbij wordt jaarlijks verantwoording afgelegd over DigiD, Suwinet, de paspoortuitvoeringsregeling (PUN), de Basisregistratie Personen (BRP), de Basisregistratie Adressen en Gebouwen (BAG) en de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergronden (BRO). In 2021en 2022 is de ENSIA zelfcontrole over de Basisregistratie Waardering Onroerende Zaken (WOZ) ook een wettelijke verplichting geweest. Vanaf 2023 is dit uit het ENSIA zelfverantwoordingsproces gehaald en vindt de verantwoording plaats met controles door de Waarderingskamer.

De verantwoording sluit aan bij de gemeentelijke P&C-cyclus en is in lijn met de Baseline Informatieveiligheid Overheid.

Achtergrond
De kern van ENSIA is dat de gemeentelijke organisatie transparant is en verantwoording aflegt over de manier waarop zij in control is op het thema 'informatieveiligheid'. Die verantwoording legt de gemeentelijke organisatie af aan haar eigen toezichthouder, in dit geval de gemeenteraad. Gemeenten hebben over dit principe in de algemene ledenvergadering van de VNG van november 2013 overeenstemming bereikt.
Gemeenten leggen niet alleen verantwoording af aan de eigen toezichthouder maar ook aan landelijke toezichthouders. Van oudsher bestonden verplichtingen ten aanzien van het ministerie van BZK rond de Basisregistratie Personen (BPR), de PUN en DigiD, en het ministerie van Infrastructuur en Waterstaat (IenW) rond de BAG. Naar aanleiding van de onderzoeken van de inspectie SZW is de regelgeving Suwinet aangescherpt en moeten gemeenten zich ook daarover verantwoorden.
ENSIA integreert al deze typen verantwoordingen in één werkwijze, met één eenduidige taal: de Baseline Informatiebeveiliging Overheid (BIO). Alle bestaande verantwoordingen zijn in goed overleg met de toezichthouders aangepast op ENSIA. Voor alle verantwoordingen geldt dat waar mogelijk is aangesloten op de BIO. Specifieke toezichtinformatie is nodig en waar mogelijk verwerkt in de ENSIA-vragenlijst die de bevraagbare versie van de BIO als basis kent. Daarnaast blijft de noodzaak aanwezig om domein specifieke toezichtinformatie te blijven leveren. Het voornemen is dat ENSIA met andere registraties verder zal worden uitgebreid.

Hoewel deze methodiek tot een vereenvoudiging van de audits moet leiden hebben de eerdere ENSIA verantwoordingen geleerd dat de werkzaamheden op dit gebied elk jaar weer verder toeneemt.
Dit komt met name doordat de normenkaders op het gebied van informatiebeveiliging en privacy substantieel worden uitgebreid en de reikwijdte op een toenemend aantal domeinen en registraties van toepassing is geworden (BGT, en BRO) of nog wordt. Ook de omzetting naar de BIO leverde andere maatregelen op of vraagt andere bewijslast voor de audit op de specifieke onderdelen zoals Suwinet en DigiD.

De ENSIA-verantwoording en de BIO biedt ons de kans om het proces rondom de verplichte aantoonbaarheid van informatieveiligheid te optimaliseren. De sterk toegenomen en nog steeds toenemende digitalisering binnen de gemeente en de maatschappij vraagt veel aandacht voor de kwaliteit van informatieveiligheid de privacybescherming. We beheren veel informatie waarvan veel persoonsgegevens en dat neemt toe door decentralisatie van overheidstaken. Elk jaar verantwoorden we ons over de kwaliteit van informatieveiligheid en/of de hierbij gebruikte informatiesystemen/-platformen.

Uitvoering van ENSIA 2023
ENSIA ondersteunt zowel het horizontale als het verticale verantwoordingsproces. De ontwikkeling gaat daarbij steeds meer in de richting van horizontale verantwoording. Hieronder is het ENSIA-proces voor het verantwoordingsjaar 2023 grafisch weergegeven. Meer informatie over ENSIA en de werkwijze is terug te vinden op www.ensia.nl.
Zo werkt ENSIA:



ENSIA	Verantwoording over informatiebeveiliging aan gemeenteraad		Verantwoording aan toezichthouders
Zelfevaluatie	• Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO). • Domeinspecifieke vragenlijsten voor diverse stelsels. • Zelfevaluatie afronden en vastleggen in ENSIA.	1 JUL 2023	Vragenlijsten: • RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). • BKWI: Informatiebeveiliging Suwinet (BIO). • Logius: Informatiebeveiliging DigiD. • DGBRW: Datakwaliteit en -integriteit BAG, BGT en BRO.
Opstellen	• Genereren en opstellen verantwoordingsrapportages. • Audit door gecertificeerde RE-auditor over collegeverklaring Suwinet en DigiD. • Opstellen rapportage ENSIA t.b.v. de gemeenteraad.	31 DEC 2023	Producten: • Collegeverklaring over Suwinet en DigiD. • Rapportage BAG, BGT en BRO door college van B&W. • Uittreksels BRP en Reisdocumenten. • Rapportage ENSIA voor de gemeenteraad.
Verantwoorden	• Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W. • Uploaden en aanleveren verantwoordingsrapportages via ENSIA (Uittreksels BRP en Reisdocumenten verwerken in de rapportages uit de Kwaliteitsmonitor en daar uploaden).	30 APR 2024	Resultaten: • De toezichthouders BKWI, Logius en DGBRW krijgen via ENSIA de verantwoordingsrapportages aangeleverd. • RvIG krijgt de informatie uit de Uittreksels BRP en Reisdocumenten via de Kwaliteitsmonitor aangeleverd.
Versturen	• Opstellen paragraaf verantwoording informatiebeveiliging voor de paragraaf Bedrijfsvoering in het jaarverslag. • Gemeenteraad neemt kennis van rapportage ENSIA. • College van B&W stelt jaarverslag vast. • Gemeenteraad keurt jaarverslag goed. • Het college van B&W stuurt het gemeentelijk jaarverslag aan de provincie.	15 JUL 2024	• De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd. • De vastgestelde jaarstukken zijn aan de provincie toegestuurd.

Sinds 2020 wordt de zelfevaluatie uitgevoerd door middel van het invullen van de vragenlijsten gebaseerd op de BIO. Op basis van de uitkomsten van deze zelfevaluatie is een collegeverklaring opgesteld waarop een audit heeft plaatsgevonden.
De scope van deze audit over 2023 beperkt zich net als de eerdere jaren nog tot Suwinet en DigiD. Zo wordt 'horizontaal' de collegeverklaring (waarin de gemeente de algehele status van informatieveiligheid verantwoordt) als bijlage van dit jaarverslag verwerkt. Deze collegeverklaring wordt vervolgens als integraal rapport meegeleverd als bijlage bij dit jaarverslag informatiebeveiliging (zie ook hoofdstuk 3).

Het horizontale verantwoordingsproces vormt een belangrijke basis voor de IT-auditor en de gemeente.

Toelichting werkwijze zelfevaluatie.
Via de online ENSIA tool zijn aan de gemeentelijke ENSIA-coördinator zelfevaluatie vragenlijsten beschikbaar gesteld. Deze zijn gericht op informatieveiligheid bij gemeenten over de volle breedte van de BIO met inbegrip van de specifieke normen op het gebied van informatiebeveiliging:
- Basisregistratie Personen (BRP)
- Paspoortuitvoeringsregeling (PUN)
- Digitale persoonsidentificatie (DigiD)
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratie Ondergrond (BRO)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)

In de periode van 1 juli tot 31 december 2023 zijn deze vragenlijsten door onze domeinbeheerders ingevuld en door de ENSIA-coördinator ingeleverd bij de landelijke toezichthouders.

Over de proceseigen normenkaders over de basisregistraties BAG, BGT en BRO zijn aparte verantwoordingsrapportages als bijlagen toegevoegd.

Verticale verantwoording
'Verticaal' verantwoorden we met de collegeverklaring de specifieke status per auditonderdeel (over 2023 Suwinet en DigiD) richting de betreffende landelijke toezichthouder. Daarnaast rapporteren we onze zelfevaluatie over de BAG, BGT en BRO naar de verticale toezichthouder (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.)
De rapportagedeadline hiervoor is tot 1 mei 2023.

Hieronder vindt u de conclusies uit de betreffende verantwoordingsrapportages.

Verantwoordingsrapportages zelfevaluatie 2023

De verantwoordingrapportages over de ingevulde ENSIA vragenlijsten zijn als bijlagen bijgevoegd voor college va B&W en raad.

De verantwoordingsrapportage over de BIO bevat de vragen die wettelijk gericht zijn op de specifieke normen (BRP,PUN, SUWINET, en DigiD).
Daarnaast zijn apart de verantwoordingsrapportages over de BAG, BGT en BRO als bijlagen van dit jaarverslag bijgevoegd. Deze bevatten ook de niet BIO gebaseerde vragen, die specifiek gericht zijn op de normenkaders van BAG, BGT en BRO.
De normen uit de Algemene Verordening Gegevensbescherming (AVG) zijn in de vragen over de BIO en de specifieke domeinen geïntegreerd.

Samen met de collegeverklaring over SUWI en DIGID vormt het jaarverslag IB inclusief de verantwoordingsrapportages BAG, BGT en BRO de horizontale verantwoording aan de gemeenteraad.

Zelfevaluatie BIO

Onderwerpen uit de BIO zijn:

- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig Personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

In de hoofdstukken 4 en 6 wordt uitgebreid ingegaan op de resultaten van 2023 en de op basis van de BIO geïmplementeerde maatregelen.

Resultaten zelfevaluaties per stelsel

Via de ENSIA systematiek is verantwoording afgelegd aan het Rijk. In de volgende paragrafen wordt per zelfevaluatie een toelichting gegeven. De bijbehorende rapportages zijn als bijlagen opgenomen bij deze rapportage.

Zelfevaluaties BRP en PUN

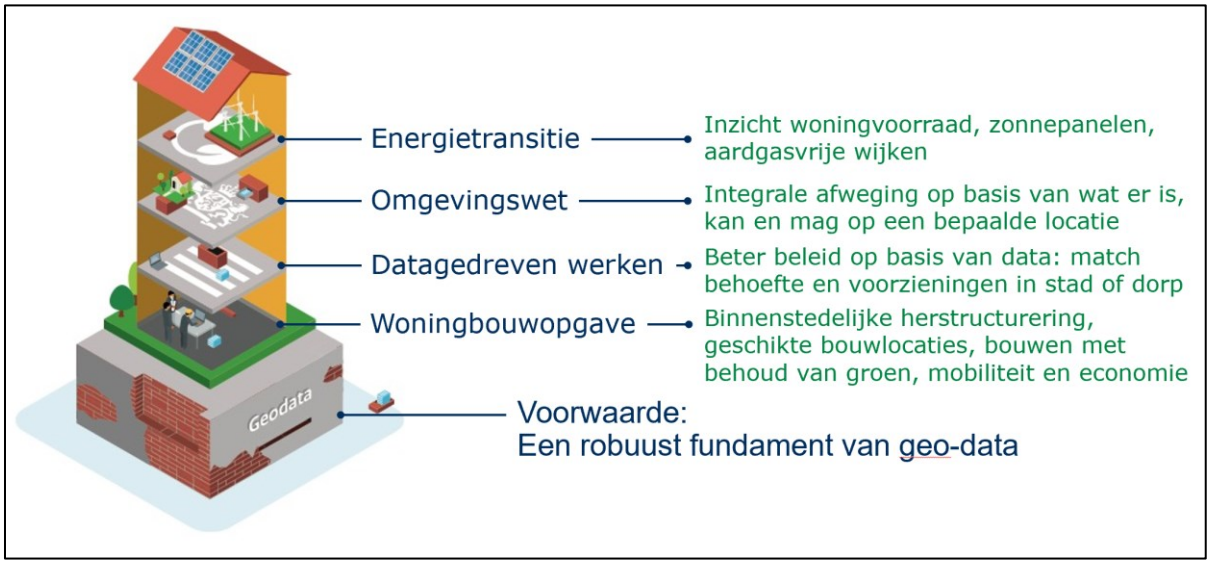
De Basisregistratie Personen (BRP) is onderdeel van het stelsel van basisregistraties van de Nederlandse overheid. De Nederlandse overheid registreert persoonsgegevens in de BRP. Alle overheidsinstellingen en bestuursorganen (zoals de Belastingdienst) zijn verplicht voor hun taken gebruik te maken van die gegevens. Het gaat daarbij onder andere om naam, geboortedatum, geboorteplaats, verblijfplaats en familierelaties. Met deze gegevens wordt bijvoorbeeld een paspoort en identiteitskaart verstrekt of wordt de hoogte van een studietoelage berekend. Voor het uitgeven van reisdocumenten hebben gemeenten met wetgeving te maken zoals de Paspoortuitvoeringsregeling Nederland 2001 (PUN).
Jaarlijks moeten gemeenten verantwoording afleggen over het gebruik van de BRP en de reisdocumenten. Met de komst van ENSIA is het inhoudelijke deel afgesplitst van het beveiligingstechnische deel. Het inhoudelijke deel, dat onder andere kijkt naar de kwaliteit van de persoonsgegevens in het BRP en de inrichting van de verwerkingsprocessen, wordt door de vakafdeling uitgevoerd. Het technische deel wordt op basis van de BIO-richtlijnen uitgevraagd. De zelfevaluaties BRP en Reisdocumenten zijn ingediend zodat de externe toezichthouder (het ministerie van Binnenlandse zaken en Koninkrijkszaken) zich hierover een oordeel kan vormen.
Op het inhoudelijke deel van de zelfevaluaties scoort gemeente Midden-Delfland binnen de gestelde normen. De scores van het ENSIA-deel voor de zelfevaluatie BRP en Reisdocumenten treft u hieronder aan.

Resultaat uit zelfevaluatie informatieveiligheid BRP 2023 (ENSIA)			
Thema BRP	**Totaal behaalde punten Midden-Delfland**	**Totaal mogelijk**	**Percentage**
1. Organisatie van de beveiliging	400	400	100 %
2. Toegangsbeveiliging	400	400	100 %
3. Naleving	400	400	100 %
Totaal	1.200	1.200	100%

Resultaat uit zelfevaluatie informatieveiligheid Reisdocumenten 2023 (ENSIA)			
Thema Reisdocumenten	**Totaal behaalde punten Midden-Delfland**	**Totaal mogelijk totaal**	**Percentage**
1. Organisatie van de beveiliging	400	400	100 %
2. Toegangsbeveiliging	400	400	100 %
3. Naleving	400	400	100 %
Totaal	1.200	1.200	100 %

Zelfevaluatie basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO).

In ons land worden geo-basisgegevens jaarlijks meer dan 5 miljard keer gebruikt via de landelijke voorzieningen. Indirect gebruik, via bijvoorbeeld de doorlevering van geo-data door fabrikanten van navigatiesoftware, komt daar nog bovenop. Het gebruik blijft jaarlijks stijgen en het maatschappelijk belang van deze gegevens, als onderdeel van de geo-informatie infrastructuur, is daarmee groot. Het is daarom cruciaal om de gegevenskwaliteit landelijk op peil te houden.



Afbeelding: nationale geo-informatie infrastructuur (NGII) als basis voor maatschappelijke vraagstukken (bron: BZK)

Wij leggen als bronhouderorganisatie verantwoording af over het beheer van de basisregistraties adressen en gebouwen (BAG), grootschalige topografie (BGT) en ondergrond (BRO). Dat doen we intern richting de gemeenteraad en aan het Rijk via het directoraat-generaal Bestuur, Ruimte en Wonen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De hieronder vermelde scores, zijn het resultaat van door ons uitgevoerde zelfevaluaties. Deze evaluaties betreffen de gegevenskwaliteit en de borging van beheerprocessen. Informatiebeveiliging maakt hiervan vooralsnog geen onderdeel uit.

In 2023 hebben we in een project alle schuurtjes die nog niet in de BAG waren opgenomen, omdat ze vóór Wet BAG 2.0 geen pand waren, opgenomen in de BGT en daarna in de BAG. Ook alle luifels, overkappingen, silo's, open werktuigenbergingen hebben we opgenomen in de BGT. Hierdoor hebben we nu alle objecten in de BGT opgenomen.

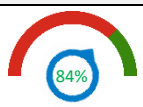
Scores geo-basisregistraties 2023 (tijdvak 1 januari 2023 tot en met 31 december 2023):

Basisregistratie	Score	Consequenties score
BAG		We zijn in "Control" en blijven alert op aandachtspunten. Omgevingswet heeft consequenties voor de registraties in de BAG. Als er niet genoeg gegevens komen bij de aanvragen, kan niet alles op een goede manier in de BAG geregistreerd worden.

< 75% onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BGT		Kwalitatieve BGT → kwalitatief beheer openbare ruimte, adequate voorbereiding plannen en projecten. Essentieel bij de uitvoering van de nieuwe omgevingswet Onvoldoende beheercapaciteit BGT → hogere kosten beheer openbare ruimte langere termijn omdat de ondergrondkaart voor BOR dan niet meer klopt.

< 75% Onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BRO		Indien aanlevering van aannemers niet NEN-conform is, dus niet volgens de richtlijn, dan aanpassen c.q. verduidelijken contracten.

< 60% Onvoldoende vanaf 60% voldoende

Trend score geo-basisregistraties

Registratie	Score 2018	Score 2019	Score 2020	Score 2021	Score 2022	Score 2023
BAG	90%	95%	95%	92%	92%	**92%**
BGT	70%	60%	60%	72%	100%	**100%**
BRO	N.v.t.	50%	54%	44%	100%	**84%**

De organisatie is “in control” voor wat betreft de basisregistraties BAG, BGT en BRO

Voorgestelde verbetermaatregelen voor 2024
Door de verbetermaatregelen door te voeren zoals hieronder beschreven hopen we bij de volgende verantwoordingsrapportage beter te scoren.

BAG
- Zorgen dat de processen juist blijven werken, zodat alle mutaties tijdig verwerkt kunnen worden.
- Jaarlijks een mutatie-signalering uit blijven voeren en de resultaten in de BGT en de BAG verwerken.
- Het hele jaar door zijn we met het proces bezig. Zodra er een proces anders gaat lopen, dan passen we het processenhandboek daaraan aan.

BGT
- De processen met de BAG en de BOR worden gecontroleerd en eventueel bijgewerkt. Als het niet gelukt is vóór eind december 2023 de mutatiesignalering 2023 te karteren in de BGT, dan moet dit nog begin januari 2024 worden doorgevoerd. Ook in 2024 zal er een mutatiesignalering zachte topografie worden uitgevoerd.
- Volgen wat de kwaliteitseisen zijn van de BGT voor 2024 en daar uitvoering aan geven.
- Er moet onderzocht worden of een koppeling tussen BOR en de BGT zinvol is. Zo ja, dan moet deze koppeling gerealiseerd gaan worden.
- We zijn in 2021 gestart met het opstellen van een objectenhandboek BGT. Dit handboek wordt geregeld gecontroleerd en aangevuld

BRO
- Processenhandboek optimaliseren.
- Processenhandboek zorgen dat dit ingebed wordt in de organisatie.

Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet

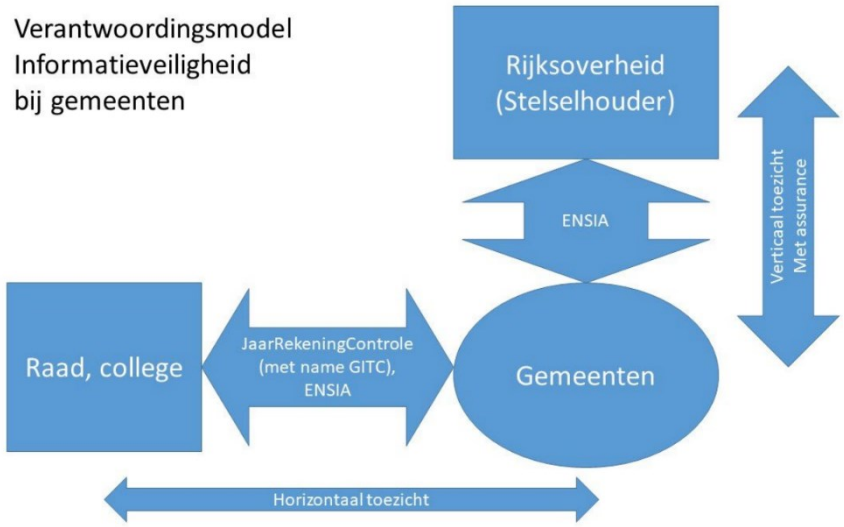
Het college van Burgemeester en wethouders geeft in een verklaring aan in hoeverre de beheersmaatregelen voldoen aan de voor de ENSIA verantwoording geselecteerde normen voor DigiD en Suwinet.

Bij de ENSIA vragenlijsten is geconstateerd dat bij gemeente Midden-Delfland op 31 december 2023 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake DigID.

Voor wat betreft de normen inzake Suwinet is geconstateerd dat aan alle normen wordt voldaan.

U treft de collegeverklaring als bijlage van dit jaarverslag aan.

Een gecertificeerd auditor toetst of onze interne beheersingsmaatregelen in opzet en bestaan voldoen aan de normen inzake DigID en Suwinet. Hierover levert de auditor een Assurance verklaring af en bekrachtigt de collegeverklaring. Deze documenten zijn van belang voor de verticale verantwoording aan de departementen.



4. Samenvattend beeld en resultaten informatiebeveiliging 2023

Achtergrond
Dit is het vierde jaarverslagslag is over onze informatiebeveiliging. Vorig jaar gaven we u een beeld van onze activiteiten en behaalde resultaten vanaf het moment dat we in 2015 gestart zijn met ons informatiebeveiligingsbeleid. In dit verslag beperken wij ons tot de activiteiten en behaalde resultaten van het afgelopen jaar ten opzichte van een meting over 2022.

Ons gemeentelijk informatiebeveiligingsbeleid is actueel. We hebben ons in 2015 geconformeerd aan het normenkader van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en sinds 2020 de Baseline Informatiebeveiliging Overheid. In 2023 hebben we ons Strategisch Informatiebeveiligingsbeleid vervangen door een geactualiseerde versie.

We zijn als gemeente aangesloten bij de Informatiebeveiligingsdienst (IBD).
De IBD is de sectorale CERT / CSIRT (Computer Emergency Response Team en Computer Security Incident Response Team)voor alle Nederlandse gemeenten. Het is onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD draagt namens gemeenten bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.
Voor meer informatie over de IBD, zie hun site https://www.informatiebeveiligingsdienst.nl/



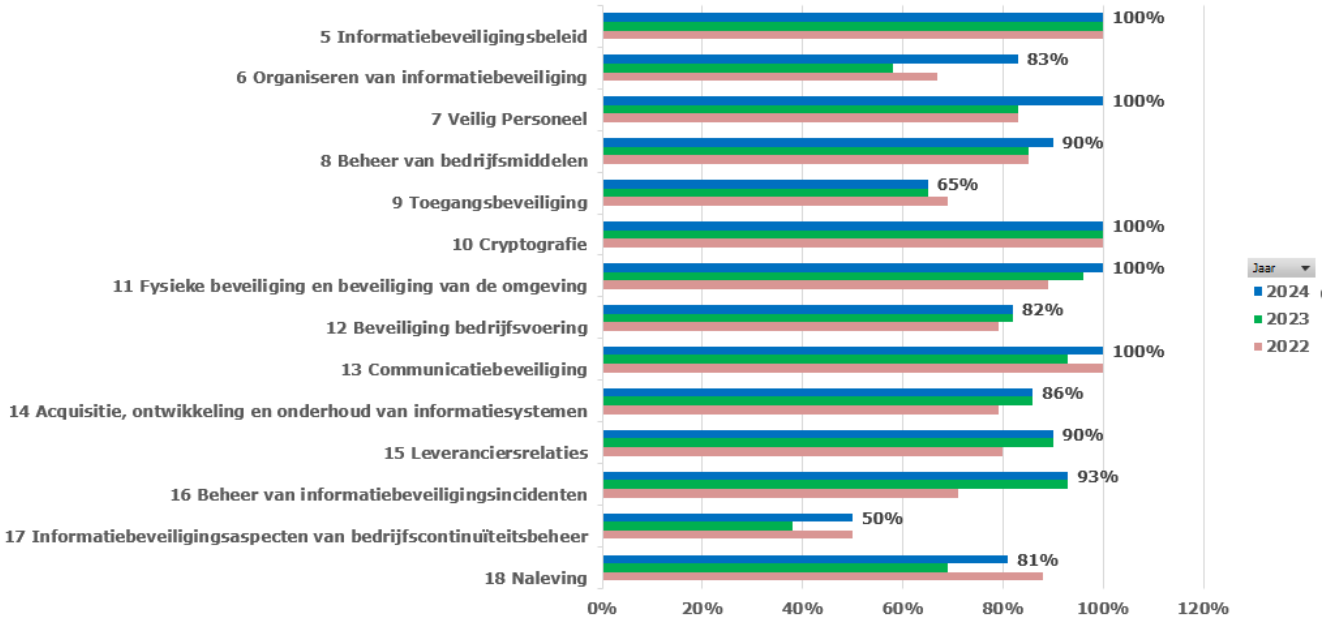
Van GAP-analyse naar planning en prioritering.
Om het informatiebeveiligingsbeleid goed te implementeren, werken we op basis van een "GAP-analyse/risicoanalyse". Deze analyses zijn uitgevoerd in directe samenspraak met de betrokken collega's van de vakafdelingen. Hiermee is het "GAP" of "gat" tussen de huidige en de gewenste situatie (volgens de geldende normen) in beeld gebracht. Vanuit deze analyse en het actuele dreigingsbeeld van het NCSC en IBD hebben we een planning en rangschikking van maatregelen gemaakt, om aan de normen met de hoogste prioriteit te voldoen. Deze planning en prioritering is vormgegeven en geactualiseerd in een jaarlijkse top 10 te nemen maatregelen en quick-wins waaraan in 2023 verder is gewerkt. Voortdurend wordt na de genomen maatregelen de top 10 aangevuld met nieuwe actuele, op de gap-analyse gebaseerde, acute dreigingen en de aanbevelingen uit de audit over ENSIA verantwoording.

Om inzicht te verschaffen waar we met onze informatiebeveiliging nu precies staan hebben we met ons ISMS meting uitgevoerd over 2021, 2022 en 2023.



Resultaat meting BIO

Op basis van de resultaten ENSIA 2023 is begin 2024 een meting uitgevoerd op de 112 normen in de BIO. Grafisch ziet het resultaat van meting 3 uit ons ISMS er als volgt uit:



Tabel 1 De in de grafiek getoonde onderdelen betreffen de hoofdstukken uit de BIO.

Wat valt op?

Zo is het beleid op het hybride werken (thuiswerken) geactualiseerd. In 2023 is ook gestart met het vormgeven van bedrijfscontinuïteitsmanagement en is bijvoorbeeld ons beleid voor Coordinated Vulnerability Disclosure (voorheen Responsible Disclosure) vastgesteld. Daarnaast hebben we het ISMS verder ingericht en uitgerold. Op hoofdstuk 9 van de BIO scoren we nog relatief laag. Het gaat dan vooral om het beheer van toegangsrechten in de vak-applicaties zelf. Hier ligt een belangrijke rol voor onze functioneel applicatiebeheerders. Dit gaat met de ingezette bredere uitrol van het ISMS meer aandacht krijgen.

Hoofdstuk 12 scoort ook nog relatief laag en dat heeft vooral te maken met onduidelijkheid over hoe het bij Westland belegde ICT-beheer organisatorisch is vorm gegeven in de nieuwe nog vast te stellen beschreven dienstverleningsovereenkomst. We stemmen de eisen uit de BIO die gerelateerd zijn aan het ICT beheer door Westland af met Westland. Het gaat vooral om de bedieningsprocedures, het monitoren van ons datanetwerkverkeer, hoe zij omgaan met (controle op) logging, het installeren van software en het beheer van technische kwetsbaarheden. Het wordt in de praktijk goed uitgevoerd en voldoet aan de eisen maar uitgangspunt is om dit helder op papier te hebben. Met name het lopende project voor de van de verSAASing van applicaties en de cloud-omgeving vragen om andere expertise en dienstverlening. Hierop heeft in 2023 een onderzoek plaatsgevonden. De uitkomsten daarvan betrekken we bij de actualisering van de Dienstverleningsovereenkomst met Westland voor het ICT-beheer. Deze wordt naar verwachting in 2024 vastgesteld.

Op de te nemen maatregelen van hoofdstuk 17 van de BIO ofwel informatieveiligheidsaspecten van bedrijfscontinuïteit hebben we een aantal verbeterstappen gezet. Vorig jaar haalden we nog een score van 38% en nu 50%. We hebben veel maatregelen ingericht zoals back-up, uitwijk, noodstroomaggregaat etc. maar dat is allemaal nog niet compleet en in samenhang tot een (crisis) plan gevormd. Dit het crisisplan wordt in 2024 ter vaststelling aangeboden. Het spectrum van

bedrijfscontinuïteitsbeheer is veel meer dan dat. Bedrijfscontinuïteitsmanagement (BCM) moet duidelijkheid geven over hoe we onze meest essentiële dienstverlening naar onze burgers kunnen continueren bij uitval van ICT voorzieningen. Hiervoor ligt een concept BCM beleid klaar voor vaststelling. Daarbij is ook een noodproces vastgelegd voor het uitkeren van uitkeringen bij uitval van onze systemen. In 2024 wordt voor meer van dergelijke kritieke processen noodscenario's opgesteld.



Verderop in dit jaarverslag gaan we in de hoofdstuk 6 nader in op de voorgenomen verbeterpunten en activiteiten die onder de categorie actualisatie/onderhoud vallen voor 2024 voorzien van een toelichting. Deze verbeterpunten gaan we na goedkeuring van dit jaarplan als actiepunten opnemen in het ISMS en van daaruit monitoren.

De vergaande digitalisering en de daarmee gepaard gaande dreigingen zoals bijvoorbeeld ransomware[6] (Hof van Twente) noodzaakt ons als gemeente alert te zijn en aandacht te blijven vragen en geven aan informatieveiligheid. Bewustwording van digitaal handelen onder het personeel blijft dan ook een continu aandachtspunt.

[6] Ransomware ofwel gijzelsoftware is schadelijke software die computers en bestanden gijzelt. Criminelen geven toegang weer vrij als hiervoor losgeld is betaald.

Algemene Verordening Gegevensbescherming (AVG)

Sinds 25 mei 2019 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Op 3 juni 2019 heeft het college van de gemeente Midden-Delfland het privacy beleid vastgesteld. Dit beleid bevat de algemene beleidsuitgangspunten over de bescherming van persoonsgegevens door de gemeente Midden-Delfland. Het laat zien hoe de gemeente omgaat met persoonsgegevens en welke maatregelen zij treft om te voldoen aan de AVG. De functionaris gegevensbescherming controleert jaarlijks of aanpassingen aan dit beleid nodig zijn.

Ook in 2023 hebben we op basis van de AVG met leveranciers en dienstverleners verwerkersovereenkomsten en dataleveringsovereenkomsten afgesloten. Hierin zijn de verantwoordelijkheden geregeld voor de beveiliging van het gebruik van onze privacygevoelige gegevens. We hebben naast technische maatregelen, ook gewerkt aan bewustzijn bij de medewerkers.

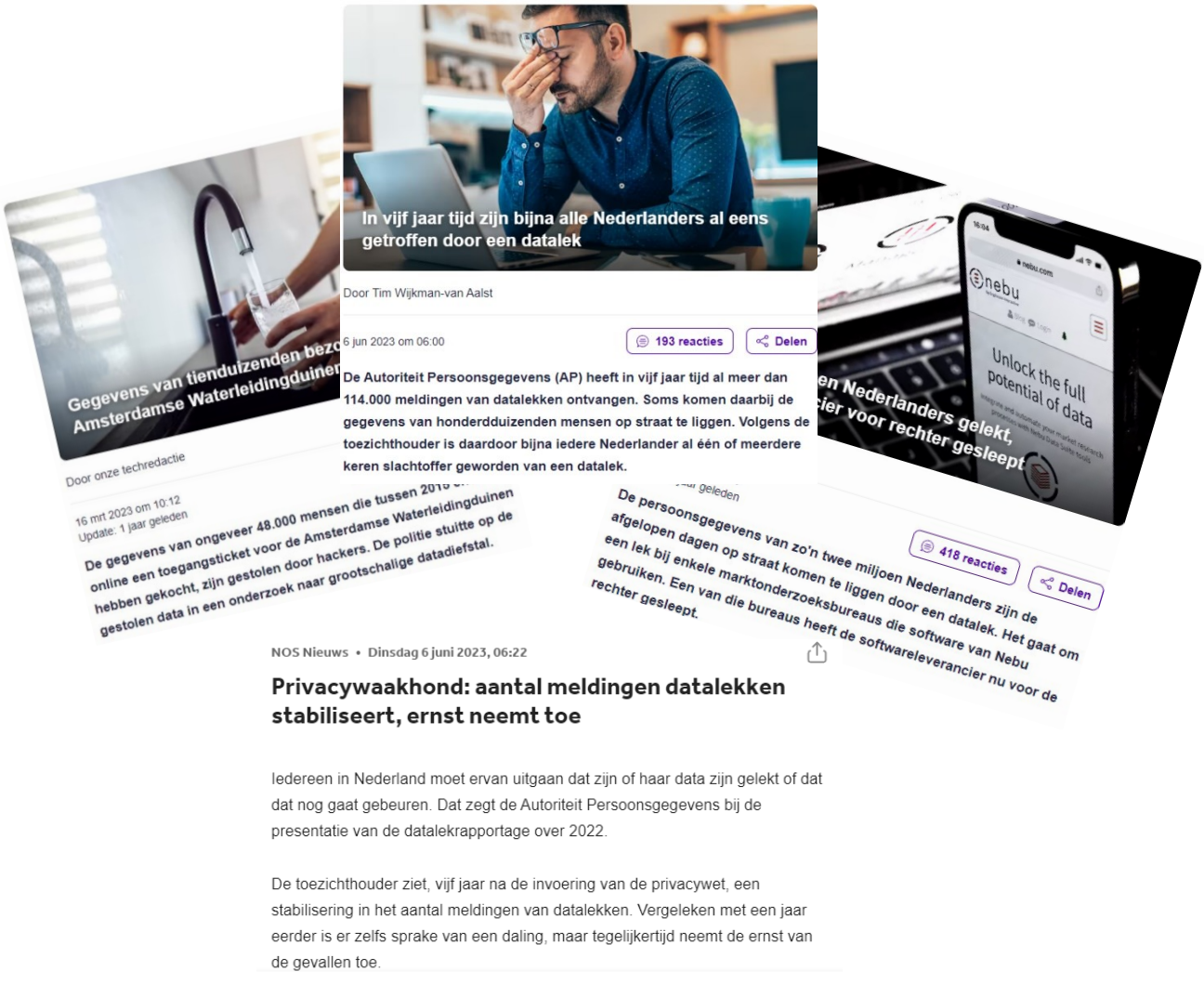
Informatiebeveiliging en privacybescherming hebben een grote 'houding en gedrag'- kant. Vanwege de inwerkingtreding van de AVG zijn door de projectgroep Privacy gemeente-brede bijeenkomsten georganiseerd waarbij vooral is ingegaan op hoe er vertrouwelijk met persoonsgegevens van personen moet worden gegaan. Onze interne beveiligingsorganisatie bestaat uit medewerkers van de verschillende teams die binnen hun team zorgen voor bewustzijn en aanspreekpunt zijn voor informatiebeveiliging voor hun team.
Daarnaast zijn er voor de borging van de AVG en de privacybescherming medewerkers binnen de organisatie aangewezen als privacy-ambassadeur.



Bij het incidenten overzicht informatiebeveiliging in hoofdstuk 8 leest u ook het aantal en soort datalekken over 2023.

5. Disclaimer

Beveiligingsincidenten zijn helaas niet te voorkomen; 100% beveiliging is een utopie. De vraag is dan ook niet zozeer of er een beveiligingsincident met een hoge impact zal plaatsvinden, maar wanneer. Beveiligingsincidenten kunnen leiden tot onderbreking van werkzaamheden, reputatieschade en aanzienlijke financiële schade als gevolg van het bestrijden van een incident en het herstellen naar een normale situatie.
De maatregelen die we nemen zijn erop gericht de risico's zoveel mogelijk te minimaliseren tegen aanvaardbare kosten. Daarnaast houden we rekening met de impact op dienstverlening en bedrijfsvoering. Een hele goede maatregel is bijvoorbeeld het uitschakelen van alle internetverbindingen van het gemeentehuis. Een hacker van buiten het kantoor zou dan geen enkele kans meer hebben. Dit is in deze tijd onwerkbaar omdat onze gegevensuitwisseling met inwoners en andere overheden voor een groot gedeelte via het internet lopen.
Naast preventieve maatregelen richten we ons ook op procedures en maatregelen wanneer zich een incident voordoet. Zodat we met onze dienstverlening en bedrijfsvoering zo snel mogelijk weer operationeel zijn.



6. Realisatie doelstellingen IB-beleid

Hieronder geven we aan met welke genomen maatregelen we invulling hebben gegeven aan de in hoofdstuk 1 genoemde strategische doelen.

De strategische doelen van het informatiebeveiligingsbeleid:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

De drie belangrijkste punten, die in grote mate het succes bepalen van de implementatie van de BIO:

Maatregel	**Doelstelling**
Informatiebeveiligingsbeleid Er is op dit moment een compleet gemeente-breed informatiebeveiligingsbeleid. In december 2019 is het op de BIO gebaseerde nieuwe informatiebeveiligingsbeleid 2020-2023 vastgesteld. We hebben de verplichting dit elke 3 jaar te actualiseren. In 2023 is ons nieuwe informatiebeveiligingsbeleid voor 2023-2026 door het college van burgemeester en wethouders vastgesteld.	Het managen van de informatiebeveiliging
Informatiebeveiligingsorganisatie (IB-organisatie) De IB-organisatie is op 1 maart 2017 door het college vastgesteld. Zonder IB-organisatie is het onmogelijk om tot een goede borging van informatiebeveiliging te komen binnen de ambtelijke organisatie. Elk bedrijfsproces bestaat uit verschillende informatiestromen, waarbij ook verschillende (informatie-)systemen gebruikt worden. Voor al deze onderdelen zijn de taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging vastgelegd en toegewezen aan een functie/rol in de organisatie. De leden van de IB-organisatie worden sinds 2017 opgeleid. In 2024 wordt de IB-organisatie gebaseerd op het in 2023 geactualiseerde Informatiebeveiligingsbeleid aangepast naar de nieuwe organisatiestructuur en de kaders van de BIO.	Het managen van de informatiebeveiliging
ISMS Er is een ISMS (Information Security Management System) geïmplementeerd binnen de gemeente Midden-Delfland. Deze software gebruiken we als ondersteunende tool om alle bedrijfsprocessen in relatie met informatiebeveiliging in kaart te brengen, te monitoren en te borgen binnen de gemeentelijke organisatie. Ook verantwoorden we in het ISMS de stand van zaken per proces en per norm. Het ISMS wordt op in 2024 nog verder uitgerold over de IB-organisatie en vak-applicaties.	Het managen van de informatiebeveiliging

Hiermee zijn de randvoorwaarden ingevuld voor een succesvolle verdere implementatie van het IB-beleid.

Controls & beheersmaatregelen IB

In de BIO staan controls en maatregelen.
Het vraagt meerdere jaren om deze maatregelen te implementeren in onze gemeentelijke processen en systemen.
Het is daarom nodig om inzicht te krijgen in wat er moet gebeuren met welke prioriteit.
Met een delegatie van applicatie- en procesbeheerders is daarom op basis van de Baseline Informatiebeveiliging Gemeenten (BIG) in 2016 een GAP- en Impactanalyse uitgevoerd op gemeente-brede maar ook systeem specifieke maatregelen. Met de GAP-analyse zoeken we uit waar we staan met genomen maatregelen ten opzichte van de normen en risico's.
Een meting dus over wat we aan maatregelen al 'in huis' hebben, wat is hiervan nog up to date en wat moet er nog aan maatregelen georganiseerd worden.
Hierbij is het van belang om alvast na te denken of maatregelen gemeente-breed of systeem specifiek zijn. Deze stap geeft ook al inzicht in hoe het nu geregeld is, dus wie voert feitelijk welke informatiebeveiligingsmaatregelen uit.

Hiermee is er inzicht gekomen in waar we de focus voor het komende jaar qua BIO-implementatie op leggen:

a. De status van belangrijke gemeente-brede maatregelen.
b. Essentiële processen.
c. Kritische systemen.
d. De status van systeem specifieke maatregelen.

Conclusies GAP-en impactanalyse

Uit de eerste (BIG-gebaseerde) GAP-analyse kwamen 155 nog te implementeren maatregelen.
Om de juiste prioriteit te krijgen bij deze 155 openstaande maatregelen die de gemeente Midden-Delfland als eerste op moet pakken is naast de Gap-analyse ook een risico- en impactanalyse gemaakt.

Omdat het onmogelijk was om alle maatregelen tegelijk op te pakken, hebben we ons na de risico- en impactanalyse) gericht op een top 10 lijst. De te implementeren maatregelen op deze top 10 lijst pakten we als eerste op. Daarna richten we ons jaarlijks op 10 nieuwe normen en te nemen maatregelen van de BIG, volgens de prioritering uit de impact- en risicoanalyse. Met de inwerkingtreding van de BIO is het aantal maatregelen omlaag gegaan maar wel met de komst van een aantal verplichte maatregelen. Welke maatregelen je moet nemen als organisatie hangt af van de risico's. Deze worden inzichtelijk gemaakt aan de hand van wat de kans is dat zich iets voor doet, wat de impact dit heeft en welke schade er mee gemoeid is.

De BIO Baselinetoets
Na de impactanalyse voor de BIG hebben we een in 2019/2020 de (BIO) baselinetoets uitgevoerd waarmee we een dataclassificatieschema hebben opgesteld. Hiermee bepalen we of een proces, informatiesysteem een bepaald Basis Beveiliging Niveau (BBN) heeft binnen de BIO en welke maatregelen nodig zijn. Er wordt hierbij gekeken naar 3 beveiligingsaspecten: beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De uitkomsten gebruiken we om te bepalen of er meer maatregelen nodig zijn voor een proces en onderliggende informatiesystemen. Deze maatregelen kunnen worden verkregen uit een voor gedefinieerde lijst met maatregelen bovenop de baseline, of door een aanvullende diepgaande risicoanalyse. De normen en (genomen en nog te nemen) maatregelen houden we bij in ons ISMS.
Daarnaast gebruiken we de baselinetoets bij de fase voor het starten van nieuwe gemeentelijke taken, een project of voor een nieuw informatiesysteem. De vragenlijst vormt dan input voor de eventueel te nemen additionele beveiligingsmaatregelen, welke in de definitiefase van het project nader worden uitgewerkt. Bijvoorbeeld door middel van een aanvullende diepgaande risicoanalyse.

Het resultaat van de baselinetoets BIO kan duiden op een zwaartepunt in het te beschermen belang, er is bijvoorbeeld een hogere score voor Beschikbaarheid, maar niet op Integriteit en Vertrouwelijkheid. In de daarna uit te voeren risicoanalyse dient dan de nadruk te liggen op verhogen van Beschikbaarheid. Ook geeft de opgeleverde dataclassificatie de volgorde van voor het opnieuw operationeel maken van systemen aan bij uitval.

Er is getoetst wat al is geïmplementeerd en nog actueel is volgens de BIO normen. Met name de generieke beveiligingsmaatregelen die gemeente-breed gelden.

Bij deze generieke beveiligingsmaatregelen gaan we uit van.:

- Het gemeentelijk informatiebeveiligingsbeleid, dit is gelijk voor de gehele gemeente
- Het toewijzen van de Chief Information Security Officer (CISO)-rol
- Verantwoordelijkheden van de lijnmanagers (te verankeren in het beleid)
- (ITIL) beheerprocessen en aandacht voor beveiliging
- Personele beveiligingsmaatregelen
- Fysieke toegangsbeveiligingsmaatregelen
- Beveiligingsmaatregelen voor apparatuur en software
- Malware scanning als generieke dienst (dus niet ten behoeve van één informatiesysteem)
- Omgang met (mobiele) gegevensdragers
- Het hebben van een Information Security Management Systeem (ISMS)

Verbeterpunten op basis van meting BIO

De focus voor verbetering richt zich vooral op de hoofdstukken in BIO die volgens de meting lager of rond de 75% scoren. Deze hoofdstukken vindt u in onderstaande tabel terug met de beschrijving van de verbeterpunten voor 2024.

Hoofdstuk BIO	**Onderwerp**	**Beschrijving verbeterpunten**
6.1.3	Organiseren van Informatie-beveiliging	Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden. We maken een overzicht wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.
6.2.2	Telewerken	We hebben het beleid op hybride (tele) werken vastgesteld, we moeten echter nog verscherpen en regels opstellen over de fysieke beveiliging en de communicatieverbinding van de telewerklocatie.
8.1 / 8.2	Dataclassificatie	In 2024 actualiseren we ons dataclassificatie-overzicht en maken we procedures om onze informatie te labelen in de vak-applicaties (dit is wel georganiseerd in ons zaaksysteem).
9	Toegangs-beveiliging	Het gaat dan vooral om het beheer van toegangsrechten in de vak-applicaties zelf. Hier ligt een belangrijke rol voor de functioneel applicatiebeheerders. Dit gaat met de ingezette bredere uitrol van het ISMS in 2024 meer aandacht krijgen.
12	Beveiliging bedrijfsvoering en Communicatie-beveiliging	Het is nog onvoldoende duidelijk hoe het bij Westland belegde ICT-beheer organisatorisch wordt vorm gegeven in de nieuwe nog vast te stellen beschreven dienstverleningsovereenkomst. We stemmen de eisen uit de BIO die gerelateerd zijn aan het ICT beheer door Westland af met Westland. Het gaat vooral om de bedieningsprocedures, het monitoren van ons datanetwerkverkeer, hoe zij omgaan met (controle op) logging, het installeren van software en het beheer van technische kwetsbaarheden. Het wordt in de praktijk goed uitgevoerd maar uitgangspunt is om dit beschrijvend vastgelegd te hebben. Met name de veranderingen en ontwikkelingen in het kader van de verSAASing van applicaties vragen om andere expertise en

		dienstverlening. De uitkomsten van het hierover in 2023 uitgevoerde onderzoek betrekken we bij de actualisering van de Dienstverleningsovereenkomst met Westland voor het ICT-beheer.
17	Informatiebeveiligings-aspecten van bedrijfs-continuïteitsbeheer	We hebben veel maatregelen ingericht zoals back-up, uitwijk, noodstroomaggregaat etc. maar dat is allemaal nog niet compleet en in samenhang tot een (crisis) plan gevormd. Dit het crisisplan wordt in 2024 ter vaststelling aangeboden. Het spectrum van bedrijfscontinuïteitsbeheer is veel meer dan dat. Bedrijfscontinuïteitsmanagement (BCM) moet duidelijkheid geven over hoe we onze meest essentiële dienstverlening naar onze burgers kunnen continueren bij uitval van ICT voorzieningen. Na afstemming de algemene crisisorganisatie van team Openbare Orde en Veiligheid wordt dit BCM beleid ter vaststelling aangeboden. Daarbij is ook een noodproces vastgelegd voor het uitkeren van uitkeringen bij uitval van onze systemen. In 2024 wordt voor meer van dergelijke kritieke processen noodscenario's opgesteld.
18.2.2	Uitbreiden gebruik ISMS	Het ISMS is ons managementsysteem dat helpt om op een aantoonbare en controleerbare wijze verantwoording af te leggen op het gebied van informatiebeveiliging. Het breder uitrollen van het ISMS onder applicatiebeheerders op basis van de PDCA-cyclus en de daaruit voortkomende periodieke rapportages is van belang. De verbeterstap is dat organisatie vertrouwd raakt met het ISMS gericht op continu verbeteren van de informatiebeveiliging. Dit proces is bij een aantal applicatie beheerders in 2023 succesvol vorm gegeven en krijgt in 2024 een vervolg.
18. (en 5.)	Organisatorische aanpassingen op de zelfevaluatie informatiebeveiliging als gevolg van de Europese wetgeving NIS2 en de BIO 2.0	Naar verwachting neemt vanaf 2024 de auditlast toe op informatiebeveiliging en privacy als gevolg van de aangescherpte regelgeving. Het ENSIA proces wordt daar ook op aangepast en moet er ook op actieve werking van genomen beveiligingsmaatregelen worden getoetst. Hiervoor organiseren we in 2024 met de betreffende domeinbeheerders werkbare processen in ons ISMS. Daarnaast is de verwachting dat ons Strategisch Informatiebeveiligingsplan moet worden geactualiseerd op de nieuwe regelgeving.

De verwachting is dat de meeste in deze paragraaf vermelde punten binnen het reguliere werk kunnen worden gerealiseerd. Er is alleen goede wil en voldoende medewerking nodig vanuit de organisatie en daarin is alle vertrouwen omdat we het belang van informatiebeveiliging voor het succes van onze organisatie steeds meer als randvoorwaarde onderkennen.

Er zijn verbeterpunten die relatief veel tijd vergen en projectmatig met ondersteuning van expertise moeten worden uitgevoerd. Dit zijn onder andere de SIEM/SOC implementatie, en het realiseren van een bedrijfscontinuïteitsplan met crisisplannen per proces/taakveld.

Cybersecurity op SCADA-automatisering en Europese richtlijn NIS2
Bovenstaande maatregelen gaan voornamelijk over onze administratieve en dienstverlenende processen. Automatisering en internetkoppelingen zien we echter ook steeds meer in vitale fysieke systemen terugkomen zoals zogenaamde internet-of-things. In onze beweegbare bruggen, verkeerslichten, CCTV systemen en rioolgemalen wordt steeds meer gebruik gemaakt van (industriële) automatisering, ook wel Industrial Control Systems en Supervisory Control And Data Aquisition (ICS/ SCADA) genoemd.

Met de komst van NIS2 (NIB2 voor Nederland), de nieuwe Europese wetgeving op het gebied van cyberweerbaarheid worden beveiligingseisen aangescherpt, ook voor leveranciers, worden rapportageverplichtingen gestroomlijnd en komt er verscherpt toezicht. De verwachting is dat deze nieuwe richtlijn bovenop de BIO een grote impact gaat hebben op de eisen voor cyberweerbaarheid voor overheden en een groter aantal vitale organisaties.
De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties zegt hierover in de Kamerbrief van 29/09/2023) "Intussen is in Europa een voorlopig politiek akkoord bereikt over een herziening van Netwerk- en Informatiebeveiligingsrichtlijn (NIB2-richtlijn). Een belangrijke wijziging ten opzichte van de huidige richtlijn is dat overheidsdiensten binnen de reikwijdte van de richtlijn worden gebracht, en daarmee aan wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen moeten voldoen. Dit geldt in ieder geval voor de Rijksoverheid. De conceptrichtlijn stelt verder dat regionale en lokale overheden na een risicobeoordeling kunnen worden aangewezen. Daarbij nemen we de geldende criteria als uitgangspunt, zoals de hierboven genoemde 'vitaal' criteria.
Inmiddels is de verwachting dat met de nieuwe Europese richtlijn NIS2 wij ook als gemeenten nadrukkelijker aandacht moeten gaan geven aan de beveiliging van onze vitale infrastructurele systemen. Hiervoor wordt een nieuwe versie van de BIO verwacht.

Regionale samenwerking

Sinds 2017 zijn medewerkers (Ciso en informatieadviseurs) van Midden-Delfland op regionaal niveau betrokken bij structureel overleg over informatiebeveiliging.
Het doel van het overleg is met name om kennis en ervaringen te delen en waar mogelijk ondersteunen bij informatiebeveiligingsincidenten.



7. Incidenten en ontdekte kwetsbaarheden

Rapportage van incidenten zoals datalekken en de afhandeling daarvan.

In 2023 zijn 29 spammails, 23 incidenten en 317 geconstateerde kwetsbaarheden gemeld bij de CISO en adviseurs Informatiebeveiliging. Het gaat hierbij ook om ontdekte kwetsbaarheden die met updates van software en aanpassingen van de hardware zijn opgelost. De gemelde kwetsbaarheden kwamen voornamelijk van de Informatie Beveiligingsdienst (IBD) en betroffen ondermeer meldingen over geconstateerde kwetsbaarheden in gebruikte software en hardware.

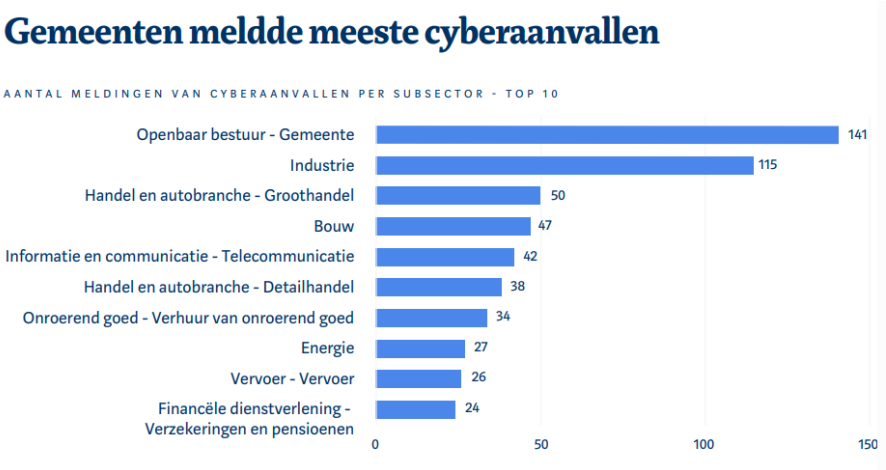
In 2023 zijn 10 datalekken gemeld bij de privacy officers. In 2020 waren dit er nog 17 in 2021 maar 11 en 10 in 2022. Het lijkt hier om een neerwaartse trend te gaan die aandacht verdient. Van een organisatie met de omvang van de gemeente Midden-Delfland kan verwacht worden dat elk jaar enkele tientallen datalekken plaatsvinden, waar gewerkt wordt worden immers ook fouten gemaakt.
De FG heeft nader onderzoek gedaan naar de registratie van gemelde datalekken in het datalekkenregister en hierover een rapportage opgesteld.
Uit het onderzoek komen vier onvolkomenheden naar voren in de datalekkenregistratie:

1. Onvolkomenheden in meldplicht en de wettelijke afhandeltermijn
2. Onzorgvuldige afhandeling en registratie
3. Afhandeling niet in overeenstemming met de wettelijke bepalingen
4. Geen zicht op uitvoering van preventieve maatregelen

In geen van de datalekken bleek het nodig om de Autoriteit Persoonsgegevens te informeren.
In één van de datalekken bleek het wel nodig om de betrokkenen te informeren. Geconstateerd wordt dat het datalekkenregister adequaat wordt bijgehouden

Buiten het melden van datalekken daalt ook het aantal door medewerkers gemelde incidenten al 7 jaar. Een van de redenen hiervoor zou kunnen zijn dat de organisatie en ketenpartners bewuster met gevoelige informatie omgaat. Het is daarom van belang om te blijven investeren in bewustwording over informatiebeveiliging en privacy.

De verplaatsing van applicaties naar de cloud gaat de komende jaren toenemen waardoor de kwetsbaarheid van ons eigen ict-netwerk ook afneemt.



Bron: Autoriteit Persoonsgegevens

Melding Datalekken in 2023

Sinds 2016 geldt de wet Meldplicht datalekken en per 25 mei 2019 is de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) van kracht geworden. Als onze organisatie niet voldoet aan deze wetten, is dat een risico op een bestuurlijke boete van de Autoriteit Persoonsgegevens van maximaal 20 miljoen euro.

Van de bij ons gemelde incidenten zijn er geen incidenten als datalek gemeld bij de Autoriteit Persoonsgegevens (AP). Binnen 72 uur worden daarvoor in aanmerking komende datalekken bij de Autoriteit Persoonsgegevens (AP) gemeld. Er vindt dan direct verder onderzoek plaats naar de risico's voor personen waarvan de gegevens zijn gelekt. Dit is ook bepalend of deze personen worden geïnformeerd over dit datalek.

De hieronder beschreven incidenten die niet als datalek bij de AP zijn gemeld betreffen incidenten waarbij gegevens niet buiten de organisatie zijn gekomen of waarbij door snel te handelen het risico op schade voor de persoon in kwestie teniet is gedaan.

Meldings-datum	Omschrijving	Melding aan AP
16-5-2023	Een herinnering inzake erfpachtcanon nota is verstuurd naar een verkeerd mailadres. Hierdoor kwam een mail retour dat de nota niet voor die persoon bestemd is. In het gebruikte verkeerde mailadres bleek 1 letter te ontbreken.	Nee
17-5-2023	Een derde partij kreeg de verkeerde bijlages (nota's van debiteuren) toegestuurd via de email. Hierdoor kreeg hij onbevoegd toegang tot de op de nota's vermelde persoonsgegevens van betrokkene.	Nee
17-5-2023	Gedurende een bepaalde periode was het mogelijk om alle documenten van een collega te bekijken door andere onbevoegde medewerkers. In deze documenten waren persoonsgegevens te vinden, zoals namen in combinatie met gespreksverslagen. Hierbij waren de autorisatie(s) van medewerker(s) verkeerd ingesteld.	Nee
15-6-2023	Documenten waren binnen SharePoint (Teams) per abuis korte tijd inzichtelijk voor alle medewerkers. Dit betreft vertrouwelijk documenten met personeelsgegevens.	Nee
22-6-2023	Er werd ontdekt dat in een bepaald systeem waar bepaalde persoonsgegevens waren opgeslagen onbedoeld ook toegankelijk was buiten de organisatie voor diegenen die het exacte systeemadres van het desbetreffende domein kenden. Het gaat enkel om contact informatie en hardware informatie van onze werknemers, bijvoorbeeld het type hardware dat de werknemer zou ontvangen.	Nee
3-8-2023	Een toekenningsbrief van een gehandicaptenparkeerkaart is aan de verkeerde persoon verzonden. Hierin stond alleen de naam van de persoon en dat deze een gehandicaptenparkeerkaart krijgt. Verder geen andere persoonlijke gegevens. De onbevoegde ontvanger heeft dit lek bij de gemeente gemeld en vervolgens heeft zij bevestigd de brief te vernietigen.	Nee
10-8-2023	Door een systeemtechnische fout is een aangevraagde echtscheidingsakte naar het oude (verkeerde) adres van de aanvrager gestuurd. De akte wordt altijd opgestuurd naar het in de BRP bekende adres. Deze gegevens herleiden we uit ons Zaaksysteem en zouden in de regel ten alle tijden actueel moeten zijn. Dit was door een systeemfout niet het geval waardoor er een oud adres van de klant zichtbaar was. De beheerder van ons datadistributiesysteem heeft bij de leverancier nagevraagd waarom de oude gegevens worden doorgestuurd naar zaaksysteem en er niet eerst een vraag aan de landelijke voorziening wordt gesteld voor de meest actuele gegevens. Daarbij is ook gevraagd om maatregelen die dit soort systeemfouten voorkomen.	Nee
27-9-2023	Op 23-8-2023 is de geboortedatum, bsn en privéadres ten onrechte gedeeld van een persoon per email.	Nee
9-11-2023	op 13 oktober 2023 is er een e-mail verstuurd aan een collega . Bij het opstellen van de mail bleken er twee mailadressen te verschijnen. Dit heeft ervoor gezorgd dat het verkeerde mailadres is gebruikt.	Nee

Met leveranciers en ketenpartners zijn verwerkers- of datalevering-overeenkomsten afgesloten om de beveiliging van privacygevoelige gegevens te borgen. De in deze overeenkomsten opgenomen informatiebeveiligingseisen zorgen ervoor dat de risico’s aanzienlijk verkleind zijn.

Daarnaast wordt gewerkt aan het implementeren van technische componenten zoals het SIEM/SOC. Hiermee wordt het mogelijk om systematisch in de gaten houden wat er gebeurt in de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren. Detectie zorgt voor het vroegtijdig signaleren van afwijkingen en bedreigingen en geeft daarmee ruimte om incidenten te voorkomen voordat ze manifest worden. Detectie zorgt dat kosten als gevolg van incidenten laag blijven en incidenten uiteindelijk zelfs voorkomen kunnen worden, maar ook dat zaken die niet of nooit gezien worden wel aan het licht komen en kunnen worden aangepakt. Detectie en de reactie op meldingen vereist echter tijd van beheerders, die deze tijd vaak niet beschikbaar hebben.
Als de gemeente niet weet wat er gebeurt, dan kan ook niet worden gestuurd op risico's. Gebrek aan inzicht in wat er feitelijk gebeurt is onwenselijk omdat dit het bestuur belet om adequaat te kunnen sturen op risico's, ernaar te handelen en ervan te leren. Het implementeren van de BIO en de AVG brengt de basis op orde. Daarmee kan informatiebeveiliging en privacybescherming als proces worden ingericht waarmee de focus op detectie en actieve preventie gezien wordt als de logische vervolgstap.

8. Meerjarenperspectief

Inwoners, ondernemingen en instellingen moeten erop kunnen vertrouwen dat we zorgvuldig omgaan met (persoons)gegevens. Het is daarom van groot belang dat gegevens alleen onder strikte voorwaarden gebruikt worden en goed beveiligd zijn tegen onbevoegd gebruik. Ons meerjaarlijks informatiebeveiligingsbeleid kent passende technische en organisatorische maatregelen om informatie te beschermen. Ook waarborgt het beleid dat de gemeente voldoet aan de relevante wet- en regelgeving. De beveiligingsfunctionaris (CISO) zorgt voor de coördinatie en het toezicht op de naleving van beveiligingsmaatregelen en -procedures, voor elk onderdeel van het informatiebeveiligingsbeleid. Jaarlijks toetsen we door middel van zelfevaluatie en externe audits de maatregelen voor de waardedocumenten, BRP, BAG, BGT, BRO, DigiD en Suwinet.

We houden rekening met ontwikkelingen en nieuwe opkomende bedreigingen.
Dat vraagt om tijdig anticiperen en middelen beschikbaar stellen om maatregelen te nemen.

We hebben afgelopen jaren te maken gehad met nieuwe trends en ontwikkelingen, dit zal ook de komende jaren niet anders zijn. Zo heeft de Coronacrisis gezorgd voor de toename van digitaal plaats en tijd onafhankelijk werken.
Diverse ontwikkelingen in de nabije toekomst maar ook die de afgelopen periode al zijn ingezet mogen niet onderbelicht blijven.

In feite zijn de hieronder uitgewerkte punten onder te brengen in een aantal dreigingen. Deze moeten gezien worden als reminders waar nu en de komende jaren rekening mee moet worden gehouden.

De gemeentelijke informatievoorziening is kwetsbaar. We onderscheiden hieronder[7] een aantal categorieën van dreigingen in volgorde van belangrijkheid.

Grootste risico's voor gemeenten

Wat zijn op dit moment de grootste risico's op het gebied van de informatiebeveiliging en gegevensbescherming?

Uitval van dienstverlening en bedrijfsvoering
Als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering. Nagenoeg ieder proces, van uitgifte van paspoorten tot het betalen van uitkeringen, wordt uitgevoerd of ondersteund door digitale informatie- en communicatievoorzieningen. In het ergste geval moeten gemeenten dienstverleningsprocessen stilleggen.

Vertrouwelijke informatie in verkeerde handen
In principe is overheidsinformatie openbaar. Tenzij deze informatie privacygevoelig is, schade kan toebrengen aan de overheid of commercieel voor- of nadelig kan zijn voor derden. Gemeenten verwerken voor hun wettelijke taken veel vertrouwelijke informatie. Denk aan gegevens over werk en inkomen, zorg, veiligheid of commercieel interessante informatie over gebiedsontwikkeling, aanbestedingen en bedrijfsgevoelige informatie. Onterechte toegang tot deze informatie kan uiterst nadelig uitvallen voor inwoners en ondernemers. Een datalek of een overtreding van de AVG kan leiden tot hoge boetes.

Fouten in de dienstverlening
Informatiebeveiligingsincidenten kunnen leiden tot fouten in de dienstverlening. Kwaliteit en integriteit van data worden in het algemeen niet direct gezien als doel van informatiebeveiliging. Toch dient dit risico nadrukkelijk op het netvlies te staan van de directie. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

[7] Bron: IBD, tweejaarlijks dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023/2024

Actueel dreigingsbeeld 2023-2024

De IBD ziet dat in het bijzonder drie soorten dreigingen opvallen sinds het uitbrengen van het vorige dreigingsbeeld over 2021- 2023.

Meer ransomware met destructievere gevolgen

De dreiging van ransomware-aanvallen neemt toe. Aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger: het wordt merkbaar. Het fenomeen ransomware (gijzelsoftware) komt al jaren voor. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken. De IBD ontving de afgelopen jaren steeds meer meldingen van situaties waar gemeentelijke proces- sen langdurig(er) verstoord zijn als gevolg van destructieve gijzelsoftware. Criminelen aarzelen niet om privacygevoelige gegevens van inwoners, bedrijven en medewerkers online te publiceren.

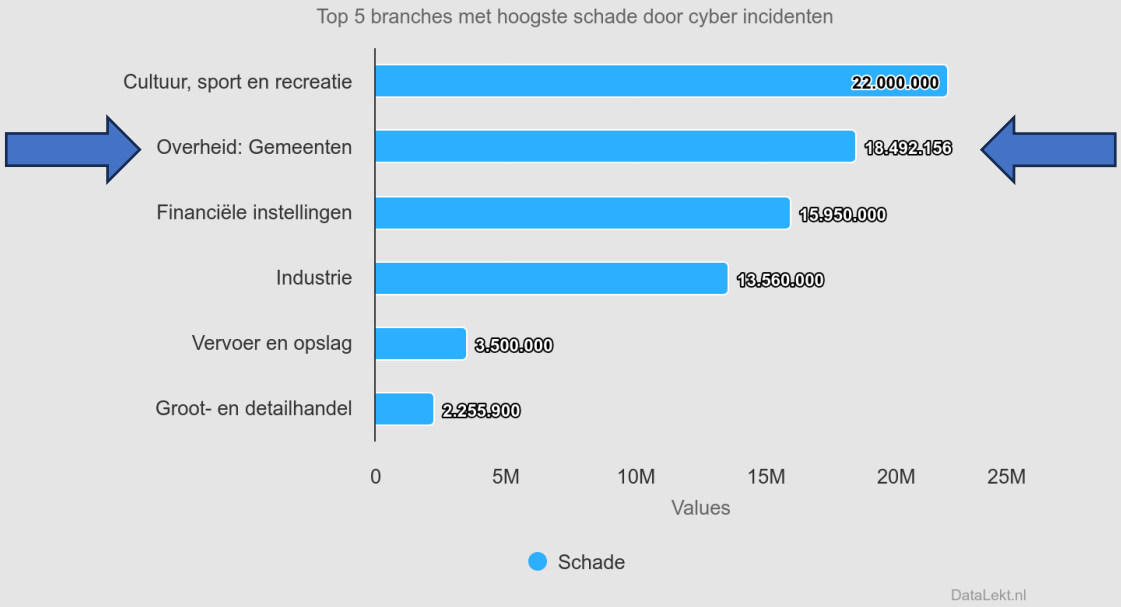
Steeds meer en ernstiger kwetsbaarheden in software
Alle hard- en software bevat kwetsbaarheden en fouten. Deze zouden kunnen worden misbruikt door kwaadwillenden. Het is daarom zaak om kwetsbaarheden tijdig te verhelpen.
In 2021 heeft de IBD 1841 kwetsbaarheden gesignaleerd. De ene kwetsbaarheid is de andere niet en daarom wordt per geval een risicoschatting gemaakt op basis van kans en impact. Gevallen met een hoge kans op misbruik en ernstige gevolgen komen in de afgelopen jaren relatief steeds vaker voor. Vaak is het verhelpen van een kwetsbaarheid een kwestie van updaten, maar soms is het complexer en moeten systemen ingrijpend gewijzigd worden.

Gevaren in ketens uit het zicht
Een gemeente neemt deel in gemiddeld 30 samenwerkingsverbanden en maakt gebruik van diensten van derden zoals softwareleveranciers. Omdat men bij uitbesteding vooral stuurt op de kwaliteit van de uiteindelijke dienstverlening en informatiebeveiliging en privacy gezien worden als operationele details, is daar weinig aandacht voor in de samenwerkingsafspraken. Politiek gezien is uitbesteding en/of samenwerking bedoeld om zaken tegen lagere kosten op een hoger kwaliteitsniveau te krijgen.
Informatiebeveiliging is in die zin een kostenpost. Als er al concrete afspraken zijn over informatiebeveiliging en privacy dan staat controle op de naleving beperkt op de agenda. Gemeenten vertrouwen erop dat bij een samenwerkingsverband dergelijke zaken ‘gewoon geregeld zijn’. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico’s als taken zijn uitbesteed. Gemeenten zijn in de afgelopen twee jaar regelmatig geconfronteerd met incidenten die ontstaan zijn bij derden waarbij de gevolgen in de eigen gemeente merkbaar waren.

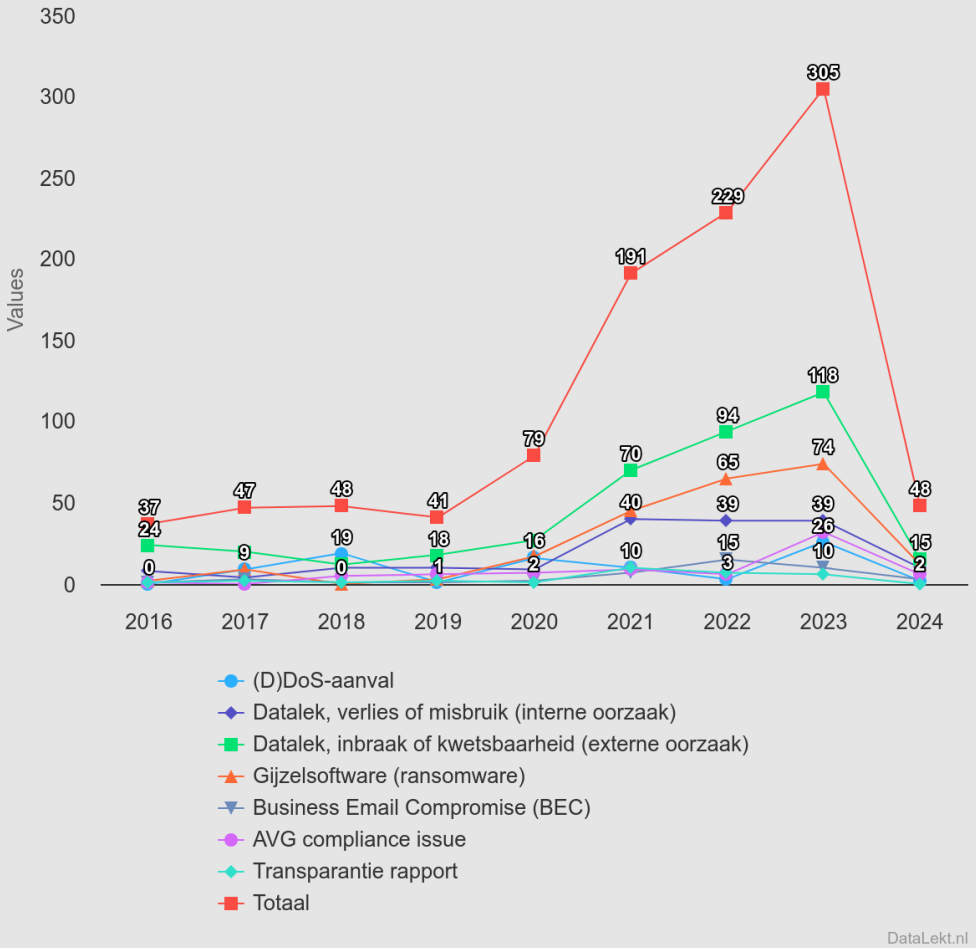
Speerpunten Nederlandse Cybersecuritystrategie 2023 – 2028
(Bron: Nationaal Cyber Security Centrum (NCSC))
De Nederlandse samenleving wordt in hoog tempo steeds meer afhankelijk van digitale systemen. Hierdoor groeien de risico's en is digitale veiligheid, cyberweerbaarheid, steeds belangrijker. De Nederlandse Cybersecuritystrategie richt zich op het ontwikkelen van een veilig en digitaal ecosysteem, met vijf speerpunten:

- Beter zicht op de dreiging. Het kabinet investeert in mensen en systemen die scherper zicht geven op de herkomst van dreigingen en tegen wie ze gericht zijn.
- Meer cybersecurityspecialisten. We nemen verschillende acties om meer ICT-specialisten op de arbeidsmarkt te krijgen.
- Overheid en sectoren nemen verantwoordelijkheid. De verantwoordelijkheid voor veiligheid wordt deels verplaatst van eindgebruikers naar de overheid en specifieke sectoren. De meest volwassen en bepalende organisaties dragen de zwaarste verantwoordelijkheden. Voor de gehele overheid zelf zullen stevige wettelijke eisen voor veiligheid en toezicht op naleving erop worden ingericht.
- Beter toezicht en de noodzakelijke wet- en regelgeving. Herschikking van verantwoordelijkheden vergt uitbreiding van wettelijke regels en toezicht. Veiligheid moet het fundament worden waarop nieuwe systemen worden ontworpen. Er komen nieuwe regels waar (rijks)overheden, vitale aanbieders, en leveranciers van digitale producten en diensten aan moeten voldoen.
- Heldere informatie via een nationale cyberautoriteit. Er komt een centrale cyberautoriteit in Nederland: het nationale Cyber Security Incident Response Team. Deze nieuwe organisatie zal in samenwerking met publieke en private partners, vitale en niet-vitale organisaties, overheden en burgers voorzien van informatie over (dreigende) cyberincidenten om hen in staat te stellen zich te beveiligen.

Wake-up call:
Sinds januari 2016 zijn al meer dan 550 cyberincidenten bij Nederlandse organisaties vermeld in de media. Of het nu gaat om DDoS-aanvallen, fraude via phishing, verloren USB-sticks of gijzelsoftware. (Bron: DataLekt.nl)



Aantal soorten cyberincidenten in Nederland per jaar (gemeten 13 maart 2024):



Hoewel we er alles aan doen om de risico's zo klein mogelijk te maken maar incidenten zijn ook voor Midden-Delfland niet uit te sluiten.