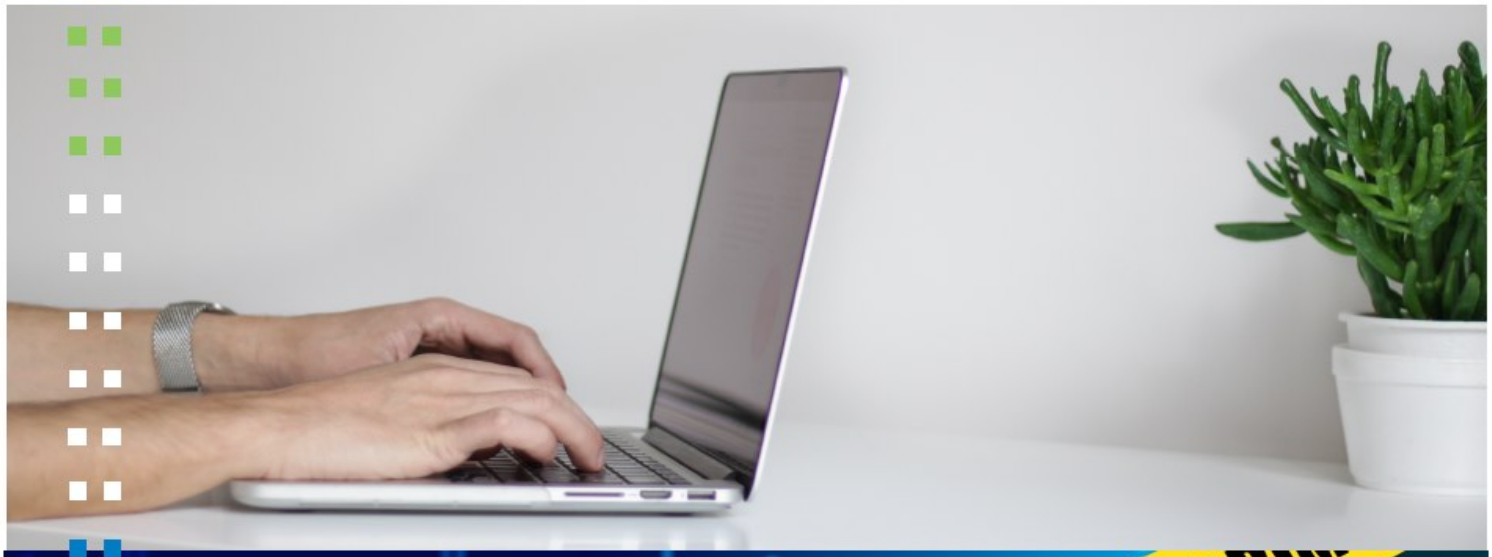
Gemeente Midden-Delfland

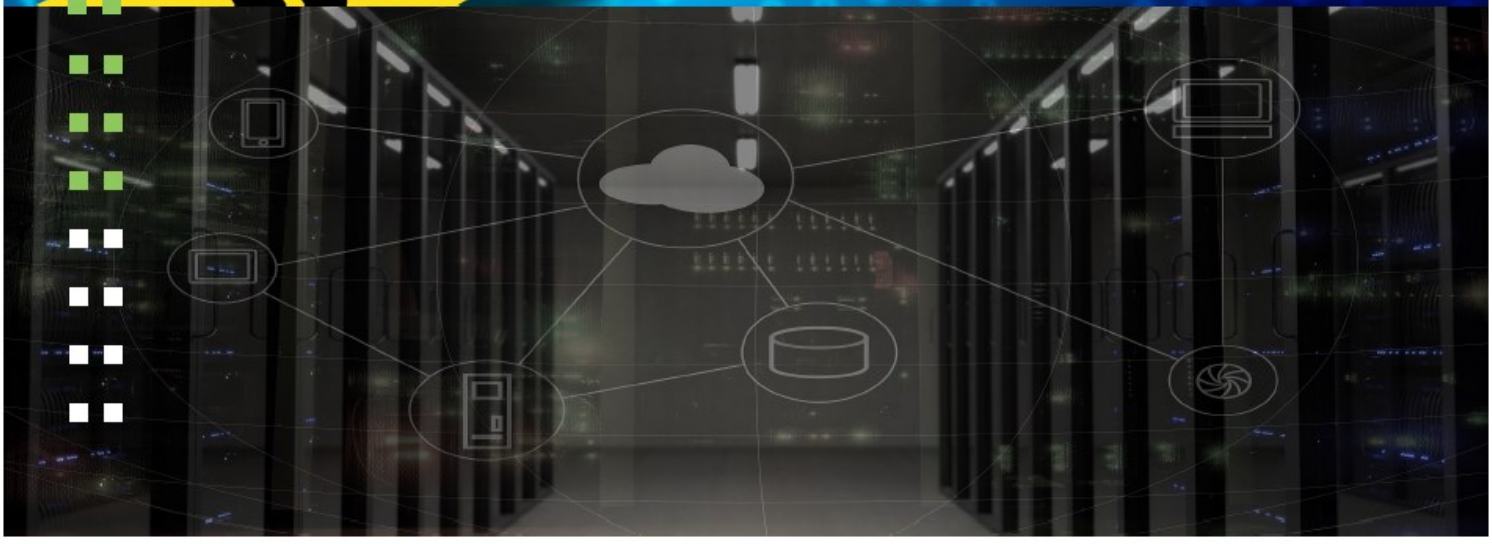
cittaslow

Jaarverslag Informatiebeveiliging Midden-Delfland

2022







Inhoud

Managementsamenvatting 3
Activiteiten in 2022 3
Beveiligingsincidenten 3
Zelfevaluaties 4
Vooruitblik 2023 op het gebied van de informatiebeveiliging 4
1. Inleiding 5
2. IB-beleid, doelstellingen en ambities 6
Wat is informatiebeveiliging? 6
Baseline Informatiebeveiliging Overheid (BIO) 6
Uitgangpunten en doelen van ons informatiebeveiligingsbeleid 7
Relatie met privacy 7
3. Horizontale en verticale verantwoording op basis van ENSIA 9
Verantwoordingsrapportages zelfevaluatie 2022 11
Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet 18
4. Samenvattend beeld en resultaten informatiebeveiliging 2022 19
Resultaat meting BIO 20
5. Disclaimer 23
6. Belangrijkste beheersmaatregelen IB 24
Verbeterpunten op basis van meting BIO 25
7. Realisatie doelstellingen IB-beleid 27
8. Incidenten en ontdekte kwetsbaarheden 32
9. Meerjarenperspectief 35
Grootste risico’s voor gemeenten 35

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 2022 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[2]). Hierin zijn ook de resultaten uit de Eenduidige Normatiek Single Information Audit (ENSIA[3]) 2022 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 2022 en de DigiD/Suwi-audit. De verbeterpunten met de hoogste risico's vormen het jaarplan 2023.

Het college van B&W wordt verzocht het jaarverslag informatiebeveiliging 2022 vast te stellen en de CISO het mandaat te geven het jaarplan met verbeteracties uit te (laten) voeren.

Activiteiten in 2022

In 2022 is op het gebied van informatiebeveiliging het volgende gerealiseerd:

- In 2022 zijn we van het gebruik van privé-smartphones voor personeel overgestapt op beter te beveiligen bedrijfs-smartphones met 2 factor authenticatie voor toegang tot bedrijfstoepassingen of gegevens.
- We zijn gestart met de overgang naar Office 365 als cloud-oplossing waarbij we belangrijke beveiligingsaspecten integreren in de verbeterde toegankelijkheid, dit project loopt nog door in 2023.
- We zijn ook gestart met vernieuwing van onze WiFi-omgeving in het gemeentehuis die sterkverouderd was en niet meer aan alle informatiebeveiligingseisen voldeed. Dit project loopt door in 2023.
- In 2022 is ons nieuwe zaaksysteem in gebruik genomen waarmee we beter kunnen voldoen aan de AVG door het bij het inrichten van het systeem doelbinding toe te passen voor toegang tot informatie.
- Er is structureel aandacht gegeven aan bewustwording over informatiebeveiliging onder het personeel.
- Er zijn ad-hoc verschillende maatregelen genomen om kwetsbaarheden in gebruikte software op te lossen.

Beveiligingsincidenten

In 2022 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 voornamelijk geconstateerde kwetsbaarheden in software met advies over hoe deze te verhelpen.

In 2022 zijn 10 datalekken gemeld bij de privacy officers. In 2020 waren dit er nog 17 en in 2021 11. 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. In één datalek bleek het nodig om de Autoriteit Persoonsgegevens en betrokkenen te informeren. Geconstateerd wordt dat het datalekkenregister adequaat wordt bijgehouden.

[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] BIO staat voor Baseline Informatiebeveiliging Overheden
[3] ENSIA staat voor Eenduidige Normatiek Single Information Audit

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), de Waardering Onroerende Zaken (WOZ) 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 inmiddels 2 aansluitingen[4]: onze website en de Persoonlijke Internetpagina en web-formulieren van ons zaaksysteem. Door een externe IT-auditor is vastgesteld dat wordt voldaan aan het gestelde normenkader.
- Gemeente Midden-Delfland gebruikt Suwinet. Door een externe IT-auditor is 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 100% goed op de norm.
- Over de zelfevaluatie van de WOZ is geconstateerd dat deze nog niet op alle onderdelen binnen de norm scoort, daarom worden verbeteracties voorgesteld.

Vooruitblik 2023 op het gebied van de informatiebeveiliging

Activiteiten voor 2023:

- We stellen in 2023 een nieuw geactualiseerd strategisch informatiebeveiligingsbeleid op, het huidige is 3 jaar oud en verloopt daarmee.
- Het sterk verouderde thuiswerkbeleid is nog niet geactualiseerd naar de huidige eisen. Inmiddels is de verwachting dat in 2023 het beleid voor hybride werken wordt vastgesteld.
- 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 opm 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 helder vastgelegd te hebben ook in het kader van de verSAASing en de nieuwe cloud-technologie.
- We stellen een bedrijfscontinuïteitsbeleid vast en starten met het opstellen van crisisplannen voor onze meest kritieke processen op om voorbereid te zijn op crisissituaties.
- 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 2023 wordt er een nieuwe meting gedaan onder de medewerkers op de mate van bewustzijn op informatiebeveiliging en privacy.
- We kopen en implementeren een nieuw systeem voor "uitwijk' van onze meeste kritieke software en data bij calamiteiten zoals bijv. brand in ons gemeentehuis of langdurige uitval van apparatuur.
- Ons Responsible Disclosure beleid[5] wordt vastgesteld en gepubliceerd op onze website.
- We doen (samen met Westland) een aanbesteding voor een siem/soc systeem. Hiermee kunnen we 24/7 beveiligingsinformatie verzamelen, combineren en analyseren uit verschillende bronnen, zoals firewalls, IDS/IPS-systemen[6], antivirussoftware en logboeken van servers en netwerkapparaten. Het identificeert potentiële beveiligingsincidenten en genereert waarschuwingen die kunnen worden onderzocht door een medewerkers in een SOC.

[4] In 2022 zijn 2 DigiD-aansluitingen in gebruik geweest vanwege de overgang van de digitale aanvragen via onze website naar de nieuwe aansluiting voor de web-formulieren en PIP-pagina van ons Zaaksysteem. Voor 2023 is alleen de aansluiting voor het zaaksysteem in gebruik.

[5] 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.

[6] Inbraakdetectiesystemen (IDS) en inbraakpreventiesystemen (IPS) houden ons netwerk constant in de gaten. Ze identificeren mogelijke incidenten en loggen informatie daarover, waarop gehandeld kan worden.

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 2022 opnieuw een zelfevaluatie informatiebeveiliging uit. Deze is onder meer gericht op beveiligingsnormen van de BIO, AVG, BRP, PUN, BAG, BGT, DigiD, Suwinet en voor het eerst dit jaar de WOZ. 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 'Collegeverklaring ENSIA' over een aantal geselecteerde beveiligingsnormen (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 in zijn functie als CIO.
- Aan de hand van een GAP-analyse (0-meting) 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.

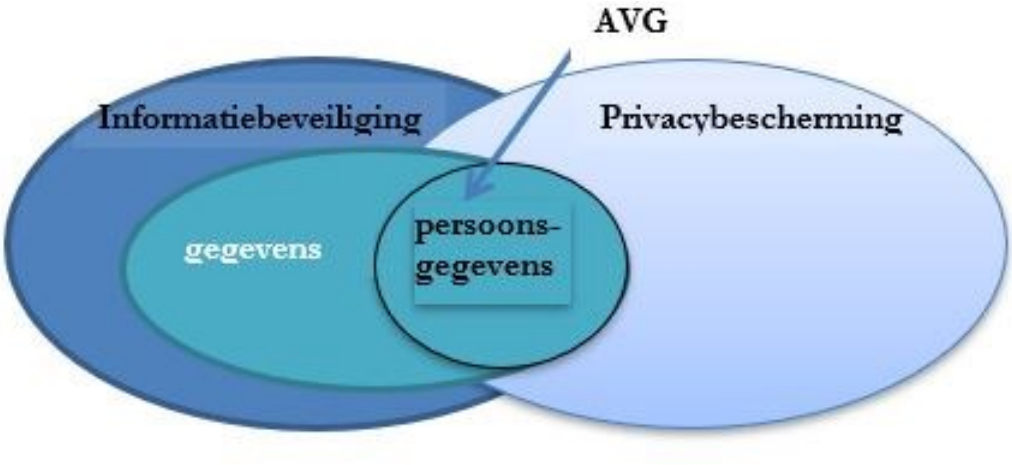
1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
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). Vanaf 2021 is de ENSIA zelfcontrole over de Basisregistratie Waardering Onroerende Zaken ook een wettelijke verplichting.
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. Van oudsher bestonden verplichtingen ten aanzien van het ministerie van BZK rond de Basisregistratie Personen (BPR), de PUN en DigiD, en het ministerie van IenW rond de BAG en de BGT. 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, BRO en WOZ) 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 2022
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 2022 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 2022 31 DEC 2022	Vragenlijsten: • RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO). • BKWI: Informatiebeveiliging Suwinet (BIO). • Logius: Informatiebeveiliging DigiD. • DGBRW: Datakwaliteit en -integriteit BAG, BGT en BRO. • Waarderingskamer: Informatiebeveiliging, systeembeheer en architectuur WOZ.
Opstellen	• Genereren en opstellen verantwoordingsrapportages. • Audit door gecertificeerde IT-auditor over collegeverklaring Suwinet en DigiD. • Opstellen rapportage ENSIA t.b.v. de gemeenteraad.		Producten: • Collegeverklaring over Suwinet en DigiD. • Rapportage BAG, BGT en BRO door college van B&W. • Rapportage WOZ 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 via Kwaliteitsmonitor).	30 APR 2023	Resultaten: • De toezichthouders BKWI, Logius, DGBRW en Waarderingskamer krijgen via ENSIA de verantwoordingsrapportages aangeleverd. • RvIG krijgt 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 BZK.	15 JUL 2023	• De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd. • De vastgestelde jaarstukken zijn aan de provincie toegestuurd.

Over 2019 vormde de BIG nog de kern van de horizontale verantwoording aan de gemeenteraad. 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 2022 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 mee geleverd 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)
- Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
- Basisregistratie Ondergrond (BRO)
- De Waardering Onroerende Zaken (WOZ)

De normen uit de Algemene Verordening Gegevensbescherming (AVG) zijn in de vragen over de BIO en de specifieke domeinen geïntegreerd.

In de periode van 1 juli tot 31 december 2022 zijn deze vragenlijsten door de domeinbeheerders ingevuld en door de ENSIA-coördinator ingeleverd bij de landelijke toezichthouders.

De beantwoording van de vragen over deze normen is terug te vinden in de verantwoording over de BIO. Daarnaast zijn over de proceseigen normenkaders over de BAG, BGT, BRO en de WOZ aparte verantwoordingsrapportages als bijlagen toegevoegd.

Verticale verantwoording
'Verticaal' verantwoorden we met de collegeverklaring de specifieke status per auditonderdeel (over 2022 Suwinet en DigiD) richting de betreffende toezichthouder (zoals Logius voor DigiD). Daarnaast rapporteren we over de BAG, BGT, BRO en WOZ naar de verticale toezichthouders. De rapportagedeadline hiervoor is tot 1 mei 2023.

Hieronder vindt u de conclusies uit de betreffende verantwoordingsrapportages.

Verantwoordingsrapportages zelfevaluatie 2022

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 BIG gebaseerde vragen, de zogenaamde specifiek op de normenkaders van BAG, BGT en BRO gerichte vragen.
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, BRO en WOZ 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, 6 en 7 wordt uitgebreid ingegaan op de resultaten van 2022 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

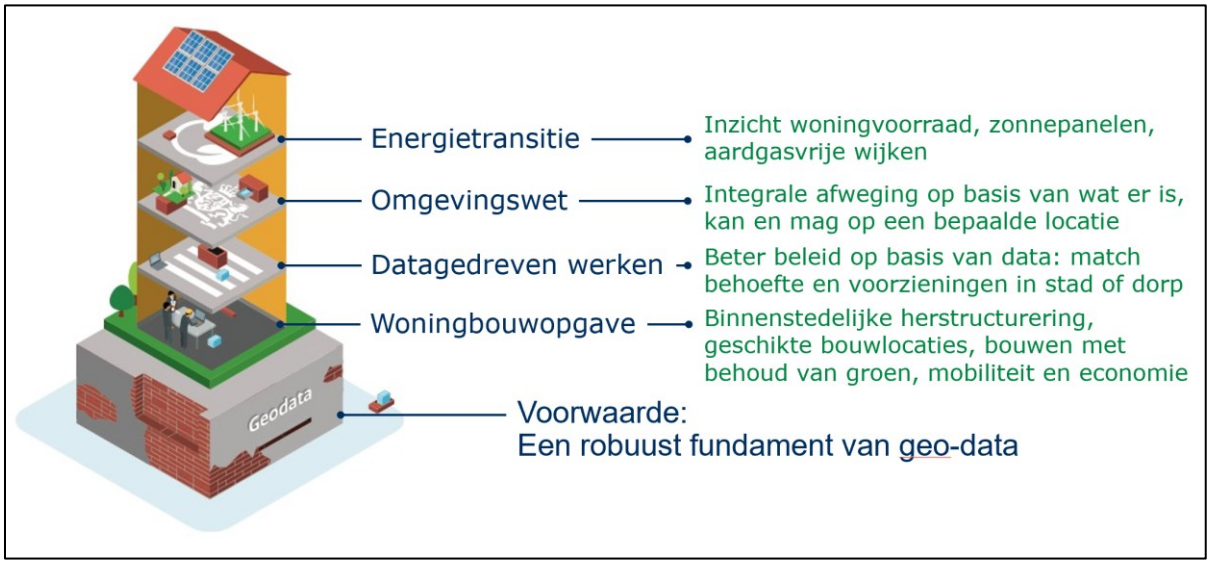
De Basisregistratie Personen (BRP) is onderdeel van het stelsel van basisregistraties van de Nederlandse overheid. De Nederlandse overheid registreert persoonsgegevens in de BRP. Alle overheidsinstellingen en bestuursorganen (zoals de Belastingdienst) zijn verplicht voor hun taken gebruik te maken van 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 2022 (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 2022 (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.

De BAG is al jaren op een stabiel hoog nivo. De iets lagere waarden over 2021 en 2022 is verwaarloosbaar en wordt veroorzaakt door gewijzigde ENSIA.
Deze BGT scoort in 2022 goed. In 2022 zijn er veel achterstallige werkvoorraden weggewerkt, er is een processenhandboek gemaakt en geïmplementeerd. De lage scores uit 2019 en 2020 komt doordat er deze jaren geen BGT beheerder was. Sinds maart 2021 is er weer een BGT beheerder. dit ziet u direct terug in het verbeterde cijfer.
Ook de op BRO is een inhaalslag gemaakt en scoort over 2022 goed.

Scores geo-basisregistraties 2022 (tijdvak 1 januari 2022 tot en met 31 december 2022):

Basisregistratie	Score	Consequenties score
BAG		Geen, we zijn in "Control" en blijven alert op de aandachtspunten. Omgevingswet: zonder geodata geen DSO, en zonder DSO geen functionerende Omgevingswet. Immers bij elke vergunningsaanvraag moeten de volgende vragen beantwoord worden: Om welk object gaat het, wat is het, waar staat het, op welk perceel, van wie is dat? Deze gegevens komen uit verschillende basisregistraties WOZ, BAG, BGT en BRKZorgen 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 aandacht blijven geven aan aan de borging van het proces, bij wijzigingen in het proces passen we ons processenhandboek daaraan aan.

< 75% onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BGT		Geen, We zijn in "Control" en blijven allert op de aandachtspunten. Aandacht voor de Omgevingswet: zonder geodata geen DSO, en zonder DSO geen functionerende Omgevingswet. Immers bij elke vergunningsaanvraag moeten de volgende vragen beantwoord worden: Om welk object gaat het, wat is het, waar staat het, op welk perceel, van wie is dat? Deze gegevens komen uit verschillende basisregistraties WOZ, BAG, BGT en BRK.

< 75% Onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BRO		Geen, We zijn in "Control" en blijven alert op de aandachtspunten.

< 60% Onvoldoende vanaf 60% voldoende

Trend score geo-basisregistraties

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

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

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

BAG
Verbetermaatregelen voor 2023:

- Zorgen dat de processen juist blijven werken, zodat alle mutaties tijdig verwerkt kunnen worden.
- Een mutatiesignalering uitvoeren met de luchtfoto die in het voorjaar 2023 gevlogen gaat worden.
- De resultaten van de mutatiesignalering in de BGT en de BAG verwerken.
- Periodiek de gebruiksoppervlakte afstemmen met de BAG en de WOZ.
- Processenhandboek optimaliseren.

BGT
Verbetermaatregelen voor 2023:

- Mutatiesignalering BGT uitvoeren met de luchtfoto die in het voorjaar 2023 gevlogen gaat worden.
- Uitvoering geven aan de kwaliteitseisen BGT zoals genoemd in het jaarplan 2023
- Onderzoeken of koppeling tussen BOR (Beheer Openbare Ruimte) en de BGT zinvol is. Zo ja, dan moet deze koppeling gerealiseerd worden.
- Op termijn alle blokhutten opnemen in de BGT en BAG. Op termijn alle luifels en overkapping opnemen in de BGT. De start in 2022 moet in 2023 een vervolg krijgen.
- Processenhandboek optimaliseren.

BRO
Verbetermaatregelen voor 2023:

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

Zelfverantwoording Waardering Onroerende Zaken

Gemeenten en uitvoeringsorganisaties zullen bij de interne beheersing van risico's in het WOZ-proces voldoende aandacht moeten hebben voor de beheersing van geautomatiseerde systemen. Beheersingsaspecten die te maken hebben met architectuur, informatiebeveiliging, continuïteit, beschikbaarheid en algemene IT-beheersingsmaatregelen, moeten voldoende worden beheerst. Door maatschappelijke ontwikkelingen op het terrein van de verwachte privacybescherming en minimale beveiligingsmaatregelen en door veranderende visie op de voor een gemeentelijke organisatie gewenste architectuur vergen deze aspecten mee-ontwikkelende beheersingsmaatregelen.



Bij de WOZ speelt de tegenstelling tussen enerzijds de maatschappelijke behoefte aan WOZ-waarden en WOZ-gegevens van hoge kwaliteit met de mogelijkheid tot inbreng van gegevens door belanghebbenden en anderzijds de behoefte aan privacybescherming bij burgers. De Staatssecretaris van Financiën roept in een brief aan de Tweede Kamer (reactie op WODC-rapport over no cure no pay) gemeenten op om meer ruimte te bieden aan burgers om op laagdrempelige wijze gegevens uit de WOZ-administratie te controleren en aan te vullen, Dit vergt adequate aandacht niet alleen voor functionaliteit gericht op digitale dienstverlening, maar juist ook voor informatie-veiligheid en een eigentijdse informatie-architectuur. Kortom aandacht voor investeringen in de vernieuwing van automatiseringssystemen.

In onderstaande tabel zijn de uitkomsten van de WOZ-vragenlijst zoals deze binnen ENSIA voor de eerste keer zijn ingevuld samengevat.

Onderwerp	Score	Conclusie score	Achtergrond
1.Naleving BIO	✗	De BIO is nog niet (volledig) geïmplementeerd in de organisatie, er worden daarom op dit moment geen controles uitgevoerd op naleving van de BIO voor de WOZ.	Ook voor de WOZ-systemen moet door de organisatie bekeken zijn, welke BIO-controls nodig zijn. De naleving van deze controls dient periodiek gecontroleerd te worden en de resultaten van deze beoordeling, in hoeverre de WOZ-systemen binnen de organisatie aan de BIO voldoen, dienen beschikbaar te zijn.
2. Ontwikkelingen BIO	✗	Er worden op dit moment geen controles uitgevoerd op naleving van de BIO voor de WOZ.	Elke gemeente en gemeentelijke uitvoeringsorganisatie dient te voldoen aan de BIO. In de BIO zijn diverse controles verplicht voorgeschreven.
3. Common Ground	✗	Er zijn nog geen stappen gezet in de richting van een common ground conforme informatie-architectuur voor de WOZ.	Met Common Ground willen gemeenten de informatievoorziening eenvoudiger, flexibeler en slimmer inrichten. Zodat ze op een moderne en flexibele manier kunnen inspelen op maatschappelijke opgaven.
4. Ontwikkelingen koppelvlakken	✗	Er wordt nog gebruik gemaakt van koppelvlakken op basis ASCII-bestanden (Stuf-TAX) voor de communicatie tussen de diverse applicaties voor de WOZ-uitvoering.	De Stuf-TAX bestandsuitwisselingen voldoen niet meer aan de hedendaagse eisen die gesteld worden aan informatiebeveiliging. De uitwisseling van data dient plaats te vinden door middel van beveiligd berichtenverkeer.

Onderwerp	Score	Conclusie score	Achtergrond
5. Inzicht in koppelvlakken	✓	Tussen de applicaties die de uitvoering van de WOZ-processen ondersteunen vindt interactie plaats. Er is een volledig overzicht van de onderlinge relaties tussen deze systemen.	Een volledig overzicht van de verschillende koppelvlakken / interfaces is van belang voor het beheer hiervan.
6. Externe systemen	✓	Er is onderzocht of de verschillende geautomatiseerde systemen informatie juist delen met externe systemen zoals bijvoorbeeld de Landelijke voorziening WOZ (LV WOZ) en MijnOverheid.	Gemeenten moeten verifiëren of de gegevens in de LV WOZ nog overeenkomen met die van de gemeentelijke Basisregistratie WOZ.
7. Interne systemen	✓	Er zijn audits uitgevoerd om te beoordelen of alle voor de WOZ-uitvoering gebruikte systemen de gegevens uit interne systemen juist verwerken.	Om te waarborgen dat de informatie op een consistente wijze wordt gebruikt en verwerkt, is het belangrijk dat ook de consistentie van de gegevensverwerking regelmatig wordt beoordeeld.
8. Beschikbaarheid managementinformatie	✓	Op terrein van de beheersing van informatieveiligheid conform BIO is voor de WOZ-uitvoering de gewenste management informatie beschikbaar.	Interne beheersing is uitsluitend mogelijk wanneer er inzicht is in de mate waarin de beheersingsdoelen zijn bereikt.
9. Ontwikkelingen managementinformatie	✓	Op terrein van de beheersing van informatieveiligheid conform BIO en van synchronisatie met externe systemen is voor de WOZ-uitvoering de gewenste management informatie beschikbaar.	Interne beheersing is uitsluitend mogelijk wanneer er inzicht is in de mate waarin de beheersingsdoelen zijn bereikt.

Conclusies:
Verbetering is nodig voor brongegevens uit de KVK, automatische controle gegevens LV WOZ, en upgrade van de applicatie nodig om bij te blijven met de huidige ontwikkelingen.
De benodigde upgrade van de applicatie is aangeschaft. Helaas kan leverancier Centric hier pas in 2024 mee van start gaan en hopen wij begin 2025 over te zijn.

Verbetermaatregelen:
De planning was de genoemde verbeterpunten in 2022 te laten implementeren, onze software leverancier heeft echter aangegeven dat dit het eerste kwartaal 2024 gaat worden. Voor die tijd wordt er aan de softwareleverancier opdracht gegeven om de software te updaten naar de laatste versies, waardoor de uitval bij synchronisatie met de externe systemen gereduceerd wordt.
De laatste versies zijn inmiddels geplaatst en de opdracht voor het oplossen van foutmeldingen wordt momenteel uitgevoerd.

Aanbevelingen:
Dat de gewenste verbeterpunten daadwerkelijk in het eerste kwartaal 2024 geïmplementeerd gaan worden. Toezien op implementatie BIO. Dit is mede van belang omdat de huidige voor de WOZ gebruikte software na deze periode niet meer ondersteund wordt.

Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet

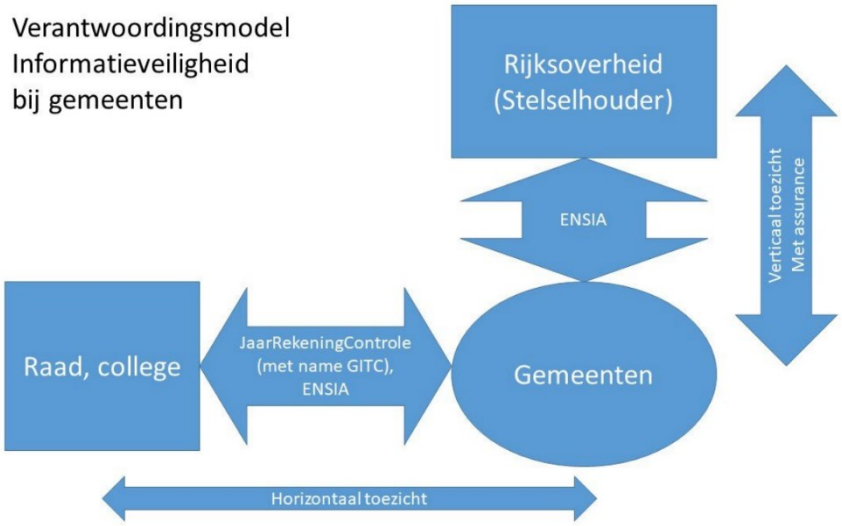
Het college van Burgemeester en wethouders geeft in een verklaring aan in hoeverre de beheersmaatregelen voldoen aan de voor de ENSIA verantwoording geselecteerde normen voor DigiD en Suwinet.

Bij de ENSIA vragenlijsten is geconstateerd dat bij gemeente Midden-Delfland op 31 december 2022 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 2022

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 2021.

Het 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 loopt het huidige informatiebeveiligingsbeleid af en wordt 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/



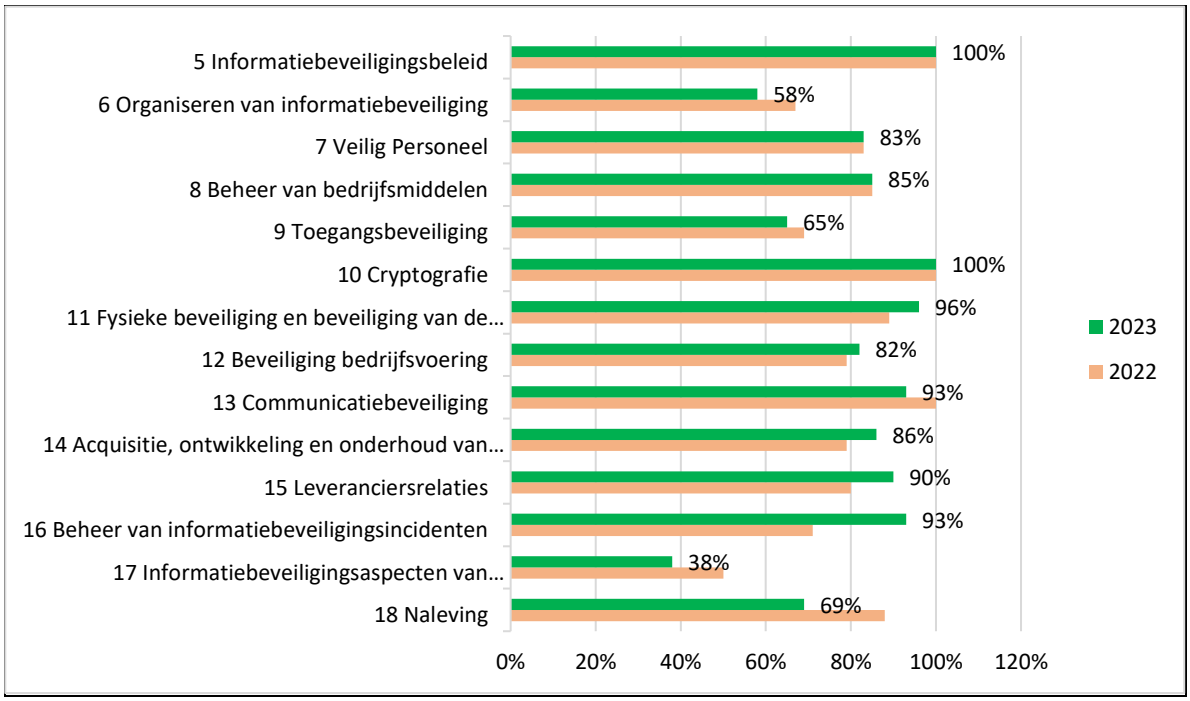
Om het informatiebeveiligingsbeleid goed te implementeren, werken we op basis van een "GAP-analyse/risicoanalyse". Deze analyses zijn uitgevoerd in directe samenspraak met de betrokken collega's van de vakafdelingen. Hiermee is het "GAP" of "gat" tussen de huidige en de gewenste situatie (volgens de geldende normen) in beeld gebracht. Vanuit deze analyse 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 2022 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 en 2022.

BIO
Baseline
Informatiebeveiliging
Overheid

Resultaat meting BIO

Op basis van de resultaten ENSIA 2022 is begin 2023 een meting uitgevoerd op de 112 normen in de BIO. De gemiddelde score is 74% en ligt iets lager dan over 2021 die toen 80% was. Reden is vooral dat we scherper inzoomen en bij twijfel kritischer zijn. Grafisch ziet het resultaat van meting 3 uit ons ISMS er als volgt uit.



Wat valt op?

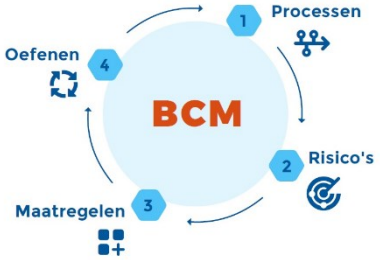
Ook 2022 is vanwege de nasleep van coronamaatregelen en het grote personeelsverloop, een moeilijk jaar geweest voor alle medewerkers van de gemeente. Er is getracht om een inhaalslag te maken op de verschillende uitgelopen projecten, dit is helaas niet overal gelukt. Mede door het verloop op personeelsgebied. Dat gold ook voor de projecten of verbeteracties op het gebied van informatiebeveiliging.

Hoofdstuk 6 van de BIO scoort relatief laag. Dat heeft vooral te maken met de contacten met overheidsorganisaties, informatiebeveiliging in projecten en telewerken of thuiswerken. Met name het sterk verouderde thuiswerkbeleid is nog niet geactualiseerd naar de huidige eisen. Inmiddels is de verwachting dat in 2023 het beleid voor hybride werken wordt vastgesteld.

Hoofdstuk 9 scoort relatief laag. Het gaat dan vooral om het beheer van toegangsrechten in de vak-applicaties zelf. Hier ligt een belangrijke rol voor de applicatiebeheerders. Dit gaat met de ingezette bredere uitrol van het ISMS in 2023 meer aandacht krijgen.

Hoofdstuk 12 scoort relatief laag en dat heeft vooral te maken dat nog onvoldoende duidelijk is 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 maar uitgangspunt is om dit helder op papier te hebben. Met name de veranderingen en ontwikkelingen in het kader van de verSAASing van applicaties vragen om andere expertise en dienstverlening. Hierop vindt in het eerste kwartaal van 2023 een onderzoek plaats. De uitkomsten daarvan betrekken we bij de actualisering van de Dienstverleningsovereenkomst met Westland voor het ICT-beheer.

Opvallende achterblijver is hoofdstuk 17 van de BIO ofwel informatieveiligheidsaspecten van bedrijfscontinuïteit met een score van 38%. Hoewel we veel maatregelen hebben ingericht zoals back-up, uitwijk, noodstroomaggregaat etc. is dat allemaal nog niet compleet en in samenhang tot een (crisis) plan gevormd. Het spectrum van bedrijfscontinuïteitsbeheer is veel meer dan dat. Het gaat ook over crisisbeheer, kritische bedrijfsprocessen, liquiditeiten, verzekeringen, huisvesting, veiligheid personeel en bezoekers en archiefbeheer. Ook moet BCM duidelijkheid geven over hoe we onze meest essentiële dienstverlening naar onze burgers kunnen continueren bij uitval van ICT voorzieningen. Vanwege coronamaatregelen, capaciteitgebrek als gevolg het grote personeelsverloop en andere projecten nog niet kunnen uitvoeren. Naar verwachting wordt het beleid over Bedrijfscontinuïteit Management in het 2e kwartaal van 2023 ter besluitvorming aangeboden.



Hoofdstuk 18 heeft een lagere score vanwege een te beperkte scope over de in gebruik zijnde vak-applicaties die in eerdere jaren is gehanteerd. 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 wordt bij een aantal applicatie beheerders in het eerste kwartaal van 2023 al succesvol vorm gegeven.

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 2023 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[7] (Hof van Twente) en 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.

[7] 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. Het beleid is verouderd op diverse onderdelen. Belangrijkste onderdelen daarbij zijn dat het beleid alleen is gericht op de AVG en niet op de Wpg. Verder is ook de bepaling m.b.t. cameratoezicht verouderd (de gemeente is nl. geen verwerkersverantwoordelijke van de camerabeelden in geval van cameratoezicht op grond van artikel 151c Gemeentewet).
In 2022 is een start gemaakt met de implementatie van de Wet Politiegegevens (Wpg) binnen de gemeente. Daarvoor zijn verschillende beleidsdocumenten opgesteld:
- Procedure rechten van betrokkenen (vastgesteld door het college in 2022)
- Beleid Wet Politiegegevens (nog niet vastgesteld in 2022)
- De wet politiegegevens: beheersingsmaatregelen en uitvoering.

Ook in 2022 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.

De bescherming van persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers. Samenvattend kan worden geconcludeerd dat de gemeente Midden-Delfland voor grote uitdagingen staat. Het advies is om in 2023 vooral prioriteit te gaan leggen op de bewustzijn, het afronden van het register van verwerkingen, het in beeld krijgen van de stand van zaken met betrekking tot verwerkersovereenkomsten en het uitvoeren van de maatregelen van de externe Wpg audit.
(Bron: Jaarverslag Bescherming Persoonsgegevens gemeente Midden-Delfland 2022)

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. Zij zijn in 2019 opgeleid en werden ook in 2020 bijgeschoold door Fox IT om te zorgen dat hun kennis up to date is en blijft. 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 2022.

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. Belangrijkste 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 BIG in 2016 een GAP- en Impactanalyse uitgevoerd op gemeente-brede maar ook systeem specifieke maatregelen.
De GAP-analyse is het uitzoeken waar men staat ten opzichte van de maatregelen.
Een soort 0-meting, wat hebben we aan maatregelen al 'in huis' en wat is hiervan nog up to date.
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 weten we welke taakvelden/processen strenge en minder strenge maatregelen behoeven. Om te bepalen of een proces, informatiesysteem en/of informatie een bepaald Basis Beveiliging Niveau (BBN) heeft binnen de BIO, of meer maatregelen nodig heeft, nadat de GAP-analyse en impactanalyse ten opzichte van de BIO organisatie-breed is uitgevoerd. 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.
Daarnaast gebruiken we de baselinetoets bij de fase voor het starten van 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 dan 75% scoren. Deze hoofdstukken vindt u in onderstaande tabel terug met de beschrijving van de verbeterpunten voor 2022.

Hoofdstuk BIO	**Onderwerp**	**Beschrijving verbeterpunten**
5	Informatiebeveiligingsbeleid	We stellen in 2023 een nieuw geactualiseerd strategisch informatiebeveiligingsbeleid op, het huidige is 3 jaar oud en verloopt daarmee.
6.2.2	Telewerkbeleid	Aandacht voor veilig gebruik van telewerken of thuiswerken, actualisering van het verouderde thuiswerkbeleid. Dit is in 2022 gestart. Het sterk verouderde thuiswerkbeleid is nog niet geactualiseerd naar de huidige eisen. Inmiddels is de verwachting dat in 2023 het beleid voor hybride werken wordt vastgesteld.
9	Toegangs-beveiliging	Het gaat dan vooral om het beheer van toegangsrechten in de vak-applicaties zelf. Hier ligt een belangrijke rol voor de applicatiebeheerders. Dit gaat met de ingezette bredere uitrol van het ISMS in 2023 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 helder vastgelegd te hebben. Met name de veranderingen en ontwikkelingen in het kader van de verSAASing van applicaties vragen om andere expertise en dienstverlening. Hierover vindt in het eerste kwartaal van 2023 een onderzoek plaats. e uitkomsten daarvan betrekken we bij de actualisering van de Dienstverleningsovereenkomst met Westland voor het ICT-beheer.

17	Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer	Hoewel we veel maatregelen hebben ingericht zoals back-up, uitwijk, noodstroomaggregaat etc. is dat allemaal nog niet compleet en in samenhang tot een (crisis) plan gevormd. Het spectrum van bedrijfscontinuïteitsbeheer is veel meer dan dat. Het gaat ook over crisisbeheer, kritische bedrijfsprocessen, liquiditeiten, verzekeringen, huisvesting, veiligheid personeel en bezoekers en archiefbeheer. Ook moet BCM duidelijkheid geven over hoe we onze meest essentiële dienstverlening naar onze burgers kunnen continueren bij uitval van ICT voorzieningen. Dit was al een verbeteractie voor 2022 maar hebben we vanwege coronamaatregelen, gebrek aan capaciteit als gevolg het grote personeelsverloop en andere projecten nog niet kunnen uitvoeren. Naar verwachting wordt het beleid over Bedrijfscontinuïteit Management in het 2e kwartaal van 2023 ter besluitvorming aangeboden.
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 het eerste kwartaal van 2023 succesvol vorm gegeven.

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.

7. 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. Dit is in 2016 door het college van burgemeester en wethouders vastgesteld. Volgens regelgeving is dit beleid drie jaar geldig en zou daarom in 2019 geactualiseerd moeten worden. Vanwege het overgangsjaar 2019 van BIG naar BIO (Baseline Informatiebeveiliging Overheden) en de impact daarvan heeft ons college ingestemd met het voor een jaar (2019) verlengen van ons huidige beleid gebaseerd op de BIG. In december 2019 is het op de BIO gebaseerde nieuwe informatiebeveiligingsbeleid 2020-2023 vastgesteld.	Het managen van de informatiebeveiliging
Informatiebeveiligingsorganisatie 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 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 2023 wordt de IB-organisatie in samenhang met het nieuwe 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 2023 nog verder ingericht en 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.

Hieronder volgen de overige punten die als prioriteit zijn aangeduid bij de GAP-, risico- en impact-analyse. Hierbij is een hoge mate van urgentie van implementatie zeer gewenst en in sommige gevallen zelfs noodzakelijk:

Maatregel	**Doelstelling**
Bewustwording Er wordt in de organisatie aandacht gegeven aan bewustwording over informatiebeveiliging. Onderzoek heeft aangetoond dat incidenten op het vlak van informatiebeveiliging voor 80% te wijten zijn aan menselijke fouten. Zo geven we periodiek aandacht aan phishingmail en ransomware. In 2022 is dat vooral via intranet gedaan en ad-hoc na signalering van actuele dreiging of ontvangen phishingmail. Door de inwerkingtreding van de AVG is in 2022 veel ad-hoc aan bewustwording gedaan op het gebied van privacybescherming. Sinds 2021 bieden we medewerkers met behulp van e-learning structureel leerstof aan medewerkers aan op een leuke interactieve manier. Hierbij wordt ook gemonitord hoe het met het bewustzijn, de kennis en gedrag rond informatiebeveiliging en privacy is gesteld. Daarmee kunnen we ook gerichter sturen op het aanbod en actualiteit van de leerstof. Deze e-learning wordt in 2023 gecontinueerd en aangepast baan actuele onderwerpen. Ook voeren we in 2023 een nieuwe uitgebreide meting uit (Cyberbarometer) over het kennisniveau van de medewerkers op het gebied van informatiebeveiliging en privacy.	Het minimaliseren van risico's van menselijk gedrag
In- en uitdienst-treden en functieverandering van medewerkers Onze in- en uitdienst-treden procedure voor medewerkers moet worden geactualiseerd naar de huidige normen voor informatiebeveiliging. Toegangsregelingen van onder andere applicaties tijdens verandering van functie worden onvoldoende vastgelegd. Toegangsregelingen van kernapplicaties zijn nog onvoldoende in kaart gebracht. Dit heeft ook een grote relatie met de nieuwe Europese privacywetgeving (AVG) die sinds 2019 van kracht is. Dit is al vanaf de eerder door onze auditor als belangrijk verbeterpunt aangedragen. Om dit proces te verbeteren is in 2022 gestart om maatregelen door te voeren en de huidige procedure te actualiseren. Inmiddels is dit breder opgepakt. Het totale proces is in 2022 geautomatiseerd. In 2023 worden de fouten uit het proces gehaald en verder gestroomlijnd.	Het voorkomen van ongeautoriseerde toegang.
Besmetting door virussen en malware Op diverse ICT-niveaus zijn technische maatregelen getroffen om dit risico tot een minimum te beperken. Toch blijft dit een groot punt van	· Het voorkomen van ongeautoriseerde toegang. · Het garanderen van correcte en veilige informatievoorzieningen.

aandacht en zorg. De zwakste schakel is de mens. Dit geven we voornamelijk in de diverse bewustwording sessies grote aandacht. Zo nemen hebben we in 2022 extra technische maatregelen genomen om schade te voorkomen of te beperken. Het gaat hierbij om o.a. beveiligingstoepassingen van Microsoft voor onze in de cloud opgenomen en op te nemen applicaties en informatie.	· Het beheersen van de toegang tot informatiesystemen. · Het beschermen van kritieke bedrijfsprocessen.
Mobile Device Management / digitaal vergaderen Eind 2018 zijn we gestart om ons mobile devicemanagement (MDM) beleid te actualiseren naar de beveiligingsnormen. Begin 2019 is het beleid geformaliseerd. Daarnaast zijn gebruik van mobiele devices en thuiswerken nauw verbonden met bewustwording en gedrag van medewerkers. In 2020 zijn de vaste computers op de werkplekken vervangen door mobiele apparatuur. Daarmee is het mogelijk om veilig plaats onafhankelijk te werken. In 2022 zijn we ook over gestapt van het werken met prive-smartphones naar beter te beveiligen bedrijfssmartphones. Het op afstand vergaderen van met MS Teams is vanwege Corona ad-hoc versneld mogelijk gemaakt. Teams draait het beste onder Office 365 waarvoor in 2022 de gefaseerde implementatie is gestart en we in 2023 verder vorm geven.	· Het voorkomen van ongeautoriseerde toegang. · Het beheersen van de toegang tot informatiesystemen. · Het waarborgen van veilige informatiesystemen.
Logging en monitoring Er zijn al oplossingen geïmplementeerd en geactualiseerd om goede logging- en monitoring-procedures op ons netwerkverkeer te kunnen borgen. Gemeenten moeten aantoonbaar bewijs kunnen overhandigen aan allerlei instanties om: - te bewijzen dat de gemeente er alles aan heeft gedaan wat binnen haar macht ligt om de inwoner zo goed mogelijk te helpen. Met een in te richten SIEM kunnen we log-gegevens van verschillende domeinen combineren. De voorbereiding op de implementatie van een SIEM/SOC start in 2022 en naar verwachting wordt in 2023 een aanbesteding gedaan voor een SIEM/SOC. - aan te tonen dat het in- en uitgaand gegevensverkeer wordt gemonitord en er snel proactief op dreigingen kan worden gereageerd.	· Het managen van de informatiebeveiliging. · Het adequaat reageren op incidenten.
Pentesten Om onze technische infrastructuur te kunnen beoordelen op de mate van informatiebeveiliging voeren we in 2023 een pentest uit.	· Het managen van de informatiebeveiliging
Bedrijfscontinuïteit In 2023 stellen we een bedrijfscontinuïteitbeleid vast en daaraan gerelateerde crisisplannen. Dit is een eis uit de BIO en de ervaringen bij Lochem en Hof van Twente maken duidelijk dat dit essentieel is om de organisatie met haar processen snel weer operationeel te krijgen. Hierbij geven we voorrang aan de meest kritieke processen rond onze dienstverlening aan onze burgers en bedrijven.	· Het managen van de informatiebeveiliging. · Het adequaat reageren op incidenten.

Naast de hierboven genoemde TOP 10 aan maatregelen benoemen we hieronder nog andere genomen en te nemen maatregelen die bijdragen aan de informatiebeveiliging.

Maatregel	**Doelstelling**
Protocol incidentmanagement Een incident in onze informatiehuishouding is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentmanagement is het geheel van organisatorische maatregelen, om een incident adequaat te detecteren, melden en behandelden. Hiermee minimaliseer of voorkom je de kans op uitval van bedrijfsvoering of ontstane schade. 100% beveiligen van informatie is niet mogelijk. Het is niet de vraag of er iets gaat gebeuren maar wanneer. Met dit protocol beschrijven we de handelwijze voor beveiligingsincidenten op onze informatievoorziening en de afhandeling hiervan. Het melden van datalekken maakt hier ook deel van uit. In 2018 is het protocol incidentmanagement aangepast aan de normen voor het melden van datalekken op grond van de in werking getreden AVG. Het moet nu nog worden aangepast op het gebied van forensisch onderzoek en aansluiten bij het beleid op bedrijfscontinuïteitmanagement.	Het adequaat reageren op incidenten.
Verwerkersovereenkomsten met externe partijen of ketenpartners Steeds meer privacygevoelige gegevens worden verwerkt en opgeslagen bij ketenpartners en leveranciers. De gegevens staan dan niet meer bij ons in huis opgeslagen of worden gedeeld. Informatiebeveiliging wordt daarom meegewogen bij het besluit om samenwerking met een externe partij aan te gaan. Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur wordt bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn. Wanneer externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt zoals bepaald in de AVG altijd een verwerkersovereenkomst of dataleveringsovereenkomst afgesloten. Ook bij uitbesteding van werkzaamheden blijft de gemeente verantwoordelijk voor de gegevensverwerking. Bijzondere aandacht gaat uit naar het sociaal domein waar sprake is van een groot aantal ketenpartners, met name zorgverleners. Wij hebben met de meeste partijen inmiddels een verwerkersovereenkomst afgesloten. In 2023 blijven we hier aandacht aan geven, ook vanwege de migratie van applicaties naar de cloud. Onderdeel daarvan zijn ook afspraken hoe om te gaan met datalekken.	Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.

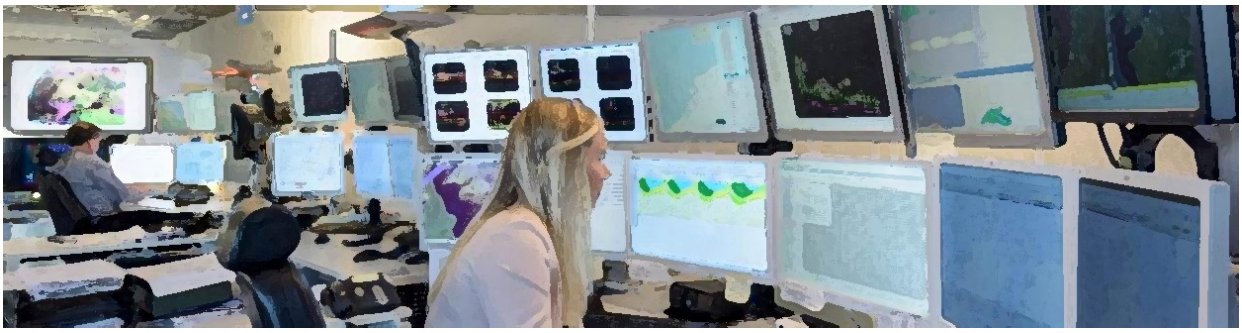
Cybersecurity op SCADA-automatisering en Europese richtlijn NIS2
Bovenstaande maatregelen gaan voornamelijk over onze administratieve en dienstverlenende processen. Automatisering en internetkoppelingen zien we echter ook steeds meer in vitale fysieke systemen terugkomen zoals zogenaamde internet-of-things. 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 29/09/2022) "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 beveiligingscalamiteiten.



8. Incidenten en ontdekte kwetsbaarheden

Rapportage van incidenten zoals datalekken en de afhandeling daarvan.

In 2022 zijn 29 (dit was in 2021 nog 97) spammails, 23 incidenten (20 in 2021) en 317 geconstateerde kwetsbaarheden (263 in 2021) 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 bijvoorbeeld ook de phishing campagne gericht op lokale politici en een kwetsbaarheid in een onderdeel van Centric voor gegevensdistributie. Het lage aantal van gemelde spammails dit jaar kan veroorzaakt zijn doordat medewerkers dit soort email door onze bewustwordingsacties zelf als phishing herkennen en verwijderen en niet meer melden.

In 2022 zijn 10 datalekken gemeld bij de privacy officers. In 2020 waren dit er nog 17 en 11 in 2021. 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. In één datalek bleek het nodig om de Autoriteit Persoonsgegevens en betrokkenen te informeren. Geconstateerd wordt dat het datalekkenregister adequaat wordt bijgehouden

Al 6 jaar daalt het aantal door medewerkers gemelde incidenten. 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 opgetreden incidenten kunnen op diverse manieren worden ingedeeld. De belangrijkste indeling is die in het kader van de AVG en de Wet meldplicht datalekken. Een incident in de informatiehuishouding is niet per definitie melding plichtig is in het kader van de AVG. Bij een incident wordt onderzocht of er persoonsgegevens in verkeerde handen kunnen zijn gekomen. Als dat het geval is dan wordt het incident gemeld met de maatregel die we hebben genomen om het datalek te dichten.

Van de Informatie Beveiligingsdienst (IBD) worden we met grote regelmaat geïnformeerd over ontdekte kwetsbaarheden in gebruikte systemen en software. Deze zijn met de geboden software-updates meestal snel opgelost.
In 2022 ontvingen we maar liefst 317 meldingen van de IBD over ontdekte kwetsbaarheden, in 2020 waren dat er nog 171. De daarmee gepaard gaande updates of maatregelen zijn allemaal met de grootste urgentie uitgevoerd.
Gezien het grote aantal van deze IBD-meldingen hebben we deze niet in het overzicht op pagina 32 opgenomen. Indien u als college van B&W of gemeenteraad behoefte aan heeft kunnen we u deze lijst alsnog toesturen.

In 2022 hebben we nog wel een aantal dagen problemen gehad met onze Citrix-omgeving waardoor medewerkers niet altijd op ons netwerk konden inloggen. De oorzaak van dit probleem is met behulp van externe expertise ontdekt in een bepaald onderdeel van onze systeemsoftware. Omdat er al veel software als cloud-versie buiten ons Citrix-netwerk om is op te starten kon hiermee wel gewerkt worden.
De verplaatsing van applicaties naar de cloud gaat de komende jaren toenemen waardoor de kwetsbaarheid van ons eigen ict-netwerk ook afneemt.

Melding Datalekken in 2022

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.

In 2022 ontving de Autoriteit Persoonsgegevens (AP) 24.866 datalekmeldingen.
Van de bij ons gemelde incidenten zijn er uiteindelijk zes incidenten als datalek gemeld bij de Autoriteit Persoonsgegevens (AP). Binnen 72 uur worden 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.
Andere 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.

Datum	**Omschrijving**	**Melding aan AP**
13-1-2022	Er is een mail 'Voorschot levensonderhoud' naar de verkeerde afzender gestuurd. De ontvanger van de mail is een betrouwbare ontvanger en heeft op het verzoek van de gemeente de mail ongelezen verwijderd.	Nee
1-3-2022	Persoonslijst naar het verkeerde adres gestuurd wegens verkeerd voorblad. Op dit voorblad staan de NAW gegevens van mensen die ook een persoonslijst ontvangen voor hun pasgeborene. Er is een brief opgesteld waarin is opgenomen wat er is gebeurd, wat de mogelijke gevolgen zijn, wat de gemeente hiertegen doet om dit voorval in de toekomst te voorkomen en dat er een melding is gedaan bij de AP. Ook is er een contactpersoon in de brief opgenomen voor mogelijke vragen van de betrokkenen.	Ja
11-5-2022	Een van de medewerkers heeft per ongeluk een e-mail verzonden uit de algemene mailbox naar het e-mailadres van diens moeder in plaats van de eigen werkmailadres.	Nee
14-9-2022	E-mail per ongeluk verzonden aan een externe ketenpartner met als bijlage kopie van de beschikking (voorschot levensonderhoud) + betaalopdracht en kopie bankrekening). Er is direct telefonisch contact opgenomen met de ontvanger en deze is verzocht de e-mail ongelezen te verwijderen. Hiervan is een schriftelijke verklaring overlegd.	Nee
10-10-2022	Een email gestuurd naar een familie in het AZC met mogelijkheden om een studie voort te zetten in Nederland. Deze mail is naar een andere familie verstuurd die ook in het AZC verblijft. Er is direct na het versturen van de verkeerde mail nogmaals gemaild naar de ontvanger dat deze mail niet voor hem is bestemd. Er is ook contact gezocht met een medewerker van het COA, die de ontvanger helpt om de mail te verwijderen	Nee
26-10-2022	Zes bevestigingsbrieven verwerking persoonsgegevens bij verhuizing/wijziging gegevens BRP is in één envelop verzonden aan een van de zes ontvangers.	Nee
10-11-2022	Vanuit ICT beheer zijn we geïnformeerd dat wij 5 phishingmails hebben ontvangen met daarin eigen inhoud van eerder verzonden mailcorrespondentie met een burger. Deze phishingmails zijn afgevangen door onze mailfilters. Er is onderzocht hoe de inhoud van de correspondentie in de phishingmail terecht kon komen. De betrokken burger is door de geïnformeerd over de phishingmails.	melding gedaan, maar ingetrokken
17-11-2022	Namen van burgers met afspraak met de gemeente was inclusief het onderwerp organisatiebreed zichtbaar in reserveringssysteem voor vergaderruimten. Er is contact opgenomen met de beheerder van het systeem om de omschrijvingen in het systeem aan te passen, ook in het vervolg.	Nee
29-11-2022	Bij het aanvragen van het paspoort kreeg de aanvrager een afhaalformulier mee met daarop de gegevens van een ander persoon. Het lek werd ontdekt op het moment dat ontvanger het paspoort ophaalde.	Nee

	Ontvanger heeft aangegeven het zelf ook niet te hebben opgemerkt. Het betreffende formulier is ingenomen bij KCC.	
1-12-2022	Er is een mail over een Tozo uitkering naar de verkeerde afzender gestuurd. De e-mail is weliswaar door de ontvanger ingezien, maar daarna verwijderd. De ontvanger is bovendien een betrouwbare partij.	Nee



Omnicell lijdt aan een geval van ransomware

Bij een ransomware-aanval zijn de privégegevens van ruim 128.000 klanten van het Amerikaanse zorgbedrijf Omnicell blootgelegd. Verzwarende factor bij dit lek is dat er veel extra gevoelige privégegevens bij de gest data zat, zoals creditcardinfo, financiële status, sofinumme

Mailchimp wordt gek

Verschillende medewerkers van Mailchimp trapten in een geraffineerde phishing-poging waardoor hun inlogs voor de bedrijfssystemen werden buitgemaakt. De daders kregen daarmee toegang tot 102 gebruikersaccounts. Vervolgens gebruikten ze deze accounts om phishing e-mails te verzenden naar de mailinglijsten van die accounts.

Omdat de e-mails voor de ontv ers uit een vertrouwde bron de mails erg een klant niet te hep was. Er zijn (nog) n de gevolgen van

Gemeente is té open met verkeerde bijlage

Een Nederlandse gemeente had in december een gevoelig lek. Tijdens Corona konden ondernemers financiële steun aanvragen bij de overheid, de Tozo. Eind 2022 werden definitieve berekeningen gemaakt en moesten sommigen de steun geheel of gedeeltelijk terugbetalen. Drie ondernemers wilden een meer gedetailleerde berekening om te bepalen of alles voor hen correct is afgehandeld.

Als je e-mailbeveiliging niet op orde is, dan is de kans groter dat je eigen mensen de oorzaak zijn van een datalek dan een hacker.

Maar die verzonden bijlage was een Excel-bestand met 'verborgen' tabellen met alle sofinummers van alle 8.200 aanvragers.

Met leveranciers en ketenpartners zijn verwerkers- of datalevering-overeenkomsten afgesloten. De in deze overeenkomsten opgenomen informatiebeveiligingseisen zorgen ervoor dat de risico's aanzienlijk verkleind zijn.

Daarnaast wordt gewerkt aan het implementeren van technische componenten. 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.

9. 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, WOZ, 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 nu al een enorme invloed op 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 een aantal categorieën van dreigingen in volgorde van belangrijkheid. (Bron: IBD)

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.

Actueel dreigingsbeeld 2023-2024

De IBD ziet dat in het bijzonder drie soorten dreigingen opvallen sinds het uitbrengen van het vorige dreigingsbeeld over 2021- 2022.

Meer ransomware met destructievere gevolgen

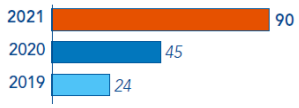
De dreiging van ransomware-aanvallen neemt toe. Aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger: het wordt merkbaar. Het fenomeen ransomware (gijzelsoftware) komt al jaren voor. Criminelen versleutelen gegevens en persen het slachtoffer af om deze gegevens na het betalen van losgeld weer toegankelijk te maken. De IBD ontving de afgelopen twee jaar 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.

- De gemeente Buren werd in 2022 getroffen door een ransomwareaanval. Bij de hack zijn gegevens van de gemeente gestolen. Vervolgens is een grote hoeveelheid data gepubliceerd op het darkweb, een afzonderlijk en anoniem deel van het internet.
- Ook in het buitenland zijn de afgelopen jaren veel lokale overheden getroffen door ransomware zoals Palermo (IT), Atlanta, Baltimore, Knoxville, Albany, New Orleans (VS), Luik (BE), Frankfurt (DE), Weiz (AT).
- De Ierse gezondheidszorg heeft een forse prijs betaald voor de ransomware-aanval in 2021. De kosten zijn opgelopen tot net iets minder dan 52 miljoen euro. Het leeuwendeel daarvan is voor herstel van de versleutelde en daarmee gegijzelde systemen. Een relatief kleine kostenpost (van nog altijd miljoenen) is voor preventieve maatregelen.

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.

Jaar en aantal kwetsbaarheden met hoge kans op misbruik, hoge mogelijke impact:



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 2022 – 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 500 cyberincidenten bij Nederlandse organisaties vermeld in de media. Of het nu gaat om DDoS-aanvallen, fraude via phishing, verloren USB-sticks of gijzelsoftware.

Van de 518 cyberincidenten (gemeten in 22 september 2022) was 127 keer de overheid het slachtoffer. Dat is meer dan 25% van het totaal aantal incidenten. De gemeenten werden met een aandeel van 45% binnen de overheid het vaakst getroffen door een cyberaanval. Datalekken met een interne oorzaak zijn met 28% de grootste veroorzaker. Op de voet gevolgd door datalekken met een externe oorzaak (22%). Gijzelsoftware, ook wel ransomware genoemd, was in 18 gevallen de boosdoener, wat ongeveer 14% vertegenwoordigt. DDoS-aanvallen, AVG compliance issues en aanvallen via email vertegenwoordigen een aandeel van 37%. De rest van de gevallen kwam voort uit publicaties door verschillende overheidsinstanties.
Bron: Datalekt.nl

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.