Gemeente Midden-Delfland

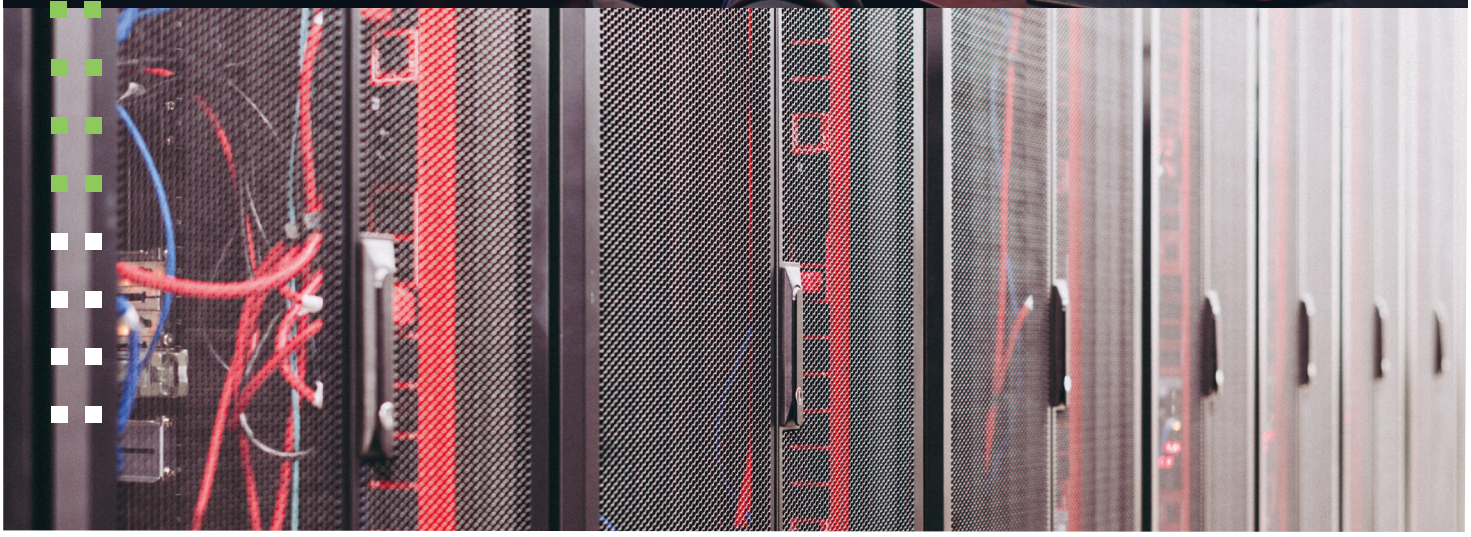
cittaslow

Jaarverslag Informatiebeveiliging Midden-Delfland

2021







Inhoud

Managementsamenvatting 3
Activiteiten in 2021 3
Beveiligingsincidenten 3
Zelfevaluaties 4
Vooruitblik 2022 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 8
3. Horizontale en verticale verantwoording op basis van ENSIA 9
Verantwoordingsrapportages zelfevaluatie 2021 11
Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet 17
4. Samenvattend beeld en resultaten informatiebeveiliging 2021 18
Resultaat meting BIO 19
5. Disclaimer 22
6. Belangrijkste beheersmaatregelen IB 23
Verbeterpunten op basis van meting BIO 24
7. Realisatie doelstellingen IB-beleid 27
8. Incidenten en ontdekte kwetsbaarheden 31
9. Meerjarenperspectief 34

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 2021 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]) 2021 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 2021 en de DigiD/Suwi-audit. De verbeterpunten met de hoogste risico's vormen het jaarplan 2022.

Het college van B&W wordt verzocht het jaarverslag informatiebeveiliging 2021 vast te stellen en de CISO het mandaat te geven het jaarplan met verbeteracties uit te (laten) voeren.

Activiteiten in 2021

In 2021 is op het gebied van informatiebeveiliging het volgende gerealiseerd:

- In 2021 is de vervanging van onze hardware zoals servers, opslag en backup-systemen afgerond. De nieuwe hardware is voorzien van actuele beveiligingsoplossingen waarmee we op dat vlak aan de BIO voldoen.
- Er is speciale software geïnstalleerd om patronen te detecteren van ongewenst netwerkverkeer (hackers, ransomware) en daarop dit verkeer te blokkeren.
- Er is structureel aandacht gegeven aan bewustwording over informatiebeveiliging onder het personeel.
- Er zijn ad-hoc maatregelen genomen

Beveiligingsincidenten

In 2021 zijn 97 spammails, 20 incidenten en 263 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 bijvoorbeeld de LOG4J-kwetsbaarheden.

In 2021 zijn er 11 van de beveiligingsincidenten aangemerkt als datalek. Daarvan hebben we in twee gevallen zelf melding moeten doen bij de Autoriteit Persoonsgegevens (AP) een maal is daar door een partnerpartij melding gemaakt. De betrokkenen slachtoffers zijn geïnformeerd. In 2020 was er nog sprake van 16 beveiligingsincidenten waarbij er toen negen zijn aangemeld als datalek.

[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):

- Voor BRP en PUN scoort de gemeente Midden-Delfland binnen de gestelde normen.
- De gemeente Midden-Delfland is DigiD aansluithouder. 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 voldoende derhalve worden nog verbeteracties voorgesteld.
- BGT scoort nog niet op alle onderdelen binnen de norm daarom worden verbeteracties voorgesteld.
- BRO scoort nog niet op alle onderdelen binnen de norm daarom worden verbeteracties voorgesteld.
- Over de eerste zelfevaluatie van de WOZ is geconstateerd dat deze nog niet op alle onderdelen binnen de norm scoort, daarom worden verbeteracties voorgesteld.

Vooruitblik 2022 op het gebied van de informatiebeveiliging

Activiteiten voor 2022:

- 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.
- We stellen een bedrijfscontinuïteitsplan en crisisplan op om voorbereid te zijn op crisissituaties veroorzaakt door bijvoorbeeld gijzelsoftware.
- Gegevens zijn één van de belangrijkste bedrijfsmiddelen van de gemeente. Aandacht voor de kwaliteit, actualiteit en compleetheid van de basisregistraties is daarom van groot belang.
- Het Information Security Management System (ISMS) wordt met taken verder uitgerold naar de verantwoordelijke medewerkers om de plan-do-check-act cyclus voor informatiebeveiliging structureel vorm te geven. Dit moet tevens voor lastenverlichting zorgen bij de zelfverantwoordingstaken met betrekking tot ENSIA.
- Ons Responsible Disclosurebeleid wordt vastgesteld en gepubliceerd op onze website.
- Het Thuiswerkbeleid wordt aangepast naar de actuele beveiligingsnormen uit de BIO.

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 2021 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 vijfde 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, 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).

De BIO is een doorontwikkeling, ofwel een 'update', van de BIG. Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk (middels ENSIA) op deze BIO. De werkzaamheden die voor de BIG zijn verricht zijn al grotendeels in lijn met de BIO.

Meer gericht op risicomanagement

De BIO legt meer nadruk op risicomanagement dan de BIG, die zich meer richtte op specifieke maatregelen. De rol van de bestuurder en lijnmanager is ten aanzien van risicomanagement explicieter dan de BIG aangaf. 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.

De BIO verschilt op een aantal punten van de BIG. De grootste verschillen zijn:

1. Minder maatregelen (bijna 60% minder)
2. Maatregelen zijn altijd verplicht
3. Meer risicomanagement
4. Gaat uit van drie basis beveiliging niveaus (BBN)
5. Selectie van ontbrekende maatregelen vooraf
6. Toewijzing van maatregelen op eindverantwoordelijke
7. Een baselinetoets die rekening houdt met die drie niveaus uit de BBN

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 welke maatregelen nog moeten worden ingericht.

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 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.

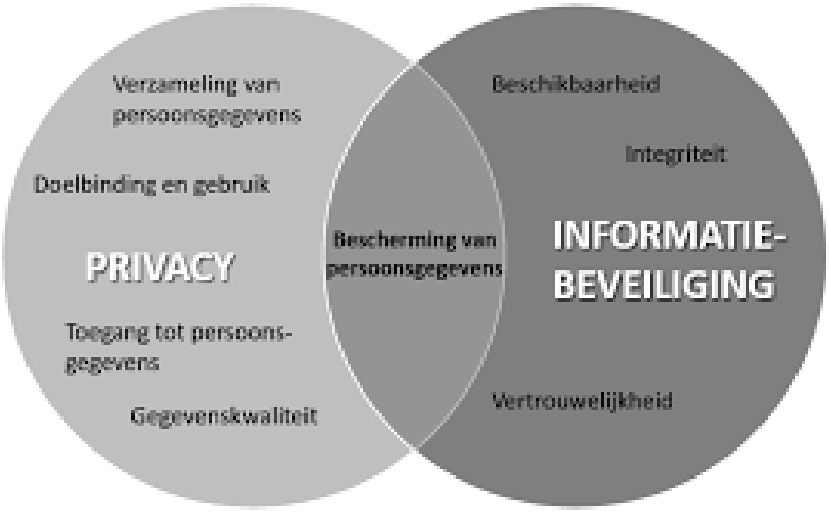
1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
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)

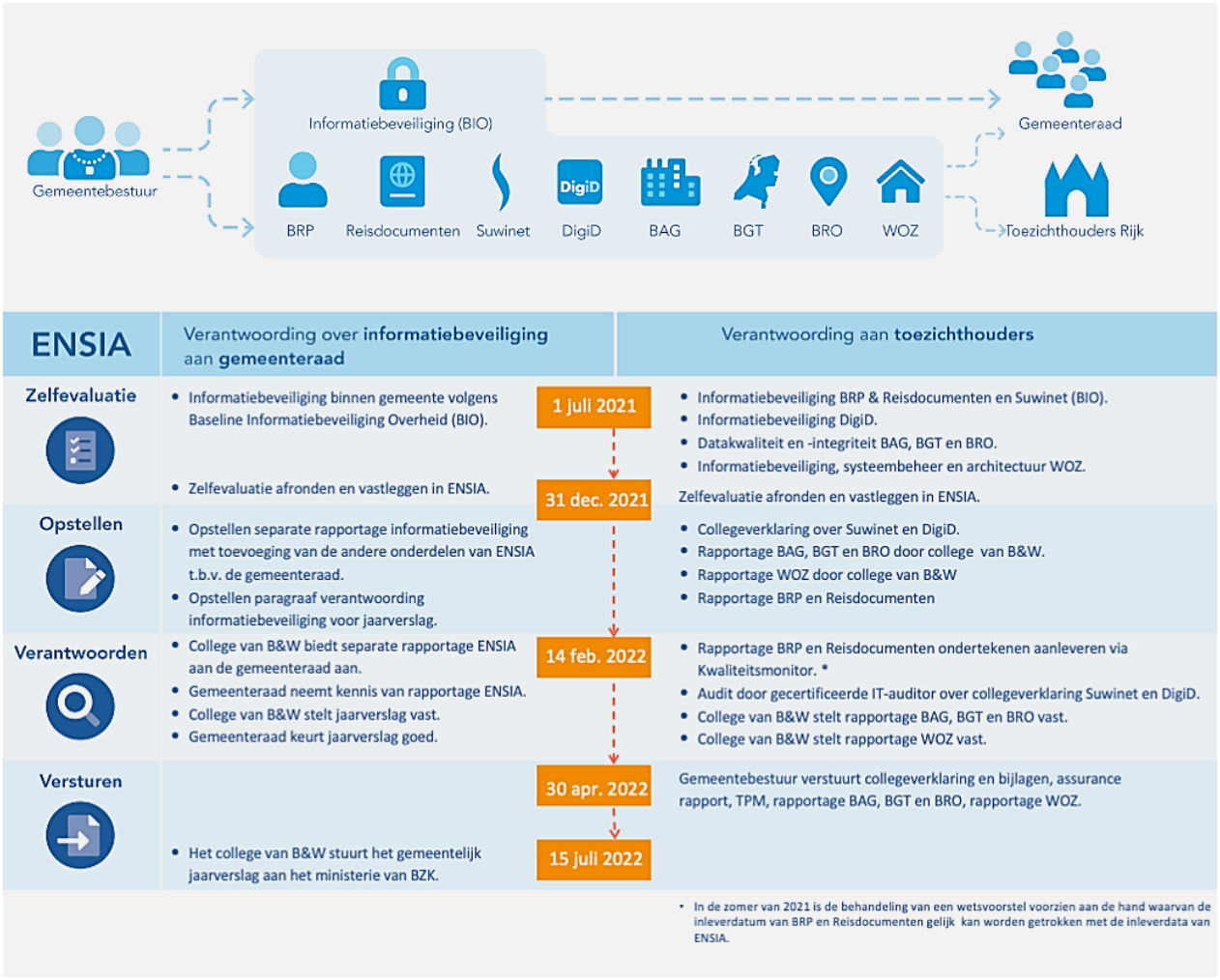
Aanleiding
Sinds 1 juli 2017 is ENSIA (Eénduidige Normatiek Single Information Audit) een verplichte verantwoordingmethodiek voor gemeenten. ENSIA is gezamenlijke methodiek van het ministerie van Binnenlandse Zaken (BZK), gemeenten, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), het ministerie 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 2021
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 2020 grafisch weergegeven. Meer informatie over ENSIA en de werkwijze is terug te vinden op www.ensia.nl.
Zo werkt ENSIA:



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 2021 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 2021 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 (voor 2021 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 2022.

Hieronder vindt u de conclusies uit de betreffende verantwoordingsrapportages.

Verantwoordingsrapportages zelfevaluatie 2021

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 BIO, 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 2021 en de 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

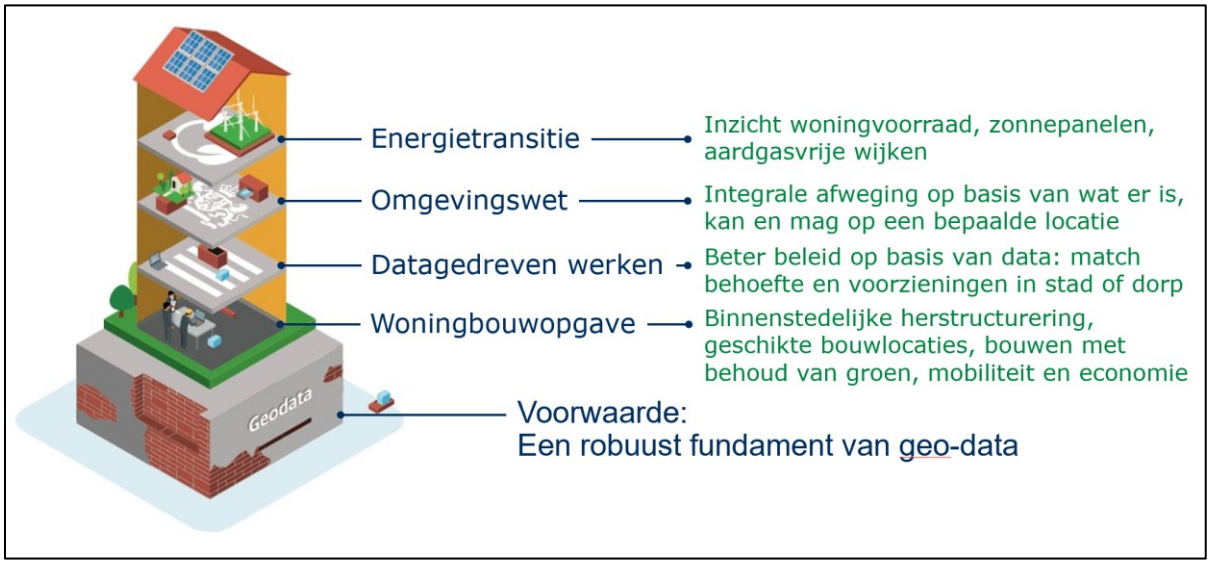
De Basisregistratie Personen (BRP) is onderdeel van het stelsel van basisregistraties van de Nederlandse overheid. De Nederlandse overheid registreert persoonsgegevens in de BRP. Alle overheidsinstellingen en bestuursorganen (zoals de Belastingdienst) zijn verplicht voor hun taken gebruik te maken van 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 2021 (ENSIA)			
Thema BRP	**Totaal behaalde punten Midden-Delfland**	**Totaal mogelijk**	**Percentage**
1. Organisatie van de beveiliging	370	400	92,5 %
2. Toegangsbeveiliging	400	400	100 %
3. Naleving	400	400	100 %
Totaal	1.170	1.200	97 %

Resultaat uit zelfevaluatie informatieveiligheid Reisdocumenten 2021 (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).

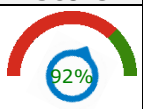
In ons land worden geo-basisgegevens jaarlijks meer dan 5 miljard keer gebruikt via de landelijke voorzieningen. Indirect gebruik, via bijvoorbeeld de doorlevering van geo-data door fabrikanten van navigatiesoftware, komt daar nog bovenop. Het gebruik blijft jaarlijks stijgen en het maatschappelijk belang 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.



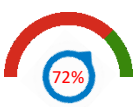
Afbeelding: nationale geo-informatie infrastructuur (NGII) als basis voor maatschappelijke vraagstukken (bron: BZK)

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 scores, die op de volgende pagina te zien zijn, vormen het resultaat van door ons uitgevoerde zelfevaluaties. Deze evaluaties betreffen de gegevenskwaliteit en de borging van beheerprocessen. Informatiebeveiliging maakt hiervan vooralsnog geen onderdeel uit.

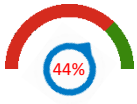
In 2019 en 2020 heeft de gemeente Midden-Delfland geen BGT beheerder gehad. De BGT taken zijn toen uitgevoerd door een extern bedrijf (minimum). Per maart 2021 is de vacature weer ingevuld. Er is een BGT/BAG beheerder aangesteld. De BGT en BAG zijn niet in dezelfde afdeling ondergebracht, maar er wordt wel intensief samengewerkt.
In 2021 is de aandacht vooral naar de BAG en BGT gegaan en in mindere maten naar de BRO.
Scores geo-basisregistraties 2021 (tijdvak 1 januari 2021 tot en met 31 december 2021):

Basisregistratie	Score	Consequenties score
BAG		Zorgen dat de kwaliteit van de gegevens in de BAG hoog blijft.
		Zorgen dat de processen van de BAG goed blijven werken.

< 75% onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BGT		In 2019 en 2020 was er geen BGT beheerder. Hierdoor zijn er achterstanden ontstaan. In 2021 is er al een inhaalslag geweest → we zijn op de goede weg.

< 75% Onvoldoende vanaf 75% voldoende

Basisregistratie	Score	Consequenties score
BRO		Nog niet voldoende belegd in de organisatie → we zijn op de goede weg.

< 60% Onvoldoende vanaf 60% voldoende

Trend score geo-basisregistraties:

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

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

BAG

Verbetermaatregelen voor 2022:
- Zorgen dat de processen juist blijven werken, zodat alle mutaties tijdig verwerkt kunnen worden.
- Een mutatiesignalering uitvoeren met de luchtfoto die in het voorjaar 2022 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 2022:
- de achterstanden moeten worden weggewerkt.
- De processen moeten beschreven worden en ingebed worden in de organisatie.
- Mutatiesignalering BGT 2021 moet bekeken en verwerkt worden in de BGT
- Mutatiesignalering BGT 2022
- Uitvoering geven aan de kwaliteitseisen BGT zoals genoemd in het jaarplan 2022
- 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. Mogelijk kan hier in 2022 een start mee gemaakt worden.

BRO

Verbetermaatregelen voor 2022:
- Beschrijven van de processen en zorgen dat ze ingebed worden in de organisatie
- Controleren of er projecten geweest zijn, waar mogelijk BRO gegevens aangeleverd hadden moeten worden aan het Bronhoudersportaal. Zo ja alsnog aanleveren aan het Bronhoudersportaal.
- Aanwijsbesluit BRO Coördinator laten vaststellen.

Zelfverantwoording Waardering Onroerende Zaken

Er bestaat een maatschappelijke behoefte aan WOZ-waarden en WOZ-gegevens van hoge kwaliteit met de mogelijkheid tot inbreng van belanghebbenden (regie op gegevens). Gezien de ontwikkelingen rond basisregistraties en het tot stand brengen van één objectenregistratie zullen gemeenten en uitvoeringsorganisaties zich moeten realiseren dat hiervoor aanzienlijke investeringen nodig zijn in de komende jaren. Dat betreft voor een belangrijk deel investeringen in de vernieuwing van automatiseringssystemen, gericht op het benutten van geografische informatiesystemen (GIS), het benutten van AI-technieken in taxatiemodellen en de overgang naar een andere informatie-architectuur. Deze andere informatie-architectuur is nodig om mee te gaan met ontwikkelingen in techniek, op het terrein van informatieveiligheid, rond basisregistraties en het tot stand brengen van één objectenregistratie. Maar zeker ook de communicatie met inwoners en het realiseren van "regie op gegevens" vergt op korte termijn investeringen in de ICT-infrastructuur rond het WOZ-domein. Concrete stappen zijn bijvoorbeeld vervangen van bestandsuitwisselingen door beveiligd berichtenverkeer. Tot slot is de verwachting dat voor de geo-basisregistraties en de WOZ in de komende jaren verdere samenwerking aan de orde is, ook in onze gemeente. Daarbij is aandacht voor de datakwaliteit van groot belang.

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

Status	Conclusie	Verbetermogelijkheden (indien nodig)
✗	De BIO is niet volledig geïmplementeerd in de organisatie, 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. Ook voor de WOZ-systemen moet daarom door de organisatie bekeken zijn, welke BIO-controls van toepassing 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.
✗	De overgang naar Common Ground conforme architectuur voor de WOZ is nog niet gestart.	Bekijk hier (https://commonground.nl/) wat deze ingrijpende hervorming van de informatievoorziening voor uw organisatie gaat betekenen en wat u al kunt doen.
✗	Er wordt nog gebruik gemaakt van een koppelvlak 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. Kijk hier (https://www.waarderingskamer.nl/basisregistratie-woz-lv-woz/stuf-woz-0312/) voor meer informatie.
✓	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.	Het is raadzaam een volledig overzicht van de verschillende koppelvlakken / interfaces te hebben zodat u deze kunt beheren.
✓	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. Indien dit niet gebeurt bestaat het risico dat afnemers niet de juiste gegevens krijgen, inwoners niet tijdig hun WOZ-waarde op www.wozwaardeloket.nl zien en de belastingcapaciteit per gemeente, die het CBS op basis van de LV WOZ vaststelt, niet klopt.

✔	Er zijn audits uitgevoerd om te beoordelen of alle voor de WOZ-uitvoering gebruikte systemen de gegevens uit interne systemen juist verwerken.	Contact met een inwoner in het kader van de WOZ-waarde kan ook gaan over gegevens die met betrekking tot deze belanghebbende (deze onroerende zaak) vastliggen in andere (basis)registraties. Om te waarborgen dat de informatie uit andere basisregistraties op een doelmatige en consistente wijze wordt gebruikt en verwerkt, is het belangrijk dat ook de aansluiting van de WOZ-uitvoering op deze (basis)registraties regelmatig wordt beoordeeld.
✔	Op terrein van de beheersing van informatiebeveiliging conform BIO is voor de WOZ-uitvoering de gewenste managementinformatie beschikbaar.	Op pagina 88 en 91 van de Waarderingsinstructie (https://www.waarderingskamer.nl/hulpmiddelen-gemeenten/waarderingsinstructie/) is onder het kopje "stuurinformatie" beschreven welke managementinformatie er belangrijk is bij het inzicht krijgen in de naleving van beveiligingsbeleid en -normen (BIO).

Conclusie	Tips/Verbetermaatregelen
De BIO is niet volledig geïmplementeerd in de organisatie, er worden op dit moment geen controles uitgevoerd op naleving van de BIO voor de WOZ.	Er wordt wel periodiek gecontroleerd of de gegevens in de systemen juist en volledig zijn (ontvangen, bevatten, verwerken en leveren van gegevens). Ook de uitwisseling tussen de systemen (zoals met de andere basisregistraties) worden gecontroleerd op juistheid en volledigheid. Het daadwerkelijk vastleggen van deze controles en daarbij ook het in kaart brengen van de controles en de normen, zodat goed vastgelegd kan worden welke controle voor welke norm wordt gedaan, is een te nemen verbetermaatregel. Uit de huidige controles komen vanzelfsprekend ook verbeterpunten, maar het documenteren van de controles blijft achter.
De overgang naar Common Ground conforme architectuur voor de WOZ is nog niet gestart.	De softwareleverancier werkt (nog) niet volledig volgens deze principes. Een maatregel is bij de softwareleveranciers meer nadruk leggen en aandringen op het implementeren van deze principes waar mogelijk.
Er wordt nog gebruik gemaakt van een koppelvlak op basis ASCII-bestanden (Stuf-TAX) voor de communicatie tussen de diverse applicaties voor de WOZ-uitvoering.	Het huidige pakket is verouderd en wordt dit kalenderjaar vervangen. Met dit nieuwe pakket is het mogelijk om een waarderingskoppeling tussen het taxatiepakket en de belastingapplicatie tot stand te brengen. Daarmee is het uitwisselen van stuf-tax bestanden verleden tijd. De nog aan te brengen nuance is nog wel dat het stuf-tax bestand in de huidige situatie via de webinterface in de beveiligde omgeving van het taxatiebureau wordt geplaatst. De uitwisseling vindt dus wel beveiligd plaats.

Collegeverklaring ENSIA inzake informatiebeveiliging DigiD en Suwinet

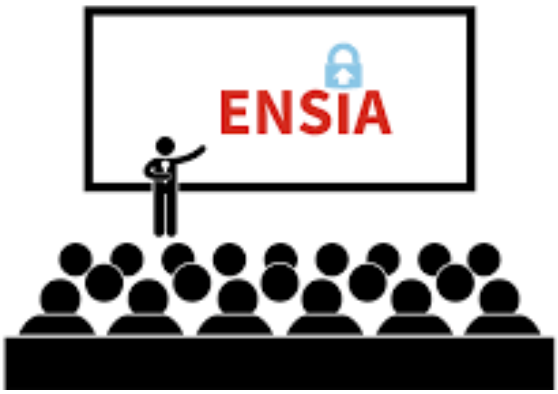
Het college van Burgemeester en wethouders geeft in een verklaring aan in hoeverre de beheersmaatregelen voldoen aan de voor de ENSIA verantwoording geselecteerde normen voor DigiD en Suwinet.

Bij de ENSIA vragenlijsten is geconstateerd dat bij gemeente Midden-Delfland op 31 december 2021 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 2021

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.

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/

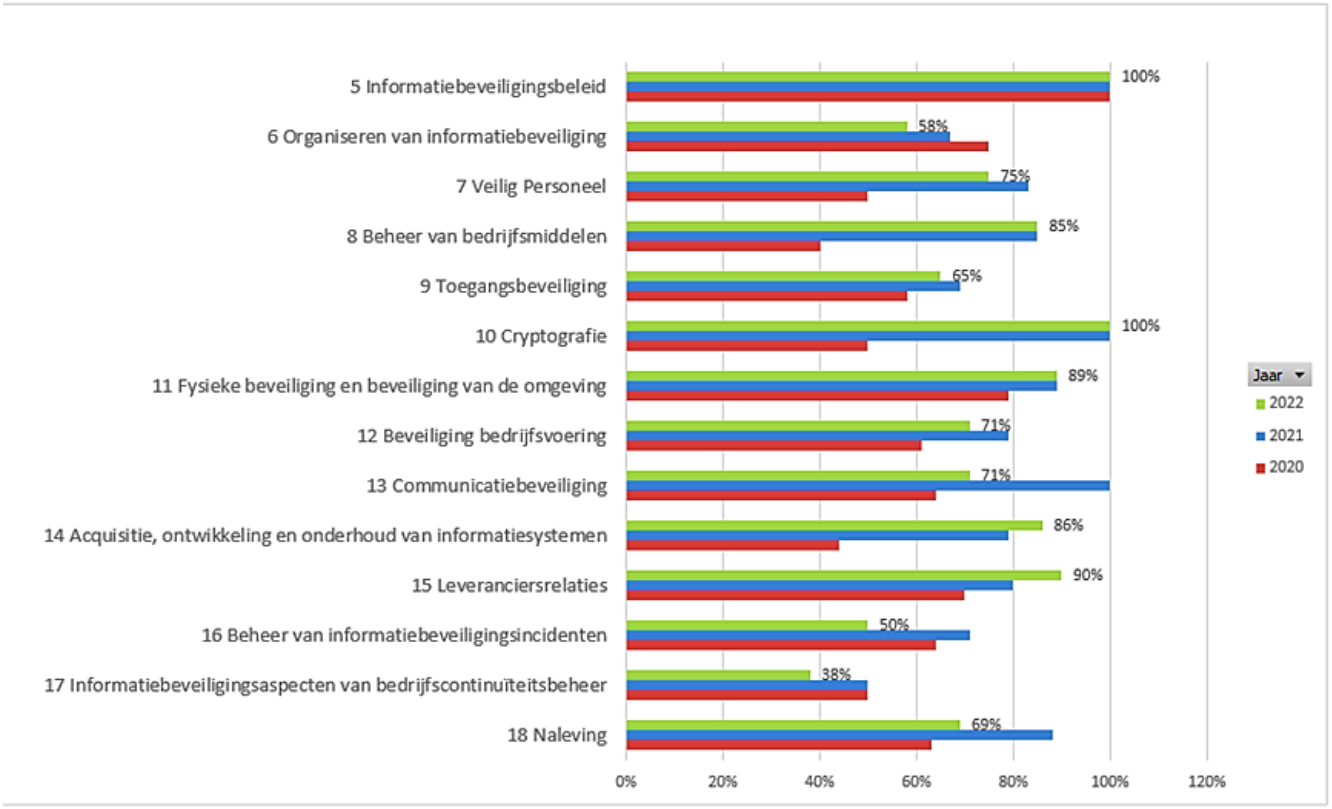
Om het informatiebeveiligingsbeleid goed te implementeren, werken we op basis van een "GAP-analyse/risicoanalyse". Deze analyses zijn uitgevoerd in directe samenspraak met de betrokken collega's van de vakafdelingen. Hiermee is het "GAP" of "gat" tussen de huidige en de gewenste situatie (volgens de normen van de BIG) 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 2021 verder is gewerkt. Voortdurend wordt na de genomen maatregelen de top 10 aangevuld met nieuwe, 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 2019, 2020 en 2021.



Resultaat meting BIO

Op basis van de resultaten ENSIA 2021 en meting 2 is een meting 3 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 2021 is vanwege de coronamaatregelen en uitval vanwege quarantaine, een moeilijk jaar geweest voor alle medewerkers van de gemeente. De (nieuwe) digitale communicatiemiddelen maakten het werk (ook tijdens de 'lock-downs') werkbaar maar minder efficiënt. Dit heeft zijn neerslag op de uitvoering van het dagelijks werk maar ook in de verschillende projecten die daardoor uitliepen of opgeschort werden. Dat gold ook voor de projecten of verbeteracties op het gebied van informatiebeveiliging.

Hoofdstuk 6 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 moet worden geactualiseerd naar de huidige eisen.

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 bredere uitrol van het ISMS in 2022 meer aandacht krijgen.

Hoofdstukken 12 en 13 scoren relatief laag en dat heeft vooral te maken dat onvoldoende duidelijk is hoe het bij Westland belegde ICT-beheer organisatorisch is vorm gegeven naast de 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 het 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. Dit kan worden meegenomen bij de actualisering van de Dienstverleningsovereenkomst met Westland voor het ICT-beheer.

Hoofdstuk 16 scoort relatief laag en dat komt vooral omdat hoewel we een eigen interne procedure hebben voor incidentmelding en vastlegging, dit nog aanscherping vraagt. Als het gaat om incidenten die de techniek raken, ligt een groot deel bij ICT-beheer Westland. Het is van belang dat er helderheid is hoe incidentenbeheer is geregeld in combinatie met de uitvoering door ICT-Westland en dat dit schriftelijk is vastgelegd in een protocol.

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. Dit was al een verbeteractie voor 2021 maar hebben we vanwege coronamaatregelen, gebrek aan capaciteit als gevolg van vacatures en andere projecten nog niet kunnen uitvoeren.

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.

In de hoofdstuk 6 gaan we nader in op de voorgenomen verbeterpunten en activiteiten die onder de categorie actualisatie/onderhoud vallen voor 2022 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[4] (Hof van Twente) en de recente Log4J kwetsbaarheid 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.

[4] 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. Deze verordening vervangt de Privacyrichtlijn 95/46, waarop de huidige Wet Bescherming Persoonsgegevens (WBP) is gebaseerd. Het doel van de AVG is de bescherming van persoonsgegevens te vergroten. Alle organisaties die met persoonsgegevens werken, zoals de gemeente Midden-Delfland, zijn verplicht de privacybescherming op orde te hebben.
Aan het niet of niet goed naleven van de AVG zijn grote risico's verbonden. Door de Autoriteit Persoonsgegevens kunnen forse boetes worden opgelegd. Ook kan de betrokken organisatie reputatieschade naar de burgers toe oplopen. Om die reden heeft de Rekenkamer Midden-Delfland de recente invoering van de AVG aangegrepen om te kijken naar de manier waarop de gemeente de benodigde maatregelen heeft genomen.

In oktober en november 2018 heeft de Rekenkamer Commissie (RKC) van de gemeente Midden-Delfland onderzoek gedaan naar het volwassenheidsniveau van de gemeentelijke organisatie in de bescherming van de privacy bij de verwerking van persoonsgegevens van inwoners uit Midden-Delfland. Het doel van het onderzoek is de gemeenteraad van Midden-Delfland inzicht te geven in het gemeentelijk privacybeleid en aanbevelingen te doen over mogelijke verbeteringen van dit beleid.
Op 14 mei 2019 presenteerde de rekenkamercommissie haar bevindingen over het onderzoek naar Privacy In het rapport van de RKC zijn verschillende aanbevelingen gedaan. Deze aanbevelingen zijn waardevol om een scherpe blik te houden op de implementatie van de AVG. De resultaten en ambtelijke reactie op het rapport geven een afdoende beeld als horizontale verantwoording. Daarom laten we een verdere uiteenzetting over de AVG in dit jaarverslag IB achterwege. De Functionaris Gegevensbescherming draagt vanuit de AVG zelf zorg voor een jaarverslag.

Ook in 2021 hebben we op basis van de AVG met leveranciers en dienstverleners verwerkersovereenkomsten en dataleveringsovereenkomsten afgesloten. Hierin zijn de verantwoordelijkheden geregeld voor de beveiliging van het gebruik van onze privacygevoelige gegevens. We hebben naast technische maatregelen, ook gewerkt aan bewustzijn bij de medewerkers.



Informatiebeveiliging en privacybescherming hebben een grote 'houding en gedrag'- kant. Vanwege de inwerkingtreding van de AVG zijn door de projectgroep Privacy gemeente-brede bijeenkomsten georganiseerd waarbij vooral is ingegaan op hoe er vertrouwelijk met persoonsgegevens van personen moet worden gegaan. Onze interne beveiligingsorganisatie bestaat uit medewerkers van de verschillende teams die binnen hun team zorgen voor bewustzijn en aanspreekpunt zijn voor informatiebeveiliging voor hun team. 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 2021.

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 155 punten 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 Beveiligings 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 voorgedefineerde 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.

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**
6.2.2	Telewerkbeleid	Aandacht voor veilig gebruik van telewerken, actualisering van het verouderde thuiswerkbeleid. Dit is voor 2022 een actie voor Personeelszaken. (Hierin worden ook de kennis en ervaring van het hybride werken in Coronatijd meegenomen).
9	Toegangs-beveiliging	Voor functioneel applicatiebeheer een eenduidige functie- en taakbeschrijving opstellen gericht op het verder professionaliseren van hun beheeractiviteiten. Dat is een belangrijke stap indien we de kritische applicaties gaan volgen in het ISMS. Denk aan het opstellen van een autorisatiematrix, periodiek controle toegangsrechten, activeren, bewaren en aantoonbaar controleren van loggings, gebruik van query tooling en afspraken over maken van downloads voor analysedoeleinden (denk aan accountant en andere auditors), omgaan met testen en testgegevens.
12 en 13	Beveiliging bedrijfsvoering en Communicatie-beveiliging	Afstemming met ICT-beheer Westland over de BIO-normen en maatregelen die bij Westland liggen en dat in eerste instantie goed vastleggen. Kijken wat de mogelijkheden zijn voor TPM of andere wijze van 'assurance'. Hiervoor een afzonderlijk document opstellen die we periodiek onderhouden (gedocumenteerde informatie ICT-beheer Westland). Dit indien mogelijk betrekken bij de actualisatie van de Dienstverleningsovereenkomst
16.1.7	Beheer van informatiebeveiligingsincidenten en –verbeteringen: Verzamelen van bewijsmateriaal	We hebben interne procedures te voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen. Er is een redelijk compleet protocol maar hierin ontbreekt nog het laten uitvoeren van forensisch onderzoek. In het geval van incidenten die de techniek raken, ligt een groot deel bij ICT-beheer Westland waarvan eventueel beschreven procedures opgevraagd of gemaakt moeten worden. Het is van belang dat er helderheid is hoe incidentenbeheer is geregeld in combinatie met de uitvoering door ICT-Westland en dat dit schriftelijk is vastgelegd in een protocol.

		Dit hangt ook samen met 17.1.1 over het hebben van een continuïteitsplan bij een cybercrisis.
17	Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer	Dit hoofdstuk impliceert dat de organisatie aandacht moet besteden aan bedrijfscontinuïteitsbeheer (BCM). Het is overigens niet de verantwoordelijkheid van de CISO om dit te realiseren. Die verantwoordelijk ligt bij de directie. Wel is het een taak van de CISO om dit onderwerp onder de aandacht te brengen van de directie (responsible) en het bestuur (accountable). Als gemeente scoren we fors laag als het gaat om BCM en dat is zorgelijk. We hebben immers een maatschappelijke (voorbeeld) functie en we verkeren op dit moment in een crisis in de vorm van COVID-19. Dat zal zeker niet de laatste zijn, alleen - en dat is kenmerkend voor een crisis - weten we niet wanneer de volgende zich aandient. Zo kan ransomware of een brand in het gemeentehuis aanleiding zijn voor een lokale crisis bij de gemeente en dan moet opeens ingegrepen worden onder hoge psychische druk met zeer beperkte informatie en met grote belangstelling vanuit de media waarbij de kans op datalekken en beveiligingsincidenten enorm toeneemt als geen passende beveiligingsmaatregelen zijn getroffen. BCM gaat niet alleen over ICT, maar raakt de hele organisatie. Het gaat dus ook om de veiligheid van personeel en bezoekers, het beschikbaar houden van huisvesting en archief en vooral het beschikbaar houden van kritische bedrijfsprocessen onder alle omstandigheden. Voor 2022 is de planning om het onderwerp BCM onder de aandacht te brengen van de directie en bestuur door een inventarisatie op hoofdlijnen uit te voeren en dit in de vorm van een rapport aan te bieden met adviezen om BCM structureel te borgen in de organisatie. We gaan in 2022 een QuickScan BCM uitvoeren, uitmondend in een rapport ten behoeve van de directie college van B&W. Tevens plannen we voor 2022 een oefening op een cybercrisis. Dit is in 2021 vanwege de Coronamaatregelen niet gelukt.
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. De kracht van dit systeem wordt groter naarmate meer gebruikers hun bijdrage leveren aan dit systeem en waarbij de CISO het beheersproces dat hieraan verbonden is, beter kan gaan monitoren. Het ISMS maakt dan echt onderdeel uit van de hele organisatie en daarmee worden we als geheel minder kwetsbaar op de continuïteit van informatiebeveiliging. Voor een groot deel rust dit nu op de schouders van de CISO en informatiebeveiligingsadviseurs. Uiteraard is het verhogen van het gebruik een groeiproces. We gaan medewerkers die direct of indirect betrokken zijn bij het vormgeven van een ISMS en daarvoor input moeten leveren in 2022 benaderen om hun verantwoordingsbijdrage namens de directie zelf in te voeren in het ISMS. Dat vergt op zich nauwelijks inspanning voor de gebruiker vanwege de gebruikersvriendelijkheid van het ISMS. We gaan in 2022 het gebruik van het ISMS in de organisatie gefaseerd verbreden naar de overige informatiebeveiligings-beheerders.

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 2021 wordt de IB-organisatie 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 2021 nog verder ingericht en uitgerold over de IB-organisatie.	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 ransomeware. In 2021 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 2021 veel ad-hoc aan bewustwording gedaan op het gebied van privacybescherming. In 2021 is gestart om met behulp van e-learning structureel leerstof aan medewerkers aan te bieden op een leuke interactieve manier. Hierbij is 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 2022 gecontinueerd en aangepast baan actuele onderwerpen.	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 per 25 mei 2019 van kracht is. Dit is al vanaf de ENSIA verantwoording over 2017 door onze auditor als belangrijk verbeterpunt aangedragen. Om dit proces te verbeteren is in 2019 bij het team Personeelszaken gestart om maatregelen door te voeren en de huidige procedure te actualiseren. Inmiddels is dit breder opgepakt. Het totale proces is in 2021 geautomatiseerd. In 2022 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 aandacht en zorg. De zwakste schakel is de mens. Dit geven we voornamelijk in de diverse bewustwording sessies grote aandacht.	· Het voorkomen van ongeautoriseerde toegang. · Het garanderen van correcte en veilige informatievoorzieningen.

Zo nemen hebben we in 2021 extra technische maatregelen genomen om schade te voorkomen of te beperken. In 2022 wordt gestart met de voorbereiding van de implementatie van een SIEM/SOC	· 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 normen uit de BIG. 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. Het op afstand vergaderen van met Teams is vanwege Corona ad-hoc versneld mogelijk gemaakt. Teams draait het beste onder Office 365 waarvoor in 2022 de gefaseerde implementatie start. We werken nu nog met Office 2016.	· 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. - aan te tonen dat het in- en uitgaand gegevensverkeer wordt gemonitord en er snel proactief op dreigingen kan worden gereageerd. In 2022 gaan we organisatie breed protocollen doorvoeren om ook te voldoen aan de BIO-eisen op logging binnen de vak-applicaties	· 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 2022 een pentest uit.	· Het managen van de informatiebeveiliging
Bedrijfscontinuïteit In 2022 stellen we een bedrijfscontinuïteitsplan en een daaraan gerelateerd crisisplan. Dit is een eis uit de BIO maar 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.	· 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	Het adequaat reageren op incidenten.

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 nog worden aangepast op het gebied van forensisch onderzoek en aansluiten bij het bedrijfscontinuïteitmanagement en op te stellen crisisplan. protocol	
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 2021 volgen de resterende. Onderdeel daarvan zijn ook afspraken hoe om te gaan met datalekken.	Het beschermen en correct verwerken van persoonsgegevens van inwoners en medewerkers.
Vervangen van hardware Het afgelopen jaar hebben we samen met ICT-Westland een aanbesteding uitgevoerd voor de vervanging van ons inmiddels afgeschreven serverpark, opslag en back-upsysteem. De nieuwe hardware is in 2021 vervangen en voldoet aan de meest actuele eisen van de BIO.	· 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 beschermen van kritieke bedrijfsprocessen.

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 2021 zijn 97 spammails, 20 incidenten en 263 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 bijvoorbeeld ook de LOG4J-kwetsbaarheden.

In 2021 zijn er 11 van de beveiligingsincidenten aangemerkt als datalek. Daarvan hebben we in twee gevallen zelf melding moeten doen bij de Autoriteit Persoonsgegevens (AP), een maal is daar door een partnerpartij melding gemaakt. De betrokkenen slachtoffers zijn geïnformeerd. In 2020 was er nog sprake van 16 beveiligingsincidenten waarbij er toen negen zijn aangemeld als datalek.

Sinds 5 jaar is het aantal door medewerkers gemelde incidenten gedaald. 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.

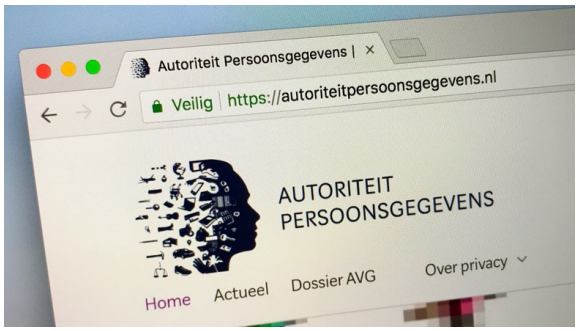
De opgetreden incidenten kunnen op diverse manieren worden ingedeeld. De belangrijkste indeling is die in het kader van de AVG en de Wet meldplicht datalekken. Een incident in de informatiehuishouding is niet per definitie meldingsplichtig is in het kader van de AVG. Bij een incident wordt onderzocht 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 2021 ontvingen we maar liefst 263 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.

2021 was met alle coronamaatregelen wederom een bewogen jaar. Ook voor de gemeentelijke ICT-beveiliging was het einde van 2021 hectisch.
Op 10 december ontving de IBD informatie over ernstige kwetsbaarheden in het softwareonderdeel Log4j, een veelgebruikte bouwsteen voor het loggen van gebeurtenissen in hard- en software. Voor deze kwetsbaarheid was een exploit gepubliceerd, dit is een mogelijkheid voor hackers om misbruik te maken. Hierop zijn we als gemeenten met ondersteuning en aanbevelingen van de IBD de nodige maatregelen gaan nemen en software die de kwetsbaarheid bevat uit te schakelen. De softwareleveranciers kwamen op een bepaald moment met aanpassingen van hun software of tijdelijke noodoplossingen. Lastig hierbij is dat duidelijk moet zijn welke software het kwetsbare onderdeel bevat. Ook is het in- en extern netwerkverkeer met extra aandacht gemonitord. Dit betekende een extra belasting is voor de ICT-medewerkers. Samen met Westland hebben wij onze netwerken laten scannen op kwetsbaarheden. Gelukkig zijn er geen schadelijke virussen, mallware of sporen van kwaadwillenden ontdekt op onze netwerken.
Al met al geeft ook deze crisis wederom de kwetsbaarheid van onze digitale bedrijfsvoering aan. 2020 staat ons ook nog de Citrix-kwetsbaarheid vers in het geheugen. We konden toen vanwege die kwetsbaarheid niet thuiswerkend inloggen op onze Citrix omgeving.

Incidenten / datalekken in 2021

Datum	Omschrijving	Melding aan AP
11-1-2021	Zonder doelbinding is er intern binnen de organisatie een mutatieformulier met meer persoonsgegevens van een medewerker gebruikt dan nodig is.	Nee
29-3-2021	Opnieuw een zelfde soort incident als bij incident nr.1. Wederom een mutatieformulier met meer persoonsgegevens van een nieuwe medewerker dan nodig.	Nee
14-5-2021	Formulier 'Meldformulier voor professionals' op straat gevonden. Het gaat om een veroorzaakt datalek door een partner organisatie: geen getroffen maatregelen vanuit Midden-Delfland noodzakelijk	Ja door verantwoordelijke partij
2-6-2021	Batch brieven verzonden met per abuis een brief van andere burger op de achterzijde geprint.	Ja
27-5-2021	Naar verkeerd adres verzonden indicatie cliënt jeugdhulp. Ontvangende partij werkt voor jeugdinstelling en heeft beroepsgeheim.	Nee
4-6-2021	Brief over loonbeslag medewerker ontvangen door een medewerker van een niet betrokken afdeling binnen Midden-Delfland.	Nee
24-6-2021	Ziekteverzuim medewerkers bij toeval te zien door onbevoegde medeweker. Gevolgen zijn nihil, het gaat om een intern incident.	Nee
1-11-2021	Nota voor een vereniging is per abuis naar de verkeerde afzender verstuurd. Alleen naam en adres van vereniging stonden op de nota. Notabedrag zou eventueel gevoelig kunnen zijn, maar is dus alleen door één andere vereniging ontvangen.	Nee
11-11-2021	Openstaande deur van de serverruimte tijdens openingstijden gemeentehuis. Is geconstateerd door een medewerker van Midden-Delfland.	Nee
15-12-2021	Documenten Ww-gegevens waren incidenteel in te zien in financieel softwarepakket door onbevoegde medewerkers Midden-Delfland.	Nee
13-12-2021	Teamleider en een medewerker binnen een team hebben een mail ontvangen met een terugkoppeling van een spreekuur van de bedrijfsarts met daarbij per ongeluk de terugkoppeling over de verkeerde medewerker toegevoegd.	Ja



Melding van datalekken

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. Bij een van de datalekken lag de oorzaak bij een externe partij.



Incidenten met veiligheid

Een datalek komt vaker voor dan we zouden willen. Regelmatig haalt een datalekincident uit de zorgsector de krant en nieuwssites.

Rechts zie je bijvoorbeeld een deel uit een artikel uit april 2018 dat gaat over een veiligheidsincident door het ongeoorloofd inkijken van een medisch dossier.

Bron: NRC, 5 april 2018

Usb-stick met gegevens 2000 patiënten VUmc

"AP onderzoekt Haags ziekenhuis om inbreuk dossier Barbie

Tientallen medewerkers van het Haga-ziekenhuis hebben ongeoorloofd de medische gegevens bekeken van de realityster, die eigenlijk Samantha de Jong heet.

De Autoriteit Persoonsgegevens (AP) is een onderzoek begonnen naar het Haga-ziekenhuis in Den Haag omdat tientallen medewerkers daar ongeoorloofd het medisch dossier van realityster Samantha de Jong hebben ingezien. Dat meldt persbureau ANP donderdagmiddag.

Aanleiding van het onderzoek is berichtgeving van actualiteitenrubriek EenVandaag eerder op donderdag. De Jong werd in januari bewusteloos in haar woning aangetroffen en naar het Haga-ziekenhuis gebracht. Daar zouden volgens EenVandaag niet alleen haar behandelend artsen haar gegevens hebben geraadpleegd, maar ook tal van anderen die niets met De Jong te maken hadden."

Met leveranciers en ketenpartners zijn verwerkers- of dataleveringsovereenkomsten afgesloten. De in deze overeenkomsten opgenomen eisen op het gebied van informatiebeveiliging 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)

Intern en onbedoeld
In de eerste plaats zijn er dreigingen door onbedoelde neveneffecten van logisch menselijk handelen. Medewerkers van gemeenten doen hun best om het werk snel, efficiënt en kwalitatief goed te doen. Bureaucratie is ‘uit’ en ondernemerschap is ‘in’. De kortste weg naar het resultaat is er vaak één met valkuilen.
Voorbeelden:
Van dergelijke dreigingen zijn e-mails met gevoelige gegevens aan de verkeerde geadresseerde, verloren USB-sticks en het per ongeluk wissen van bestanden.

Extern, bedoeld maar ongericht
Verreweg het grootste deel van de incidenten vanuit een externe actor komt voort uit geautomatiseerde bulkaanvallen. Kwaadwillenden scannen het internet af op bekende zwakheden in hard- en software, proberen veelvoorkomende gebruikersnaam-wachtwoordcombinaties of sturen honderdduizenden phishing-berichten aan elk adres dat ze tot hun beschikking hebben. Gemeenten zijn dan gewoonweg het slachtoffer omdat ze aangesloten zijn op het internet, doorgaans niet omdat ze de Nederlandse overheid zijn. De gevolgen van ongerichte aanvallen kunnen groot zijn: de meeste aanvallen met gijzelsoftware zijn in eerste instantie ongericht. Het komt voor dat buitgemaakte inloggegevens van ongerichte aanvallen worden aangeboden aan de hoogste bieder. In zo’n geval kan een ongerichte aanval het opstapje vormen voor een gerichte aanval.

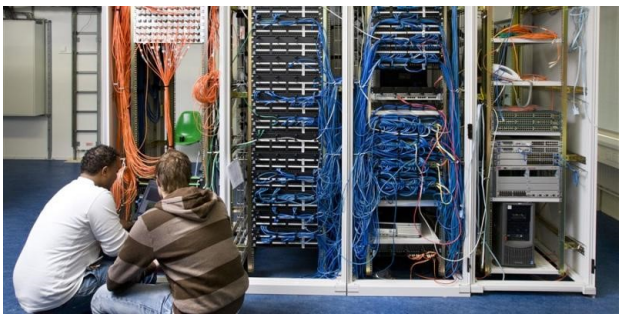


Extern, bedoeld en gericht
Veel aandacht gaat uit naar gerichte dreigingen van hackers en criminelen. Dit fenomeen levert spannende verhalen op in de media. Dit zijn tevens de gevallen die we maar heel moeilijk kunnen ontdekken en die men ook bij de IBD (dus) relatief weinig tegenkomt.
Een dergelijke gerichte aanval start vaak met onderzoek door de hacker naar informatie die kan worden gebruikt bij een hack. Op sociale media zoals LinkedIn is veel op het oog onschuldige

zakelijke informatie te ontdekken waar een kwaadwillende zijn voordeel mee kan doen. De wat meer gesloten bronnen leveren nog meer informatie op. Er circuleren lijsten met miljarden gestolen gebruikersnamen en wachtwoorden van eerdere hacks. De IBD krijgt meldingen van doelgerichte inlogpogingen op systemen of gerichte phishing-mail met een keurige aanhef en een plausibele aanleiding met het doel om geld of (inlog) gegevens buit te maken. Digitaal vandalisme zoals het platleggen van websites scharen we ook onder deze dreigingscategorie.

Intern en bedoeld
De meest riskante dreiging komt van binnen de organisatie.
Medewerkers met kwade bedoelingen kunnen uit hoofde van hun functie bij veel gegevens en systemen. Vooral medewerkers met verhoogde toegangsrechten zoals ICT-beheerders en management kunnen grote schade aanrichten. Deze dreiging is nog moeilijker te ontdekken. Interne medewerkers kennen de interne processen en controlemechanismen en kunnen die daarom beter omzeilen dan iemand van buiten.

We weten niet wat we niet weten
Het feit dat er in de gemeente weinig of geen incidenten lijken te zijn, hoeft niet te betekenen dat er niets gebeurt. Besef dat er in elke organisatie incidenten zijn. Als de directie en het management die niet kennen, dan is dat zorgelijk. Het boven tafel krijgen van incidenten vereist een open cultuur waarin medewerkers zich vrij voelen om situaties te melden.
Daarnaast is er ook een technische component: systematisch in de gaten houden wat er gebeurt in de gemeentelijke systemen, afwijkingen herkennen en hier vervolgens adequaat op reageren.

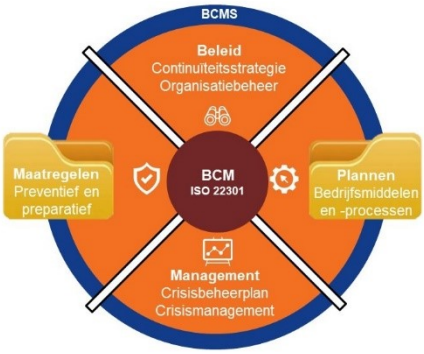


Risico's voor de ambtelijke organisatie

De meest prominente risico's manifesteren zich in de ambtelijke organisatie; bij de ambtenaren die iedere dag gebruikmaken van informatie- en communicatiesystemen om hun werk te doen. In 2021 deden zich twee situaties voor die het belang van beschikbaarheid van informatiesystemen onderstrepen, storingen na de overgang op nieuwe hardware en de Log4J crisis waardoor we meerdere systemen uit moesten zetten voor een bepaalde periode..

Risico: bedrijfscontinuïteit in het geding
Of het nu door een technische oorzaak komt (fouten in hard- en software) of door een niet technische oorzaak (een faillissement van een dienstverlener, een pandemie, een brand, een vlooienplaag, een overstroming, enzovoort). Het kan voorkomen dat het werk niet kan doorgaan zoals dat normaal gaat. Deze risico's vinden een oorzaak in de digitale wereld of ze manifesteren zich uiteindelijk in het feit dat een computersysteem niet werkt.

Per proces hoort bekend te zijn wat de kernfunctie is en hoe die door middel van een informatiesysteem wordt ondersteund. Gemeenten dienen een plan te hebben voor uitval of onbeschikbaarheid van een informatiesysteem. Risico's met betrekking tot de bedrijfscontinuïteit nemen toe, omdat online processen steeds meer de standaard worden en de offline alternatieven verdwijnen. Waarbij vroeger voor een aanvraag een papieren formulier met handtekening nog werd overgenomen in een computersysteem, is nu de online aanvraag de directe start van een aanvraagproces. Wanneer een systeem uitvalt kan niet worden teruggevallen op papieren processen.



Integriteit van gegevens is niet gewaarborgd
We vertrouwen erop dat de persoon die inlogt in een systeem ook degene is aan wie we toestemming geven om dat te doen en dat deze persoon op dat moment ook een gegronde reden

heeft om in te loggen. Om technische (een hack) en niet-technische (een medewerker met kwade bedoelingen) redenen kan het zijn dat iemand werk uitvoert dat niet de bedoeling is. Een kwaadwillende kan in zo'n geval gegevens wijzigen, wissen of toevoegen. Een onterechte factuur indienen of goedkeuren, vergunning verstrekken, een uitkering toewijzen, het bepalen van een hoogte van een vergoeding, het verstrekken van een paspoort: dat begint allemaal met het invoeren van gegevens in informatiesystemen.



Vertrouwelijke gegevens in verkeerde handen
Een e-mail aan een verkeerd mailadres, een foutje in de toegangsrechten van een gedeelde map (menselijke fouten) of een onontdekt lek in een systeem (technische fouten) of een ongedicht lek in een systeem (een combinatie van menselijke en technische fouten) kunnen ertoe leiden dat vertrouwelijke informatie onbedoeld onder ogen van ongeautoriseerde personen komt. De gemeente werkt met legio vertrouwelijke gegevens over inwoners, maar ook over de eigen bedrijfsvoering: denk aan aanbestedingen, plannen, memo's, salarissen.

Risico's voor het openbaar bestuur en de politiek

Imagoschade
Fouten van medewerkers worden het bestuur aangerekend.
Daarnaast krijgen bestuurders en politieke ambtsdragers veel gevoelige en vertrouwelijke informatie onder ogen. Een zorgvuldige omgang is vereist. Het vertrouwen in de gemeente en de ambtsdragers kan ernstig worden aangetast als (vertrouwelijke) informatie wordt gebruikt om er zichzelf of anderen mee te bevoordelen. Belangrijk is ook om (digitale) stukken goed op te bergen en de interne beveiligingsinstructies op te volgen die gelden voor gebruik van smartphones, tablets en pc's, et cetera. Het vertrouwen in de overheid hangt onder meer samen met de wijze waarop men omgaat met gegevens. Dat wil zeggen: inwoners van de gemeenten moeten er op kunnen vertrouwen dat de gemeente gegevens op een passende manier beschermt en plannen uitvoert zoals ze zijn afgesproken.

Financiële schade
Op meerdere manieren kan een gemeente geconfronteerd worden met financiële schade als gevolg van ontbrekende informatiebeveiliging. De gemeente Lochem werd op een haar na slachtoffer van gijzelsoftware maar had toch enkele tienduizenden euro's schade als gevolg van het stilleggen van de dienstverlening, het forensisch onderzoek en het herstellen van de ICT-omgeving. Wanneer de gemeente daadwerkelijk zou zijn getroffen door gijzelsoftware hadden de kosten kunnen oplopen tot honderdduizenden of zelfs miljoenen euro's.
Een ambtenaar, bestuurder of raadslid kan bedoeld of onbedoeld informatie verschaffen waar een kwaadwillende zijn voordeel mee kan doen (en de gemeente gedupeerd achterblijft). Informatie rond bestemmingsplannen, aanbestedingen of veranderende regels kan zeer waardevol zijn.
Onzorgvuldige omgang met persoonsgegevens en overtredingen van de Algemene verordening gegevensbescherming (AVG) kunnen leiden tot aansprakelijkheidsstellingen van getroffenen of boetes van de privacy-toezichthouder.
Een boete wegens onzorgvuldig handelen met de privacy van inwoners zou bovendien leiden tot grote imagoschade.

Schade aan democratische processen
Inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen kunnen het democratische proces aantasten. Dit geldt voor zowel verkiezingen als stemprocessen

van volksvertegenwoordigers. Raadsleden moeten ervan op aan kunnen dat hun stem op de juiste wijze wordt verwerkt en dat ze hun stem kunnen baseren op de juiste informatie. Bovendien is bij verkiezingen het stemgeheim een groot goed.

Risico's voor de inwoners en de ondernemers

Gegevens in verkeerde handen
Gemeenten worden geacht als goed huisvader om te gaan met de gegevens die ze onder hun hoede hebben. Als de informatie van de overheid in verkeerde handen komt zijn de mogelijke gevolgen voor inwoners en ondernemers bijna niet te overzien. Inwoners zijn voor veel gevoelige zaken afhankelijk van de overheid: zorg, werk, inkomen en andere voorzieningen. Tijdens de coronacrisis is een derde van de Nederlandse werkenden afhankelijk van regelingen die geheel of gedeeltelijk worden uitgevoerd door gemeenten. Bijna één op de tien kinderen en jongeren maken gebruik van jeugdzorg. Als over individuele gevallen informatie uitlekt, zijn de betrokkenen daar direct de dupe van.

Dienstverlening van de gemeente niet beschikbaar
Als de dienstverlening van de gemeente niet of verminderd beschikbaar is, dan kunnen inwoners en ondernemers daar hinder van ondervinden. In sommige gevallen zal er sprake zijn van licht ongemak wanneer een inwoner diensten of producten een paar dagen later geleverd krijgt. Uitval van meerdere dagen of zelfs langer kan serieuze maatschappelijke, economische en sociale gevolgen hebben.



Ontwrichting van alledaagse processen
Veel van de systemen die ervoor zorgen dat alledaagse processen goed verlopen worden aangestuurd door computersystemen. Procesautomatisering gaat onder andere over doorstroming van het verkeer, regulering van de waterstand of de toegangsverlening tot gebouwen of faciliteiten. Ook hier kunnen menselijk handelen (bedoeld of onbedoeld) of de techniek leiden tot verstoringen van de beschikbaarheid (uitval van systemen) en integriteit (groen licht in plaats van rood licht, brug open in plaats van brug dicht of ontregeling van rioleringspompen).

Wake-up call: Gijzelhackers Hof van Twente
Aan het eind van 2020 volgde het meest ingrijpende gemeentelijke cyberveiligheidsongeluk. Medio december legden gijzelhackers de systemen van Hof van Twente plat. De gemeentelijke dienstverlening kwam abrupt tot stilstand. De Overijsselse gemeente moest op de blaren zitten en zag al haar systemen onbruikbaar worden, omdat de hackers alle data hadden afgegrendeld of vernietigd. Op de eis van losgeld werd niet ingegaan.
Burgemeester Ellen Nauta kon haar inwoners vertellen dat de naweeën van de cyberaanval groot zijn. De dienstverlening moest nog grotendeels handmatig verlopen. Volgens Nauta zijn er vooralsnog geen aanwijzingen dat er persoonsgegevens zijn buitgemaakt. Een jaar na de hack heeft de gemeente 78 procent van de programmatuur en data weer hersteld. Een deel van de data is voor altijd weg. Kosten tot nu toe: 3,9 miljoen euro. Overigens was de gemeente niet tegen cyberinbraak verzekerd.

Hoewel we er alles aan doen om het risico zo klein mogelijk te maken is dit scenario ook voor Midden-Delfland niet uit te sluiten.