gemeente Rheden

Informatiebeveiligingsbeleid gemeente Rheden 2019-2021

“Naar een risicogerichte beveiliging van onze informatievoorziening”



Inhoud

1. Inleiding 2
2. Aansluiten op de Baseline Informatiebeveiliging Overheid 2
3. Uitgangspunten informatiebeveiliging Rheden 3
4. Dreigingsanalyse gemeente Rheden 4
5. Organisatie van de informatiebeveiliging 6
6. Hoe gaan we het informatiebeveiligingsbeleid realiseren 7
7. Producten informatiebeveiliging 9
8. Wat zijn de risico's bij het uitvoeren van dit beleid 9

Bijlage I: Baseline Informatiebeveiliging Overheid: BIO 11

Bijlage II Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2019 12

Bijlage III: proces informatiebeveiliging in Rheden 14

Bijlage IV: uitwerking rollen informatiebeveiliging 14

Bijlage V: Beveiligingsnivo's uit de BIO 15

1. Inleiding

De gemeente Rheden verwerkt veel informatie die gevoelig of vertrouwelijk van aard is. Het gaat om informatie om de dienstverlening aan inwoners en bedrijven uit te kunnen voeren, informatie om samen te werken met onze ketenpartners (incl. de landelijke overheid) en informatie om de juiste besluiten te nemen en het bestuur en de gemeenteraad juist te informeren.

Het verantwoord omgaan met die informatie is essentieel: inwoners en bedrijven hebben er recht op dat de gemeente Rheden zorgvuldig omgaat met de gegevens waarover ze beschikt. Het juist en zorgvuldig omgaan met persoonsgegevens is bovendien wettelijk verplicht (vastgelegd in de Algemene Verordening Gegevensbescherming (AVG)). Een betrouwbare overheid (global goal 16) is gebaat bij juiste en actuele informatie.

Uit diverse analyses blijkt dat de dreigingen rond onze informatievoorziening groter worden en de beschikbaarheid, vertrouwelijkheid en integriteit van informatie steeds meer onder druk staat. Aanvallen op systemen worden steeds geavanceerder, mails om ons informatie te ontfutselen (phishing) steeds geraffineerder. Door digitalisering zijn de gevolgen van een datalek of aanval op systemen steeds groter. Onze digitale informatie zit in systemen die gekoppeld zijn aan informatiesystemen van ketenpartners. Informatiesystemen kunnen uitvallen of door onbevoegden aangepast kunnen worden. Veel informatie staat ook nog gewoon op papier en het zorgvuldig omgaan met die informatie vraagt aandacht van alle medewerkers.

In dit informatiebeveiligingsbeleid is beschreven welke risico's en bedreigingen we onderkennen (risicoanalyse), welke beveiligingsnormen we toepassen en is beschreven hoe we tot een adequaat beveiligingsniveau komen (nemen van maatregelen).
De maatregelen uit dit informatiebeveiligingsbeleid dragen bij aan het voldoen aan het privacybeleid[1] .
Dit informatiebeveiligingsbeleid is extern afgestemd met: de CISO's[2] van de Gemeente Arnhem, Renkum en met bedrijfsvoeringsorganisatie De Connectie en intern met de Functionaris Gegevensbescherming (FG) van Gemeente Rheden.

2. Aansluiten op de Baseline Informatiebeveiliging Overheid

Door de rijksoverheid, provincies, waterschappen en gemeenten is gewerkt aan een landelijk normenkader voor informatiebeveiliging: De Baseline Informatiebeveiliging Overheid (BIO). De BIO is door het VNG bestuur als standaard verklaard[3]. Op 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen. De baseline is interbestuurlijk

[1] Zie privacybeleid gemeente Rheden (wordt begin mei 2019 aangeboden ter besluitvorming)
[2] Zie hoofdstuk 5
[3] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatieveiligheid/brieven/standaardverklaring-baseline-informatiebeveiliging-overheid

bekrachtigd in het Overheids Brede overleg Digitale Overheid (OBDO). Het jaar 2019 geldt als een voorbereidings- en overgangsjaar. In bijlage I is meer informatie over de BIO opgenomen.
De BIO helpt om informatiebeveiliging goed te regelen, doordat de maatregelen concreet zijn en de verantwoordelijkheden helder belegd. Door de procesgerichte insteek, als gevolg van de toepassing van de BIO, is de kans groter dat informatiebeveiligingsmaatregelen ook toegepast worden in de dagelijkse praktijk van onze gemeente.

De BIO biedt ook goede handvaten om afspraken te maken met interne of externe leveranciers. Door een eenduidig beleid voor de gehele overheid, is informatiebeveiliging met alle partijen (intern en extern) contractueel goed vast te leggen.

3. Uitgangspunten informatiebeveiliging Rheden

Gemeente Rheden hanteert de volgende uitgangspunten rond Informatiebeveiliging:

1. We zorgen dat informatie op het juiste niveau wordt beveiligd, waarbij beschikbaarheid, vertrouwelijkheid of integriteit van informatie op een voldoende niveau gebracht zijn en blijven.
2. Op basis van een risicoanalyse bepalen we per proces welke maatregelen nodig zijn om tot dit 'voldoende' niveau te komen. Gemeente Rheden gebruikt de Baseline Informatiebeveiliging Overheid (BIO) als kader voor deze maatregelen. We hanteren daarbij het "pas toe of leg uit" principe, d.w.z. we passen maatregelen toe tenzij uit de risicoanalyse blijkt dat maatregelen (nog) niet nodig zijn.
3. De gemeente Rheden heeft als ambitie het continu verbeteren van de informatieveiligheid en verder professionaliseren van de informatiebeveiligingsfunctie. Het beveiligen van informatie is dus een cyclisch proces waarbij de veiligheid van de informatievoorziening continu wordt verbeterd. Zie bijlage III voor een toelichting op dit proces.
4. De scope bij informatiebeveiliging is informatie in alle verschijningsvormen, zowel elektronisch, op papier als mondeling.
5. Informatiebeveiliging is een verantwoordelijkheid van het management c.q. de eigenaar van de informatie die beveiligd moet worden. Het management maakt op basis van de risicoanalyse de afweging welke beveiligingsmaatregelen noodzakelijk zijn en welke niet. Daarbij is de gemeentesecretaris ambtelijk eindverantwoordelijk voor de beveiliging van informatie binnen de gemeente. De proceseigenaar of manager is verantwoordelijk voor de beveiliging binnen de eigen werkprocessen.
6. Bij informatie-uitwisseling met andere overheden gaan we uit van het 'Schengen'-principe. Dit houdt in, dat onderdelen van de overheid elkaar beschouwen als vertrouwde[4] partner. Uitgangspunt is hierbij dat iedere overheidsorganisatie afzonderlijk zijn omgeving beveiligd en 'schoon' houdt en dat de andere omgevingen hierop kunnen vertrouwen.
   Bij informatie-uitwisseling met partners (semi-overheid) passen we dit principe ook toe, maar leggen dit wel vast in convenanten, welke voldoen aan de eisen uit de AVG (artikel 26).

[4] De uitwisseling van persoonsgegevens met andere overheden dient wel aan de AVG te voldoen.

7. Informatiebeveiliging richten we in door een slimme combinatie van technische en organisatorische maatregelen. We kiezen daarbij bij voorkeur voor veilig faciliteren in plaats van verbieden, waar nodig schermen we informatie af. Techniek faciliteert een verantwoorde informatiebeveiliging, maar mag niet onnodig belemmerend werken.
8. Verantwoord en bewust gedrag is essentieel voor informatieveiligheid. We verwachten dat medewerkers bewust en verstandig omgaan met de informatie die ze nodig hebben voor hun werk, zij worden daarbij ondersteund door hun leidinggevende. Waar medewerkers zich niet aan afspraken houden worden ze hierop aangesproken.
9. Informatiebeveiliging is iets wat alle medewerkers, collegeleden en raadsleden aangaat. Iedere medewerker, zowel vast als tijdelijk, stelt zich op de hoogte van de richtlijnen voor informatiebeveiliging, en beschermt de informatie waar hij/zij mee omgaat tegen ongeautoriseerde toegang. De wijze waarop medewerkers dat kunnen doen, zijn begrijpelijk weergegeven op ons Intranet. Daarnaast zal de Gemeente Rheden medewerkers voorzien van gepaste training op het gebied van informatiebeveiliging en gegevensbescherming.
10. Alle medewerkers zijn verplicht om, bij vermeende inbreuken op de veiligheid van informatie, hiervan melding te maken.
11. We maken het voldoen aan informatiebeveiligingseisen transparant door het vastleggen van risicoafwegingen, beveiligingsniveaus, maatregelen en incidenten. We gebruiken hiervoor de verplichte audit (ENSIA[5]) en een interne status rapportage voor de directie.

4. Dreigingsanalyse gemeente Rheden

Ook in gemeente Rheden hebben we te maken met dreigingen rond de veiligheid van de informatievoorziening. Er zijn de afgelopen jaren een aantal kleinere beveiligingsincidenten geweest (zoals diefstal van een laptop) deze hebben er gelukkig niet toe geleid dat vertrouwelijke informatie bij derden is terecht gekomen. Tot op heden zijn er binnen de gemeente Rheden geen grote beveiligingsincidenten geweest waarbij schade voor inwoners is opgetreden.
De Informatie Beveiligingsdienst (IBD) van de VNG maakt jaarlijks een dreigingsanalyse, of dreigingsbeeld, op basis van incidenten die bij de IBD gemeld zijn[6].
Hier zijn 5 belangrijke bedreigingen van de informatieveiligheid uit naar voren gekomen (zie verder bijlage II). Aan de hand van deze algemene analyse hebben we de belangrijkste risico's in Rheden in kaart gebracht en maatregelen beschreven.

1. INFORMATIEBEVEILIGING KAMPT MET EEN IMAGOPROBLEEM

Ook in Rheden zien we dat de aandacht voor het onderwerp snel minder wordt als de tijd verstrijkt. Iedereen wil veiligheid maar niemand wil er last van hebben.

[5] Eenduidige Normatiek Single Information Audit
[6] https://vng.nl/files/vng/brieven/2019/attachments/ibd-dreigingsbeeld-2019-20.pdf

Maatregel: De invoering van de AVG is gebruikt om opnieuw aandacht te vragen voor informatiebeveiliging. De aanpak die in Hoofdstuk 7 wordt voorgesteld helpt om de verantwoordelijkheid voor informatiebeveiliging helder te maken en de aandacht voor het onderwerp te behouden. In 2019 zal opnieuw een bewustwordingscampagne gestart worden om medewerkers meer inzicht te geven in de risico's van b.v. phishing.

2. INZICHT IN RISICO'S IS NOG ONVOLDOENDE INTEGRAAL

Ook in Rheden is deze dreiging actueel. Er is een redelijk beeld van risico's, mede ook naar aanleiding van de ENSIA zelfevaluatie en privacy evaluaties (zelfscan en PIA). Risico's en maatregelen worden tot nu toe niet structureel per proces vastgelegd en integraal gemonitord.
Maatregel: Met de aanpak uit hoofdstuk 7 en met name ook de invoering van een Security Monitoring Systeem (ISMS) kunnen we deze dreiging verminderen.

3. AANVALLERS BLIJVEN SUCCESVOL DOOR ONTBREKEN BASISMAATREGELEN

Uit het rekenkameronderzoek van gemeente Arnhem (wat voor een groot deel ook van toepassing was op de situatie in Rheden) bleek dat een aantal basismaatregelen nog niet waren ingevuld.
Maatregel: Verbetering is ondertussen ingezet waardoor dit risico ondertussen sterk verminderd is. Door het standaard normenkader wat de BIO biedt en het regionaal uitvoeren van noodzakelijke verbetermaatregelen kunnen we ook in de toekomst zorgen dat dit risico beperkt blijft. Dit zal de komende jaren nog wel investeringen vragen.

4. TE VEEL WERK VOOR TE WEINIG MENSEN

Ook in Rheden zien we een toename in de hoeveelheid werk om informatiebeveiliging en privacy op voldoende niveau te brengen en te houden. De beschikbare formatie is op dit moment te beperkt voor de hoeveelheid werk dit er ligt.
Maatregel: Door herverdeling van taken binnen bedrijfsvoering, fasering en te focussen op de belangrijkste risico's verwachten we deze dreiging beheersbaar te houden. Door de inzet van het Security Monitorring Systeem (ISMS) verwachten we op termijn de verantwoordingslast terug te brengen. De beschikbare capaciteit blijft een zorgpunt, zeker indien de BIO een wettelijke verplichting wordt[7].

5. COMPLEXITEIT NEEMT TOE

Ook in Rheden neemt de complexiteit van de informatievoorziening toe, maar risico's zijn nog aanvaardbaar.
Een maatregel om deze dreiging het hoofd te bieden is om informatiebeveiliging bij elke vernieuwing in de ontwerpfase mee te nemen. Daarnaast zullen we, waar mogelijk in landelijk verband (GGI-veilig), geavanceerde beveiligingsoplossingen gebruiken om de steeds complexer wordende informatievoorziening te beveiligen. In de praktijk wordt er soms gekozen om innovaties niet in te zetten om risico's te voorkomen (complexiteitsreductie).

[7] Eind mei 2019 is de Baseline Informatiebeveiliging Overheid (BIO) als verbindende voorschrift vastgesteld. Er wordt gewerkt aan een wettelijke grondslag.

5. Organisatie van de informatiebeveiliging

In dit hoofdstuk wordt de organisatie van de informatiebeveiliging in Rheden uitgewerkt. De organisatie sluit aan bij de uitgangspunten van hoofdstuk 3. In Bijlage IV zijn een aantal rollen verder uitgewerkt.

Bij het uitvoeren van het informatiebeveiligingsbeleid zijn in gemeente Rheden de onderstaande rollen betrokken.

College van B&W Het college vormt het dagelijks bestuur van de gemeente en is eindverantwoordelijk voor alle processen die binnen de gemeente worden uitgevoerd, inclusief de beveiliging van informatie die in de processen gebruikt wordt. Het college van B&W stelt het beleid rond informatiebeveiliging vast.

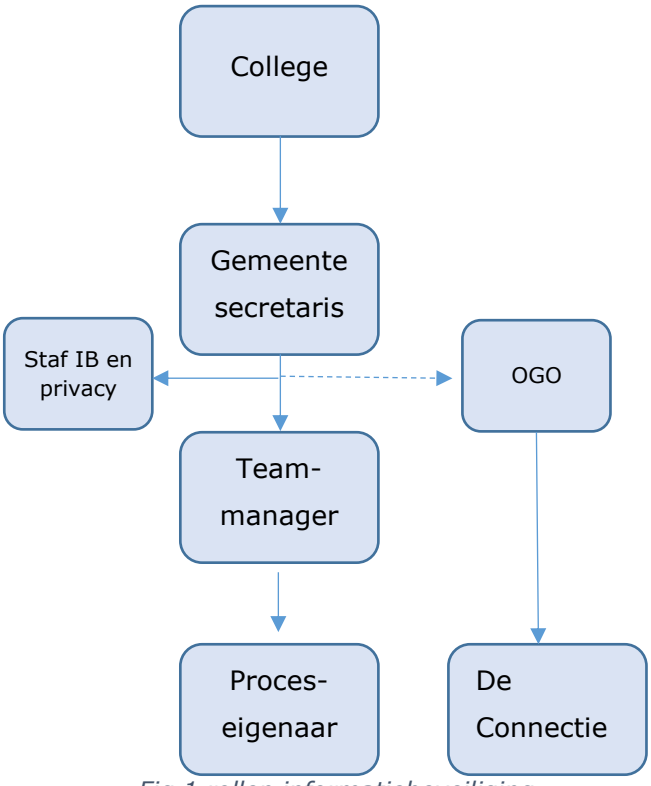


Fig 1 rollen informatiebeveiliging

Gemeentesecretaris

De gemeentesecretaris is eindverantwoordelijk voor de ambtelijke organisatie en dus ook voor de wijze waarop informatiebeveiliging wordt uitgevoerd. De gemeentesecretaris ziet toe op de naleving van het beveiligingsbeleid.

Teammanager

De teammanager is verantwoordelijk voor de inzet van personeel en de informatiebeveiliging binnen het team. Onder de verantwoordelijkheid van de teammanager vallen meerdere processen.

Proceseigenaar

De proceseigenaar is verantwoordelijk voor de informatiebeveiliging binnen de processen die onder zijn of haar verantwoordelijkheid vallen. De proceseigenaar is soms de teammanager en soms een coördinator of medewerker.

Staf informatiebeveiliging en privacy

Binnen de informatiebeveiliging worden de volgende staftaken onderkend:

Chief Information Security Officer (CISO)

De rol van CISO wordt ingevuld conform het advies van de VNG [8]. Dit houdt in dat de CISO een adviserende functie heeft naar management en bestuur. De CISO stelt beleid op en

[8] https://www.informatiebeveiligingsdienst.nl/product/handreiking-ciso-functieprofiel/

ondersteunt het management bij het uitvoeren van risicoanalyses en nemen van beveiligingsmaatregelen.

Medewerker informatiebeveiliging
Deze functionaris is belast met de uitvoerende taken rond informatiebeveiliging.

Functionaris gegevensbescherming en Privacy Officer
De functionaris gegevensbescherming (FG) is een toezichthoudende rol. De privacy Office adviseert over privacy vraagstukken. Deze functies zijn nader uitgewerkt in het privacy beleid.

Dienstenleverancier
Daar waar delen van een proces zijn uitbesteed aan een interne of extern dienstverlener gaat de verantwoordelijkheid[9] voor het nemen van de juiste beveiligingsmaatregelen over op de externe dienstverlener. In de BIO wordt bij een groot aantal maatregelen expliciet verwezen naar de Dienstenleverancier.
Voor de dienstverlener Connectie verloopt de aansturing via de demandmanager en het Opdrachtgevers Overleg.

Crisisorganisatie
Indien er grote informatiebeveiligingsincidenten ontstaan (maximale schade boven “Basis Beveiligings Niveau 1 (BBN1)”[10]) wordt er een crisisorganisatie ingericht. Deze crisisorganisatie wordt ook ingezet bij overige calamiteiten (bedrijfscontinuïteit). De opzet en samenstelling van deze crisisorganisatie wordt uitgewerkt in het bedrijfscontinuïteitsplan.

6. Hoe gaan we het informatiebeveiligingsbeleid realiseren

Of de beveiliging van de gemeente daadwerkelijk op voldoende niveau is wordt bepaald door het concrete gedrag en handelen van medewerkers en het nemen van de juiste organisatorische en technische maatregelen bij de inrichting van processen en systemen en netwerken. Het is daarom belangrijk om over een helder proces te beschikken waarmee we daadwerkelijk de veiligheid vergroten, leren van incidenten en verbetermaatregelen nemen.

Zoals in Hoofdstuk 3 is aangegeven hanteren we een procesgerichte en cyclische aanpak om informatiebeveiliging te implementeren. Hierbij wordt het landelijke normenkader uit de BIO gevolgd.
De BIO bevat 3 soorten maatregelen:

[9] Met verantwoordelijkheid wordt hier bedoeld het nemen van de juiste technische en organisatorische maatregelen. De gemeente blijft eindverantwoordelijk voor het uitbestede proces.
[10] BBN is een term uit de BIO. Op basis van de risicoanalyses wordt een BBN bepaald. Zie bijlage V

A. Maatregelen die aan een specifiek proces gekoppeld zijn. De verantwoordelijke hiervoor is de proceseigenaar. Per hoofdproces zullen we in een workshop, op basis van de dreigingen voor dat proces een risicoanalyse uitvoeren. In deze workshops nemen we zowel bedrijfscontinuïteit als informatiebeveiliging mee. Op basis van de normen uit de BIO bepalen we de verbetermaatregelen en stellen een plan op. We starten in 2019 met de meest kritische processen.
B. Maatregelen die vragen om detail beleid of procedures gemeentebreed (b.v. beveiligingsbeleid rond thuiswerken). Deze zullen in 2019 worden opgesteld en aan het DT ter besluitvorming voorgelegd. De verantwoordelijkheid ligt hier bij de gemeentesecretaris.
C. Maatregelen die uitgevoerd moeten worden door dienstenleveranciers (intern of extern). Voor het realiseren van het merendeel van deze meer technische maatregelen zal in 2019 een regionaal (Arnhem, Renkum, Rheden en De Connectie) project worden opgestart. Op basis van de normen uit de BIO wordt een analyse gemaakt van uit te voeren verbetermaatregelen, worden op basis van risico's prioriteiten bepaald en wordt een regionaal uitvoeringsplan opgesteld.

De rapportage over het voldoen aan de hierboven genoemde BIO maatregelen zal plaatsvinden middels de ENSIA verantwoordingssystematiek en een interne rapportage aan de directie.

Om dit informatiebeveiligingsbeleid te kunnen uitvoeren zullen de volgende randvoorwaarden ingevuld moeten worden:

1. Het inrichten van de organisatie zoals in hoofdstuk 5 beschreven.
2. Het implementeren van een informatiesysteem (ISMS) om per hoofdproces bij te houden aan welke beveiligingsnormen we voldoen en welke verbetermaatregelen zijn afgesproken. Het systeem ondersteunt bij het aanleveren van informatie aan ENSIA en vergemakkelijkt de communicatie met de dienstenleverancier (De Connectie). Dit systeem is reeds gezamenlijk door Arnhem, Renkum, Connectie en Rheden aangeschaft.
3. Capaciteit en betrokkenheid van afdelingen (proceseigenaren) en dienstenleveranciers om relevante maatregelen uit te voeren.
4. De BIO vraagt een aanzienlijk zwaardere invulling van de informatiebeveiligingstaak. De BIO is nog geen wetgeving, maar wel een standaard normenkader[11] waar gemeenten aan geacht worden te voldoen. De ENSIA zal steeds vaker niet alleen bestaan, maar ook de werking van beveiligingsnormen gaan toetsen. De BIO is een autonome ontwikkeling. De uitvoering van het informatiebeveiligingsbeleid vraagt daarom aanvullende financiële middelen:
    - Capaciteit voor de uitvoering van dit beleid en het samen met procesverantwoordelijken uitvoeren van maatregelen. Deze capaciteit is momenteel onvoldoende beschikbaar en zal in 2020 opgenomen worden in de programmabegroting. .

[11] https://www.informatiebeveiligingsdienst.nl/nieuws/bio-gepubliceerd-in-de-staatscourant/

- De realisatie van maatregelen categorie C brengen extra kosten met zich mee. Deze aanvullende middelen worden aangevraagd via de P&C cyclus in 2020.

7. Producten informatiebeveiliging

Bij de uitvoering van dit beveiligingsbeleid worden de volgende producten opgeleverd. Per product is een verantwoordelijke aangegeven.

Product	Termijn	verantwoordelijk	Vaststelling door
Dreigingsanalyse gemeente breed	Tweejaarlijks	CISO	Directie
Risicoanalyse gemeentebreed	Tweejaarlijks	CISO	Directie
Risicoanalyse per proces	Tweejaarlijks onderhoud	proceseigenaar	Teammanager
Verbetermaatregelen per proces	Continu	Proceseigenaar en medewerker informatiebeveiliging	Teammanager
Overzicht verbetermaatregelen gemeentebreed	Continu	Medewerker informatiebeveiliging	Directie of OGO
Informatie beveiligingsbeleid	1 x per 3 jaar, jaarlijks actualisering	CISO	College
Beleid specifieke thema's	1 x per 3 jaar	CISO	Directie
ENSIA rapportage	jaarlijks	ENSIA coördinator	College
Overzicht status BIO maatregelen	jaarlijks	Medewerker informatiebeveiliging	Directie of OGO

8. Wat zijn de risico's bij het uitvoeren van dit beleid

. Beveiliging is nooit leuk, en in de dagelijkse hectiek worden beveiligingsmaatregelen soms als hinderlijk ervaren. Beveiliging krijgt vaak pas aandacht als het mis gaat, terwijl voorkomen beter en goedkoper is dan genezen.

Draagvlak kan op de volgende manier verkregen worden:

- vanuit de directie het belang van informatiebeveiliging actief uitdragen
- in gesprek gaan met teams en hulp bieden bij het oplossen van praktische vraagstukken ("hoe moet ik veilig …")

- samen met proceseigenaren en medewerkers bespreken van risico's (hoe vertrouwelijk is deze informatie en wat zijn de gevolgen als informatie in handen van onbevoegden komt) en het nemen van maatregelen om de risico's te voorkomen.
- per team en dienstenleverancier transparant zijn over de stand van informatiebeveiliging (rapportage over maatregelen)
- deze rapportage op hoofdlijnen opnemen in bijvoorbeeld de P&C cyclus.

Bijlage I: Baseline Informatiebeveiliging Overheid: BIO

Vanaf 2013 staat informatiebeveiliging op de bestuurlijke agenda van gemeenten. Binnenlandse zaken heeft destijds samen met de VNG een normenkader opgesteld (Baseline Informatiebeveiliging Gemeenten of BIG). Een deel van de BIG eisen is opgenomen in een landelijke audit: ENSIA. De BIG is echter verouderd.

Vanaf 2016 is door vertegenwoordigers van de Rijksoverheid, de provincies, waterschappen, gemeenten (VNG) en het Centrum voor Informatiebeveiliging en Privacy (CIP), gewerkt aan een gezamenlijke baseline die alle bestaande losse overheidsbaselines zal gaan vervangen. De Baseline Informatiebeveiliging Overheid (BIO) verschilt op een aantal punten van de BIG. De grootste verbeteringen zijn:

- Minder maatregelen (bijna 60% minder)
- Maatregelen zijn wel altijd verplicht
- Gebaseerd op risicomanagement
- Toewijzing van maatregelen op eindverantwoordelijke

De BIO is gebaseerd op moderne en internationaal erkende ISO normen (ISO 27002 standaard). De BIO heeft als voordeel dat het normenkader ook van toepassing is op de regiogemeenten en voor de Connectie tot een eenduidig/geharmoniseerd kader leidt waar de informatiebeveiliging aan moet voldoen.
In de BIO zijn in totaal 114 beveiligingsmaatregelen (ook wel beheersmaatregelen of controls genoemd) opgenomen. Per maatregel is aangegeven wie verantwoordelijk is voor het uitvoeren van de maatregel.

In de BIO is gekozen voor een goede balans tussen veiligheid en werkbaarheid, de acceptatie van de maatregelen zal daarom groter zijn. De maatregelen zijn nuttig en relevant voor beveiliging en toch uitvoerbaar. Een organisatie die aan de BIO voldoet heeft de beveiliging goed geregeld.

Hieronder is voor de beeldvorming een klein stuk overgenomen uit de opbouw van de BIO.

5.1 Aansturing door de directie van de informatiebeveiliging

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

5.1.1	1	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Secretaris/algemeen directeur

Voor meer informatie over de BIO zie:
https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

Bijlage II Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2019

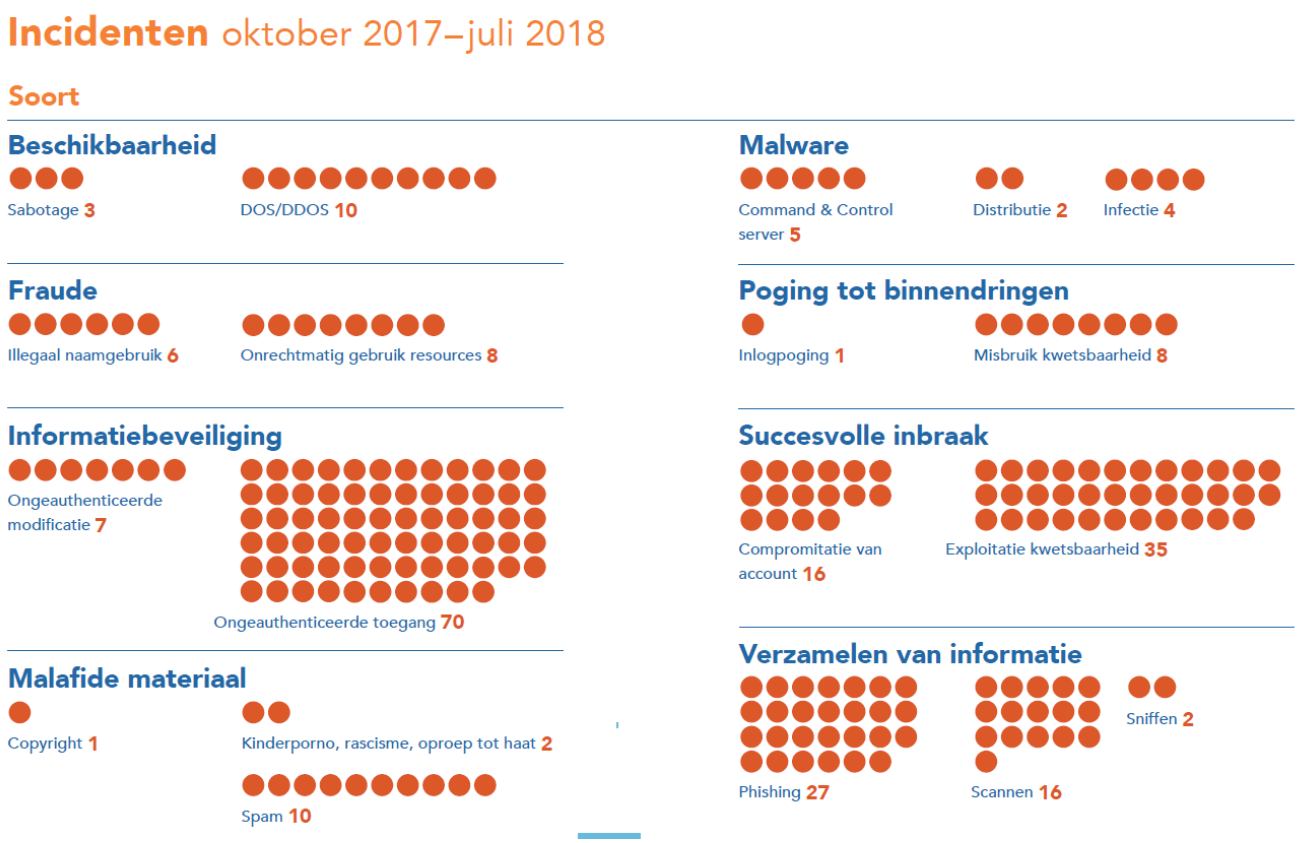
De informatiebeveiligingsdienst stelt jaarlijks een dreigingsbeeld op. Via onderstaande link vindt u het dreigingsbeeld voor 2019.

https://vng.nl/files/vng/brieven/2019/attachments/ibd-dreigingsbeeld-2019-20.pdf

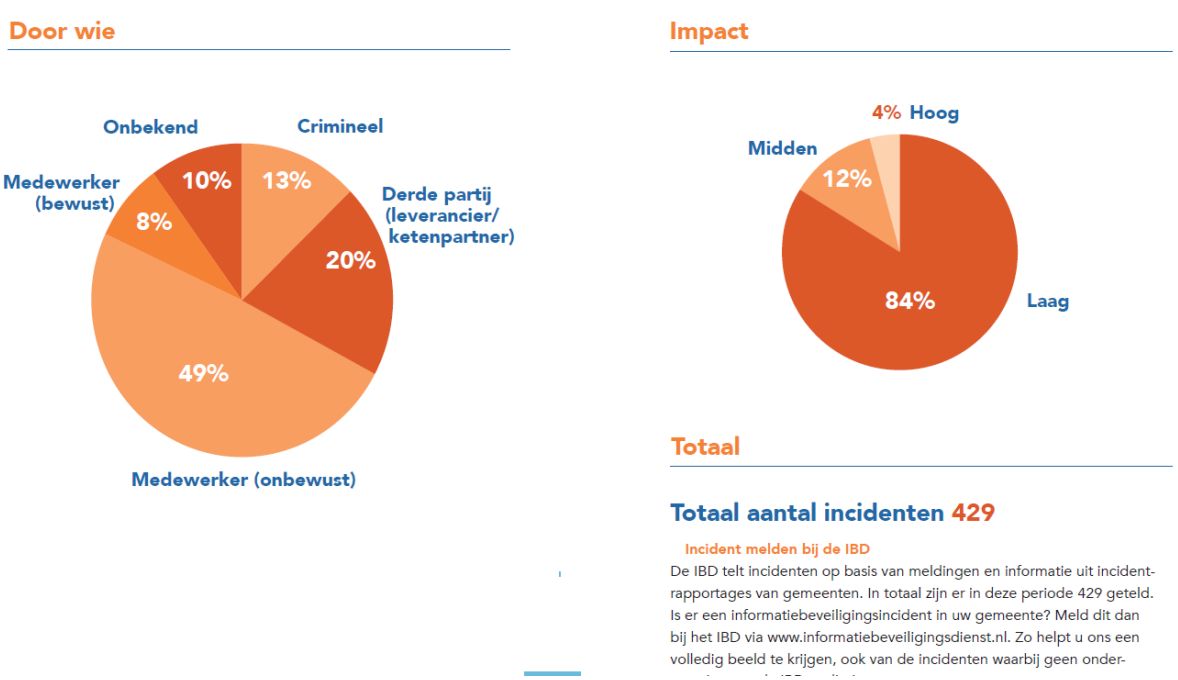
Op basis van deze analyse komt de IBD tot de volgende prioriteiten.



Hieronder is een overzicht opgenomen van de landelijke incidenten informatiebeveiliging die bij de IBD zijn gemeld.



De incidenten betreffen vooral medewerkers die onbewust fouten maken. Gelukkig is de impact van de meeste incidenten laag.



Bijlage III: proces informatiebeveiliging in Rheden

Het verbeteren van de informatiebeveiliging is een cyclisch proces. De kern van dit proces is:

1. Op basis van een Quick Scan maken we een analyse wat kritische processen zijn. Per hoofdproces maken we een risico afweging. Er wordt een inschatting gemaakt van de dreigingen waartegen beschermd moet worden. Vervolgens wordt een inschatting gemaakt van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt.
2. Op basis van de risico afweging wordt een Basis Beveiligings Niveau (BBN) bepaald.
3. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken en dus maatregelen waar de informatievoorziening aan moet voldoen. We hanteren hierbij het normenkader uit de BIO (normen verschillen per BBN) en bepalen welke maatregelen relevant en noodzakelijk zijn voor het proces. Dit betekent dus dat maatregelen afhankelijk zijn van de risico's.
4. Waar we nog niet voldoen worden verbeterplannen opgesteld. Per hoofdproces wordt een plan gemaakt.
5. De verbetermaatregelen worden uitgevoerd.



Bijlage IV: uitwerking rollen informatiebeveiliging

Hieronder worden enkele rollen die belangrijk zijn bij informatiebeveiliging verder uitgewerkt.

Proceseigenaar:

- Is verantwoordelijk voor de processen die aan hem of haar zijn toegewezen en voor de classificatie van de processen (belang voor de organisatie).
- Bepaalt met welke informatiesystemen het proces wordt ondersteund, en is bij voorkeur ook eigenaar van deze systemen.
- Stelt op basis van een dreigingsanalyse en expliciete risicoafweging de betrouwbaarheidseisen voor zijn of haar informatievoorziening vast.
- Is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de beveiligingsmaatregelen die direct betrekking hebben op zijn of haar processen.
- Controleert of deze maatregelen worden nageleefd.
- Evalueert periodiek de betrouwbaarheidseisen en stelt deze waar nodig bij.

- Rapporteert over de implementatie van de maatregelen.

De Proceseigenaar is hierbij een rol, waarbij de taken wellicht door meerdere personen uitgevoerd kunnen worden.

De CISO:

- Is betrokken bij het uitvoeren van het proces van bijlage III.
- Houdt overzicht welke beveiligingsmaatregelen per proces worden toegepast en rapporteert daarover.
- Adviseert het management en bestuur over informatiebeveiliging.
- Evalueert tweejaarlijks het beleid en doet voorstellen tot verbetering.
- Rapporteert jaarlijks over beveiligingsincidenten en inbreuken op de informatieveiligheid.
- Heeft zitting in het privacyteam en zorgt samen met privacy officer en FG voor de aansluiting van informatiebeveiligingsbeleid op privacybeleid.
- Geeft opdracht aan de dienstenleverancier voor het realiseren van gemeentebrede beveiligingsmaatregelen.

Bij (bijna) beveiligingsincidenten of inbreuken op de Integriteit, Beschikbaarheid of Vertrouwelijkheid van de informatievoorziening informeert de betreffende proceseigenaar of dienstenleverancier de CISO over het incident. De proceseigenaar stelt samen met de medewerker informatiebeveiliging een verbeterplan op, gericht op het voorkomen van het incident in de toekomst, en informeert de CISO hierover.

Voor de functiebeschrijving van de CISO gaan we uit van de functiebeschrijving zoals deze door de VNG wordt voorgesteld: (https://www.informatiebeveiligingsdienst.nl/product/handreiking-ciso-functieprofiel/).

De medewerker informatiebeveiliging:

- Is verantwoordelijk voor het uitvoeren van verbetermaatregelen rond de informatiebeveiliging.
- Ondersteunt de CISO in de registratie van beveiligingsmaatregelen, incidenten en verbetermaatregelen.
- Organiseert jaarlijks een bewustwordingscampagne, waarbij het accent ligt op communicatie en in gesprek gaan met afdelingen.
- Is het dagelijks aanspreekpunt voor medewerkers die vragen hebben over informatiebeveiliging.

Het aannemen van een medewerker informatiebeveiliging zorgt ook voor het verminderen van de kwetsbaarheid (op dit moment is er slechts 1 medewerker met kennis van informatiebeveiliging).

Bijlage V: Beveiligingsnivo's uit de BIO

In de BIO worden een drietal Basis Beveiligings Niveaus (BBN) onderkend. Wij bij elk hoofdproces de analyse maken welk niveau van toepassing is.

BBN 1

BBN1 is het niveau waar alle overheidssystemen als minimum aan moeten voldoen.

Controls en overheidsmaatregelen komen voort uit:

- wet- en regelgeving;
- algemeen geldende beveiligingsprincipes (fundamentele controls en maatregelen).

Informatiesystemen op BBN1 niveau zijn systemen waarvoor BBN2 als te zwaar wordt gezien.

BBN2

Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien:

- er vertrouwelijke informatie wordt verwerkt;
- mogelijke incidenten leiden tot bestuurlijke commotie;
- er onzekerheid bestaat of ook alle informatie van derden open is;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

Het gaat verder om commercieel vertrouwelijke informatie of informatie in het kader van beleidsvorming die nog niet geschikt is voor openbaarheid.

De controls van het BBN2 omvatten de controls van BBN1. Maatregelen van BBN2 komen voort uit:

- wet- en regelgeving, in het bijzonder beveiligingseisen a.g.v. WBP/AVG;
- aansluitvoorwaarden van generieke/gemeenschappelijke diensten;
- afhankelijkheden in ketens en netwerken;
- minimale eisen ten behoeve van een efficiënte beveiliging van BBN3.BBN3

BBN3

BBN3 richt zich op de bescherming van informatie waarbij weerstand geboden moet worden tegen de dreiging, die uitgaat van statelijke actoren en beroepscriminelen.

BBN3 is van toepassing indien:

- verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3;
- informatie met een rubricering BBN3 wordt geleverd door derden;
- aansluiting op een infrastructuur BBN3 is vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen);

Dit betekent dat BBN3 voornamelijk van toepassing zal zijn op de verkiezingen.

De maatregelen uit BBN3 sluiten aan op relevante NAVO-regelgeving.