DEFINITIEF RAPPORT

Onderzoek Rekenkamercommissie Informatiebeveiliging Gemeente Velsen

In opdracht van de Rekenkamercommissie
RKC Velsen Onderzoek Informatiebeveiliging - Definitief Rapport - 20220720
Versie 1.01 Referentie: 21040349.01/2021095/A&A/MSL
28 september 2022

DOCUMENT STATUS

Versie	Datum	Door	Opmerkingen
0.1	21/09/2021	Mario Sleegers	Eerste versie
0.2	25/10/2021	Mario Sleegers	Aanpassingen na feedback interviews
0.6	12/11/2021	Mario Sleegers	Eerste concept naar RKC
0.7	22/12/2021	Mario Sleegers	Tweede concept na update RKC
0.71	17/02/2022	Mario Sleegers	Aanpassingen na feedback RKC
0.8	10/05/2022	Mario Sleegers	Inclusief ambtelijke reactie
0.9	20/07/2022	Mario Sleegers	Inclusief bestuurlijke reactie
1.0	20/07/2022	Mario Sleegers	Definitief rapport
1.01	28/09/2022	Mario Sleegers	Definitief rapport (inclusief nawoord RKC)

Secura B.V.
Vestdijk 59
5611 CA EINDHOVEN
Nederland

Karspeldreef 8
1101 CJ AMSTERDAM
Nederland

T +31 (0)40 23 77 990
E sales@secura.com
W secura.com

INHOUDSOPGAVE

1. BESTUURLIJKE RAPPORTAGE BEVINDINGEN OP HOOFDLIJNEN EN AANBEVELINGEN

1.1. Aanleiding en opdracht

Net als bij vele bedrijven, is de dienstverlening van gemeenten aan burgers en bedrijven in hoge mate afhankelijk van geautomatiseerde informatiesystemen. Gemeenten krijgen steeds meer taken toebedeeld waar in de uitvoering intensief gebruik wordt gemaakt van informatiesystemen en daarin opgeslagen gegevens. Hierbij vervult de gemeente ook vaak niet onbelangrijke taken als onderdeel van een keten van organisaties en is daarmee tegelijkertijd afhankelijk van andere organisaties en externe databases en vormt tevens zelf ook een cruciale schakel in het realiseren van een voldoende beveiligingsniveau over de keten heen.

Dat de bedreigingen toenemen, en de kans dat deze plaatsvinden groter worden, blijkt uit recente incidenten en onderzoeken zoals die van de IBD (Informatiebeveiligingsdienst als onderdeel van de VNG). Ransomware incidenten, recente phishing aanvallen met opvolgende hacks bij gemeenten en in het bedrijfsleven en daarnaast datalekken, zoals bij de GGD, die publiek zijn geworden bevestigen dat de menselijke factor vaak doorslaggevend is. Is in de regel bij phishing aanvallen de oorzaak vooral gelegen in de onwetendheid van de medewerker, een data lek zoals bij de GGD of KvK, leert ons ook dat juist het goed afschermen van gegevens kan voorkomen dat medewerkers in de verleiding kunnen komen om een data lek te veroorzaken. Tenslotte hebben recente aanvallen bij VDL en de MediaMarkt aangetoond dat kwetsbaarheden vanuit andere vestigingen en locaties verstrekkende gevolgen kunnen hebben.

Het Nationaal Cyber Security Centrum (NCSC) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) constateren tevens een toename van cyberaanvallen op overheidsinstellingen waaronder gemeenten. Gemeenten hebben gegevens die niet in verkeerde handen mogen vallen zoals bevolkingsdata, privacygevoelige informatie van burgers, (bovenregionale) beleidsstukken, informatie over bedrijfseconomische ontwikkelingen, aanbestedingsinformatie, vertrouwelijke bedrijfsgegevens, inrichtingsinformatie over ICT-beveiliging etc.
De IBD geeft daarbij aan dat risico's toenemen doordat gemeenten meer gebruik maken van Cloud oplossingen, het gebruik van moeilijker te beveiligen mobiele apparaten toestaan en steeds meer diensterlening doen met inzet van digitale informatiesystemen. Door in gemeenten gebruik te gaan maken van apparaten die, ook via internet, met elkaar communiceren zoals camera's, energievoorzieningen op wijkniveau, smart parkeermeters etc., kortgezegd: "Smart Cities", zullen bedreigingen en de impact van incidenten in en rond informatiesystemen navenant toenemen.

De taken, bevoegdheden en verantwoordelijkheden van met name de colleges van B&W op het gebied van informatiebeheer en informatiebeveiliging, nemen als gevolg van deze ontwikkelingen sterk toe. In de praktijk blijkt dat, voor het kunnen realiseren en waarborgen van informatieveiligheid, deskundigheid nodig is en vanuit het college van B&W specifiek aandacht vraagt. En daarbij komt dan ook nog dat naast de implementatie van de Baseline Informatiebeveiliging Overheid (BIO), de implementatie van de Europese privacyregelgeving sinds 25 mei 2018, de AVG. Dit is complexe materie met voor burgers en gemeenten belangrijke regels en handvatten over hoe om te gaan met het verwerken van persoonsgegevens en voorzien van stevige boetebepalingen. Nog steeds een forse uitdaging!

De gemeente Velsen heeft halverwege 2021 de stap gezet om een groot deel van het technische ICT-beheer aan een externe partij over te dragen. Dergelijke overgangsperiodes bieden vaak de mogelijk om (opnieuw) vast te stellen wat de gemeente zelf wil doen, en waar ze dit aan een uitbestedingsorganisatie willen of kunnen overlaten. Het risico bestaat dat de gemeente onvoldoende voortvarend deze uitdagingen oppakt en te weinig werk maakt van informatieveiligheid, of dat door onduidelijke afspraken beide organisaties verwachten dat de andere partij verantwoordelijk is voor de uitvoering en/of controle.

Hoe nu bevestigd te krijgen dat de gemeente voldoende is voorbereid op deze bedreigingen, relevante aandachtspunten helder zijn en het college van B&W voldoende handvat heeft voor het aangaan van deze uitdagingen?

De Rekenkamer Commissie van de gemeente Velsen heeft het initiatief genomen om een QuickScan onderzoek te laten uitvoeren naar de wijze waarop het college grip heeft op informatieveiligheid en het voldoen aan de actuele privacyregelgeving. Zij heeft daarvoor de volgende centrale onderzoeksvraag geformuleerd:

"Is de informatiebeveiliging en privacybescherming bij de gemeente Velsen voldoende georganiseerd en geborgd?"

Aan Secura B.V. is de opdracht gegeven dit onderzoek uit te voeren. De uitvoering en de resultaten van dit onderzoek zijn in eerste instantie niet gericht op het (met zekerheid) afgeven van een oordeel over de kwaliteit van de informatiebeveiliging maar heeft als doelstelling inzicht te krijgen in de wijze waarop het college van B&W een organisatie heeft ingericht, medewerkers heeft betrokken en technische en/of procedurele maatregelen heeft getroffen reeds, als onderdeel van de Planning & Control cyclus, ingerichte verantwoordingen en uitgevoerde audits. Oftewel de mate waarin de gemeente beschikt over een ingerichte organisatie voor het realiseren en het indien nodig aanpassen (meebewegen) van informatieveiligheid en tegelijkertijd het kunnen voldoen aan (in ieder geval) de BIO en de AVG. Door de rekenkamercommissie is Secura verzocht het onderzoek verder op te delen in een aantal relevante vragen en sub-vragen die een meer gedetailleerd antwoord geven op de centrale onderzoeksvraag.

Deze rapportage geeft de uitkomsten van dit onderzoek verricht door Secura in de periode van 15 juli 2021 tot en met 17 september 2021.

1.2. Aanpak

De gekozen aanpak voor de gemeente Velsen is tweeledig.

- Fase 1: Informatiebeveiliging en privacybescherming in de P&C-Cyclus, waarin de beleidsmatige en procedurele aspecten van informatiebeveiliging en privacybescherming zijn ondergebracht
- Fase 2: Operationele informatiebeveiliging en privacybescherming, waarin de maatregelen implementatie en monitoring/opvolging hiervan zijn ondergebracht

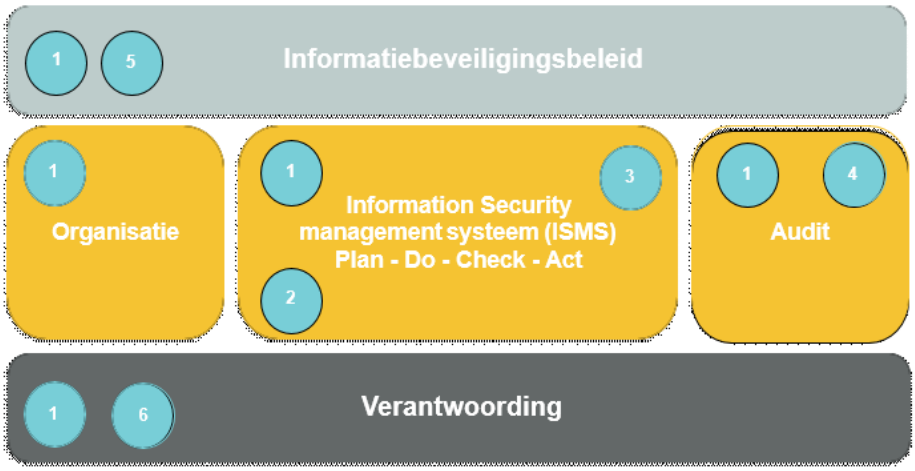
Fase 1: Informatiebeveiliging en privacybescherming in de P&C-Cyclus.

Omdat de verantwoordelijkheid voor het ontwerpen, inregelen en monitoren van een voldoende niveau van informatiebeveiliging en volgens de wet- en regelgeving beveiliging van de verwerking van persoonsgegevens bij het College van B en W ligt, stellen wij in fase 1 vast op welke wijze digitale informatiebeveiliging en privacybescherming is meegenomen in de Planning & Control cyclus van de gemeente. De BIO (Baseline Informatiebeveiliging Overheid) zullen wij hierbij als uitgangspunt hanteren. Dit onderzoek is grotendeels gebaseerd op documentatiereview en een beperkt aantal interviews, waarin de hiervoor genoemde onderzoeksvragen worden meegenomen:

1. Is er beleid vastgesteld voor informatiebeveiliging en privacybescherming?
2. Heeft de gemeente de risico's op informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie in beeld of benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?
3. Wordt het beleid adequaat uitgevoerd en wordt het gemonitord?

4. Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of penetratietesten?
5. Is de gemeente aangesloten en maakt zij gebruik van de diensten en producten van de Informatiebeveiligingsdienst (IBD)?
6. Hoe wordt het college van B&W en de gemeenteraad geïnformeerd over informatiebeveiliging en privacybescherming?

In het onderstaande P&C-cyclus overzicht zijn de Fase 1 deelvragen in onderlinge samenhang weergegeven.



Figuur 1: Onderzoeksgebieden en onderwerpen

Fase 2: Operationele informatiebeveiliging en privacybescherming.

In deze fase stellen wij daarna vast hoe het beleid is vertaald naar operationele informatiebeveiligingsmaatregelen en privacybeschermende maatregelen. Daarbij onderzoeken wij de ingerichte monitoring en controle processen en tenslotte de opvolging en eventuele aanpassingen ter verbetering:

7. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers op het gebied van informatiebeveiliging en privacy?
8. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van een informatiebeveiligingsincident en hoe is dat geregeld?
9. Is het mogelijk oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Velsen in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?
10. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?
11. Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?

Binnen het onderzoek is afgesproken dat geen technische testen plaatsvinden maar de onderzoeker wel degelijk inventariseert welke maatregelen de gemeente zelf heeft genomen, of door anderen en welke informatie over de kwaliteit van de inrichting daarvan al voorhanden is. Vanuit de bevindingen en aanbevelingen zal, indien relevant, een voorstel worden gedaan voor meer gerichte technische testen. Indien relevant hebben wij bij het onderzoek gevraagd om bewijsstukken die antwoorden en uitspraken staven. Ons onderzoek hebben wij uitgevoerd aan de hand van interviews met sleutelfunctionarissen

(waarbij de interviews middels een verslag zijn teruggekoppeld aan de respondenten), de analyse van diverse beschikbare audit rapporten en opvolging van de bevindingen opgenomen in die rapporten, het bestuderen van de diverse interne verantwoordingen en daarop gegeven opvolging en diverse vastlegging rond en in de beheerprocessen. Eventuele latere (vervolg) technische testen kunnen gerichter en efficiënter worden uitgevoerd naar aanleiding van de uitkomsten van dit onderzoek.

1.3. Bevindingen op hoofdlijnen

Vanuit de vraagstelling en de informatiebeveiligingsmodellen, die we hanteren in dit onderzoek (zie verderop in dit rapport) voor het inzicht in de huidige status van informatiebeveiliging en privacy concluderen we dat, ondanks dat de gemeente Velsen al veel heeft gedaan op dit vlak, informatiebeveiliging en privacy op een aantal fundamentele onderdelen nog onvoldoende is geborgd. De gemeente Velsen heeft nog veel werk heeft te verrichten, een aantal fundamentele en belangrijke bevindingen dienen daarbij op korte termijn te worden opgepakt.

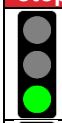
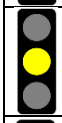
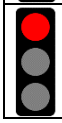
De belangrijkste bevindingen betreffen:

- Het ontbreken van een actueel en getest uitwijkplan voor de BRP-applicatie en andere bedrijf kritische applicaties.
- Het back-up proces wat op dit moment niet volledig bestand is tegen ransomware aanvallen
- Er is nog niet voor alle bedrijf kritische applicaties een diepgaande privacy impact analyse (DPIA) uitgevoerd.
- Het informatiebeveiligingsbewustzijnsniveau van de medewerkers van de gemeente Velsen is laag.
- Scenario's ontbreken vooralsnog voor de aanpak van de (op dit moment) meest voorkomende informatiebeveiligingsincidenten, zoals phishing mails, ransomware en gecompromitteerde wachtwoorden.

Wij bevelen aan om daar zo snel mogelijk mee te starten. Gezien de hoeveelheid verbeteringen is het daarnaast aan te bevelen om elk half jaar een herijking te doen van de status en voortgang van de verbeterpunten. Hierdoor ontstaat tevens de mogelijkheid om adequaat te kunnen reageren op actuele situaties en deze in de verbeteractiviteiten te verwerken.

1.4. Aanbevelingen en prioriteiten

In de vorige paragraaf hebben wij beschreven wat de belangrijkste bevindingen zijn uit het onderzoek bij de gemeente Velsen zoals deze bijdragen aan het uiteindelijk kunnen beantwoorden van de centrale onderzoeksvraag. Deze bevindingen zijn per onderzoeksvraag verderop in het rapport in detail uitgeschreven. Hierbij wordt gebruik gemaakt van het stoplichtmodel om de status van het betreffende onderwerp aan te geven. Daarbij zijn de volgende definities toegepast.

Stoplicht	Betekenis
	Het onderwerp is op orde, volledig in control.
	Het onderwerp is gedeeltelijk op orde, maar verdient nog enige aandacht.
	Het onderwerp ontbreekt en verdient ruime aandacht.

Voor de belangrijkste bevindingen, die zijn gekenmerkt door een rood stoplicht, zijn hierna de aanbevelingen en prioriteiten vermeld. Ten aanzien van de belangrijkste aanbevelingen zijn de volgende definities aangehouden:

Prioriteit	Betekenis
Hoog	Het verdient aanbeveling om hier direct mee te starten, zodat het uiterlijk binnen 6 maanden is opgelost.
Gemiddeld	Het verdient aanbeveling om hier mee te starten, zodat het uiterlijk binnen 6 tot 12 maanden is opgelost.
Laag	Het verdient aanbeveling om hier mee te starten, zodat het uiterlijk binnen 24 maanden is opgelost.

Voor de bevindingen en verbeteringen die gedeeltelijk op orde zijn, verwijzen we voor de details naar de volgende hoofdstukken in het rapport.

Allereerst de aanbevelingen met hoge prioriteit

1. Privacy Officer/FG: start met het completeren van de belangrijkste onderdelen die in het privacy/AVG-jaarplan zijn vermeld, waaronder met name het DPIA-proces, maar ook andere maatregelen kunnen worden opgestart.

2. CISO/ Privacy Officer: Continueer de bewustwordingscampagne in een minder vrijblijvende opzet, zodat de medewerkers van de gemeente Velsen ook in de huidige manier van (thuis-) werken up-to-date blijven van informatiebeveiliging, Privacy/AVG en de bijbehorende gevaren.

3. Contract-/servicemanager/CISO: Stem de punten af die zijn opgenomen in het re-transitie document, met name de back-up afspraken en inrichting op korte termijn, waaronder de beschermingsmaatregelen tegen mogelijke ransomware aanvallen. Zorg tevens dat alle relevante informatiebeveiligingsonderwerpen in de servicelevel rapportage worden opgenomen.

4. CISO/Eigenaren: Opstellen uitwijkplan voor BRP en andere belangrijke, bedrijf kritische applicaties en daarnaast voor (minstens) BRP de uitwijk test daadwerkelijk uitvoeren, evalueren en verbeteringen doorvoeren.

5. CISO/OGD: Opstellen scenario's, in overleg met OGD, hoe om te gaan met de meest voorkomende, meest impact hebbende beveiligingsincidenten indien deze optreden. Mogelijke voorbeelden kunnen zijn phishing mail, ransomware mail, blokkering web-diensten (DDOS-aanval), gecompromitteerd wachtwoord.

Aanbevelingen met gemiddelde prioriteit

6. CISO/Management: Zorg tevens dat de verbeteringen die in het informatiebeveiligingsjaarplan zijn opgenomen, daadwerkelijk worden uitgevoerd en neem controlemaatregelen hierin op zodat ze kunnen worden bewaakt door de CISO-functie.

7. CISO: Aanvulling van het beleid op tactische en operationeel niveau, zodat de gedefinieerde beleidsuitgangspunten kunnen worden uitgewerkt in praktische maatregelen en kunnen worden bewaakt en gemonitord. De keuze om standaard voor SaaS/Cloud applicaties te kiezen en/of het gebruik van BYOD-apparaten zijn enkele voorbeelden, waarvoor een beleid kan helpen in standaardisatie. Verder kan worden gedacht aan beleid over, het gebruik van sociale media,

mobiele apparatuur, leveranciers voorwaarden en rapportages en tenslotte een breder wachtwoord (of authenticatie) beleid, waarin is vastgelegd, wat de minimumvoorwaarden zijn om toegang te krijgen vanaf het Internet, het interne netwerk, vanuit thuis etc.

8. CISO: Afstemming omtrent de definities, registratie, afhandeling en rapportage ten aanzien van informatiebeveiligingsincidenten, en de vastlegging van de taken en verantwoordelijkheden wie welke activiteiten uitvoert (OGD of gemeente Velsen) ten aanzien van informatiebeveiligingsincidenten beheer.

9. CISO/Management: Opstellen escalatie en crisisbeleid en uitwerken van de bijbehorende procedures, waarna in overleg met OGD wordt afgestemd, welke stappen worden doorlopen en met name wie welke taken en verantwoordelijkheden in dit proces krijgt toebedeeld.

10. CISO/Contractmanager: Opstellen randvoorwaarden voor de toegangscontrolemaatregelen (waaronder multi-factor authenticatie) noodzakelijk voor de via het Internet beschikbaar gestelde systemen en applicaties van de gemeente Velsen en opstarten configuratie aanpassingen aan die systemen en applicaties die daar niet aan voldoen.

<u>Aanbevelingen met lagere prioriteit</u>

11. Het Management/Proceseigenaren/CISO: Richt een risicomanagementproces in voor het identificeren, analyseren en evalueren van risico's en voor het bepalen van de risicohouding: accepteren of maatregelen treffen. Dit dient een continu proces te zijn. Maak hierbij o.a. gebruik van de best practices van de IBD en andere gemeenten, zodat de minimumeisen (BBN) vanuit de BIO (Basis Beveiliging Niveau) zijn vastgesteld. Leg daarbij de risico afwegingen vast, voor latere referenties.

12. CISO/Eigenaren: Opstellen continuïteitseisen voor (minimaal) de belangrijke, bedrijf kritische applicaties en daarnaast onderzoeken in overleg met OGD welke verbeteringen wanneer doorgevoerd kunnen/moeten worden en in een implementatieplan vastleggen.

13. CISO/Management: Stel een meer jarenplan op, waarin beschreven wanneer welke escalatie/crisis situaties worden geoefend. Daarnaast voer de oefening uit volgens plan zodat de opgestelde escalatie en crisis procedures in de praktijk worden getoetst, waarna via de evaluatie eventuele verbeteringen kunnen worden doorgevoerd.

2. INLEIDING

2.1. Informatieveiligheid en gemeenten

Informatieveiligheid en het voldoen aan de eisen van de AVG (Algemene Verordening Gegevensverwerking) staan hoog op de agenda van gemeenten. Gemeenten hebben een groot aantal wettelijke taken te verrichten waar enerzijds in toenemende mate automatisering bij wordt ingezet en anderzijds veel gegevens van burgers worden verwerkt. Automatisering helpt gemeenten om hun dienstverlening efficiënt en effectief in te richten.

De verregaande digitalisering van de informatie introduceert nieuwe bedreigingen dat deze informatie niet betrouwbaar blijkt, niet op het juiste moment beschikbaar is en toegankelijk is voor onbevoegde gebruikers. Om de informatie betrouwbaar, beschikbaar en exclusief te krijgen zijn specifieke informatiebeveiligingsmaatregelen noodzakelijk. Net als in voorgaande jaren heeft de IBD (Informatiebeveiligingsdienst), als de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten, een onderzoek gedaan naar het 'Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2021/2022[1]'. Het risicobeeld dat de IBD heeft samengesteld op basis van dit onderzoek stelt bestuurders in staat om in afstemming met de gemeenteraad, het management en de informatiebeveiligers prioriteiten te stellen en bewust risico's te mitigeren of juist te nemen. Daarbij levert het dreigingsbeeld inzichten voor het opstellen van een strategie en aanpak van informatiebeveiliging:

Vanuit Ambtelijke Organisatie
1. Bedrijfscontinuïteit in het geding;
2. Integriteit van gegevens is niet gewaarborgd;
3. Vertrouwelijke gegevens in verkeerde handen;

Vanuit openbaar bestuur en politiek
4. Imagoschade;
5. Financiële schade;
6. Schade aan democratische processen;

Vanuit inwoners en ondernemers
7. Gegevens in verkeerde handen;
8. Dienstverlening van de gemeente niet beschikbaar;
9. Ontwrichting van alledaagse processen;

De impact van een beveiligingsincident kan heel groot zijn. Gemeenten werken met persoonlijke en vertrouwelijke gegevens en zijn sterk afhankelijkheid voor hun dienstverlening van geautomatiseerde systemen. Als deze niet betrouwbaar werken, of uitvallen, dan heeft dat direct effect op de kwaliteit van de dienstverlening aan burgers, bedrijven en andere organisaties en dat raakt het maatschappelijk verkeer. Los van het feit dat het maatschappelijk verkeer van de overheid, en dus ook gemeenten, verwacht dat zij een voorbeeldfunctie is voor hoe veilig om te gaan met gegevens van haar burgers, introduceert de AVG ook een zwaardere boeteregeling bij het niet naleven van de AVG. Beveiligingsincidenten kunnen daardoor ook leiden tot forse financiële boetes.

Wat beveiligingsonderzoeken en recente beveiligingsincidenten (zoals het data lek bij de GGD en KvK en de aanvallen bij VDL en de MediaMarkt) ons leren is dat het nagenoeg onmogelijk is een organisatie

[1] "Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2021/2022"; IBD; 2021

100% te beveiligen tegen de steeds maar toenemende en ook veranderende bedreigingen, of dat door omstandigheden (zoals tijdsdruk of beperkte capaciteit) onvoldoende aandacht aan de juiste beveiliging wordt besteed. Het inrichten van informatiebeveiliging betekent derhalve keuzes maken en ook accepteren dat zich incidenten kunnen voordoen. Daarmee is het van het grootste belang inzicht te hebben in de (ontwikkeling van) de risico's en processen te hebben ingericht die waarborgen dat tijdig de juiste actie op een eventueel incident wordt genomen.

2.2. Informatiebeveiliging handvatten

De rijksoverheid en de VNG zien het belang van een goed niveau van informatiebeveiliging bij gemeenten. Daarvoor zijn al diverse gezamenlijke initiatieven genomen. De al genoemde IBD is daarbij een belangrijk initiatief en als collectieve voorziening in 2013 opgericht door en voor alle Nederlandse gemeenten, om hen te ondersteunen bij het verbeteren van de informatiebeveiliging. De IBD is ook actief met het signaleren van (nieuwe) bedreigingen en het geven van adviezen over hoe deze het hoofd te bieden. De gemeente Velsen maakt ook gebruik van deze dienst.

Het belangrijkste initiatief vanuit de IBD betreft de ontwikkeling van de Baseline Informatiebeveiliging Overheid (BIO). De IBD heeft ter ondersteuning van de implementatie van informatiebeveiliging aan de hand van de BIO een groot aantal operationele producten ontwikkeld en beschikbaar gemaakt voor de gemeenten. Dit zijn zeer praktische handvatten die gemeenten helpen bij het snel op orde brengen en houden van informatiebeveiliging.

De laatste versie van de BIO is al weer van enige tijd geleden (versie 1.04). De introductie heeft ook impact gehad op een ander initiatief in de gemeentesector: ENSIA (Eenduidige Normatiek Single Information Audit). Deze had tot doel om in de plaats van de vele audits die, uit hoofde van wet- en regelgeving, jaarlijks moeten plaatsvinden bij gemeenten één alomvattende audit te laten verrichten. ENSIA is ingegaan per 2017. Een belangrijk facet van ENSIA is dat deze benadrukt dat de verantwoordelijkheid voor een voldoende beveiligingsniveau nadrukkelijk bij de gemeenten zelf ligt. Dit is kracht bij gezet door het college zich jaarlijks, met een 'In Control' verklaring, zich te laten verantwoorden over het niveau van informatiebeveiliging. Deze verantwoording is dan het object van onderzoek voor de 'ENSIA-audit' geworden middels een onafhankelijke en deskundige auditor.

Het college van de gemeente Velsen heeft ook zo'n 'In Control' verklaring in de vorm van een Collegeverklaring afgegeven over de DigiD aansluiting en Suwinet en door een (ENSIA) auditor laten toetsen. Voor andere diensten (Bag, BGT, BRP, BRP, Reisdocumenten, WOZ en de algehele BIO) wordt verantwoording afgelegd middels verantwoordingsrapportages, gebaseerd op zelfevaluaties. Voor de BIO wordt de verantwoordingsrapportage naar de gemeenteraad gestuurd. Met de opstart van de BIO is het minimumniveau (het BBN) geïntroduceerd. Het is raadzaam voor gemeenten inzicht te krijgen en te houden in hun status informatiebeveiliging volgens de BIO om aantoonbaar te voldoen aan het van toepassing zijnde BBN:

1. Bepalen van het BBN (Basis beveiligingsniveau);
2. Uitvoeren van een Fit Gap analyse;
3. Uitvoeren van een nulmeting (het onderzoek naar het daadwerkelijk geïmplementeerd zijn van maatregelen).

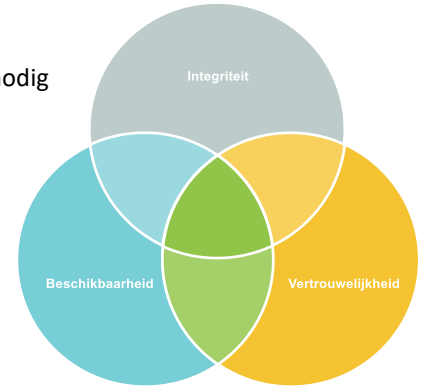
De BIO-gapanalyse (nulmeting) geeft een goed handvat voor het jaarlijks vaststellen van de te realiseren verbeterpunten en het bewaken van de opvolging daarvan, zodat de collegeverklaring over de status van informatiebeveiliging eenvoudig is op te stellen en te onderbouwen. Privacy-controles en –maatregelen vanuit het ISO27002 normenkader zijn daar eveneens in opgenomen.

2.3. Aspecten informatiebeveiliging

Samenvattend betekent dit dat gemeenten alert moeten zijn, de juiste prioriteiten moeten stellen en naast preventieve maatregelen ook zich hebben voorbereid op het snel en adequaat kunnen opvolgen van beveiligingsincidenten. Het management, het college en de raad moeten daarin een voorbeeldfunctie vertolken en de trekker- en sturende rol vervullen.

Vanuit de BIO als sectorspecifieke implementatie handvat voor informatiebeveiliging zijn 3 kwaliteitscriteria gedefinieerd (conform ISO 27001 normen) die relevant zijn, vaak afgekort als 'BIV'. Samengevat:

- *Beschikbaarheid*: de mate waarin een informatiesysteem in een organisatie aanwezig is op het moment dat de organisatie deze nodig heeft;
- *Integriteit (of betrouwbaarheid)*: de mate waarin informatie juist volledig en actueel is.
- *Vertrouwelijkheid (of exclusiviteit)*: de mate waarin de toegang tot, en de kennisname van, een informatiesysteem en de informatie daarin is beperkt tot een gedefinieerde groep gerechtigden;

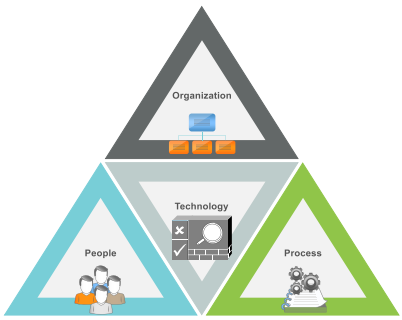


Figuur 2: Kwaliteitscriteria

Informatiebeveiliging is dan het treffen en onderhouden van een samenhangend stelsel van maatregelen om deze kwaliteitsaspecten van de informatievoorziening te garanderen.

Bij het realiseren van voldoende informatieveiligheid door het treffen van informatiebeveiligingsmaatregelen komen verschillende aspecten naar voren die in hun onderlinge samenhang bepalen wat de effectiviteit van die informatiebeveiliging is. Bijvoorbeeld het signaleren van potentiële datalekken vergt dat er technische maatregelen zijn om bijzonder gedrag of dataverkeer signaleert en filter, in de organisatie verbijzonderde functies bestaan die als taak hebben de signalering op te volgen volgens een standaard proces met benodigde vastleggingen. De uitvoerende medewerker zal zich bewust moeten zijn van de relevantie van de signalen en de mogelijke impact die dat kan hebben op de gemeente en zorgvuldig en alert handelen.

Wij vatten deze aspecten samen als het PPOT-model. PPOT staat voor de aspecten:



Figuur 3: Aspecten informatiebeveiliging

People: De mensfactor is zeer bepalend voor het realiseren van informatiebeveiliging omdat die vaak is betrokken bij de gegevensverwerking en een rol speelt bij het uitvoeren van beveiligingsmaatregelen.

Process: Het standaardiseren van processen en daarin verbijzonderen van beveiligingsmaatregelen geeft een grotere zekerheid over het daadwerkelijk op de juiste wijze toepassen en uitvoeren van beveiligingsmaatregelen.

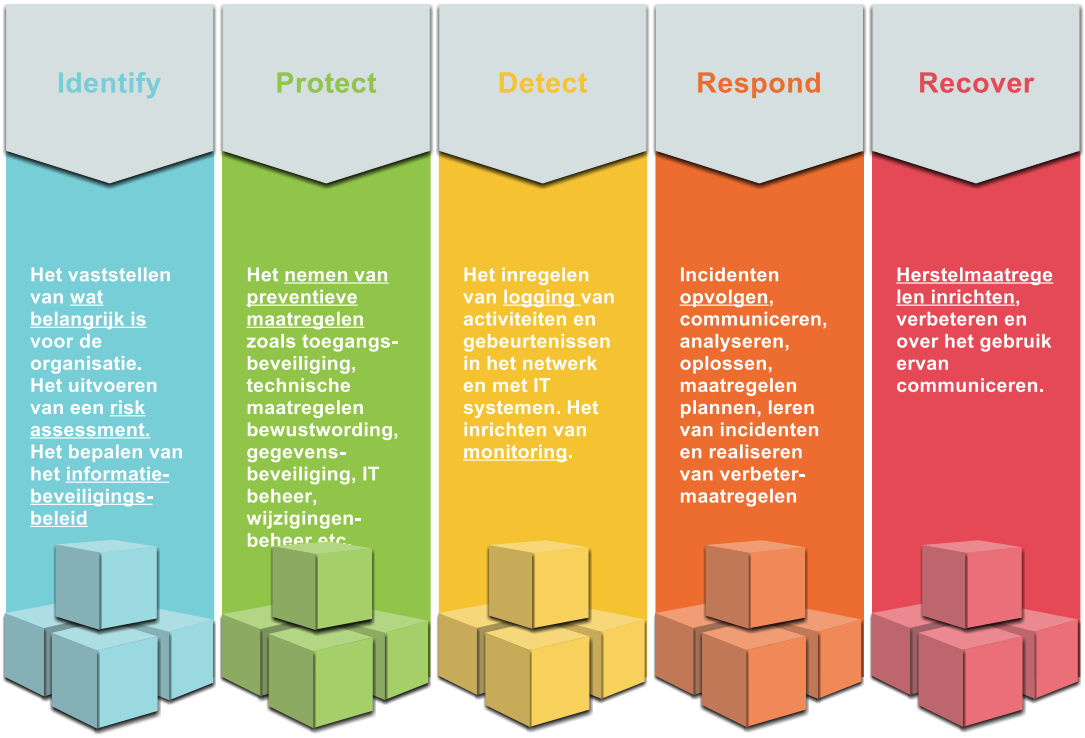
Organization: Delegatie van bevoegdheden (waaronder het realiseren van beveiliging technische functiescheidingen) en met expliciete aandacht voor de bevoegdheden en verantwoordelijkheden rond de gegevensverwerking en beveiligingsfuncties

Technology: Technische maatregelen gericht op het beveiligen van de informatiesystemen, de communicatie en de data die in de informatiesystemen is opgenomen.

Voor de uitvoering van beveiligingsprocedures, zoals bijvoorbeeld het opvoeren van (nieuwe) gebruikers in een systeem, dient duidelijk te zijn wie deze mogen/moeten uitvoeren, op basis van welke standaardprocedure dit dient te gebeuren, de techniek ervoor zorgt dat de bevoegdheden goed kunnen worden ingeregeld en de betrokken medewerkers de juiste handelingen doen en zich bewust zijn van het belang en de impact daarvan. Als één van deze aspecten tekortkomingen kent dan kan het bijvoorbeeld gebeuren dat onterecht een gebruiker in het systeem wordt aangemaakt of niet de juiste rechten krijgt.

De praktijk wijst uit dat het onmogelijk is alle beveiligingsincidenten uit te bannen. Het is steeds belangrijker te zijn voorbereid op eventuele incidenten. Dit vergt een alerte en voorbereide organisatie.

Vrij vertaald op basis van het 'NIST Cybersecurity Framework' kan daar het volgende onderscheid in maatregelen voor worden gehanteerd:



Figuur 4: Alerte organisatie op cybersecurity (vrij vertaald van NIST Cybersecurity framework v 1.1)

Vorenstaande aandachtsgebieden en beveiligingsraamwerken zijn in onze onderzoekaanpak verweven.

2.4. Leeswijzer

In hoofdstuk 1 hebben wij een samenvatting van de uitkomsten van de beide fases van het onderzoek weergegeven. Voor een toelichting op informatieveiligheidsaspecten bij de gemeente Velsen en de uitgangspunten voor het realiseren van informatiebeveiligingsmaatregelen hebben wij ter inleiding van de beantwoording van de vragen hoofdstuk 2 gebruikt. De opdracht waarmee wij aan de slag zijn gegaan en de daarbij gevolgde aanpak is toegelicht in hoofdstuk 3.

In het daar opvolgende hoofdstuk 4 behandelen wij per paragraaf een onderzoeksvraag die in een aantal situaties tevens een verdieping is van de in hoofdstuk 1 opgenomen bevindingen. Per onderzoeksvraag is een toelichting gegeven van de huidige invulling, aangevuld met de bevindingen en samenvattende voorstellen ter verbetering (indien relevant gekoppeld aan het PPOT-model).

In de bijlagen hebben wij tenslotte een overzicht van de geïnterviewde functionarissen en de, voor de beantwoording van de vragen, meest relevante bewijsstukken opgenomen, waar in dit rapport naar wordt verwezen.

3. UITVOERING OPDRACHT

3.1. Centrale onderzoeksvraag

De Rekenkamercommissie van de gemeente Velsen wil graag inzicht krijgen in de wijze waarop de gemeente omgaat met informatiebeveiliging. Zij heeft hiervoor een opdracht gegeven aan Secura B.V. om onderzoek te doen naar de status van de informatiebeveiliging en hoe de gemeente daarmee omgaan. Voor dat onderzoek dient Secura B.V. zich te baseren, naast het houden van interviews met betrokkenen en verantwoordelijken, op de reeds voorhanden documentatie en uitgevoerde technische en overige onderzoeken bij de gemeente. Het betreft onderzoeksvragen die niet zijn gericht op het krijgen van een oordeel met enige mate van zekerheid maar om inzichtelijk te krijgen wat de belangrijkste aandachtspunten zijn bij de gemeente en op welke wijze de gemeente grip houdt op informatiebeveiliging en in staat is daar alert in te acteren.

De centrale onderzoeksvraag in het onderzoek is:

"Is de informatiebeveiliging en privacybescherming bij de gemeente Velsen voldoende georganiseerd en geborgd?"

Voor het onderzoek is deze hoofdvraag uitgewerkt in de volgende deelvragen:

1. Is er beleid vastgesteld voor informatiebeveiliging en privacybescherming?
2. Heeft de gemeente de risico's op informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie in beeld of benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?
3. Wordt het beleid adequaat uitgevoerd en wordt het gemonitord?
4. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers op het gebied van informatiebeveiliging en privacy?
5. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van een informatiebeveiligingsincident en hoe is dat geregeld?
6. Is het mogelijk oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Velsen in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?
7. Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of penetratietesten?
8. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?
9. Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?
10. Is de gemeente aangesloten en maakt zij gebruik van de diensten en producten van de Informatiebeveiligingsdienst (IBD)?
11. Hoe wordt het college van B&W en de gemeenteraad geïnformeerd over informatiebeveiliging en privacybescherming?

De uitvoering en de resultaten van dit onderzoek hebben als doelstelling inzicht te verschaffen in de wijze waarop het college van B&W een organisatie heeft ingericht, medewerkers heeft betrokken en technische en/of procedurele maatregelen heeft getroffen reeds, als onderdeel van de Planning & Control cyclus, ingerichte verantwoordingen en uitgevoerde audits en in de operationele processen. Oftewel de mate waarin de gemeente nu beschikt over een ingerichte organisatie voor het realiseren en waar nodig aan te passen en te verbeteren van informatieveiligheid en het kunnen voldoen aan de AVG.

Ter beantwoording van de vragen zijn interviews gehouden met medewerkers van de gemeente Velsen en voor ICT technische ondersteuning vanuit OGD.

3.2. Uitgevoerde werkzaamheden

In ons onderzoek hebben wij de voorgestelde aanpak gevolgd. Bij aanvang hebben wij, ten behoeve van het soepel verlopen van de audit en op verzoek van de betrokkenen, een bijdrage geleverd aan het juist informeren van de betrokkenen over het doel en de aanpak van het onderzoek. Op hoofdlijnen hebben wij de volgende werkzaamheden verricht:

1. Voorbereiding en kick-off;
2. Interviews betrokkenen;
3. Analyse documentatie (beleid, risicomanagement, audits, verslagen, opvolging, etc.);
4. Rapportage.

Stap 1: Voorbereiding en kick-off
In de voorbereidende fase hebben wij een lijst opgesteld van gewenste/verwachte documenten en initieel geanalyseerd op aandachtspunten en het verkrijgen van een eerste beeld met:

- Het huidige informatiebeveiligingsbeleid van de gemeente;
- De verantwoording over informatiebeveiliging;
- De laatste op raad en collegeniveau behandelde stukken rond informatiebeveiliging;
- De huidige (organisatorische) inrichting van de informatiebeveiliging en het informatielandschap opgevraagd en doorgenomen.

Hiermee kregen wij een initieel inzicht in de wijze waarop de gemeente omgaat met informatiebeveiliging en de verwerkingen van persoonsgegevens conform de komende regelgeving AVG. Vervolgens hebben wij bepaald welke functionarissen wij in ons onderzoek wilden interviewen. Aangezien de gemeente Velsen een deel van de ICT-dienstverlening heeft uitbesteed aan OGD hebben wij ook functionarissen van deze organisatie geïnterviewd.

Voordat de interviews werden uitgevoerd is met de stakeholders een kick-off sessie gehouden om de grond van het onderzoek en de aanpak toe te lichten.

Stap 2: Interviews betrokkenen
In de voorbereidende fase hebben wij een lijst opgesteld van functionarissen waarvan verwacht wordt dat zij een bijdrage kunnen leveren aan het beantwoorden van de vragen uit het onderzoek.

Functionaris
CISO / Security Officer / ENSIA coordinator
Privacy Officer
Functionaris Gegevensbescherming / Interne auditor
Contract/Service Level Manager
Gemeentesecretaris
Portefeuillehouder
ICT Dienstverlening OGD
Security Officer OGD
Hoofd Informatie

Functioneel Applicatiebeheer HR applicaties
Functioneel Applicatiebeheer Samenleving applicaties
Functioneel Applicatiebeheer Financiën/Treasury applicaties
Projectleider bedrijfsvoering

Door de interviews te houden is inzicht verkregen in de rollen, taken, activiteiten en processen van de geïnterviewde functionarissen, met focus op antwoorden verzamelen op de eerder gestelde vragen. Waar relevant en mogelijk is documentatie (bewijs) daarvan opgevraagd en is tijdens de interviews inzicht verkregen in systemen en tools/registraties.

Stap 3 Analyse documentatie (beleid, risicomanagement, audits, verslagen, opvolging, etc.);
In deze stap hebben wij kennisgenomen van de diverse beleidsstukken ten aanzien van informatiebeveiliging en privacy en andere documenten.

De plaats van risicomanagement (betreffende informatieveiligheid) binnen de gemeente Velsen. Voor het vaststellen van de inhoudelijk uitgevoerde risicoanalyses door de gemeente Velsen hebben wij onder andere gebruik gemaakt van de BIO/ENSIA-nulmeting uitgevoerd door de CISO van de gemeente Velsen, de basis voor het verbetertraject/jaarplan en interviews met de CISO. Aan de hand hiervan is een indruk verkregen over de wijze waarop de gemeente omgaat met veranderingen in de risico's. Ook hebben wij kennisgenomen van de ontvangen auditrapportages van de gemeente Velsen. De belangrijkste bevindingen en de opvolging daarvan door de gemeente hebben wij geanalyseerd.

Ten aanzien van de opvolging hebben wij kennisgenomen van de verantwoordingsrapportages van de Security Officer (CISO) en de wijze waarop de verantwoording over de voortgang van het AVG-compliant worden plaatsvindt via de Privacy Officer en de FG. Hierin hebben wij ook aandacht geschonken aan de wijze van opvolgen van de bevindingen uit de diverse audits waaronder de Suwinet audit en de Digid assessment.

Stap 4: Rapportage
Bovenstaande werkzaamheden zijn uitgevoerd in de periode van 15 juli 2021 tot en met 17 september 2021, inclusief de periode van het ontvangen van nagestuurde bewijsstukken.

Het onderzoek hebben wij afgerond met deze rapportage waarbij wij de relevante uitkomsten van het onderzoek per onderzoeksvraag samenvatten. Voor de relevante bevindingen houden wij aandacht voor de onderscheiden aspecten van PPOT voor het kunnen realiseren van effectieve informatiebeveiliging.

4. UITWERKING ONDERZOEK IN DEELVRAGEN

4.1. Inleiding

Zoals aangegeven is, voor het onderzoek, de centrale onderzoeksvraag uitgewerkt in 11 deelvragen in de onderzoeksopzet van de rekenkamercommissie [1]. Aan de hand van deze deelvragen hebben wij de beide fases van het onderzoek verricht en de bevindingen verzameld. Het betreft de volgende 11 vragen, onderverdeeld in de eerdergenoemde 2 fases (P&C-Cyclus en Operationeel).

Fase 1: P&C-Cyclus

1. Is er beleid vastgesteld voor informatiebeveiliging en privacybescherming?
2. Heeft de gemeente de risico's op informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie in beeld of benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?
3. Wordt het beleid adequaat uitgevoerd en wordt het gemonitord?
4. Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of penetratietesten?
5. Is de gemeente aangesloten en maakt zij gebruik van de diensten en producten van de Informatiebeveiligingsdienst (IBD)?
6. Hoe wordt het college van B&W en de gemeenteraad geïnformeerd over informatiebeveiliging en privacybescherming?

Fase 2: Operationeel:

7. Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers op het gebied van informatiebeveiliging en privacy?
8. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van een informatiebeveiligingsincident en hoe is dat geregeld?
9. Is het mogelijk oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Velsen in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?
10. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?
11. Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?

Let op: Tijdens de kick-off is afgesproken om een status update ten aanzien van de implementatie van AVG/Privacy als vraag toe te voegen. Deze is als vraag 7 aan fase 1 (P&C Cyclus) toegevoegd, waardoor het totale aantal vragen op 12 uitkomt.

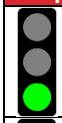
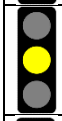
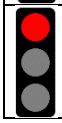
Ons onderzoek hebben wij uitgevoerd aan de hand van interviews met sleutelfunctionarissen, de analyse van documenten, inzicht in systemen, processen, verslagen, beleidsstukken en diverse beschikbare audit rapporten en opvolging, het bestuderen van de diverse interne verantwoordingen en daarop gegeven opvolging en diverse vastlegging rond en in de beheerprocessen.

In de navolgende paragrafen beschrijven wij de uitgevoerde werkzaamheden en de resultaten per fase en daarbinnen per onderscheiden deelvraag, bestaande uit:

- Een samenvatting van de interview(s) per deelvraag
- Bevindingen en eventuele aandachtspunten (met aanbevelingen) worden vermeld.
- Via het stoplichtmodel wordt de status van het betreffende aandachtspunt weergegeven.
- Prioriteiten worden bij de aanbevelingen toegelicht.

- Tussen haakjes “[..]” wordt verwezen naar de relevante aanbevelingen en prioriteiten uit hoofdstuk 1.
- Indien geclassificeerd middels een rood stoplicht zijn de aanbevelingen met prioriteit in hoofdstuk 1 opgenomen.
- Indien geclassificeerd middels een geel stoplicht, zijn de aanbevelingen eveneens gekoppeld aan de prioriteit, waarvoor de verbetering direct bijdraagt in de vorm van een verdieping van of aanvulling op een belangrijke bevinding.

Tenslotte is het mogelijk dat een voorstel wordt gedaan voor een verbetering, waarbij deze echter niet is voortgekomen uit een bevinding of omissie in de informatiebeveiliging, maar bijvoorbeeld kan bijdragen aan een efficiënter uitvoeren van een proces. Dit wordt dan als zodanig vermeld en uiteraard niet voorzien van een stoplicht.

Stoplicht	Betekenis
	Het onderwerp is op orde, volledig in control.
	Het onderwerp is gedeeltelijk op orde, maar verdient nog enige aandacht.
	Het onderwerp ontbreekt en verdient ruime aandacht.

4.2. Fase 1: P&C-Cyclus deelvragen

Een aantal deelvragen zijn het fundament van informatiebeveiliging en privacy. In deze paragraaf worden deze deelvragen uitgeschreven met de bijbehorende bevindingen en tevens worden voorstellen tot verbetering vermeld voorzien van een prioriteitsindicatie.

4.2.1. Is er beleid vastgesteld voor informatiebeveiliging en privacybescherming?

De volledige vraag:

"Is er beleid vastgesteld voor informatiebeveiliging en privacybescherming?"

In het onderzoek zijn wij bij deze deelvraag uitgegaan van de algemene visie van de gemeente Velsen, het daarvan afgeleide informatiebeveiligingsbeleid en het gelieerde privacy beleid. Verder wordt hier de organisatie onderzocht op de invulling van de informatiebeveiliging en privacy functies en wordt tenslotte gekeken naar de volledigheid van het beleid.

4.2.1.1. *Toelichting*

Algemene visie en beleid
Strategische beslissingen worden afgeleid van diverse beleidsdocumenten, visiedocumenten, informatieplannen, die door de specialisten worden opgesteld. De rode draad daarbij is samengevat als bij de tijd blijven, maar niet per sé vooroplopen, maar vooral een "slimme volger" zijn, wat overigens door veel gemeenten wordt gedaan.

Er is een uitbestedingsstrategie over de ICT van de gemeente Velsen opgesteld, en door het College goedgekeurd. Voor de uitbesteding van het ICT-beheer is recent een aanbestedingsproces afgerond en de opdracht uiteindelijk aan OGD gegund. In de nabije toekomst zal bij vervanging van applicaties steeds verder gemigreerd worden naar het rekencentrum van OGD. Tussentijds (komende 2 jaar) zal ook meer naar Saas/Cloud Diensten worden overgeschakeld om kostenstijging te voorkomen. Uitgangspunten die gebruikt worden bij (uitbestedings-) projecten bestaan uit generieke componenten (zoals verwerkersovereenkomsten en GIBIT-voorwaarden) en specifieke beveiligingscomponenten (zoals het beveiligingsbeleid) die door de CISO worden aangeleverd.

Aan de "bovenkant" is de basis gelegd middels de besturingsfilosofie, waarin een belangrijk kernpunt is opgenomen. Vrij vertaald komt dit neer op het uitgangspunt dat verantwoordelijkheden (waar mogelijk) zo laag mogelijk in de organisatie worden belegd.

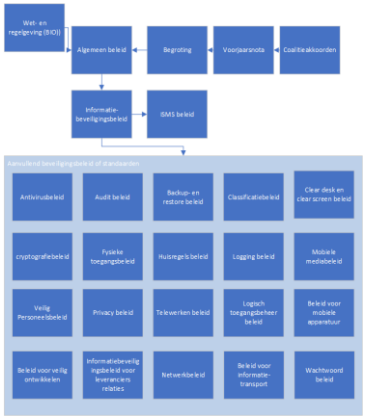
Informatiebeveiligingsbeleid
De structuur van het beleid bestaat aan de "onderkant" uit het Informatiebeveiligingsbeleid, wat uiteenvalt in een algemeen deel en een aantal specifieke stukken, zoals het sleutelbeleid of encryptiebeleid. Deze beleidsstukken worden opgesteld door de CISO en formeel vastgesteld door/in het directieteam. Ook het bewustwordingsproces en het eigen verantwoordelijkheidsbeleid zijn onderdeel van dit pakket.

Er is een overkoepelend strategisch beleid aanwezig uit 2019, dit bevat de hoofdlijnen (organisatie, BIO-normenkader + toelichting, afgeleid van de IBD-templates). Verder zijn er uitwerkingen voor o.a.

logische toegangsbeveiliging en wachtwoorden. Deze zouden echter wel weer up-to-date kunnen worden gebracht.

In haar strategische informatiebeveiligingsbeleid (2019-2022) heeft de gemeente Velsen vastgelegd welke eisen zij stelt aan haar informatiebeveiliging. Zij heeft hiervoor gebruik gemaakt van de NEN-ISO/IEC-27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Tevens zijn hierin opgenomen de 10 principes voor informatiebeveiliging zoals opgesteld door de VNG. Door gebruik te maken van het BIO strategische beleidstemplate van de IBD bestaat zoveel mogelijk aansluiting met de in wet- en regelgeving opgenomen eisen aan informatiebeveiliging bij gemeenten. Op tactische niveaus wordt dit beleid aangevuld met specifieke tactische beleidsregels. In het informatiebeveiligingsjaarplan worden de tactische en operationele aspecten verder uitgewerkt en geconcretiseerd.

In het beleid heeft de gemeente Velsen haar strategische doelen opgesteld en belangrijke uitgangspunten gedefinieerd. Op deze uitgangspunten is een nadere invulling geformuleerd.



Het informatiebeveiligingsbeleid loopt tot en met 2022 en is op 12 november 2019 formeel vastgesteld. Op basis van dit geldende informatiebeveiligingsbeleid constateren wij dat deze nog handvatten ontbeert voor een aantal (belangrijke) onderdelen van informatiebeveiliging die bij de gemeente Velsen nog niet (voldoende) zijn ingericht, zoals de uitgangspunten ten aanzien van Cloud/SaaS-diensten en uitbestede diensten.

Privacy beleid

Binnen een gemeente vinden logischerwijs veel verwerkingen plaats van persoonsgegevens of zijn systemen gekoppeld aan centrale bestanden/registers met persoonsgegevens. De belangrijkste regels voor de verwerking van persoonsgegevens in Nederland zijn vastgelegd in de AVG. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van deze wet- en verbonden regelgeving. Binnen de gemeente Velsen wordt druk gewerkt om aan alle voorwaarden te voldoen en daarna in controle te blijven. De implementatie van de AVG/Privacy -stappen wordt uitgevoerd volgens het VNG-model en is vastgelegd in de Key2Control applicatie.

Het overkoepelende Privacy beleid stamt uit 2016, waarbij nog verwezen wordt naar de BIG i.p.v. de huidige BIO en naar de gezamenlijke aanpak van de IJmond-gemeenten. Voor het sociaal domein is er een separaat privacy beleidsdocument opgesteld, dat echter tot 2018 geldig was. Ook voor het HR-domein is een separaat beleidsdocument in wording.

De implementatie van beleid, procedures en maatregelen om te voldoen aan de AVG (Algemene Verordening Gegevensbescherming) is onderhanden. Binnen de gemeente Velsen bestaat onder andere al een “Procedure beveiligingsincidenten en datalekken”. Met ondersteuning van de Functionaris Gegevensbescherming (FG) zijn diverse activiteiten opgestart of verder vormgegeven, zoals:

- Opstellen van een Privacy beleid;
- Opzetten en zo compleet mogelijk maken van een Register van verwerkingen;
- Opzetten en regelen van Verwerkersovereenkomsten met verwerkers waar verwerkingen van persoonsgegeven van burgers uit de gemeente Velsen plaatsvinden.
- Opzetten diverse procedures voor de afhandeling verzoeken etc.
- Bewustwording binnen de organisatie vergroten.

Een aantal belangrijke fundamenten zijn reeds ingericht en opgesteld, zoals beleidsdocumenten en de diverse procedures waaronder rechten van betrokkenen en het melden van datalekken. Er is echter nog genoeg te doen door de Privacy Officer (PO) en de Functionaris Gegevensbescherming (FG). De status wordt vastgelegd in Key2Control en wordt deels gebruikt om een Privacy jaarplan op te stellen.

Wij constateren dat deze activiteiten al deels zijn ingericht, maar nog niet afgerond zijn. Het opgestelde AVG/Privacy jaarplan geeft inzicht in de diverse onderdelen die nog verder dienen te worden uitgewerkt. Verdere details ten aanzien van de implementatie van de AVG/Privacy maatregelen komen verderop terug, bij de vraagstelling over de status van de AVG/Privacy processen.

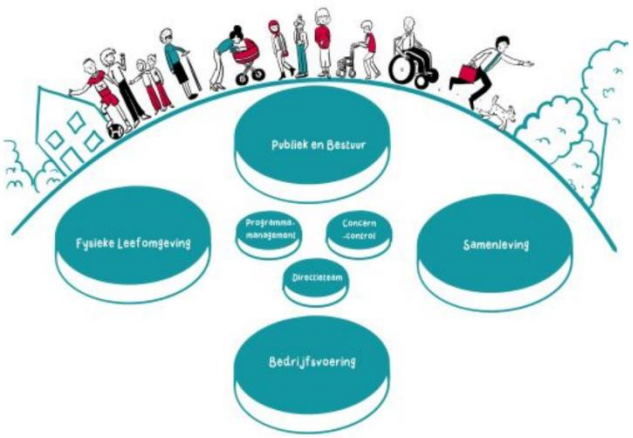
Organisatie

De organisatie van informatiebeveiliging en privacy moet onderdeel zijn van de planning- en control cyclus om te waarborgen dat informatiebeveiliging en privacy een integraal onderdeel is van de gemeente en een aspect is waarover de gemeente via de reguliere verantwoordingslijnen transparant over kan zijn naar haar burgers, andere belanghebbenden en toezichthouders. Door de organisatieonderdelen verantwoording te laten afleggen via reguliere voortgangsrapportages, wordt beveiliging zowel bestuurlijk als ambtelijk in de organisatie te geborgd. Alle geledingen van de organisatie zijn betrokken. Aansluiting op de planning & control cyclus voorkomt daarmee dat informatiebeveiliging als een zelfstandig onderwerp een lage prioriteit krijgt.

Volgens het informatiebeveiligingsbeleid en privacy beleid is het college van B&W eindverantwoordelijk en het lijnmanagement zorgt voor de implementatie, uitvoering en het monitoren van de informatiebeveiliging en privacy in de gemeente. De volgende organisatorische inrichting bestaat bij de gemeente Velsen voor de functies rond informatiebeveiliging en privacy:

- College B&W;
- Portefeuillehouder informatiebeveiliging en privacy (B&W);
- Bedrijfsvoering (Gemeentesecretaris);
- CISO/ ENSIA-coordinator (Afdeling Concern control);
- FG/Functionaris Gegevensbescherming;
- PO/Privacy Officer;

De organisatiestructuur



De coördinatie, namens het management, van de implementatie van informatiebeveiligingsmaatregelen, het monitoren van de status van informatiebeveiliging, en tijdig en adequaat opvolging geven aan beveiligingsincidenten, wordt door de CISO uitgevoerd. De gemeente Velsen heeft één volledige CISO-functie ingevuld. De CISO heeft een onafhankelijke functie als onderdeel van de afdeling Concern Control en rapporteert aan de portefeuillehouder informatiebeveiliging en privacy in het college B&W. De CISO vervuld ook de taken van de ENSIA-coördinator.

De FG is aangesteld in een onafhankelijke rol ook onderdeel van Concern control, in een parttimefunctie. De Privacy Officer is een fulltime functie en deze is volledig in dienst bij de gemeente Velsen. Beide personen (FG en PO) zijn sinds september 2020 in functie. Beiden hebben een aanstellingsbrief ontvangen, maar er is destijds geen collegevoorstel voor gemaakt. De FG vervult naast de FG-functie ook een interne auditfunctie. De taken en verantwoordelijkheden zijn niet vastgelegd in een functie en/of rol beschrijving vanuit de personeelsadministratie. De taken van de FG zijn in ieder geval wel opgenomen in het privacy beleidsdocument. De FG is een onafhankelijke functie binnen de gemeente Velsen. De huidige FG was voor 12 uur per week aangesteld, en voor 24 uur vanaf augustus

2021 voor de nieuwe FG, die de huidige gaat opvolgen. In de praktijk wordt het werk nu verdeeld over beide personen, uiteraard alleen waar dit kan en mag. Voorheen was dat volledig bij de voorgaande functionaris belegd.

De CISO-functie en ook de privacy functies zijn niet formeel beschreven in een takenpakket, maar zijn opgehangen aan een algemeen functieprofiel Adviseur 3. Het HR21 model is in gebruik voor functies, die zijn echter vrij algemeen: adviseur3 is voor de CISO, PO en FG en ook anderen. Hierdoor is geen inzicht in de specifieke details beschikbaar. Niet alle taken passen op dit moment in de dagelijkse uren van de CISO.

Binnen het college van B&W is een aparte portefeuille ten aanzien van Informatievoorziening en digitalisering, waaronder Informatiebeveiliging en Privacy ondergebracht. Dit betekent dat beide onderwerpen op het juiste niveau zijn geagendeerd.

Het informatiebeveiligingsbeleid wordt geschreven door de CISO, het Privacy beleid door het privacy team, waarbij de portefeuillehouder de rol van “kritische meelezer” invult. De implementatie/uitvoering wordt door de gemeentesecretaris opgepakt en indien noodzakelijk bekrachtigd door de gemeenteraad.

Ten aanzien van het beleid bestaat de rol van de gemeentesecretaris daarnaast uit de volgende activiteiten

- De vertaling van een “papieren voorstel” naar een implementatievoorstel.
- Aandacht vragen voor onderwerpen indien de voortgang en de monitoring ervan daar aanleiding toe geven.

In de huidige opzet is de FG ook verantwoordelijk voor het opstellen van het privacy beleid, maar komt daar niet helemaal aan toe, vanwege de vele andere activiteiten. Bijvoorbeeld de uitvoering/ implementatie van de WPG is er nu bijgekomen. Het reviewen van DPIA’s komt er ook aan, maar daarvoor ontbreekt nu helaas de tijd.

Er is naast de informatiebeveiligingspagina een separaat deel op de interne web-omgeving van de gemeente Velsen ingeruimd voor privacy/AVG waar de medewerkers van de gemeente ook de laatste updates kunnen vinden.

Voor de implementatie van de archiefwet wordt gebruik gemaakt van een expert die helpt bij de beveiligings- en privacy eisen die moeten worden nageleefd door de gemeente Velsen.

Ten aanzien van ICT is voor de uitbesteding van de beheer activiteiten aan de externe partij OGD een contract manager ingesteld, en zijn er 2 servicelevel managers actief om de afstemming te bewaken. De contract eigenaar is de manager/hoofd Informatie. Tijdens de transitie fase is een Velsen interne projectleider ingeschakeld om een gecontroleerde overgang te bewerkstelligen. De overgang naar OGD was gedurende de interviews in een afrondende fase.

4.2.1.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

Visie en beleid

- De gemeente Velsen heeft een algemene visie en bijbehorend beleid opgesteld, waaruit kan worden afgeleid dat in de toekomst de bedrijfsprocessen zoveel mogelijk zullen worden ondersteund door ICT van de Cloud/SaaS gedachte en de verantwoordelijkheden zo laag mogelijk in de organisatie zijn belegd.

Informatiebeveiligingsbeleid

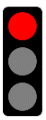
- Door het strategische beleid als kapstok te laten fungeren, vanuit de visie en het beleid, dient dit nadere invulling naar tactische en operationele beleidsstukken. Het strategische beleid vormt de toplaag van een beveiligingsbeleidsstructuur, die ook nog bestaat uit een tactische en operationele laag en (eventueel) daaronder nog richtlijnen en standaarden. De gemeente Velsen heeft op dit moment de twee vervolg lagen in dit model nog niet ingevuld. Enkele onderdelen zijn reeds eerder uitgewerkt, zo is er een logisch toegangsbeveiligingsbeleid uit 2017, fysieke toegangsbeveiliging uit 2014 en wachtwoordbeleid uit 2015 opgesteld en definitief vastgesteld. Verder kan worden gedacht aan beleid over het gebruik van sociale media, mobiele apparatuur, Saas/Cloud applicaties, het mogelijk gebruik van BYOD-apparaten en minimum leveranciers voorwaarden en rapportages. [Aanbeveling 7]

- De huidige beleidsdocumenten dienen een revisie te ondergaan om te voldoen aan de huidige situatie. Zo is een update van het wachtwoord (of authenticatie) beleid noodzakelijk, waarin naast de huidige informatie tevens is vastgelegd, wat de minimumvoorwaarden zijn om toegang te krijgen vanaf het Internet, het interne netwerk, vanuit thuis etc. [Aanbeveling 7]

- Het beleid geeft geen uitwerking aan een proces van periodieke evaluatie om vast te stellen of het beleid nog steeds voldoende invulling geeft aan de veranderende omgeving wat betreft risico's en aanpassingen in de regelgeving. Het beleid is vastgesteld in 2019, maar is nagenoeg gelijk aan het template beschikbaar vanuit het IBD en is niet aangepast op nieuwe ontwikkelingen zoals bijvoorbeeld Cloud/SaaS-services waarvoor specifieke maatregelen vanuit de gemeente Velsen noodzakelijk zijn. Wij tekenen wel aan dat veel dienstverlening is uitbesteed aan OGD, waardoor in feite de invulling van het beleid dat door OGD wordt gedaan en door de gemeente Velsen impliciet wordt overgenomen. [Aanbeveling 7]

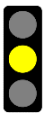
Privacy beleid

- Het privacy beleid is formeel opgesteld, maar verdient opgefrist te worden om aan te sluiten op de huidige status. Update de privacy beleidsdocumenten tevens met versienummers en formele goedkeuring. [Aanbeveling 1]



- Zorg voor een verdere uitwerking van de benodigde AVG/privacy procedures en registraties. Voor meer details zie verderop in dit rapport bij de uitwerking van de vraag over AVG/Privacy. [Aanbeveling 1]

- Net als het informatiebeveiligingsbeleid geeft dit document geen uitwerking aan een proces van periodieke evaluatie om vast te stellen of het beleid nog steeds voldoende invulling geeft aan de veranderende omgeving wat betreft risico's en aanpassingen in de regelgeving. Het beleid is vastgesteld in 2016, het beleidskader in 2018. [Aanbeveling 1]

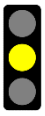


- Formaliseer domein specifieke privacy documenten, zoals voor het sociaal domein en HR. Onderzoek of wellicht voor andere domeinen ook specifieke privacy documenten noodzakelijk of nuttig zijn. [Aanbeveling 1]

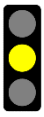
<u>Organisatie</u>

- Zowel de CISO als de FG zijn onafhankelijk in de organisatie geplaatst. In het beleid is aangegeven dat elke ambtenaar verantwoord met persoonsgegevens en andere informatie dient om te gaan. Hierover zijn vanuit Privacy oogpunt bewustwordingssessies opgestart en is een externe organisatie ingeschakeld om daarbij te ondersteunen. Ook is informatie via het Intranet beschikbaar.

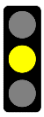
- In het informatiebeveiligingsbeleid is uitwerking gegeven aan de organisatorische inrichting van de informatiebeveiliging. Het college van Burgemeester en Wethouders is integraal verantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Het MT is verantwoordelijk voor het waarborgen van een heldere koers en zichtbare ondersteuning van het beveiligingsbeleid binnen de gegeven bestuurlijke kaders. Het lijnmanagement is verantwoordelijk voor de naleving van het beveiligingsbeleid.



- In het informatiebeveiligingsbeleid is naast de algemene taken en verantwoordelijkheden van de medewerkers niet vastgelegd wat de verantwoordelijkheden zijn van informatiemanagers, systeembeheerders, applicatiebeheerders, proceseigenaren en gegevensbeheerders. De benodigde communicatie naar de betrokkenen over hun rol in het realiseren van informatiebeveiliging is binnen het informatiebeveiligingsbeleid niet verder uitgewerkt dan dat dit als taak is geformuleerd voor de individuele ambtenaar, het managementteam en de (lijn-) managers. [Aanbeveling 6, 8, 9]



- De taken en verantwoordelijkheden (functieomschrijvingen) van de Privacy Officer, de FG en de CISO dienen uitgeschreven te worden. De rol en taken van de CISO zijn verspreid over het beleidsdocument beschreven, maar niet vastgelegd in het beleid of in een functieomschrijving. [Aanbeveling 7]



- Het aanstellen van privacy ambassadeurs om zoveel mogelijk privacy gerelateerde kennis en werkzaamheden bij de medewerkers te beleggen, helpt het privacy team te ontlasten. Wellicht is een dergelijke constructie ook zinvol voor de informatiebeveiligingsactiviteiten ter ondersteuning van de CISO. [Aanbeveling 1, 6, 8]

4.2.2. Zijn informatiebeveiligingsrisico's in control?

De volledige vraag:

"Heeft de gemeente de risico's op informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie in beeld of benoemd? Is helder in hoeverre risico's beheerst dan wel geaccepteerd worden? Zijn de (eind)verantwoordelijken aangewezen en zijn de autorisaties adequaat geregeld?"

In het onderzoek zijn wij bij deze deelvraag uitgegaan van risicoanalyse processen die vanuit informatiebeveiliging en privacy worden gedaan of gevraagd, de huidige status van uitgevoerde analyses en de opvolging door de juiste personen. Ten aanzien van de adequaatheid van de autorisaties verwijzen we voor de details naar de vraag in Fase 2 over mogelijke oneigenlijke toegang.

4.2.2.1. *Toelichting*

Informatiebeveiliging
Door inzicht te hebben in de risico's ten aanzien van betrouwbaarheid, beschikbaarheid en exclusiviteit van de gegevens van de gemeente en de verwerkingen daarvan, kan de gemeente vanuit een totaaloverzicht bepalen welke beveiligingsmaatregelen noodzakelijk zijn, op welke onderdelen/systemen, door wie en op welk niveau en in onderlinge samenhang.

De huidige risico inschatting is gebaseerd op de uitkomsten van de jaarplannen vanuit de CISO en Privacy organisatie, aangevuld met analyses van een aantal belangrijke applicaties (waaronder Donau, Decade en Cognos) volgens de BIG-baseline toets uit 2016. Daarnaast is er volgens de BIO (versie 1.02) in 2019 een baseline toets uitgevoerd. Een derde analyse variant is toegepast bij de risicoanalyse ten aanzien van de uitbesteding van de ICT-omgeving. Een diepgaande risicoanalyse (volgens de IBD-templates) is niet uitgevoerd. Het merendeel van de Velsen ICT-omgeving is volgens BBN-niveau 2 ingericht en dat lijkt ook afdoende. De BRP-omgeving bijvoorbeeld gaat al uit van dat niveau.

Eigenlijk wordt de toets gevraagd vanuit de (bedrijfs-) processen, echter die zijn nog niet compleet beschreven op dit moment, waardoor de risicoanalyse nog niet compleet worden uitgevoerd. Er ontbreekt derhalve een overkoepelend risicomanagement proces dat vanuit de belangrijkste bedrijfsprocessen ervoor zorgt dat periodiek wordt vastgesteld welke veranderingen in de risico's plaatsvinden en of dat aanleiding is om nieuwe maatregelen te nemen of het beleid aan te passen. De eigenaren van deze bedrijfsprocessen zijn verantwoordelijk voor het up-to-date houden van de risico's, terwijl de CISO een faciliterende rol kan vervullen tijdens de uitvoering van de risicoanalyse en het plannen van deze periodieke activiteit. Een volledige risicoanalyse kan nog een beter totaaloverzicht opleveren en inzicht waar eventuele gaten in controles/maatregelen zitten.

De risico's waar de gemeente mee te maken heeft zijn duidelijk anders dan enkele jaren geleden. Er wordt meer gestuurd naar en op SaaS-applicaties, waar specifieke risico's een rol spelen waaronder bijvoorbeeld de gegevensverwerking bij derden. Door het ontbreken van de (beleid)uitgangspunten en juiste afweging van de risico's en daarvan afgeleide (continuïteits-) maatregelen bestaat het risico dat te veel (kostbare) maatregelen worden geïmplementeerd of dat voor kritieke systemen maatregelen ontbreken. Deze analyse is ook essentieel voor het bepalen van de juiste acties bij incidenten (reactie en herstel) waardoor bij het ontbreken van deze analyse de gemeente minder adequaat zou kunnen optreden en daarmee systemen langer dan gewenst niet beschikbaar zijn, niet betrouwbaar werken of de vertrouwelijkheid van gegevens niet is gerealiseerd.

Het risico bestaat dat onvolledige maatregelen zijn getroffen voor de actuele risico's en onvoldoende inzicht bestaat in de daadwerkelijke risico's. Overigens worden deze risico's enigszins beperkt doordat

de gemeente Velsen gebruik maakt van diensten van OGD en is de gemeente aangesloten bij de Informatiebeveiligingsdienst Gemeenten (initiatief VNG (Vereniging van Nederlandse Gemeenten). Deze partijen signaleren acute beveiligingsrisico's voor gemeenten en mogelijke oplossingen daarvoor en melden deze actief bij de gemeente Velsen.

Begin 2021 heeft een (hernieuwde) nulmeting plaatsgevonden aan de hand van het BIO-normenkader. Dit gaf inzicht in de toen bestaande status van informatieveiligheid en verbeteringen via het jaarplan informatiebeveiliging. Daar waar de maatregelen nog ontbraken heeft een risico inschatting plaatsgevonden, uitgevoerd door de CISO. Op basis van deze risico inschatting is een maatregelverbeterplan (jaarplan) opgesteld. Hierin zijn in totaal 40 normen nog niet of niet volledig geïmplementeerd, waarvan 28 normen die volgens de risico inschatting hoog zijn geclassificeerd, en 12 normen laag.

Wij benadrukken dat het implementeren van een overkoepelend en periodiek herhaald risicomanagement proces één van de belangrijkste bouwstenen is bij het realiseren van aantoonbaar voldoende informatiebeveiliging. De implementatie van de eerdergenoemde BIO (Baseline Informatiebeveiliging Overheid) betekent ook dat een op risicomanagement gebaseerde informatiebeveiliging een eis is. Het 100% veilig zijn is niet mogelijk, de gemeente moet ook nog (gewoon) het werk kunnen doen. Uiteindelijk geeft de risicoanalyse het benodigde inzicht in afhankelijkheden van informatiesystemen en kwetsbaarheden van die systemen om gedegen

a) Keuzes te maken welke risico's te accepteren en
b) Te kunnen kiezen welke maatregelen het meeste effect hebben op het verlagen van risico's.

AVG/Privacy

Het privacy team is nog volop bezig met de vele stappen die vanuit de AVG/Privacy wetgeving van een gemeente worden gevraagd. Een aantal onderdelen daarvan hebben een direct verband met het identificeren van risico's en de daarvan af te leiden maatregelen die moeten worden getroffen ter bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie.

De belangrijkste fundamenten zijn reeds ingericht en opgesteld, zoals beleidsdocumenten en de diverse procedures, zie ook verderop de specifieke vraag over de status van de AVG/Privacy implementatie. Er zijn ongeveer 20 kritieke systemen geïdentificeerd, voornamelijk bestaande uit systemen en applicaties voor de verplichte dienstverlening van de gemeente Velsen. Deze bestaan uit systemen op de locatie van de gemeente, maar ook diensten in beheer bij een externe partij (zoals Pink Roccade), extern gehoste diensten zoals bij Dimpact en volledige SaaS-applicaties.

Er is een verwerkingsregister opgesteld, echter de jaarlijkse update die vanuit de organisatie moet worden opgepakt, heeft nog niet plaatsgevonden. Het register is uitgebreid met de VNG-eisen en daarnaast ook aangevuld met eigen Velsen specifieke informatie. Het overzicht van 470 registraties is nu niet helemaal accuraat meer en ook nieuwe registraties moeten deels nog worden toegevoegd. In principe zou dit vanaf nu door de aangestelde ambassadeurs vanuit de organisatie plaatsvinden, ondersteund door het privacy team.

Hoe het uitvoeren van een privacy impact analyse dient te geschieden (volgens het DPIA-proces) is beschreven en op het intranet beschikbaar en toegelicht. De uitvoering moet nog grotendeels plaatsvinden. Er zijn er nu 6 à 7 gedaan. Het plan is om allereerst met de 9 ambassadeurs uit de afdelingen een inventarisatie te doen van de werkzaamheden, waarna een actieplan zal worden opgesteld waarin wordt vastgelegd, welke, wanneer zullen worden opgepakt. Naar verwachting zullen hooguit enkele DPIA's worden opgeleverd per ambassadeur. Daarna zal moeten worden besloten hoe voor het DPIA-proces de inhaalslag zal worden uitgevoerd. Er zijn in totaal 470 verwerkingen, waarvan door het privacy team moet worden bepaald, voor welke een gedetailleerde DPIA noodzakelijk is.

Normaal gesproken zullen voor de belangrijke applicaties en voor die applicaties waar persoonsgegevens in verwerkt worden, DPIA's worden uitgevoerd. Er zijn op dit moment 6 DPIA's uitgevoerd en in Key2Control vastgelegd/geregistreerd.

4.2.2.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

Informatiebeveiliging

- Er hebben in het verleden enkele risicoanalyses plaatsgevonden voor een aantal belangrijke applicaties zoals Decade en Donau, op basis van de destijds geldende beveiligingsnorm BIG. Ook heeft er een analyse plaatsgevonden ten aanzien van de uitbesteding van de ICT-omgeving.

- Een organisatie brede risicoanalyse is nog niet uitgevoerd waarin de gemeente heeft vastgesteld wat de BBN eisen zijn aan de informatievoorziening, wel voor enkele belangrijke systemen. Dit is een belangrijk handvat voor het bepalen van de juiste maatregelen voor de gemeente bijvoorbeeld voor back-ups en logische toegangsbeveiliging. Slechts dan is het mogelijk om vast te stellen in hoeverre de gemeente voldoende maatregelen heeft getroffen en op welke onderdelen monitoring dient te zijn ingericht. Het risicomanagementproces dient een continu proces te zijn. De gemeente hanteert nu de risicoanalyse van de BIO-nulmeting als uitgangspunt voor de selectie en implementatie van beveiligingsmaatregelen als startpunt voor nieuwe systemen. Risicoanalyse activiteiten vinden ook plaats voor bestaande systemen en de onderliggende ICT-infrastructuur en besturingssystemen. De te implementeren maatregelen zijn daarbij gekoppeld aan actiehouders en een einddatum. Dit betreft met name die systemen die als kritiek zijn bestempeld vanuit informatiebeveiligingsperspectief, veelal systemen van de afdeling Financiën en Belastingen. [Aanbeveling 11]

- Het is aan te bevelen om in de tussentijd het BBN-2 niveau van het BIO-normenkader als minimum eisenpakket te gebruiken voor nieuwe systemen en applicaties, maar ook voor de huidige omgeving als startkader waar minimaal aan voldaan zou moet worden en waaraan dan ook direct getoetst kan worden. Het BBN-2 niveau bevat de meeste maatregelen die voor een gemeente van toepassing zouden moeten zijn. [Aanbeveling 11]

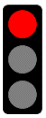
- De afweging van de risico's en de te nemen maatregelen worden door de CISO gedaan en vastgelegd in het jaarplan. Dit wordt besproken in het TIP (Team Informatiebeveiliging en Privacy) overleg, waarna het beschikbaar wordt gesteld aan de directie. De risico afwegingen worden tot op heden niet altijd vastgelegd waardoor inzicht in het geaccepteerde risico later onduidelijk kan zijn of ontbreekt. De status en voortgang van de opvolging van geïdentificeerde informatiebeveiligingsrisico's dient periodiek te worden bewaakt en indien noodzakelijk worden bijgesteld.. [Aanbeveling 6,11]

- In het informatiebeveiligingsbeleid zijn strategische doelen opgenomen, die de basis van het strategische beveiligingsbeleid vormen. Daarnaast zijn hierin de belangrijke uitgangspunten gedefinieerd en wordt tevens een eerste invulling gegeven aan deze uitgangspunten. Het meten en eventueel sturen op deze doelen en uitgangspunten is op dit moment (nog) niet ingericht door de CISO. Het risico bestaat dat door het ontbreken van periodiek inzicht, strategische doelen en uitgangspunten onvoldoende aandacht en prioriteit krijgen. [Aanbeveling 6]

AVG/Privacy

Het privacy team heeft al veel activiteiten die de AVG/Privacy wetgeving vraagt van een gemeente ook daadwerkelijk al opgepakt. In een latere deelvraag worden de inhoudelijke AVG/Privacy onderwerpen toegelicht. In dit deel ligt de nadruk op de risico's, de bijbehorende verantwoordelijkheden en maatregelen.

- Met de huidige ontwikkelingen en het effectief worden van de AVG (Algemene Verordening Gegevensbescherming) is ook de classificatie van gegevens een steeds belangrijker hulpmiddel geworden om de juiste maatregelen te bepalen. Bijzondere en/of gevoelige gegevens van burgers vereisen bij de verwerking zwaardere beveiligingsmaatregelen. Dit kan ook gelden voor andere gegevens zoals inrichtingsdocumenten van de beveiliging van de ICT, aanbestedingsstukken etc. De classificatie is in een richtlijn uitgewerkt en stamt uit 2017 en dient te worden aangepast aan de huidige situatie (waaronder Cloud/Saas omgevingen, beheer uitbesteed, AVG/Privacy wetgeving) waarin de gemeente Velsen zich bevindt. In de dataclassificatie richtlijn is het risiconiveau dat in het verwerkingenoverzicht is vastgelegd (Laag, Aanzienlijk) nog niet uitgewerkt naar de impact voor de te definiëren (beveiligings-) maatregelen. [Aanbeveling 1]



- De gemeente Velsen heeft nog niet voor alle systemen en applicaties het eigenaarschap kunnen afronden. Gesprekken zijn grotendeels gevoerd om de eigenaars bewust te maken van de verwerkingen en het verwerkingsregister en dat hierop wijzigingen plaatsvinden door bijvoorbeeld veranderingen in processen, informatie verzamelen en updates van software. Dit inzicht is noodzakelijk aangezien verwerkingen met een hoog risico om een verplichte DPIA (Data Protection Impact Assessment) vragen. Een DPIA geeft inzicht in de aard en het doel van de verwerking en de daarmee samenhangende risico's voor de beveiliging van persoonsgegevens op basis waarvan vervolgens maatregelen worden gedefinieerd om het risico zoveel mogelijk te beperken en vast te stellen of de verwerking wel is toegestaan. [Aanbeveling 1]

- De FG (Functionaris Gegevensbescherming) heeft veel werk verricht ten aanzien van de implementatie van de noodzakelijke processen en maatregelen, echter heeft hierdoor geen tijd kunnen besteden aan het opstarten van de periodieke (onafhankelijke) audits door of namens de FG om de naleving van het privacy beleid vast te stelen. [Aanbeveling 1]

- De status en voortgang van de opvolging van geïdentificeerde privacy risico's dient periodiek te worden bewaakt en indien noodzakelijk te worden bijgesteld. Hiervoor zou de Key2Control applicatie en meer nadrukkelijke rol kunnen vervullen, om bijvoorbeeld inzicht te verschaffen in de huidige status en reeds behaalde/doorgevoerde verbeteringen. [Aanbeveling 1, 11]

4.2.3. Wordt het beleid adequaat uitgevoerd en wordt het gemonitord?

De volledige vraag:

"Wordt het beleid adequaat uitgevoerd en wordt het gemonitord?"

In het onderzoek zijn wij bij deze deelvraag uitgegaan van de (dagelijkse) activiteiten die door de gemeente Velsen zelf wordt uitgevoerd om het beleid ten uitvoering te brengen en te monitoren. Dit in tegenstelling tot de hiernavolgende vraag, die vooral ingaat op de (onafhankelijke) toetsing van informatiebeveiliging. De uitvoering en monitoring van het AVG/Privacy beleid is in een latere deelvraag uitgewerkt.

4.2.3.1. *Toelichting*

Na de (recente) reorganisatie van afdelingen en teams binnen de gemeente Velsen zijn vier domeinen opgesteld, ieder met eigen managers met hun eigen aandachtsgebied binnen dat domein, sociaal domein (heet nu domein samenleving), Publiek en bestuur, Fysieke leefomgeving en Bedrijfsvoering zijn de andere domeinen. De manager Informatie (onderdeel van het domein Bedrijfsvoering) is in staat (net als de andere teammanagers) om de ander indien nodig te vervangen. Team Informatie bestaat onder andere uit de volgende functies/medewerkers:

- Automatisering (is nu grotendeels uitbesteed), regiefunctie en functioneel beheerders
- Informatie adviseurs
- Ruimtelijke informatievoorziening en BAG
- Informatiebeheer en archivering
- Statistiek en onderzoek

Team Informatie heeft een belangrijke rol in de uitvoering van informatiebeveiliging, daarnaast is uiteraard de gehele gemeentelijke organisatie verantwoordelijk voor de uitvoering. Beveiliging gaat namelijk over meer dan ICT en het nemen van maatregelen is niet alleen een ICT-aangelegenheid. Daarbij hebben de CISO en de FG een onafhankelijke rol. De CISO adviseert het team en stelt het beleid op. De Privacy Officer gezamenlijk met de FG zorgt voor de invulling van AVG/Privacy activiteiten.

De sturing van activiteiten en projecten binnen Team Informatie (onderdeel van domein bedrijfsvoering) wordt gedaan middels een projectboard, waarop alle ontwikkelingen zoals bedrijfscontinuïteit en wetgeving voorbijkomen. Vanuit de projectentafel worden voorstellen besproken en voorgelegd aan de projectboard strategische stuurgroep. Hierbij zal het hoofd Informatie en enkele andere belanghebbenden zoals de concerncontroller en de bedrijfsdirecteur gezamenlijk de keuzes maken. Prioriteiten worden bepaald door onder andere het budget, risico's en bijvoorbeeld capaciteit. Voorstellen vanuit beveiligingsoogpunt wordt vaak positief geadviseerd. De risico's worden vanuit projecten maar ook door de concerncontroller aangeleverd.

De bedoeling is om processen en systeemeigenaren aan te wijzen, maar deze zijn nog niet allemaal als formele taken/activiteiten vastgelegd. Aangezien er nog geen goed totaalinzicht is in alle bedrijfsprocessen is dit ook nog niet goed mogelijk. De CISO beschouwt derhalve op dit moment de leidinggevende van de functioneel beheerder van een systeem als systeemeigenaar maar dit heeft geen formele status.

Periodieke operationele overleggen bij de gemeente Velsen intern (o.a. TIP-overleg) vinden plaats waarin de status van zowel informatiebeveiliging als AVG/Privacy worden besproken. Vanuit de teams

worden standaard rapportages naar de gemeentesecretaris gestuurd. Specifieke rapportages ten aanzien van beveiliging en privacy worden via de teams meegenomen in de standaard rapportage cyclus. Indien noodzakelijk wordt toelichting gegeven via de diverse teams overlegstructuren.

De CISO heeft nu de afspraken met de externe dienstverlener OGD nagenoeg afgerond zijn, een vaste contactpersoon voor informatiebeveiliging bij deze dienstverlener, waardoor hij een klankbord heeft gekregen. De vorm waarin de contacten worden onderhouden is nog niet helemaal helder. Daarover worden nadere afspraken gemaakt. Andere sparringpartners voor de CISO zijn een ICT-architect die is ingehuurd door de gemeente Velsen en verder zijn er de PO, FG, informatiearchitect, controller en concerncontroller voor eventuele afstemming.

Belangrijke andere functionarissen in de Gemeente Velsen organisatiestructuur met een link naar informatiebeveiliging en AVG/Privacy:

- Systeemeigenaren, proces eigenaren
- Portefeuillehouder
- Gemeentesecretaris
- Facilitaire dienst + helpdesk = servicedesk
- Fysieke beveiliging
- Buitendienst heeft enkele posten in de gemeente, met een aansluiting op het gemeentenetwerk voor hun dagelijkse activiteiten.
- Functioneel beheerders
- Technisch beheer uitbesteed aan OGD.
- Contract en Service Level Managers

De scope van de werkzaamheden van de CISO omvat de volledige informatievoorziening van de gemeente Velsen. Openbare diensten vallen niet onder de gemeente Velsen, echter het zwembad valt weer wel in de scope. De afdeling sportzaken heeft een eigen website, en wijkt daarmee af van het beleid. Voor uitbestede diensten en processen zijn vanuit de gemeente Velsen centrale aanspreekpunten aangewezen, zoals voor verbonden partijen, commerciële partijen en samenwerkingsverbanden. Er zijn nog wel veel gemeenschappelijke regelingen zoals de reinigingsdienst, omgevingsdienst IJmond, recreatieschappen etc. Deze zijn soms wat ondoorzichtig, zoals bijvoorbeeld de uitvoering van de participatiewet. De vraag is dan bijvoorbeeld: Is dit nu goed geregeld, zoals de verantwoordelijkheid van persoonsgegevens? Gemeente Velsen heeft geen shared service center (meer).

Bij mogelijke nieuwe systemen en/of implementaties wordt steeds een projectgroep en stuurgroep opgesteld, via welke route de keuze wordt bepaald en de uitvoering bewaakt. Onder andere de directie en diverse functionarissen binnen de gemeente, zoals de CISO, privacy, architect, etc. zijn daarbij betrokken. Een standaard minimale set aan beveiligingseisen is in de inkoopvoorwaarden opgenomen. Vooral de BIO wordt daarbij genoemd. De CISO heeft een leidraad geschreven voor inhuur van externe partijen en de afname van nieuwe diensten. Vooraf wordt een risicoanalyse uitgevoerd. Van daaruit worden de maatregelen afgeleid voor de afstemming met externe partijen/leveranciers. Dit is echter een nieuw proces, dat nog moet worden opgestart.

Veel werkzaamheden zijn uitbesteed door de gemeente Velsen aan externe partijen, derhalve heeft de gemeente Velsen sinds begin augustus 2021 een ICT-contractmanager aangesteld en heeft daarnaast 2 servicelevel managers actief. De contractmanager onderhoudt de formele (contractuele) status en afspraken met de externe partijen (zoals OGD). De servicelevel managers bewaken de inhoud van de afspraken. Voor elk contract is ook een contract eigenaar aangewezen, voor OGD is dit de manager

Team Informatie. De verantwoordelijkheid voor de kwaliteit en beveiliging van de gegevensverwerking blijft, bij uitbesteding van ICT-diensten, bij de gemeente liggen. Dit vergt specifieke maatregelen vanuit de gemeente om te waarborgen dat voldoende maatregelen aantoonbaar door de leveranciers zijn getroffen. Te denken valt hierbij aan specifieke beveiligingsafspraken in de contracten, afspraken over het beheer van de geleverde serviceniveaus, het mogen auditen bij de organisatie en/of het jaarlijks verkrijgen van verantwoordingsrapporten over hun systeem van interne beheersing.

Ten aanzien van OGD is het contract recent formeel ingegaan, waarbij nog een aantal activiteiten zijn opgesteld die nog moeten afgerond na de overgang. Daarbij is afgesproken dat tot aan het einde van dit jaar nog wat terughoudendheid in de formele naleving van de afspraken kan/zal worden gehanteerd. Elke maand wordt (vanaf nu) door OGD een servicelevel rapportage opgeleverd aan de gemeente Velsen en deze wordt besproken door de servicelevel manager met OGD. Na een jaar zal volgens verwachting de huidige interne ICT-omgeving volledig door OGD zijn omgebouwd in een OGD eigen omgeving. Tot dat moment blijft de huidige situatie (interne ICT-omgeving) in stand. Algemene afspraken over het ICT-beheer zijn al wel in het contract opgenomen. De precieze detail invulling wordt nog verder gefinetuned. Zo is er een beveiligingscontactpersoon waarmee de CISO periodiek overleg kan voeren. Het technisch beheer is al bij OGD ondergebracht.

Aangezien beide organisaties (gemeente Velsen:Axxerion, en OGD: Topdesk) een eigen registratietool hebben voor incidenten, verzoeken etc., komt het voor dat het aantal openstaande meldingen van tickets niet altijd gelijk is. Hiervoor wordt nog een verbeteringstraject opgestart.

Met OGD worden wekelijks overleggen gehouden, waarin onder andere uitgevoerde patch-updates en eventuele beveiligingsincidenten worden besproken. Daarnaast zijn er leverings-overleggen en contractoverleggen. De rapportage bevat de gangbare onderdelen zoals incidenten en wijzigingen uitgevoerd etc. Wekelijks is er met de afdeling ICT/Informatie een overleg. Met het securityteam is nog geen vast overleg ingepland. Dit gebeurt op ad-hoc basis.

De verwachting is dat ook alle informatiebeveiligingsactiviteiten via de servicelevel manager worden gemeld/gerapporteerd, zoals de patch-status. Er vinden slechts zeer beperkt security incidenten plaats, volgens de rapportage. De rol van de servicelevel manager is om te bewaken dat ook de securitydienstverlening aan de gestelde voorwaarden voldoet. Nu is niet altijd duidelijk welke security gerelateerde dienstverlening is geleverd, omdat dit rechtstreeks tussen OGD en de CISO wordt besproken.

4.2.3.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Via het jaarplan en de diverse operationele overleggen wordt inzicht gegeven in de huidige status van informatiebeveiliging, worden acties opgestart en beslissingen en keuzen genomen. Over de kwaliteit van de informatiebeveiliging en de voortgang in de realisatie van de verbetermaatregelen rapporteert de huidige CISO slechts via het jaarplan, en is er niet voorzien in een kwartaalrapportage. Dit vindt nu vooral plaats in de periodieke operationele overleggen van waaruit eventuele beslissingen worden genomen. Het ligt voor de hand dat de CISO per kwartaal rapporteert aan de portefeuillehouder informatiebeveiliging, die deze dan wellicht mee kan nemen naar het collegeoverleg. Hierdoor krijgt de organisatie namelijk een completer inzicht (in vergelijking met het jaarplan) en waaruit wellicht een betere afweging en keuzes kunnen worden gemaakt. Deze kwartaalrapportage behandelt niet enkel de voortgang op de implementatie van de verbetermaatregelen uit eerdere BIO-nulmetingen maar gaat ook in op andere relevante zaken zoals:
  - Door IBD gesignaleerde bedreigingen en de wijze waarop de CISO hiermee is omgegaan of actie vraagt van het college van B&W.
  - Aanvullende verbetermaatregelen die naar voren zijn gekomen bij de implementatie van verbetermaatregelen uit de BIO/ENSIA-metingen.
  - Uitkomsten en opvolging van eventuele tekortkomingen uit audits (zoals DigiD, Suwinet, ENSIA).

  [Aanbeveling 6]

- De realisatie van de geselecteerde maatregelen vastgelegd in het informatiebeveiligingsjaarplan zijn deels gerealiseerd (status december 2020). Voortgangsbewaking vanuit de CISO is vanwege de beperkte beschikbare tijd slechts beperkt mogelijk. De meeste tijd wordt nu besteed aan de diverse (verplichte/wettelijke) audits en zelfevaluaties die periodiek terugkomen. In het informatiebeveiligingsjaarplan zijn (nog) geen controle en monitoring activiteiten opgenomen ter bewaking van de voortgang en werking van maatregelen, zodat daarop sturing kan plaatsvinden. [Aanbeveling 6]

- Het is van belang te kunnen signaleren dat mogelijke beveiligingsincidenten zich kunnen voordoen of hebben voorgedaan. Een monitoringsysteem en monitoring procedures vervullen daarin een belangrijke rol. Dit is nog niet uitgewerkt in het informatiebeveiligingsbeleid, waardoor een afhankelijkheid bestaat van de activiteiten die door OGD zijn ingericht ten aanzien van monitoring op basis van OGD-beleid, die wellicht niet overeenkomt met de voorwaarden en/of verwachtingen van de gemeente Velsen. Overigens heeft de gemeente Velsen een centraal meldpunt van (potentiële) incidenten bij de CISO (beveiligingsfunctionaris binnen de gemeente) en de Privacy Officer en bestaan korte communicatielijnen tussen deze CISO en zijn collega bij OGD. [Aanbeveling 7, 8]

4.2.4. Vindt er jaarlijkse toetsing plaats op het gebied van informatiebeveiliging?

De volledige vraag:

"Wordt jaarlijks getoetst of de organisatie in control is op het gebied van informatiebeveiliging via peer reviews, audits, self assessments (zelf tests) of penetratietesten?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van de diverse activiteiten die door de gemeente Velsen zelf wordt uitgevoerd om te toetsen of informatiebeveiliging op orde is, door middel van self-assessments, of door meer onafhankelijke onderzoeken uitgevoerd vanuit intern of door een externe partij.

4.2.4.1. *Toelichting*

De gemeente Velsen is vanuit wettelijk oogpunt verplicht om een aantal (onafhankelijke) audits en zelfevaluaties te laten uitvoeren. Audits van BAG, BRO, BRP, BGT en reisdocumenten worden via zelfevaluaties gedaan en zijn in de ENSIA-rapportage opgenomen.

Op dit moment vinden bij de gemeente naast deze verplichte audits geen andere (technische of procedurele) audits of onderzoeken plaats. Er heeft zich wel spontaan een mogelijk voorgedaan om gebruik te maken van een ethisch hacker om de logische toegangsbeveiliging te testen. De bevindingen die daar uit zijn gekomen, zijn direct opgepakt en de noodzakelijke maatregelen zijn geïmplementeerd.

Op basis van de gehouden interviews met de diverse functionarissen en de door de gemeente aangeleverde documentatie zijn wij gekomen tot de volgende opsomming van toetsingen die plaatsvinden voor de gemeente Velsen:

- Accountantscontrole;
- DigiD iBurgerzaken
- DigiD iParticipatie
- Collegeverklaring DigiD en SUWINET (ENSIA) maart 2021;
- DigiD assessment Velsen (aansluiting 999897 rapportagedatum december 2020);
- Zelfevaluatie ENSIA, BRP, BAG, BGT en BRO;
- Baselinetoetsen van onder andere E-suite, HR, Decade, Donau

Tijdens interviews is gemeld dat niet alle audit bevindingen in Key2Control worden opgeslagen, alleen de relevante. Indien bijvoorbeeld de leverancier actie moet ondernemen wordt dat wel in de agenda opgenomen, maar niet altijd in Key2Control vastgelegd. In de nieuwe versie van Key2Control wordt de mogelijkheid geboden om taken/controles beter in te kunnen passen, via een audit module. De gemeente Velsen gaat nog onderzoeken of dat relevant is, maar dit zal niet op korte termijn plaatsvinden.

Voor DigiD zijn de meeste bevindingen op te lossendoor Dimpact, de organisatie waar de DigiD gekoppelde webapplicatie wordt gehost. Het wordt ervaren dat via Dimpact niet altijd adequate opvolging wordt geleverd, terwijl deze organisatie diensten verleent aan vele gemeenten. Suwinet heeft de afgelopen periode een kleine bevinding opgeleverd tijdens de laatste audit, wat snel was opgelost.

Naast de eerdergenoemde self assessments en andere audits, worden in ENSIA ook self assessments opgenomen ten aanzien van BRP, BAG, BGT en BRO. De beperkte bevindingen die daar uit zijn gekomen worden opgevolgd en zijn slechts beperkt relevant voor informatiebeveiliging.

In de ENSIA-audit zijn de uitkomsten van de DigiD assessment en de Suwinet audit in de scope meegenomen. Het college van de gemeente Velsen heeft de ENSIA-collegeverklaring opgesteld en laten toetsen door een onafhankelijke Register EDP Auditor.

Verder is vanuit de jaarrekeningcontrole gemeld dat er niet kan worden gesteund op de General IT Controls. Dit is met name te wijten aan het financiële systeem Decade, dat verouderd is, en daardoor niet aan alle huidige beveiligings- en audit eisen kan voldoen. De gemeente Velsen is van plan om een nieuwe applicatie hiervoor te gaan aanschaffen.

Het overzicht en de beveiligingsstatus van de, door en voor de gemeente Velsen in gebruik zijnde apparaten die direct aan het Internet zijn gekoppeld ontbreekt. De taak van de CISO is in deze situatie een meer toezichthoudende rol en het monitoren van de juiste informatiebeveiligingsmaatregelen. De mogelijkheid tot een website voor bijvoorbeeld de “sportafdeling” geeft aan dat er buiten de gemeentelijke routes om toch ICT gebruikt wordt voor gemeentelijke doeleinden (zogenaamde shadow-IT). Hierdoor kunnen mogelijk kwetsbaarheden ontstaan, aangezien deze omgeving niet bewaakt wordt (in control is) vanuit informatiebeveiliging.

Het ISMS is via Key2Control deels ingericht dat via controls/toetsen activiteiten uitzet in de vorm van een self assessment in de organisatie. De uitvoering van de toetsing door de organisatie werd enige jaren geleden aan het einde van het jaar vaak pas uitgevoerd. Nu wordt een eerste (tussentijdse) inzicht in september opgesteld en door de CISO bewaakt. De voortgang (van de uitvoering) van de taken is nu niet makkelijk inzichtelijk te maken, aangezien Key2Control niet zodanig gebruikt wordt.

4.2.4.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Er worden self-assessments en audits uitgevoerd op grond van wettelijke eisen. Zo worden DigiD assessments, Suwinet audits, jaarrekeningcontrole en de zelfevaluatie voor ENSIA (inclusief delen BAG, BGT, BRO) uitgevoerd en opgevolgd. Elk jaar wordt ook een BIO zelf evaluatie uitgevoerd en in ENSIA gerapporteerd. Het jaarplan 2021 bevat een overzicht van de verbeteringen.

- Uit de diverse onderzoeken komen tekortkomingen naar voren, die niet allemaal in de ISMS-omgeving zijn opgenomen voor de bewaking van de opvolging. Deze zouden moeten worden opgenomen in de kwartaalrapportage van de CISO naar de portefeuillehouder informatiebeveiliging, zodat inzicht in de status wordt vastgelegd en daarmee tijdig een gedegen afweging kan worden gemaakt in de risico’s en de te nemen maatregelen. [Aanbeveling 6]

- Buiten de verplichte/wettelijke onderzoeken hebben in de afgelopen jaren geen andere onderzoeken (technisch of procedureel) plaatsgevonden namens de gemeente Velsen, met uitzondering van een recente spontane actie van een ethisch hacker.
    - Stel een periodiek onderzoek in om vast te stellen, welke externe (Internet gekoppelde) omgevingen van en voor de gemeente Velsen actief zijn. Hierbij kunnen technische testen ondersteunen om dit inzicht te verschaffen.
    - Voer daarnaast technische testen uit (op periodieke basis) om vast te stellen of voor deze systemen en verbindingen kwetsbaarheden aanwezig zijn. Gezien de grootte van de gemeente Velsen is niet te verwachten dat hiervoor intern voldoende kennis beschikbaar

is, waardoor het voor de hand ligt om dit (wellicht in overleg met OGD) door een externe (gespecialiseerde) partij te laten uitvoeren. Stem met de eigenaars/leveranciers af, gekoppeld aan het risico van de geconstateerde kwetsbaarheden welke oplossingstermijn daar aan verbonden wordt en zorg voor actieve bewaking van de voortgang.

- Stem af welke voor de gemeente Velsen relevante beveiligingscontrolemaatregelen door OGD moeten worden uitgevoerd en hoe daarover zal worden gerapporteerd. Door het ontbreken van inzicht in de huidige genomen technische maatregelen door OGD ter voorkoming van hackmogelijkheden en het tijdig constateren van kwetsbaarheden, ontstaat het risico dat de gemeente Velsen er onterecht vanuit gaat dat voor haar afdoende beveiligingsmaatregelen zijn getroffen.
- Voor de SaaS/Cloud applicaties die niet door OGD worden beheerd, is niet vastgelegd hoe de controle op een voor de gemeente Velsen afdoende beveiliging wordt vastgesteld en aan welke voorwaarden deze applicaties zouden moeten voldoen. Het verdient aanbeveling om te onderzoeken of deze omgevingen nu reeds aan de beveiligingsrandvoorwaarden van de gemeente Velsen voldoen en hiervoor een proces op te starten, waarin dit periodiek wordt getoetst.

[Aanbeveling 6]

4.2.5. *Maakt de gemeente gebruik van IBD diensten?*

De volledige vraag:

"Is de gemeente aangesloten en maakt zij gebruik van de diensten en producten van de Informatiebeveiligingsdienst (IBD)?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van de diverse activiteiten die de gemeente Velsen uitvoert, met gebruikmaking van diensten van het IBD.

4.2.5.1. *Toelichting*

Vanuit interviews is opgetekend dat de gemeente Velsen is aangesloten bij de Informatiebeveiligingsdienst (IBD). De CISO is contactpersoon vertrouwelijk en algemeen voor de IBD, de privacy officer is zijn vervanger.

Van diverse documenten en templates wordt door de CISO gebruikt gemaakt van de mogelijkheden die het IBD op dit vlak biedt, zoals daar zijn het informatiebeveiligingsbeleid, het BIO-normenkader en de BIO-gapanalyse voorbeelden

Naast de IBD worden ook diverse andere relevante organisaties in de gaten gehouden. Zo wordt ook de VNG info nauwlettend gecontroleerd op nieuwe aspecten die op de gemeente afkomen.

Recent is een nieuwe opzet gemaakt van een overleg, waarbij de CISO's van ongeveer 20 gemeenten uit Noord-Holland een overleg hebben. In de opzet vergelijkbaar met ISAC's, voorgezeten door CISO Haarlem. De bedoeling is om meer gezamenlijk beveiligingszaken op te pakken. Het eerste voorbeeld is de beveiliging van iBabs applicatie, waar de CISO van Velsen direct betrokken was.

Het privacy team houdt zich eveneens op de hoogte van recente ontwikkelingen die plaatsvinden op het gebied van privacy en AVG via de informatiebeveiligingsdienst (IBD) en de VNG, naast de diverse overlegstructuren intern/extern waar ook de laatste updates en ontwikkelingen op het vakgebied worden besproken. Het gebruik van sociale media (VNG) levert binnenkort een privacy update op, net als de WPG die nu wordt opgepakt.

Vanuit het privacy team zijn er ook een aantal externe overleggen, voornamelijk voor de Privacy Officer:

- Noord-Holland-Noord privacy overleg met collega's van andere gemeenten uit de regio
- IJmond overleg
- VRK (Veiligheid Regio Kennemerland)

4.2.5.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- De gemeente Velsen makt actief gebruik van templates en documenten van het IBD, de CISO is contactpersoon vertrouwelijk en algemeen bij het IBD. Ook is de gemeente actief bij de VNG.

4.2.6. Hoe wordt het college en de raad geïnformeerd over informatiebeveiliging en privacybescherming?

De volledige vraag:

"Hoe wordt het college van B&W en de gemeenteraad geïnformeerd over informatiebeveiliging en privacybescherming?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van het verkrijgen van inzicht in de informatie-uitwisseling naar de raad en college van B&W, middels interviews met de portefeuillehouder Informatiebeveiliging en Privacy van het college van B&W, de gemeentesecretaris. Er hebben geen interviews plaatsgevonden met vertegenwoordigers van de raad.

4.2.6.1. *Toelichting*

In feite zijn hier twee informatiestromen in beeld.

1. Informatie-uitwisseling vanuit de organisatie (CISO, Privacy team) naar het college (via de portefeuillehouder).

Er zijn diverse overlegstructuren aanwezig binnen de gemeente Velsen. Zo is er een TIP-overleg, een periodiek operationeel overleg, waarbij zowel Privacy, informatiebeveiliging en de controller aanwezig zijn. In dit overleg worden de "dagelijkse" operationele activiteiten besproken. Daarnaast zal bij de staf overleggen van concern control en Informatie security en privacy onderwerpen regelmatig besproken worden en indien nodig actie ondernomen.

Er is een wekelijks operationeel overleg, waarin indien noodzakelijk beveiligingsissues besproken kunnen worden. ENSIA-status/rapportages of andere uitgevoerde testen worden in team Informatie besproken, zodat er van geleerd kan worden en eventuele verbeterpunten kunnen worden opgepakt. Enkele malen per jaar is een algemeen overleg waarin security onderwerpen worden besproken. Zo was de manager Informatie direct betrokken bij de "hacking activiteiten" die vanuit het Tv-programma werden uitgevoerd, waarbij de CISO het voortouw had.

Rapportage/verantwoording is aan de gemeentesecretaris en de portefeuillehouder. Jaarlijks krijgen de gemeentesecretaris en de portefeuillehouder via de ENSIA-rapportage en het jaarplan inzicht in de status van informatiebeveiliging en middels het privacy jaarplan ook inzicht in de status van AVG/privacy. Afstemming is er tussen Privacy en CISO over gezamenlijke (overlappende) onderwerpen.

Specifieke mijlpalen worden in overleggen gemeld. Verder is het jaarplan de basis en worden er geen andere (tussentijdse) rapportages opgesteld. De ENSIA verantwoordingsrapportage over de implementatie van de BIO en de jaarrapportage Privacy worden via een collegebericht aan de raad gestuurd (de standaard route voor communicatie vanuit het team naar de raad). Indien noodzakelijk zal de portefeuillehouder actie ondernemen indien het privacy team of de CISO erom vraagt. Verder is er geen proactieve rol voor de portefeuillehouder belegd.

Er zijn diverse overlegvormen waar vanuit privacy en/of beveiliging aan wordt deelgenomen:

- Elke 6 weken met het sociaal domein (Privacy)
- Elke 6 weken met de gemeentesecretaris
- Elke 2 weken is er een stafoverleg (concerncontroller)
- Elke 4 weken met de portefeuillehouder
- Elke 3 weken een TIP (voortgangs-) overleg (Informatiebeveiliging en Privacy en de controller)

2. Informatie-uitwisseling vanuit de portefeuillehouder naar de gemeenteraad.

De techniek van de IT (en daarmee ook de daar aan gekoppelde informatiebeveiliging) is grotendeels a-politiek, waardoor het lastig is om als raadslid hier iets vanuit politiek standpunt van te vinden. Hackers hebben diepgaande kennis, raadsleden in de regel veel minder en zeker bij kleine partijen. Via de reguliere activiteiten, zoals bijvoorbeeld vanuit de accountantsrapportage en ENSIA-resultaten wordt de raad geïnformeerd over informatiebeveiliging,. Er is beperkt behoefte aan verdieping in bedrijfsvoering. Een samenvatting van de status, is minder relevant. De achterliggende info is vaak veel belangrijker. Vanuit de wettelijke regelingen zoals ENSIA, AVG en jaarrekeningcontrole zijn dit de momenten waarop de raad geïnformeerd wordt over de status. De gemeenteraad is niet bovenmatig inhoudelijk betrokken bij informatiebeveiliging en privacy, waardoor de communicatie vooral vanuit de organisatie gedaan naar de raad en slechts beperkt terugkoppeling wordt gedaan vanuit de raad.

Informatiebeveiliging en privacy staan als onderwerp op de agenda in de raadsvergadering en betreft met name de accountantscontrole plus IB-paragraaf (onder geheimhouding) en de ENSIA-rapportage. Vertrouwelijke stukken zijn via de griffie in te zien of op te vragen. Jaarlijks wordt via het jaarverslag in een paragraaf informatieveiligheid de gemeenteraad geïnformeerd door het college. Er hebben slechts beperkt beveiligingsincidenten plaatsgevonden in het verleden. Er wordt wel terughoudend (vertrouwelijk) gecommuniceerd over details van een incident, om niet te veel publiekelijk bekend te laten raken. Het is afhankelijk van het incident, welke keuze gemaakt wordt hoe te communiceren door de portefeuillehouder naar buiten (inclusief de raad) na overleg met de gemeentesecretaris en het college besloten. De spontane actie van de ethisch hacker (Tv-programma) zou wel met de gemeenteraad zijn gedeeld.

4.2.6.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Vanuit de organisatie naar het college van B&W verloopt de communicatie via de portefeuillehouder. Hiervoor zijn diverse overlegvormen aanwezig. Operationeel worden indien noodzakelijk direct acties besproken en opgevolgd.

Ter overweging willen wij het volgende mogelijke verbeterpunt naar voren brengen:

Over het algemeen heeft de raad slechts beperkt inzicht in informatiebeveiliging en privacy nodig om haar taken uit te voeren. Onderzoek welke taak/rol de gemeenteraad zich stelt op dit onderwerp en bepaal of hier specifiek aandacht voor nodig wordt geacht vanuit de raad.

Bij diverse gemeenten is een “auditcommissie” ingesteld, die vanuit de raad met name de jaarrekeningcontrole en aanverwante zaken namens de raad onderzoekt, en dit weer terugkoppelt naar de raad. Het takenpakket van deze commissie kan/dient met informatiebeveiliging te worden uitgebreid. Een dergelijke opzet kan ook voor de gemeente Velsen mogelijk zijn. Daarnaast kan de raad op deze manier de gemeente bevragen over de status van de wettelijke verplichtingen en algemeen over de beveiligingsdoelstellingen die de gemeente zich heeft voorgesteld.

4.2.7. In hoeverre voldoet de gemeente aan de privacy/AVG wetgeving?

De volledige vraag:

"In hoeverre heeft de gemeente Velsen de privacybescherming op orde?"

In het onderzoek hebben we deze vraag toegevoegd op verzoek van de rekenkamercommissie en de gemeente aan de bestaande 11 deelvragen. Bij deze deelvraag zijn we uitgegaan van de stappen die worden doorlopen zoals vermeld in het AVG-implementatiemodel van het IBD, waarin de 7 thema's gezamenlijk alle onderdelen omvatten die vanuit de wetgeving van een gemeente mogen worden verwacht.

4.2.7.1. *Toelichting*

Aan de hand van deze 7 thema's, interviews met het privacy team van de gemeente Velsen, het jaarplan 2021 en de status update van september 2021, is de huidige stand van zaken onderzocht.

<u>Privacy beleid</u>
Er is een overkoepelende Privacy beleid dat stamt uit 2016, waarbij nog verwezen wordt naar de BIG i.p.v. de huidige BIO en naar de gezamenlijke aanpak van de IJmond-gemeenten. Voor het sociaal domein is er een separaat privacy beleidsdocument opgesteld, dat echter tot 2018 geldig was. Ook voor het HR-domein is een separaat beleidsdocument in wording.

<u>Organisatorische inbedding</u>
De implementatie om te voldoen aan de AVG (Algemene Verordening Gegevensbescherming) vraagt naast een beleid en processen ook inbedding van de Functionaris Gegevensbescherming (FG) en een Privacy Officer/Functionaris (PO) op de juiste positie binnen de gemeente. Beiden zijn sinds september 2020 aangesteld, en hebben een duidelijke rol en plek in de organisatie. De FG heeft een onafhankelijke rol en vervult naast de FG-functie ook een interne auditfunctie. De taken en verantwoordelijkheden zijn niet vastgelegd in een functie en/of rol beschrijving vanuit de personeelsadministratie. De taken van de FG zijn opgenomen in het privacy beleidsdocument. De diverse taken omvatten onder andere het:

- Opstellen van een Privacy beleid;
- Opzetten en zo compleet mogelijk maken van een Register van verwerkingen;
- Opzetten en regelen van Verwerkersovereenkomsten met verwerkers waar verwerkingen van persoonsgegeven van burgers uit de gemeente Velsen plaatsvinden.
- Opzetten diverse procedures voor de afhandeling van verzoeken etc.
- Bewustwording binnen de organisatie vergroten.

Om de reikwijdte van de AVG in de organisatie te vergroten is gekozen om ambassadeurs in de organisatie aan te wijzen, die het voorportaal van het privacy team vormen en ook in de uitvoering van activiteiten een rol (zullen) kunnen spelen. De ambassadeurs zitten nog in de beginfase van hun "carrière".

<u>Processen</u>
Het privacy team is nog volop bezig met de implementatie en uitvoering van de vele stappen die vanuit de AVG/Privacy wetgeving van een gemeente worden gevraagd. Een aantal onderdelen daarvan hebben een direct verband met het identificeren van risico's en de daarvan af te leiden maatregelen die moeten worden getroffen ter bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie.

Binnen de gemeente Velsen bestaat onder andere al een “Procedure beveiligingsincidenten en datalekken”.

Verwerkingsregister
Er is een verwerkingsregister opgesteld, echter de jaarlijkse update die vanuit de organisatie moet worden opgepakt, heeft nog niet plaatsgevonden. Het register is uitgebreid met de VNG-eisen en daarnaast ook aangevuld met eigen Velsen specifieke informatie. Het overzicht van 470 registraties is nu niet helemaal accuraat meer en ook nieuwe registraties moeten nog worden toegevoegd. In principe vanaf nu mede door de aangestelde contactpersonen (ambassadeurs) vanuit de organisatie, ondersteund vanuit het privacy team.

DPIA’s
Er zijn ongeveer 20 kritieke systemen geïdentificeerd, voornamelijk bestaande uit systemen en applicaties voor de verplichte dienstverlening van de gemeente Velsen. Deze bestaan uit systemen op locatie van de gemeente, maar ook diensten in beheer bij een externe partij (zoals Pink Roccade), extern gehoste diensten zoals bij Dimpact en volledige SaaS-applicaties. Niet voor alle systemen is vooralsnog een DPIA proces doorlopen.

Hoe het uitvoeren van een privacy impact analyse dient te geschieden (volgens het DPIA-proces) is beschreven en op het intranet beschikbaar en toegelicht. De uitvoering moet nog grotendeels plaatsvinden. Er zijn er nu 6 à 7 gedaan. Het plan is om allereerst met de 9 ambassadeurs uit de afdelingen een inventarisatie te doen van de werkzaamheden, waarna een actieplan zal worden opgesteld waarin wordt vastgelegd, welke, wanneer zullen worden opgepakt. Naar verwachting zullen hooguit enkele DPIA’s worden opgeleverd per ambassadeur. Daarna zal moeten worden besloten hoe voor het DPIA-proces de inhaalslag zal worden uitgevoerd. Er zijn in totaal 470 verwerkingen, waarvan door het privacy team moet worden bepaald, voor welke een gedetailleerde DPIA noodzakelijk is. Normaal gesproken zullen voor de belangrijke applicaties en voor die applicaties waar persoonsgegevens in verwerkt worden, DPIA’s worden uitgevoerd. Er zijn op dit moment 6 DPIA’s uitgevoerd en in Key2Control vastgelegd/geregistreerd (zie ook de eerdere vraag over het in control zijn van informatiebeveiligingsrisico’s).

Andere processen
Er is een privacy email adres beschikbaar, maar de meeste datalekken worden direct bij de PO gemeld. Dit wordt in Key2Control vastgelegd, van waar uit eventueel de AP wordt geïnformeerd. Er kwam 1 incident via het Samenlevingsdomein binnen en 1 via de CISO. 90 % komt op een goede manier binnen. Specifieke rapportages hierover worden niet opgesteld. Dit komt in de standaardrapportages terecht.

<u>Rechten van betrokkenen</u>
De belangrijkste fundamenten zijn reeds ingericht en opgesteld, zoals beleidsdocumenten en de diverse procedures waaronder rechten van betrokkenen en het melden van datalekken. Er zijn sinds de inrichting een zestal verzoeken geregistreerd en tijdig opgepakt en afgerond.

De communicatie ten aanzien van datalekken en de te doorlopen stappen worden in de praktijk toegepast, echter een formeel communicatieplan is nog niet opgesteld.

<u>Samenwerking</u>
De introductiebijeenkomst voor nieuwe medewerkers bestaat ook uit een privacy agendapunt door de FG/PO gegeven, inclusief een quiz. Inhuur wordt ook in het introductieprogramma meegenomen.

De afspraken met externe partijen (inhuur) worden niet altijd op tijd gemaakt, doordat dit soms 1 dag voor de start wordt gemeld. Er worden geheimhoudingsverklaringen getekend.

Beveiliging
Er is regelmatig afstemming met CISO over gezamenlijke onderdelen, zoals het beveiligingsbeleid en de dataclassificatie. Een Datalekprotocol is aanwezig met instructie voor de gebruikers.

Actuele communicatie over recente/zinvolle privacy gebeurtenissen, wordt gedaan via de interne kanalen (intranet). Bij een recent data lek is een workshop met de betrokkenen geweest.

Verantwoording
Periodiek wordt het jaarplan opgeleverd met de actuele status. De activiteiten worden in Key2Control ondergebracht en bewaakt. De detailstatus op basis van het VNG Privacy Model wordt in een Excel document handmatig bijgehouden. Deze wordt nu 1 maal per jaar bijgewerkt.

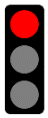
Nr.	Actie	Percentage gereed
1.	beleid	64
2.	Processen	57
3.	Organisatorische inbedding	88
4.	Rechten van betrokkenen	53
5.	Samenwerking	78
6.	Beveiliging	43
7.	Verantwoording	69

Vanuit het VNG Privacy Model zijn een groot aantal activiteiten gedefinieerd die noodzakelijk zijn om aan de AVG/Privacy wetgeving te voldoen. Deze zijn over de 7 bovenstaande onderwerpen verdeeld. Het percentage geeft aan, hoeveel procent van de activiteiten uit het VNG-model voor het betreffende onderwerp al volledig zijn geïmplementeerd volgens het privacy team.

4.2.7.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Enkele belangrijke fundamenten zijn reeds ingericht en opgesteld, zoals beleidsdocumenten en de diverse procedures waaronder rechten van betrokkenen en het melden van datalekken.

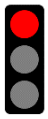


- Wij constateren dat veel activiteiten al (deels) zijn uitgevoerd, maar nog niet afgerond zijn. Er blijft nog genoeg te doen door de Privacy Officer (PO) en de Functionaris Gegevensbescherming (FG), zoals in de onderstaande tabel in procenten is weergegeven. Het onderstaande percentage geeft aan, hoeveel procent van de AVG/Privacy activiteiten vastgelegd in het VNG Privacy Model al zijn afgerond. [Aanbeveling 1]

Nr.	Actie	Percentage gereed
1.	beleid	64
2.	Processen	57
3.	Organisatorische inbedding	88
4.	Rechten van betrokkenen	53
5.	Samenwerking	78
6.	Beveiliging	43
7.	Verantwoording	69

- Het overzicht van de actuele status van de privacy implementatie werd tot nu toe slechts 1 maal per jaar bijgewerkt, terwijl gedurende het jaar vele verbeteractiviteiten worden doorgevoerd. De huidige Key2Control applicatie faciliteert daar in, echter het was vanwege de tijddruk niet haalbaar om Key2control juist te gebruiken en vaker rapportages uit te draaien en om vaker een update in het dashboard te verwerken. Gezien de vele activiteiten op dit vlak, biedt een kwartaalrapportage een beter inzicht in de actuele status en daarbij de mogelijkheid om prioriteiten te kunnen stellen. [Aanbeveling 1]

- Een communicatieplan over het belang, de implementatie de uitvoering en naleving van de AVG/Privacy aspecten voor de medewerkers van de gemeente Velsen is er niet, maar de uitvoering wordt wel gedaan. Het verdient aanbeveling om dit plan op te stellen, zodat ook de ambassadeurs dit kunnen gebruiken. Bijvoorbeeld, dat privacy afspraken rondom inhuurkrachten ook moeten worden vastgelegd, aangezien het af en toe voorkomt, dat afdelingen dit erg laat pas melden. [Aanbeveling 1]



- De Gemeente Velsen heeft inzicht in welke verwerkingen een hoog risico kennen en daarmee om een verplichte DPIA (Data Protection Impact Assessment) moeten doorlopen. Deze uitvoering moet nog deels plaatsvinden. Er zijn er nu 6/7 gedaan. Het plan is om allereerst met de 9 personen uit de afdelingen een inventarisatie te doen van de werkzaamheden, waarna een actieplan zal worden opgesteld waarin wordt vastgelegd, welke, wanneer zullen worden opgepakt. Naar verwachting zullen hooguit enkele DPIA's worden opgeleverd per contactpersoon voor het einde van het jaar. Daarna zal moeten worden besloten hoe voor het DPIA-proces de inhaalslag zal worden uitgevoerd. Het verdient aanbeveling om hier prioriteit aan te geven, aangezien dit de basis vormt van de te nemen beveiligingsmaatregelen. [Aanbeveling 1]

- Er is nog werk te verrichten in het up-to-date brengen en houden van de verwerkers-overeenkomsten (ongeveer 470). Een apart overzicht waarin de gemeente Velsen bijhoudt voor welke derde partijen een verwerkersovereenkomst is afgesloten en of deze voldoet, ontbreekt vooralsnog. Nog niet voor alle relevante derde partijen is een adequate verwerkersovereenkomst afgesloten. Daarnaast is het up-to-date houden van deze lijst een taak van de eigenaren van de systemen/processen/data. Dat deze taak periodiek moet worden uitgevoerd, is niet bij iedereen bekend en/of wordt niet periodiek uitgevoerd. [Aanbeveling 1]

4.3. Fase 2: Operationele deelvragen

Een aantal deelvragen beschrijven de operationele invulling van het fundament van informatiebeveiliging en privacy. In deze paragraaf worden deze deelvragen uitgeschreven met de bijbehorende bevindingen en tevens worden voorstellen tot verbetering vermeld voorzien van een prioriteitsindicatie.

4.3.1. Hoe is het proces rondom het informatiebeveiligingsbewustzijn van medewerkers ingericht?

De volledige vraag:

"Op welke wijze wordt aandacht gegeven aan het bewustzijn onder medewerkers op het gebied van informatiebeveiliging en privacy?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van de diverse activiteiten die door de gemeente Velsen zelf wordt uitgevoerd om bewustzijn te creëren en te toetsen in hoeverre de opgedane kennis in de praktijk wordt toegepast.

4.3.1.1. *Toelichting*

In elke organisatie, maar zeker ook gemeenten lijkt, het bewustzijn van de "gevaren" die op het gebied van informatiebeveiliging voorbijkomen, elk jaar een grotere uitdaging te worden. Er zijn genoeg voorbeelden van organisaties waar het bewustzijn (of het gebrek daaraan) heeft kunnen leiden tot vervelende gevolgen. Ook de gemeente Velsen heeft al eens (kleinere) datalekken gehad en recent heeft een tv-programma aangetoond dat met hulp van een ethisch hacker toegang tot gemeentelijke systemen kon worden verkregen.

Uit interviews is gebleken dat de medewerkers van de gemeente Velsen gemotiveerd zijn in hun werk, maar waarbij niet voor iedereen inzichtelijk is, wie waarvoor verantwoordelijk is. Daarnaast is over het algemeen het bewustzijnsniveau ten aanzien van informatiebeveiliging als vrij laag ingeschat.

600 medewerkers motiveren met steeds weer nieuwe, recente en tevens interessante informatie aanleveren is een hele klus, mede daarom is enige tijd geleden een E-learning tool aangeschaft. Met deze tool kan in de regel via een eerste actie, bijvoorbeeld via een phishing mail test, een nulmeting worden gedaan om het huidige niveau van bewustzijn te bepalen. Door dit later te herhalen kan worden vastgesteld in welke mate het bewustzijn is veranderd en hopelijk is verbeterd.

De E-learning omgeving is beschikbaar voor iedere medewerker van de gemeente Velsen, bestaande uit een drietal mogelijke vormen: Een sessie/training van een half uur met een testje om vast te stellen of de kennis is opgepikt, een flash sessie van 5 minuten en een korte update van ongeveer 1 minuut. De CISO heeft hier een schema voor opgesteld, waarbij ongeveer elke twee maanden een update of activiteit is gepland. Binnen de gemeente Velsen heeft volgens de cijfers slechts 3 % van de medewerkers hieraan mee gedaan. Dit geeft aan dat de huidige opzet niet de aandacht van de medewerkers heeft gekregen die het wel verdient. Let wel, er is hierbij vooraf geen verplichting tot deelname gesteld.

In het verleden is een "mystery guest" eenmalig langs geweest, die destijds niet snel is ontdekt. In juli 2021 is een (interne) phishing test (voor gratis oordopjes) gedaan, 50 % van de aangeschreven mensen (intern, raadsleden etc.) hadden niet als zodanig herkend en 80 % daarvan heeft zelfs de inloggegevens

gedeeld. Alle lagen binnen de organisatie zijn hierbij overigens door de mand gevallen. Hieruit zou je kunnen concluderen dat het bewustzijn relatief laag is, en dat het lerende effect (lezen van de toelichting) ook beperkt is. De noodzaak tot het vergroten van bewustzijn is daarmee wel aangetoond.

Naast deze actieve vorm om het bewustzijn van medewerkers inzichtelijk te maken en te verhogen, zijn er binnen de gemeente Velsen diverse andere activiteiten op dit terrein aanwezig.

Het securityteam en privacy team houden op het intranet informatie over recente zinvolle beveiligings- en privacyaspecten bij, zodat medewerkers daar meer detailinformatie kunnen bekijken, zoals hoe herken ik een phishing mail. Ook vanuit het College worden af en toe vragen gesteld over recente beveiligingsincidenten in overheidsland, zoals het Hof van Twente.

De CISO houdt voor nieuwe medewerkers een inleiding over informatiebeveiliging binnen de gemeente en waar de medewerker rekening mee dient te houden in zijn/haar dagelijks werk. Daarbij wordt een training aangeboden genaamd: Basistraining Informatiebeveiliging. Basisinformatie ten aanzien van informatiebeveiliging kan tevens op het intranet worden teruggevonden. De training wordt aangeboden vanuit HR. Ook Privacy bewustzijn is opgezet als een basistraining/toelichting die door het privacy team wordt gegeven tijdens de introductie van nieuwe medewerkers, waarbij ook een quiz wordt gedaan.

Tenslotte, indien relevant wordt binnen de organisatie ook een (college) bericht verstuurd, zoals het voorbeeld van het eerdergenoemde tv-programma. Aan de hand van die hackpoging is de gemeente intern geïnformeerd over de achtergrond en de inhoud van de actie.

Bij navraag over de kennis op het gebied van informatiebeveiliging zijn medewerkers vooral bekend met een aantal algemene regels, zoals

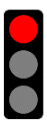
- Schermafsluiting en Cleandesk.
- Beveiligde bestandsuitwisseling wordt met externe partijen gebruikt.

Er is nog genoeg te doen ten aanzien van de algemene bewustwording op het gebied van informatiebeveiliging in de interne organisatie.

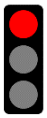
4.3.1.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Er is een bewustzijnsprogramma beschikbaar, daarnaast worden introductiesessies gehouden voor nieuwe medewerkers van de gemeente Velsen, waarin ze een toelichting krijgen van de CISO en de Privacy Officer hoe informatiebeveiliging en AVG/Privacy zijn ingericht binnen de gemeente Velsen.



- Het verdient aanbeveling om te onderzoeken hoe de medewerkers actiever het e-learning programma gaan doorlopen. Denk daarbij bijvoorbeeld aan een verplichting tot deelname hieraan te koppelen (mits dat binnen de cultuur van de organisatie past) of het winnen van een prijs. [Aanbeveling 2]



- Onderzoek of het aanbod van kennisdeling en bewustwording, naast de toetsing via phishing mailtjes en een eerdere uitgenodigde “mystery guest”, andere manieren kunnen worden ingezet om medewerkers nog meer bewust (en enthousiast) te maken voor privacy en informatiebeveiliging. [Aanbeveling 2]

- Onderzoek of het aanstellen van ambassadeurs ten aanzien van informatiebeveiliging op in de organisatie mogelijk is, naar het voorbeeld hoe privacy in de organisatie voorposten en voelsprieten heeft opgesteld. Hierdoor ontstaat een grotere impact op de organisatie en de betrokkenheid van de organisatie bij het onderwerp wordt daarmee eveneens groter. Betrokkenheid en medewerking van de organisatie krijg je niet (alleen) door vanuit het management of de directie beleid op te leggen en te bewaken. Door de organisatie meer (en actief) te betrekken, bijvoorbeeld via ambassadeurs verloopt dit soepeler. [Aanbeveling 1, 6, 8]

4.3.2. *Is de continuiteit van de dienstverlening gewaarborgd in geval van een beveiligingsincident?*

De volledige vraag:

"Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van een informatiebeveiligingsincident en hoe is dat geregeld?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van de diverse activiteiten die worden uitgevoerd door de gemeente Velsen naar aanleiding van (relatief kleine) beveiligingsincidenten. Hierbij is op onderdelen ook OGD betrokken. De continuïteitsaspecten worden bij de deelvraag over grote incidenten toegelicht.

4.3.2.1. *Toelichting*

Vanuit het informatiebeveiligingsbeleid is geen specifiek beleid uitgewerkt/opgesteld ten aanzien van de afhandeling van beveiligingsincidenten. Er bestaat een procedure (aanpak) hoe om te gaan met beveiligingsincidenten, echter die is aan vernieuwing toe. Zo is de definitie van een beveiligingsincident wellicht wat algemeen gedefinieerd. In de procedure zijn de benodigde stappen beschreven en in een workflow vastgelegd. Er is in het procesdocument ook opgenomen hoe om te gaan met privacy issues, zoals datalekken.

Op dit moment is de CISO vanuit de gedocumenteerde procedure formeel de enige contactpersoon die is aangewezen om beveiligingsincidenten op te pakken. In de praktijk is dit uiteraard niet mogelijk (vakantie/ziekte), waardoor het zinvol lijkt om de privacy officer als reserve aan te wijzen.

De procedure is beschikbaar op het intranet, waar ook een formulier is opgenomen, dat helpt bij het verzamelen van relevante informatie om zo snel en efficiënt mogelijk het incident op te lossen. De melding wordt echter in de meeste gevallen direct richting de CISO gedaan en wordt het formulier niet actief gebruikt.

Indien een beveiligingsincident zich voordoet, zal de CISO een eerste review uitvoeren van de melding en een classificatie van het incident doen. Dit bepaalt ook of opgeschaald moet worden naar een eventuele escalatiemodus/crisis. Tot nu toe zijn dit jaar 4 beveiligingsincidenten vastgelegd door de CISO en in een Excel lijst verder bewaakt. De Key2Control applicatie biedt geen ondersteuning voor dit proces. Het jaar daarvoor zijn 3 incidenten geregistreerd. De meldingen komen binnen bij de CISO of de Privacy Officer, en zijn vooral kleine incidenten, zoals verkeerd verzonden emails, via mail-distributielijsten of soortgelijke incidenten. Deze zijn uiteraard wel gemeld bij de AP.

Niet alle beveiligingsincidenten worden geregistreerd en ook niet alle incidenten worden volledig volgens de procedure afgehandeld. Bijvoorbeeld de acties van de "ethische hacker" waren ten tijde van het onderzoek nog niet helemaal verwerkt in de registratie/administratie. Deze is overigens wel gemeld aan de manager Informatie en de gemeentesecretaris. Daarnaast worden phishing mailtjes niet allemaal (meer) vastgelegd. Er is nu een tool ingericht van Symantec (Messagelabs) die veel phishing mailtjes kan blokkeren, voordat ze bij de eindgebruiker terechtkomen.

Via de servicedesk worden door medewerkers gemelde phishing mailtjes verwerkt door OGD in deze blocking tool zodat deze niet meer doorkomen binnen de organisatie. De afgelopen periode zijn er ongeveer 1-2 per week nog doorheen gekomen. Daarnaast helpt de CISO regelmatig medewerkers die om advies vragen of een mailtje een phishing mailtje is.

Rapportage over beveiligingsincidenten wordt meegenomen in de periodieke CISO-rapportages. Indien noodzakelijk zal een groter incident via de portefeuillehouder/gemeentesecretaris ook aan de raad/college worden gemeld buiten de standaard rapportages om.

Voor de meest risicovolle mogelijke beveiligingsincidenten, zoals wellicht ransomware en/of phishing mailtjes, zijn op dit moment nog geen scenario's of draaiboeken opgesteld. Hierbij wordt nu gesteund op de expertise van OGD en het team van de gemeente Velsen. Een analyse, welke beveiligingsincidenten de meeste risicovolle/relevante zijn om voor te bereiden voor het geval dat, is niet aanwezig.

Vanuit OGD is de Teamleider Servicedesk verantwoordelijk voor de uitvoering van het incident managementproces. Naast incidenten valt hier ook het afhandelen van security incidenten onder. Specifieke afspraken over het type incidenten die hieronder vallen zijn uit de definitie vanuit BIO overgenomen. SPAM-mailtjes worden ook als incidenten gezien, met name voor trendanalyses. Elke maand worden bij OGD zo'n 10-12 security incidenten gemeld, uitgezonderd SPAM/Phishing. Logging en monitoring wordt nu door OGD uitgevoerd op basis van de dienstverlening, waaruit eventueel incidenten kunnen worden afgeleid. Voor eventuele afwijkende detailafspraken is de Security Officer van de gemeente Velsen verantwoordelijk. De Teamleider Servicedesk van OGD is verantwoordelijk voor de uitvoering. Bij escalatie zijn de afspraken, die in het contract en de DAP zijn vastgelegd leidend.

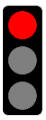
4.3.2.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Het afhandelen van incidenten inclusief beveiligingsincidenten wordt zowel door de gemeente Velsen als ook door OGD gedaan. OGD zal in de periodieke rapportages hierover rapporteren naar de CISO, via de servicelevel rapportages. Voorheen, voordat OGD de technische beheertaken had overgenomen, was de CISO vanuit de gemeente Velsen het centrale aanspreekpunt. Nu is er een Servicedesk die vanuit OGD vaak de eerste meldingen aanneemt. Nu, nadat OGD een actievere rol in het afhandelen van beveiligingsincidenten heft gekregen, verdient het aanbeveling om duidelijke afspraken te maken, over wie wanneer en wat doet en waar dit wordt vastgelegd. [Aanbeveling 8,9]

- Update de incidentafhandelingsprocedure (en stel daarbij tevens beleidsuitgangspunten op), waarbij duidelijke definities van beveiligingsincidenten zijn vastgelegd, die nu vrij algemeen zijn beschreven. Neem ook een toelichting op naar de medewerkers ten aanzien van het gebruik van het registratieformulier. Tenslotte, neem in de definities en afspraken op dat alle meldingen worden vastgelegd. Zo is het zinvol om alle phishing mailtjes die worden ontvangen ook worden geregistreerd, zodat deze kunnen worden verwerkt in een trendanalyse. [Aanbeveling 8]

- Leg vast wie het centrale aanspreekpunt vanuit de gemeente Velsen is, indien de CISO niet aanwezig/beschikbaar is. Mogelijk kan het privacy team, denk daarbij bijvoorbeeld aan de Privacy Officer hier als back-up optreden. Zorg dat dit gecommuniceerd worden binnen de organisatie, zodat er geen verwarring ontstaat met de activiteiten die door OGD (in de uitvoering) worden gedaan. [Aanbeveling 8, 9]



- Stel, in overleg met OGD, draaiboeken op voor de afhandeling van veel voorkomende beveiligingsincidenten en stel scenario's op wat te doen indien een phishing aanval plaatsvindt. Hierdoor ontstaat een efficiënte afhandeling en wordt voorkomen dat een incident grote consequenties tot gevolg kan hebben. Een geslaagde phising aanval kan een opstart tot een ransomware aanval zijn, waarna de consequenties desastreus kunnen zijn. Wellicht kan de ramp nog wat ingeperkt worden als het in een vroegtijdig stadium wordt ontdekt. Hierop voorbereid zijn zal het op gang brengen van het herstel vooral bespoedigen maar de impact zal onverminderd groot zijn, dus ook een ransomware scenario draaiboek is noodzakelijk. [Aanbeveling 5]

4.3.3. Is oneigenlijke toegang tot gemeente Velsen informatie mogelijk?

De volledige vraag:

"Is het mogelijk oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Velsen in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?"

In het onderzoek hebben we bij deze deelvraag onderzoek gedaan naar de diverse mogelijkheden om toegang te verkrijgen tot de systemen van de gemeente Velsen, waarbij tevens is onderzocht in welke vorm deze toegangspaden worden bewaakt, gemonitord. Qua uitvoering is dit onderwerp voornamelijk vanuit interviews en opgevraagde documentatie onderzocht en zijn er geen technische tests uitgevoerd. Reden hiervoor is dat het uitvoeren van een technisch onderzoek relatief veel tijd kost en indien de scope niet goed is afgebakend de resultaten beperkte toegevoegde waarde bieden, of onvolledige antwoorden opleveren. In overleg met de rekenkamercommissie is dit besproken, waarbij in de aanbevelingen en prioriteiten specifiek hier aandacht aan wordt besteed.

4.3.3.1. *Toelichting*

Hierna volgt eerst een beschrijving van de toegang tot het interne netwerk, waarna de toegang vanaf extern wordt toegelicht. Tenslotte wordt ingegaan op de consequenties die dit voor burgers kan hebben.

Intern
Het interne netwerk van de gemeente Velsen is bereikbaar vanuit het gemeentehuis (locaties Dudokplein en Plein 1945), de brandweerkazerne (als uitwijklocatie) en enkele (werkplek) aansluitingen in de gemeente voor wijkondersteuning. Het zwembad wordt wel onder de gemeentevlag beheerd, andere locaties /voorzieningen niet. Deze zijn niet aangesloten op het interne netwerk van de gemeente Velsen.

De fysieke toegang tot de gebouwen en ruimtes daarbinnen is volledig in eigen beheer bij de gemeente Velsen. Toegang wordt slechts verkregen via een toegangspas, deuren zijn voorzien van een pasjeslezer. Kantoor en werkruimtes van de gemeente zijn niet direct bereikbaar, slechts via de balie/receptie. Let wel, middels een toegangspasje is toegang tot het Dudok-gebouw mogelijk, zonder actieve bewaking aanwezig is, waardoor volledig op het bewustzijn van de medewerker wordt gesteund, om geen onbevoegden binnen te laten.

Binnen de gebouwen van de gemeente Velsen is het aansluiten van externe apparaten aan het interne netwerk afgeschermd via tooling (Quarantainenet), die herkent dat een onbekende laptop (bijvoorbeeld van een inhuurkracht) is aangesloten. Deze wordt automatisch afgeschermd, zodat alleen toegang tot het Internet wordt geleverd en geen toegang tot het interne gemeente Velsen netwerk mogelijk is.

Vanuit het interne netwerk heeft een medewerker nadat is ingelogd op het Windows domein, toegang tot een aantal applicaties via Single Sign-On (SSO). Er is beleid opgesteld ten aanzien van logische toegangsbeveiliging en het gebruik van wachtwoorden. Voor de toegang tot systemen en applicaties zijn procedures opgesteld voor de aanvraag, wijziging en verwijdering indien een medewerker de gemeente Velsen verlaat. Deze procedures zijn reeds enige tijd actief en dienen ervoor te zorgen dat medewerkers slechts toegang krijgen afgeleid vanuit het functieprofiel, waarbij de goedkeuring van de manager en de systeemeigenaar een onderdeel van het totale goedkeuringsproces uitmaken. Uitzonderingen hierop moeten separaat geaccordeerd worden.

Nadat toegang is verkregen tot de gemeente Velsen ICT-omgeving via een Windows account (en wachtwoord) hebben medewerkers nog geen directe toegang tot gemeentelijke applicaties. Hiervoor wordt door de betreffende functionele applicatiebeheerder een autorisatieformulier afgestemd met de afdelingsmanager/systeemeigenaar, zodat de medewerker de juiste rechten krijgt in de applicatie zelf. Hierbij wordt ook gekeken naar specifieke randvoorwaarden en “do’s en dont’s”. Na goedkeuring en toekenning van de rechten, is het pas mogelijk voor de medewerker om in de applicatie activiteiten uit te gaan voeren. Dit is volgens het principe “geen-toegang tenzij”.

Veel systemen bieden de mogelijkheid om gebeurtenissen te registreren, echter bij de gemeente Velsen is dit beperkt ingericht voor de Windows omgeving en de firewall (voor de Internet koppeling). Beschikbare logs worden voornamelijk gebruikt om achteraf vast te stellen, wanneer en wellicht door wie een bepaalde activiteit is uitgevoerd. Applicaties en Cloud omgevingen (zoals Azure) bieden logmogelijkheden, maar zijn niet standaard ingesteld om beveiligingsgebeurtenissen te registreren. Er zijn ook applicaties die al 5 jaar op de nominatie staan om te worden uit gefaseerd, maar nog steeds actief zijn (bijvoorbeeld Corsa). Het beheer van dergelijke applicaties is deels versnipperd. Gevolg kan dan zijn dat ook de privacy maatregelen wellicht niet up-to-date zijn of de continuïteit in het geding kan komen, doordat koppelingen gemaakt moeten worden met verouderde software.

In de Cloud oplossing i-Participatie (Pink Roccade) worden door de functioneel beheerders formulieren gemaakt voor de burger voor het digitaal indienen van aanvraagformulieren. Nieuwe gebruikers worden daarbij door PinkRoccade aangelegd. Rechten worden door de functioneel beheerders toegekend in de diverse applicaties. Zowel beheerders als eindgebruikers maken gebruik van dezelfde inlogstappen. Rechten daarna zijn gekoppeld aan rollen, waardoor de taken van beheerders en eindgebruikers zijn gescheiden.

Bij nieuwe applicaties en voor de start van een aanbestedingsproject worden diverse functionarissen aangehaakt, volgens een recent aangepast intakeproces. Betrokken functionarissen zijn onder andere de informatieadviseur, ICT-architect en juridische zaken naast de projectleider, CISO en afdelingsverantwoordelijke personen.

Extern

Vanaf een externe locatie zijn interne gemeente Velsen applicaties niet bereikbaar. Daarvoor moet eerst via een VPN-verbinding worden ingelogd. Hiervoor wordt 2 factor authenticatie gevraagd via een token. Daarna is de toegang voor een medewerker gelijk aan de situatie waarbij de medewerker vanuit het interne netwerk is ingelogd.

Toegang tot diverse gemeente Velsen applicaties die via het Internet (extern gehost/SaaS) beschikbaar zijn gesteld, zijn afgeschermd via IP-filtering. Dit zijn bijvoorbeeld het Zaaksysteem (eSuite), BRP en de City Control (BOA) applicatie. Hierdoor moet voor deze applicaties eerst (VPN) toegang tot het interne netwerk van de gemeente moet worden verkregen, voordat kan worden ingelogd op deze applicaties.

Niet alle applicaties/systemen voldoen aan deze basisrandvoorwaarden voor authenticatie. Bijvoorbeeld de Office365 omgeving, Teams en iBabs omgevingen (de laatste wordt wellicht in de toekomst nog vervangen) zijn via het Internet bereikbaar met slechts inlognaam en wachtwoord. Webmail toegang is beveiligd via een URL, gebruikersnaam, wachtwoord en telefoon/+ certificaat.

Het inloggen in CiVision (Samenlevingszaken) kan vanaf het interne (gemeente Velsen) netwerk door rechtstreeks via SSO in te loggen, nadat op het Windowsaccount is aangemeld. Daarna zal met een eigen account met bijbehorende rechten in de applicatie zelf, verder kunnen worden gewerkt.
De Cloud omgevingen zijn voorzien van een extra authenticatie stap door middel van een token. Enkele portals (CAK) zijn voorzien van een SMS-code voor extra authenticatie. Toegang voor de burger tot i-

Participatie verloopt via DigiD. Medewerkers loggen in met gebruikersnaam en wachtwoord voor toegang tot het medewerkersportaal van i-Participatie.

Voor de Bodycam Saas-applicatie (voor de BOA's) is het (tijdens de interviews) nog niet duidelijk welke beveiligingsmaatregelen hiervoor zijn ingericht.

Voor de Citrixfiles-omgeving voor de uitwisseling van bestanden is geen 2 factor authenticatie ingeregeld (ten tijde van het onderzoek was een wijziging onderweg voor een tweefactor authenticatie oplossing hiervoor). Via deze optie hebben diverse externe organisaties, via het Internet, de mogelijkheid om bestanden uit te wisselen met de gemeente Velsen. Deze organisaties zijn niet voorzien van de token oplossing voor 2FA van de gemeente Velsen. De server in gebruik voor de uitwisseling staat echter wel bij de gemeente Velsen. Daarnaast wordt Zivver gebruikt voor veilige bestandsuitwisseling

Periodiek wordt opgevraagd bij de beheerpartijen van de diverse externe portals welke gebruikers actief zijn, zodat een review kan worden gedaan. Zo zijn in Suwinet verschillende rollen ingericht, in de meeste andere portals zijn slechts beperkte rollen aanwezig.

Toegang tot systemen is beveiligd meestal doordat de leverancier de authenticatie heeft geconfigureerd. De belangrijke systemen en bijbehorende beveiligingsniveaus zijn niet door de functioneel beheerders ingericht. Er zijn beveiligingsplannen opgesteld die de basis moeten vormen voor de beveiligingsinrichting van de applicaties. Het is bijvoorbeeld niet duidelijk of voor alle applicaties in het samenlevingsdomein dit is uitgevoerd. Er zijn ook DPIA's uitgevoerd voor enkele systemen, door het privacy team, echter nog niet voor alle belangrijke systemen. In de praktijk is er sprake van de inrichting en ook naleving van een minimum beveiligingsniveau (baseline). OGD heeft eigen baselines waar de huidige systemen van de gemeente Velsen niet aan voldoen. Het is afgesproken om na de volledige overdracht naar OGD, deze baselines waar mogelijk direct te gaan toepassen.

Technisch beheer ligt bij OGD danwel bij dienstverleners zoals Pink Roccade voor bijvoorbeeld CiVision Samenlevingszaken en i-Participatie. Updates en patches worden door de leveranciers verzorgd, de functioneel beheerder wordt wel voorzien van een jaarplanning wanneer updates en nieuwe releases worden opgeleverd. Serverbeheer en werkplekbeheer wordt qua updates (patching) door OGD gedaan, waarbij de afspraak is dat systemen hooguit 1 update ronde mogen achterlopen. Bij een aantal systemen loopt men echter achter, maar dat is bekend en volgens afspraak met OGD.

Remote toegang door OGD is ingericht via een eigen VPN, voorzien van JiT (éénmalige toegangscode) en multi-factor authenticatie. Daarnaast wordt logging bij OGD vastgelegd, wie welke activiteit heeft uitgevoerd. Het beheer vindt plaats via een separaat management-VLAN specifiek ingericht voor het beheer.

Consequenties voor burgers

Indien oneigenlijke toegang kan worden verkregen tot gemeente Velsen informatie, zijn de consequenties voor burgers afhankelijk van de bron/systeem/applicatie waartoe oneigenlijke toegang is verkregen. Mogelijke varianten daarbij zijn:

- Toegang tot persoonlijke informatie van burgers betekent automatisch het opstarten van het data lek protocol door de gemeente.
- Toegang tot gemeentelijke administraties, zoals paspoortuitgifte etc., zal in ieder geval leiden tot het tijdelijk niet beschikbaar zijn van deze dienst, waardoor een onderzoek kan worden opgestart om te bepalen om welke informatie het gaat. Uiteraard zal dit eveneens het data lek protocol opstarten, echter het verdient diepgaand onderzoek hoe toegang is verkregen, zodat maatregelen kunnen worden ingesteld om dit te voorkomen.

- Toegang tot digitale dienstverlening (zoals de externe website) zal een soortgelijk plan volgen, vergelijkbaar met de gemeentelijke administraties.

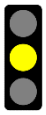
4.3.3.2. *Samenvatting en aandachtspunten*

Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

- Toegang tot het interne netwerk is middels fysieke beveiliging afgeschermd, daarnaast zijn ook maatregelen getroffen om te voorkomen dat ongeautoriseerde apparaten op het interne netwerk kunnen worden aangesloten om toegang tot gemeente Velsen informatie te verkrijgen.

- Omdat de gemeente Velsen zelf grotendeels reactief monitoring heeft ingericht (achteraf terugkijken in loghistorie, in plaats van direct actie ondernemen op het moment dat een gebeurtenis daarom vraagt), verdient het aanbeveling om
  - Te onderzoeken voor welke omgevingen in ieder geval logregistratie kan worden geactiveerd. Denk daarbij aan internet gekoppelde systemen zoals firewalls, VPN-server, interne applicaties, centrale servers zoals Windows AD etc., maar ook de Internet omgevingen, zoals Cloud/SaaS-applicaties en Microsoft Azure.
  - Onderzoek hoe een meer proactieve bewaking (zoals een SIEM-oplossing) kan worden ingezet, zodat dit proces 24x7 wordt uitgevoerd. Via een dergelijke oplossing kan ook intelligenter naar logging worden gekeken, zodat naast direct actie ondernemen naar aanleiding van een gebeurtenis ook complexere aanvallen mogelijk kunnen worden herkend en wellicht voorkomen.

  [Aanbeveling 6]

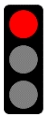


- Het verdient aanbeveling om een aantal beleidsuitgangspunten te definiëren ten aanzien van de inrichting, gebruik en bewaking van logische toegangsprocessen van Cloud/Saas omgevingen, aangezien deze niet door OGD beheerd worden. Denk daarbij met name aan
  - Alle externe applicaties (Saas/Cloud) dienen te zijn voorzien van multi-factor authenticatie voor alle gebruikers en ook beheerders.
  - Configuratie eisen voor Saas/Cloud applicaties ten aanzien van toegang/autorisatie en (bijbehorende) logging.
  - Back-up en archivering van data in de SaaS/Cloud omgevingen.

  [Aanbeveling 10]

- Het verdient aanbeveling om voor alle interne en externe systemen/servers/applicaties die toegang verlenen tot gemeente Velsen informatie in te richten volgens een beveiligingsstandaard en deze periodiek daarop te toetsen. De externe systemen wellicht via een penetratietest of vergelijkbare technische test. Denk daarbij bijvoorbeeld aan de website van de “sportafdeling” en de webformulieren die worden gebouwd door de gemeente zelf en gebruikt door burgers voor diverse aanvragen. [Aanbeveling 10]

- Onderzoek welke OT en IoT-oplossingen (zoals de Bodycam voor de BOA’s) door de gemeente gebruikt worden en stel vast op welke manier die een koppeling met de gemeentelijke systemen hebben. [Aanbeveling 6]



- Verplaats de bestandsuitwisseling server (gekoppeld aan Citrix) die nu gebruikt wordt de uitwisseling van documenten met externe organisaties, naar een beveiligde omgeving, buiten het interne netwerk van de gemeente Velsen. [Aanbeveling 3, 6]

4.3.4. *Hoe weerbaar is de gemeente Velsen tegen grootschalige uitval of verstoring van ICT?*

De volledige vraag:

"Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van de diverse activiteiten die worden uitgevoerd door de gemeente Velsen in het kader van de digitale weerbaarheid. Hierbij is op onderdelen ook OGD betrokken. Met name de continuïteitsaspecten zijn hierbij onderzocht. De opvolging van grote (en kleine) beveiligingsincidenten zijn onderdeel van andere deelvragen.

4.3.4.1. *Toelichting*

Allereerst back-ups en herstel

Vanuit het algemeen IB-beleid is geen afgeleid beleid opgesteld ten aanzien van back-ups en/of herstel randvoorwaarden. Er zijn echter wel afspraken met OGD gemaakt en vastgelegd. De bestaande inrichting van de back-up omgeving van de gemeente Velsen is ongewijzigd overgenomen door OGD.

De gehele ICT-omgeving (alle servers) is in het back-up schema opgenomen, met uitzondering van de SaaS/Cloud systemen die niet door OGD worden beheerd. Het uitgangspunt is de verplichting die voor de BRP-omgeving noodzakelijk is. Dezelfde maatregelen zijn op de andere systemen van toepassing verklaard. Dit zijn niet alleen de 20 kritieke systemen, maar alle fysieke en virtuele servers (50+). De uitvoering van de back-up activiteiten wordt gedaan door OGD, dat een schema naleeft van back-ups op disk (waar soms in minuten terug gegaan kan worden naar een vorige versie), en tevens op tape via een dagelijkse back-up, met daarnaast de gebruikelijke opzet in week, maand en jaartapes die off site worden bewaard. Het proces is als volgt ingericht:

- Snelle back-ups ingericht per dag,
- Daarnaast incrementele back-ups per dag,
- Daarna week back-ups en daarna maandback-ups.
- Via robots worden deze uiteindelijk op tapes worden bewaard.
- De dagelijkse en wekelijks back-ups worden een maand bewaard, maandelijkse back-ups worden een jaar bewaard, de jaar back-up wordt off site bewaard.
- Check of de back-up tape ook daadwerkelijk leesbaar is voor een herstel actie.

De rapportage over de back-up activiteiten wordt aangeleverd door OGD aan de gemeente Velsen (CISO). Daarnaast wordt er dagelijks (volgens de gestelde eisen) een export van de BRP-applicatie gemaakt en naar Dimpact gestuurd om als basisgegevens te gebruiken in lopende en nieuwe zaken.

De algemeen opgestelde RTO (tijd waarbinnen een omgeving hersteld moet zijn na uitval) eisen vanuit de CISO en de afgesproken voorwaarden in het contract met OGD lopen nog niet helemaal synchroon, maar zal nog verder in detail worden afgestemd. Een enkele server en individuele bestanden kunnen snel worden teruggezet. Echter, de meeste servers hebben connecties met andere systemen, waardoor het in de praktijk veel complexer is om herstel van een grotere omgeving te realiseren.

In het verleden is op willekeurige basis gedurende het jaar regelmatig een restore test uitgevoerd. Op dit moment is het niet duidelijk of dit door OGD ook is/zal worden opgepakt. Naast de servers en data van de gemeente Velsen is het nu niet duidelijk of infrastructuurcomponenten zoals firewalls ook in een back-up schema (van OGD) zijn opgenomen.

Naar verluid is de back-up omgeving van de gemeente Velsen, volgens OGD, kwetsbaar voor ransomware aanvallen, zoals die recent hebben plaatsgevonden bij andere gemeenten en organisaties. Let wel, procesmatig zijn controles en acties door OGD ingericht om zo snel mogelijk de juiste acties uit te voeren, mocht er een ransomware aanval plaatsvinden.

Continuïteit

Niet voor alle systemen, maar wel voor de ongeveer 20 belangrijkste/kritieke systemen is een dataclassificatie opgesteld ("Belangrijk"). De CISO houdt deze informatie bij in een Excel document, waaruit de continuïteitseisen kunnen worden afgeleid. De exacte getallen zijn echter niet in het dataclassificatie document vastgelegd. De definitie "belangrijk" is vertaald naar "dat er nagenoeg geen uitval van de beschikbaarheid" mag plaatsvinden. De definities zullen derhalve nog wat exacter moeten worden beschreven, zodat ook OGD hier mee uit de voeten kan.

In de praktijk zijn alle systemen zoveel mogelijk gevirtualiseerd en dubbel uitgevoerd, waardoor de beschikbaarheidseisen normaal gesproken gehaald zouden moeten kunnen worden. Echter het is niet exact vastgelegd hoe lang uitval (half uur, halve dag etc..) nog acceptabel is, dit is in algemene termen beschreven.

De totale ICT-omgeving is verdeeld over 2 server locaties, 1 op het gemeentehuis en de andere bij de brandweerkazerne. Er ligt een dataverbinding tussen beide locaties. In deze opzet is het mogelijk om nagenoeg volledig op 1 serverlocatie te draaien. Voorzieningen zoals Internet koppeling en stroom zijn voor beide locaties apart opgezet en los van elkaar.

Voor de basisvoorziening BRP is in de brandweerkazerne een ruimte gereserveerd zodat de continuïteit in geval van een calamiteit op het gemeentehuis vanaf deze locatie verder kan worden gewerkt.

Bedrijfscontinuïteit is een proces wat op dit moment niet volledig op orde is, aangezien hier normaal gesproken vanuit de diverse bedrijfsprocessen invulling aan dient te worden gegeven in de vorm van beschikbaarheidseisen en andere randvoorwaarden, maar waar in de praktijk vooral naar de ICT-afdeling wordt gekeken voor de invulling en uitvoering van continuïteitstesten. Dit is uiteraard niet de verantwoordelijkheid van de CISO, die hierin echter wel een faciliterende en controlerende en ondersteunende rol heeft. Ook OGD zal hier een belangrijke rol in gaan vervullen.

Uitwijk

De Brandweerkazerne wordt beschouwd als de uitwijklocatie voor de computerruimte van de gemeente Velsen.

De verantwoordelijkheid voor een juist en werkend uitwijk beleid en plan is een taak van de gemeente, meer specifiek de proces/systeem eigenaren. Voor bijvoorbeeld BRP is dit de verantwoordelijkheid van afdeling burgerzaken. In de praktijk lijkt het vooral, zie ook bij continuïteit, een ICT/Security aangelegenheid en verantwoordelijkheid te zijn.

In de afgelopen 2 jaar hebben naar verluid geen uitwijktesten plaatsgevonden, vanwege diverse redenen, waaronder Corona en de overdracht van het beheer naar OGD. Gedurende deze periode hebben er echter op diverse niveaus wel configuratiewijzigingen plaatsgevonden. Hierdoor is niet duidelijk/garantie (OGD) dat de inrichting van de uitwijk volledig op orde is.

Nu zijn met name de wettelijk verplichte systemen in de uitwijktest (zoals BRP, BAG etc.) opgenomen. De planning was om in Q3 2021 het proces hiervoor weer te gaan opstarten. De uitgangspunten (beleid) dienen nog door de gemeente Velsen te worden aangeleverd. De uitvoering vindt plaats grotendeels door OGD, in samenspraak/overleg met de eigenaar (gemeente Velsen).

4.3.4.2. *Samenvatting en aandachtspunten*

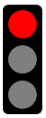
Vanuit de deelvraag zijn interviews gehouden en is informatie verzameld, waarbij de volgende samenvatting en aandachtspunten naar voren zijn gekomen.

Back-ups

- OGD heeft het back-up proces overgenomen van de gemeente Velsen en daarbij in eerste instantie geen wijzigingen doorgevoerd. Hierdoor zijn dezelfde activiteiten ingericht en wordt vanaf nu hierover in de servicelevel rapportage gerapporteerd naar de gemeente Velsen.

- In de huidige invulling vanuit OGD zijn er geen systeem/applicatie herstel testen ingericht, met uitzondering van de controle dat een back-up ook daadwerkelijk leesbaar is. Het verdient aanbeveling om een schema af te stemmen met OGD voor welke omgevingen, wanneer een hersteltest wordt uitgevoerd. [Aanbeveling 3, 12]

- Onderzoek of naast de gebruikelijke (Windows) servers ook andere (netwerk) componenten (zoals firewalls, VPN-servers) worden meegenomen in de back-up cyclus. Onderzoek tevens of het back-up proces ten aanzien van de Cloud/SaaS omgevingen voldoet aan de hiervoor genoemde beschikbaarheidseisen en hersteltijden. [Aanbeveling 12]



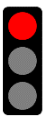
- Uit gesprekken met OGD is gebleken dat de huidige back-up processen niet volledig zijn beschermd tegen ransomware aanvallen. Het verdient aanbeveling om in overleg met OGD, aanpassingen in het proces aan te brengen, zodat de gemeente Velsen hier wel tegen is bestand. [Aanbeveling 3]

Continuïteit

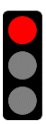
- De inrichting van de systemen van de gemeente Velsen is grotendeels gebaseerd op virtualisatie, waardoor beschikbaarheid van individuele systemen in de regel gegarandeerd is. Daarnaast is een tweede server locatie beschikbaar, met alle noodzakelijke voorzieningen.

- Stel in overleg met de eigenaren van de bedrijfsprocessen, systemen, applicaties en/of data vast welke minimale randvoorwaarden gesteld worden aan de beschikbaarheid en de hersteltijden waarmee de gemeente Velsen de dienstverlening kan en wil garanderen. Op basis daarvan zal in overleg met OGD moeten worden bepaald met welke back-up procedures en inrichting hier invulling aan kan worden gegeven. [Aanbeveling 12]

Uitwijk



- In het verleden hebben uitwijktesten plaatsgevonden voor met name de BRP-applicatie, waarbij gebruik is gemaakt van de uitwijk locatie op de brandweerkazerne. Het verdient aanbeveling om, nu OGD het technisch beheer heeft overgenomen, voor de BRP-applicatie een volledige uitwijk test uit te voeren. [Aanbeveling 4]



- Stel een meerjarig uitwijkplan op, waarin is beschreven welke (belangrijke) omgevingen getest moeten worden om te zien of de uitwijkmogelijkheden voorzien in de juiste herstelstappen en tijdige beschikbaarheid. Daarbij hoort uiteraard ook een evaluatieproces en vastlegging van de verbeteringen, waardoor het gehele uitwijk (en continuïteits-) proces verbetert. [Aanbeveling 4, 13]

4.3.5. Hoe is de opvolging van een (ernstig) beveiligingsincident geregeld?

De volledige vraag:

"Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident en is er een incidentenmanagementproces ingevoerd? Hoe ziet deze eruit?"

In het onderzoek zijn we bij deze deelvraag uitgegaan van de diverse activiteiten die worden uitgevoerd door de gemeente Velsen in de opvolging indien zich een beveiligingsincident voordoet.

4.3.5.1. *Toelichting*

In eerdere vragen zijn reeds onderdelen "in de aanloop" naar een beveiligingsincident besproken. Zo is als eerste de continuïteit van de dienstverlening onderzocht. Daarbij is geconstateerd, dat zowel bij de gemeente Velsen als ook bij dienstverlener OGD, processen zijn ingericht om een beveiligingsincident te registreren. Indien een beveiligingsincident bij OGD is gemeld, zal deze ook door OGD worden opgepakt en afgehandeld. Uiteindelijk zal indien het is opgelost, hiervan melding worden gedaan in de periodieke rapportage naar de CISO van de gemeente Velsen. Met andere woorden de opvolging van deze beveiligingsincidenten wordt volledig door OGD gedaan. Indien hier een escalatie nodig is, dan zijn in de afspraken tussen de gemeente Velsen en OGD hierover definities opgenomen in het regiemodel. De bijbehorende rollen/taken zijn vastgelegd in de DAP afspraken. Wanneer de escalatie eventueel tot een crisis leidt, dan zijn hiervoor echter geen definities opgesteld. OGD hanteert in dat geval algemene richtlijnen afgeleid van de ISO27001/2 normenkaders.

Indien niet OGD, maar de gemeente Velsen zelf de initiële registratie van een beveiligingsincident opstart, zijn er een tweetal scenario's mogelijk:

- De opvolging wordt overgedragen aan OGD, aangezien dit voor een groot aantal diensten in de scope en afspraken is vastgelegd, dat OGD de uitvoerende taken verzorgd. Uiteindelijk zal de afronding door OGD worden gedaan en via de periodieke rapportage teruggekoppeld worden aan de CISO van de gemeente Velsen. De Teamleider Servicedesk van OGD is dan in de lead en betrekt daarbij de CISO van de gemeente Velsen.

- De gemeente Velsen pakt dit zelf op. De CISO zal een eerste review uitvoeren van de melding en een classificatie van het incident doen. Dit bepaalt ook of opgeschaald moet worden naar escalatiemodus/crisis. In dat geval zal de CISO de betrokken afdelingsmanager, de gemeentesecretaris en een communicatiemedewerker verzamelen en andere voor het onderwerp relevante personen. Indien nodig wordt het IBD om advies gevraagd en wordt er eventueel een forensisch expert bij betrokken. Hiervoor is niet een standaard escalatie/crisis protocol opgesteld, maar vindt plaats vanuit praktisch oogpunt, via de diverse overleggen of ad-hoc indien de ernst dit vereist. Indien noodzakelijk zal een groter incident via de portefeuillehouder/gemeentesecretaris ook aan de raad/college worden gemeld buiten de standaard rapportages om.

Een "sprekend" voorbeeld van een beveiligingsincident dat heeft plaatsgevonden naar aanleiding van een tv-programma, waarbij een ethisch hacker uiteindelijk een wachtwoord heeft kunnen achterhalen, waarmee informatie op de externe website van de gemeente Velsen is aangepast. In goed overleg met de ethisch hacker van het tv-programma is dit besproken en zijn maatregelen getroffen om het door de hacker aangetoonde risico te mitigeren. De afhandeling van dit beveiligingsincident en de communicatie daaromheen zijn niet volledig vastgelegd in de incidentregistratie en ook de opvolgingsactiviteiten in Key2control zijn volledig beschreven. De communicatie hieromtrent is niet door iedereen als positief ervaren. Na de zomervakantie is naar verluid uiteindelijk een informatiebrief naar de medewerkers en de raad gestuurd om een toelichting te geven op de achtergrond, de uitvoering en de opvolging.

Naast dit type beveiligingsincident wordt een data lek uiteraard ook als een type beveiligingsincident beschouwd. De opvolging van een data lek wordt door de CISO gezamenlijk uitgevoerd in overleg met het privacy team. Hiervoor zijn procedures beschreven en de registratie wordt door het privacy team bijgehouden. Indien noodzakelijk wordt hierbij ook de AP op de hoogte gebracht en wordt gekeken hoe een dergelijk data lek in de toekomst kan worden voorkomen, bijvoorbeeld door een workshop of training te verzorgen.

Er worden geen activiteiten gedaan om het afhandelen van incidenten en opstarten van een escalatie/crisis te oefenen, zoals bijvoorbeeld hoe te handelen nadat een ransomware/phishing mail aanval heeft plaatsgevonden.

4.3.5.2. *Samenvatting en aandachtspunten*

Samengevat zijn vanuit de deelvraag interviews gehouden en is informatie verzameld, waarbij de volgende aandachtspunten naar voren zijn gekomen.

- In de opvolging van beveiligingsincidenten door OGD worden vastgelegde procedures gevolgd en de resultaten terug gemeld aan de CISO van de gemeente Velsen. Indien een escalatie noodzakelijk is zal dit worden overgedragen aan de CISO zoals is opgenomen in de afspraken (DAP).

- Het escalatie proces (beleid/procedure) zoals dat nu is beschreven in de procedure “beveiligingsincidenten en datalekken 2.0” verdient een update, met name een verduidelijking ten aanzien van de criteria wanneer een escalatie moet worden opgestart, wie deze beslissing neemt (zeker buiten kantoortijd), wat er vastgelegd moet worden en wat de rol is van de teamleider Automatisering in de uitvoering en communicatie. Daar dient de rol van OGD nog aan te worden toegevoegd, aangezien deze partij vooral in de uitvoering betrokken is. [Aanbeveling 9]

- Ten aanzien van het crisis proces zijn dezelfde opmerkingen te maken. Hiervoor dienen onder andere in een beleid en bijbehorende procedure duidelijke definities te worden opgesteld, wanneer en door wie de beslissing genomen mag/moet worden, welke communicatievormen en momenten van toepassing zijn. Welke functionarissen (bijv. de burgemeester) erbij betrokken moeten zijn en de rol van OGD moet worden ingevoegd. [Aanbeveling 9]

- Naast het hebben van een escalatie en een crisis procesbeschrijving is het aan te bevelen om minstens 1 maal per jaar een oefening uit te voeren, waarbij een crisis/scenario zoals een phishing mail of ransomware aanval kan worden geoefend. Het dient in een escalatie/crisis plan te zijn vastgelegd wanneer welke scenario’s worden geoefend. Uiteraard is hiervoor een evaluatie uit te voeren en de acties in een verbeterplan op te nemen. [Aanbeveling 13]

5. BESTUURLIJKE REACTIE

Leden van de Rekenkamercommissie gemeente Velsen		Gemeente Velsen Dudokplein 1 1971 EN IJMUIDEN T 14 0255 F 0255 567 760 www.velsen.nl E info@velsen.nl Correspondentieadres Postbus 465 1970 AL IJmuiden

Uw kenmerk	Ons kenmerk	Voor informatie	Bijlagen	Datum
		P. Krom/E. van Leuven		5 juli 2022

Onderwerp: Reactie op rapport Rekenkamercommissie 'informatiebeveiliging'

Geachte leden van de Rekenkamercommissie,

U heeft het bureau Secura opdracht gegeven om een onderzoek uit te voeren naar de wijze waarop het College grip heeft op informatieveiligheid en het voldoen aan de actuele privacyregelgeving. Met een brief op 25 mei jl. gaf u ons de gelegenheid om een zienswijze op het rapport te geven. Hierbij doen wij u onze reactie op bovengenoemd rapport toekomen.

Het doel van dit onderzoek is inzicht te krijgen in de mate waarin de gemeente beschikt over een ingerichte organisatie voor het realiseren en het indien nodig aanpassen (meebewegen) van informatieveiligheid en tegelijkertijd het kunnen voldoen aan (in ieder geval) de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG).

Het uitgebreide rapport van Secura geeft ons inziens een goed overzicht in de complexiteit die het voldoen aan de BIO en de privacyregelgeving met zich meebrengt. Het rapport is gecontroleerd op juistheid door ambtenaren en overige betrokken partijen die voor het onderzoek door het onderzoeksbureau zijn geïnterviewd. De reacties zijn in het rapport verwerkt.

De conclusie van het rapport is dat de gemeente Velsen al veel heeft gedaan op het vlak van informatiebeveiliging maar dat de borging nog onvoldoende is op een aantal fundamentele onderdelen.

De belangrijkste bevindingen betreffen:

1. Het ontbreken van een actueel en getest uitwijkplan voor de BRP[1]-applicatie en andere bedrijfskritieke applicaties.
2. Het back-up proces is op dit moment niet volledig bestand is tegen ransomware aanvallen
3. Er is nog niet voor alle bedrijfskritieke processen een diepgaande privacy impact analyse (DPIA[2]) uitgevoerd.

[1] Basis Registratie Personen
[2] Een DPIA is een instrument om (vooraf) de privacy risico's van een gegevensverwerking in kaart te brengen.

1

4. Het informatiebeveiligingsbewustzijnsniveau van de medewerkers van de gemeente Velsen is laag.
5. Scenario's ontbreken vooralsnog voor de aanpak van de (op dit moment) meest voorkomende informatiebeveiligingsincidenten, zoals phishing mails, ransomware en gecompromitteerde wachtwoorden.

U adviseert om daar zo snel mogelijk mee te starten en - gezien de hoeveelheid verbeteringen, elk half jaar een herijking te doen van de status en voortgang van de verbeterpunten. Het College kan zich vinden in dit advies.

Naar aanleiding van bovenstaande bevindingen komt het rapport met dertien aanbevelingen die verschillen in de mate van prioritering. De volgende vijf aanbevelingen hebben een hoge prioritering (geadviseerd tijdpad van realisatie is zes maanden):

1. Start met het completeren van de belangrijkste onderdelen die in het privacy/AVG-jaarplan zijn vermeld, waaronder met name het DPIA-proces, maar ook andere maatregelen kunnen worden opgestart.
2. Continueer de bewustwordingscampagne in een minder vrijblijvende opzet, zodat de medewerkers van de gemeente Velsen ook in de huidige manier van (thuis-) werken up-to-date blijven van informatiebeveiliging, Privacy/AVG en de bijbehorende gevaren.
3. Stem de punten af die zijn opgenomen in het re-transitie document, met name de back-up afspraken en inrichting op korte termijn, waaronder de beschermingsmaatregelen tegen mogelijke ransomware aanvallen. Zorg tevens dat alle relevante informatiebeveiligingsonderwerpen in de servicelevel rapportage worden opgenomen.
4. Opstellen uitwijkplan voor BRP en andere belangrijke, bedrijf kritische applicaties en daarnaast voor (minstens) BRP de uitwijk test daadwerkelijk uitvoeren, evalueren en verbeteringen doorvoeren.
5. Opstellen scenario's, in overleg met OGD, hoe om te gaan met de meest voorkomende, meest impact hebbende beveiligingsincidenten indien deze optreden. Mogelijke voorbeelden kunnen zijn phishing mail, ransomware mail, blokkering web-diensten (DDOS-aanval), gecompromitteerd wachtwoord.

De volgende vijf aanbevelingen hebben een gemiddelde prioritering (geadviseerd tijdpad van realisatie is twaalf maanden):

6. Zorg tevens dat de verbeteringen die in het informatiebeveiligingsjaarplan zijn opgenomen, daadwerkelijk worden uitgevoerd en neem controlemaatregelen hierin op zodat ze kunnen worden bewaakt door de CISO-functie.
7. Aanvulling van het beleid op tactische en operationeel niveau, zodat de gedefinieerde beleidsuitgangspunten kunnen worden uitgewerkt in praktische maatregelen en kunnen worden bewaakt en gemonitord. De keuze om standaard voor SaaS/Cloud applicaties te kiezen en/of het gebruik van BYOD-apparaten zijn enkele voorbeelden, waarvoor een beleid kan helpen in standaardisatie. Verder kan worden gedacht aan beleid over, het gebruik van sociale media, mobiele apparatuur, leveranciers voorwaarden en rapportages en tenslotte een breder wachtwoord (of authenticatie) beleid, waarin is vastgelegd, wat de minimumvoorwaarden zijn om toegang te krijgen vanaf het Internet, het interne netwerk, vanuit thuis etc.
8. Afstemming omtrent de definities, registratie, afhandeling en rapportage ten aanzien informatiebeveiligingsincidenten, en de vastlegging van de taken en verantwoordelijkheden

wie welke activiteiten uitvoert (OGD of gemeente Velsen) ten aanzien van beheer van informatiebeveiligingsincidenten.

9. Opstellen escalatie en crisisbeleid en uitwerken van de bijbehorende procedures, waarna in overleg met OGD wordt afgestemd, welke stappen worden doorlopen en met name wie welke taken en verantwoordelijkheden in dit proces krijgt toebedeeld.
10. Opstellen randvoorwaarden voor de toegangscontrolemaatregelen (waaronder Multi-factor authenticatie) noodzakelijk voor de via het Internet beschikbaar gestelde systemen en applicaties van de gemeente Velsen en opstarten configuratie aanpassingen aan die systemen en applicaties die daar niet aan voldoen.

De volgende drie aanbevelingen hebben een lage prioritering (geadviseerd tijdpad van realisatie is 24 maanden):

11. Richt een risicomanagementproces in voor het identificeren, analyseren en evalueren van risico's en voor het bepalen van de risicohouding: accepteren of maatregelen treffen. Dit dient een continu proces te zijn. Maak hierbij o.a. gebruik van de best practices van de IBD[3] en andere gemeenten, zodat de minimumeisen (BBN[4]: Basis Beveiliging Niveau) vanuit de BIO zijn vastgesteld. Leg daarbij de risico afwegingen vast, voor latere referenties.
12. Opstellen continuïteitseisen voor (minimaal) de belangrijke, bedrijfskritieke applicaties en daarnaast onderzoeken in overleg met OGD welke verbeteringen wanneer doorgevoerd kunnen/moeten worden en in een implementatieplan vastleggen.
13. Stel een meerjarenplan op, waarin beschreven wanneer welke escalatie/crisissituaties worden geoefend. Daarnaast voer de oefening uit volgens plan zodat de opgestelde escalatie en crisisprocedures in de praktijk worden getoetst, waarna via de evaluatie eventuele verbeteringen kunnen worden doorgevoerd.

Het College kan zich vinden in de aanbevelingen en het feit dat direct gestart moet worden met de uitvoering van tenminste de aanbevelingen met het karakter "hoog" . Voor aanbeveling nummer 1 en 3 uit de categorie hoog en aanbeveling nummer 11 uit de categorie laag, acht het College het gestelde het tijdpad voor realisatie echter niet haalbaar. Het College licht dat graag toe:

<u>Aanbeveling nummer 1</u>
Aanbeveling nummer 1 betreft het completeren van de belangrijkste onderdelen die in het privacy/AVG-jaarplan zijn vermeld, waaronder met name het DPIA-proces. Een deel van de actiepunten uit het jaarplan 2020 is gerealiseerd. Dat geldt nog niet voor het uitvoeren van data protection impact analyses (DPIA's) bij bedrijf kritische processen en het opstellen van een DPIA-procedure. Een DPIA is een instrument om (vooraf) de privacy risico's van een gegevensverwerking in kaart te brengen.

[3] Informatiebeveiligingsdienst.
[4] BBN is een indeling van niveaus van informatiebeveiliging die loopt van 1 tot en met 3. BBN1 is het niveau waaraan alle overheidssystemen minimaal dienen te voldoen. Denk daarbij aan volgen van wet- en regelgeving, de AVG en algemene beheersmaatregelen. Op dit niveau gaat het over openbare en niet-gevoelige informatie. De BIO kent 3 beveiligingsniveaus: BBN1, BBN2, BBN3. Voor de meest kritieke processen/systemen van de gemeente Velsen geldt BBN2. BBN3 is voor gemeentelijke processen te zwaar en moet meer gezocht worden in de wereld van inlichtingendiensten en defensie. Er zijn gemeentelijke processen/systemen waarvoor het lichtere niveau BBN1 voldoende is. Op dit moment houdt de CISO voor de gehele bedrijfsvoering BBN2 aan waarbij de focus op een aantal kritieke processen ligt. Die zijn benoemd in het beveiligingsbeleid.

Overeenkomstig bovengenoemde aanbeveling, is er een concept procedure voor het DPIA-proces in de maak. Dit helpt de organisatie om systematisch te werk te gaan bij het uitvoeren van de DPIA's. De procedure geeft invulling aan de verschillende stappen in het proces en regelt de verantwoordelijkheden per rol. De procedure wordt voor het einde van dit jaar vastgesteld.

Een tweede speerpunt is het uitvoeren van DPIA's bij nieuwe kritische processen. Dit zorgt ervoor dat nieuwe verwerkingen aan de voorkant voldoen aan de privacywetgeving. Dit is steeds beter geborgd. Er zijn echter ook kritische processen die al bestonden tijdens de invoering van de AVG, waar nog een DPIA op uitgevoerd moet worden. Het betreft een zeer arbeidsintensief proces. Met de huidige capaciteit is het niet mogelijk om deze achterstand binnen een half jaar weg te werken.
Het team Privacy legt dit jaar wederom de focus op het in kaart brengen van de bedrijf kritische processen. Dat is van belang omdat vervolgens DPIA's geprioriteerd en uitgevoerd kunnen worden. Team Privacy draagt er zorg voor dat verschillende domeinen stap voor stap worden meegenomen in dit proces. Met behulp van de privacycontactpersonen is er wel een kleine inhaalslag gemaakt bij de uitvoering van DPIA's over bestaande processen.

Aanbeveling nummer 3
Aanbeveling nummer drie betreft het afstemmen van de punten die zijn opgenomen in het re-transitie document met de outsource partij. Het gaat vooral om de back-up afspraken en inrichting op korte termijn, waaronder de beschermingsmaatregelen tegen mogelijke ransomware aanvallen. Ook wordt aanbevolen om alle relevante informatiebeveiligingsonderwerpen in de servicelevel rapportage op te nemen. De aanbeveling ziet erop toe dat de gemeente Velsen in staat is een disaster-recovery[5] uit te voeren na een gebeurtenis waarbij de hele digitale informatievoorziening onbruikbaar is geworden - bijvoorbeeld na een geslaagde Ransomware-aanval.

Dit wordt nu niet getest en er is ook geen andere manier om vast te stellen of dit kan. Dit moet een plek krijgen in het traject naar de OGD-werkplek (waarbij we afscheid nemen van onze eigen systemen) zodat OGD de gemeente Velsen die zekerheid kan geven. De gemeente Velsen gaat pas over 2 jaar gebruik maken van de OGD-werkplek, dus de termijn van 6 maanden is daarvoor niet mogelijk. De servicelevel rapportage kan wel afgestemd worden met OGD, voor zover nodig. In de tussentijd is er geen zekerheid te verkrijgen, tenzij er zeer hoge kosten worden gemaakt.

Aanbeveling 11
Aanbeveling 11 betreft het inrichten van een risicomanagementproces voor het identificeren, analyseren en evalueren van risico's en voor het bepalen van de risicohouding: accepteren of maatregelen treffen. Dit dient een continu proces te zijn. Het rapport geeft als advies om hierbij gebruik te maken van de "best practices" van de IBD en andere gemeenten, zodat de minimumeisen (BBN) vanuit de BIO (Basis Beveiliging Niveau) zijn vastgesteld.

De systematiek en best practices van de IBD zijn gericht op het analyseren van risico's in bedrijfsprocessen. Dat is ook logisch omdat daarmee ook gelijk het niveau wordt vastgesteld voor de onderliggende systemen en gegevensverzamelingen. Idealiter wordt het bepalen van het beveiligingsniveau gedaan met de eigenaar van een bedrijfsproces. De CISO kan tenslotte niet autonoom het beveiligingsniveau van een proces vaststellen.

In Velsen zijn niet voor alle processen proceseigenaars benoemd. Voor sommige processen is evident welke leidinggevende eigenaar is maar voor andere niet - vooral wanneer deze door

[5] Een disaster-recovery is een actie die gericht is op het zo snel mogelijk herstellen van de bedrijfscontinuïteit na een incident. Het is bedoeld om de impact en schade van een dergelijk incident zoveel mogelijk te beperken.

meerdere domeinen lopen. Daarnaast is het lastig om te bepalen welk detailniveau gehanteerd wordt en daarmee of alle processen goed in beeld zijn. Er is wel inzicht in de gebruikte informatiesystemen zodat ervoor kan worden gekozen om de toetsing voor het bepalen van het BBN-niveau op systeemniveau te doen. Dit is arbeidsintensiever omdat meerdere systemen hetzelfde proces kunnen ondersteunen.

Wel ontbreekt dan het inzicht in de onderlinge samenhang. Het uitvoeren van de BBN-toets voor de belangrijkste informatiesystemen is binnen de gestelde termijn (24 maanden, prioriteit laag) haalbaar, maar niet voor alle informatiesystemen. Vervolgens kunnen de risico's en het BBN-niveau jaarlijks geëvalueerd worden.

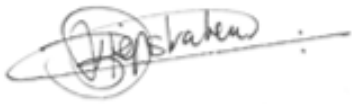
Tenslotte: het College gaat nog onderzoeken welke financiële prikkel noodzakelijk is om alle aanbevelingen wel conform het voorgestelde tijdpad te realiseren. Dit voorstel zal worden meegenomen bij behandeling van de 2e bestuursrapportage 2022.

Burgemeester en wethouders van Velsen

De secretaris

K.M. Radstake

De loco-burgemeester



B. Diepstraten

6. NAWOORD

Het nawoord van de Rekenkamercommissie Gemeente Velsen op het onderzoek, de resultaten en de bestuurlijke reactie:

“De rekenkamercommissie heeft tot haar genoegen geconstateerd dat het college zich kan vinden in de analyse en in de aanbevelingen. Het college schrijft wel dat de uitvoering van enkele aanbevelingen meer tijd zal vragen dan geadviseerd door de onderzoekers.

De rekenkamercommissie ziet in de reactie geen aanleiding voor aanpassingen in het rapport. Mochten bepaalde maatregelen praktisch niet of alleen met zeer hoge kosten binnen de geadviseerde termijnen kunnen worden gerealiseerd, dan wordt dringend geadviseerd te kijken welke mitigerende maatregelen nodig zijn om risico’s in de tussenliggende periode op een aanvaardbaar niveau te brengen.”

BIJLAGE 1: GEÏNTERVIEWDE FUNCTIONARISSEN

De volgende functionarissen zijn betrokken geweest in de interviews:

Functie / Rol / Activiteit	Naam
CISO / Security Officer	Eric van Leuven
Privacy Officer	Suzanne Prins
Functionaris Gegevensbescherming / Interne auditor	Ellen Verbeek
Contract/Service Level Manager	John Heuvel
Gemeentesecretaris	Koen Radstake
Portefeuillehouder	Jeroen Verwoort
ICT Dienstverlening OGD	Sjoerd Krake (OGD)
Security Officer OGD	Constant Wildenberg (OGD)
Hoofd Informatie	Nienke Blokker
Functioneel Applicatiebeheer HR applicaties	Jolanda van Ekeris
Functioneel Applicatiebeheer Samenleving applicaties	Ruud Thiele
Functioneel Applicatiebeheer Financiën/Treasury applicaties	Lex van Rookhuizen
Projectleider bedrijfsvoering	Robert Jaspers

BIJLAGE 2: ONTVANGEN DOCUMENTATIE

Dit is een niet-limitatief overzicht van de documentatie die is verzameld, gericht op de onderbouwing van de beantwoording van de onderzoeksvragen en de P&C Cyclus.

Daarnaast zijn van de interviews, gehouden met de diverse functionarissen, verslagen opgesteld en door de betrokkenen teruggekoppeld en vastgesteld. Ook deze verslagen (zie voor de lijst met functionarissen de vorige bijlage) zijn gebruikt ter onderbouwing, maar niet in deze lijst opgenomen als referentie.

Nr.	Document
1	Beleid_informatiebeveiliging_Velsen_2019
2	Beleid_informatieuitwisseling_Velsen
3	Beleid_logische_toegangsbeveiliging_Velsen
4	Jaarplan_IB_Velsen_2021
5	Wachtwoordbeleid_Velsen
6	Beleid_fysieke_toegangsbeveiliging_en_cameratoezicht_Velsen_vastgesteld
7	Applicatieoverzicht_Velsen
8	Tekening_overzicht_ICT-infrastructuur
9	20210325_Collegeverklaring-ENSIA-2020-inzake-Informatiebeveiliging-DigiD-en-Suwinet-Velsen_gewaarmerkt
10	20210325_DBA-VEL_Assurancerapport_DigiD_en_Suwinet
11	Dimpact_Gemeente_Velsen_TPM_DigiD_2020
12	Functiekenmerken_met_officiele_functiebeschrijving_CISO_-_1_januari_2018
13	Jaarverslag_2020_DEF
14	Managementrapportage-Informatieveiligheid-ENSIA-2020-Velsen-2
15	Verantwoordingsrapportage-BAG---2020-Velsen-20210118095850
16	Verantwoordingsrapportage-BGT---2020-Velsen-20210118100031
17	Verantwoordingsrapportage-BRO---2020-Velsen-20210118100303
18	20210325_Bijlage_1_DigiD-ENSIA-2020-Velsen_gewaarmerkt
19	20210325_Bijlage_2_Suwinet-ENSIA-2020-Velsen_gewaarmerkt
20	201905-Baselinetoets-BBN-BIO-v1.02_iparticipatie
21	BIG-Baselinetoets-Decade
22	BIG-Baselinetoets-Donau
23	Dataclassificatie_Velsen_v2019
24	Risicoanalyse_uitbesteding_ICT
25	Autorisatieprocedure gemeente Velsen
26	E-mail_Intranet_elearning_Phishing
27	Implementatieplan e-learningprogramma Gemeente Velsen
28	Incidentenregister_infobeveiliging_Velsen
29	Procedure beveiligingsincidenten en datalekken versie 2.0
30	Screenprint key2control controles i.v.m. beveiligingsniveau Decade en Donau
31	Pentest Report 2021-06-22 08_08_13
32	Lijst in dienst 28 april 2020 vs accounts Donau en Decade
33	IB_Leveranciersbeheer
34	Bijlage_M_-_Inkoopvoorwaarden_GIBIT
35	Eindrapportage_-_Restpunten_Velsen
36	Uitbestedingsstrategie_van_de_ICT_van_gemeente_Velsen_v_1.2_
37	1. verwerkingsregister
38	2. DPIA's
39	4. Jaarrapportage 2020 en Jaarplan 2021 privacy definitief.docx

40	7. Introductieprogramma
41	8. Geregistreerde datalekken
42	11. Privacybeleidskader gemeente Velsen
43	13. Stappenplan uitvoering Wpg Audit versie 25.05.2021.docx
44	11. Overkoepelend beleid Privacy & gegevensbescherming gemeente Velsen 2016
45	11. Privacybeleid Sociaal Domein, Velsen 2014-2018
46	11. Privacybeleidskader gemeente Velsen
47	18. Dataclassificatie richtlijnen
48	Boardletter_gemeente_Velsen_2020
49	Gemeente_Velsen_-_Definitief_accountantsverslag_2020
50	10. Overzicht overleggen intern en extern
51	Agenda + actielijst TIP-overleg
52	Stukken t.b.v. TIP-overleg 04.05.2021
53	GEMMA-processen in Velsen
54	Directievoorstel leidraad informatiebeveiliging uitbesteding
55	Directievoorstel jaarplan IB 2021
56	Directievoorstel ICT-beveiligingsprocedures-beleid
57	Actieve accounts Decade 28 april 2020
58	BIG-Baselinetoets-Decade
59	BIG-Baselinetoets-Donau

BIJLAGE 3: GEBRUIKTE BEGRIPPEN EN AFKORTINGEN

Informatiebeveiliging is een specialistisch vakgebied, waarbij vele afkortingen worden gebruikt. Hierdoor worden rapporten, zoals ook dit rapport door niet-experts wellicht lastig te lezen. Hieronder een overzicht van de in dit document gebruikte afkortingen met toelichting.

Afkorting / begrip	Toelichting
AP	De Autoriteit Persoonsgegevens. Deze houdt toezicht op de naleving van de AVG en daarmee verbonden regelgeving.
AVG	'Algemene Verordening Gegevensbescherming'. Engels: General Data Protection Regulation (GDPR). Dit is een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert. De AVG is de Nederlandse vertaling van deze Europese verordening.
BBN 2	Zie ook hierna bij BIO. BBN staat voor Basis Beveiligings Niveau en wordt in het BIO raamwerk/baseline gebruikt om aan te geven welke maatregelen zijn verzameld en bij elkaar horen. Er zijn 3 niveaus gedefinieerd, niveau 1 is minimaal, niveau 2 is de standaard voor de overheidssector, en niveau 3 is voor omgevingen die een zware beveiliging vereisen. De gemeente Velsen zal met BBN niveau 2 waarschijnlijk prima uit de voeten kunnen.
BIO	Baseline Informatiebeveiliging Overheid. Deze baseline vervangt de diverse sectorale baselines binnen de overheid en is gebaseerd op de internationale best practice voor informatiebeveiliging ISO 27002:2017.
CISO	Chief information Security Officer. Een functionaris die zich binnen de organisatie bezighoudt met de coördinatie van de werkzaamheden rond informatiebeveiliging en hierover verantwoording afdraagt aan de portefeuillehouder informatiebeveiliging in het college van B&W.
Cloud	Een omgeving, applicatie die volledig op het Internet beschikbaar is en niet in het interne netwerk van de organisatie. Toegang is slechts mogelijk indien een verbinding met het Internet beschikbaar is.
DigiD	DigiD staat voor Digitale Identiteit. Burgers hebben een DigiD en kunnen daarmee inloggen op websites van de overheid en in de zorg. Periodiek dient de beveiliging van deze toegang door middel van een DigiD Assessment door een onafhankelijke deskundige te worden getoetst.
DAP	Diensten Afspraken en Procedures overeenkomst over operationele activiteiten die een externe partij levert aan de organisatie. Deze kan periodiek worden aangepast in overleg, in tegenstelling tot een contract.
DPIA	Data Protection Impact assessment. Een DPIA geeft inzicht in de aard en het doel van de verwerking en de daarmee samenhangende risico's voor de beveiliging van persoonsgegevens op basis waarvan

	vervolgens maatregelen worden gedefinieerd om het risico zoveel mogelijk te beperken en vast te stellen of de verwerking wel is toegestaan. Kort gezegd is de DPIA de basis voor het, ook door de AVG verplichte, privacy by design. Voor gemeenten (overheid) voorgeschreven.
DVO	Dienst Verlenings Overeenkomst (DVO) zijn formele afspraken tussen 2 partijen, waarbij één partij de dienst levert en de andere partij deze ontvangt. Rapportages daarover zijn veelal onderdeel van de overeenkomst. Ook wel SLA genoemd. In de rapportages kan worden teruggekoppeld over beveiligingsincidenten, updates en andere activiteiten die zijn uitgevoerd.
ENSIA	ENSIA (Eenduidige Normatiek Single Information Audit). Deze had tot doel om in de plaats van de vele audits die, uit hoofde van wet- en regelgeving, jaarlijks moeten plaatsvinden bij gemeenten één alomvattende audit te laten verrichten. ENSIA is ingegaan per 2017. Een belangrijk facet van de ENSIA is dat deze benadrukt dat de verantwoordelijkheid voor een voldoende beveiligingsniveau nadrukkelijk bij de gemeenten zelf ligt. Dit is kracht bij gezet door het college zich jaarlijks, met een 'In Control' verklaring, zich te laten verantwoorden over het niveau van informatiebeveiliging. Deze verantwoording is dan het object van onderzoek voor de 'ENSIA audit' door een onafhankelijke en deskundige auditor.
IBD	'Informatiebeveiligingsdienst'. De IBD is de sectorale CERT/CSIRT *(Landelijk opererend team dat in actie komt bij beveiligingsincidenten)* voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten (VNG). De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennis deling tussen gemeenten onderling. https://www.informatiebeveiligingsdienst.nl .
FG	Functionaris Gegevensbescherming. Een door de AVG verplicht gestelde functie die binnen de organisatie adviseert, informeert en toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming.
GR	Gemeenschappelijke regeling. Deze regeling bestaat waarin meerdere gemeenten waaronder Velsen samenwerken op diverse (beleids)terreinen.
Informatiebeleid	Beleid met het geheel van doelstellingen, uitgangspunten en richtlijnen voor het omgaan met informatie en informatietechnologie binnen een organisatie.

Informatiebeveiliging	Informatiebeveiliging draagt bij aan de betrouwbaarheid (integriteit), vertrouwelijkheid en beschikbaarheid van de informatie(systemen). Betrouwbaarheid betekent dat informatie integer (juist, actueel, tijdig) moet zijn. Vertrouwelijkheid gaat dan over het enkel voor bevoegde personen toegankelijk zijn van informatie, en de beschikbaarheid dat de informatie op de plaats en het moment aanwezig is als het nodig is.
Informatiebeveiligingsbeleid	Beleid gericht op het nemen van passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving. Strategisch, hiermee wordt de link gelegd met naar het organisatiebeleid, visie en informatiebeleid en worden de hoog niveau doelstellingen bepaald. Tactisch, hiermee wordt een eerste vertaalslag gemaakt van een strategie naar concrete doelen, activiteiten en processen. Operationeel beleid beschrijft de procedurele uitgangspunten en vertaalslag naar concrete normen en maatregelen, bijvoorbeeld in de vorm van baselines.
IoT / OT	Aan het Internet gekoppelde apparaten die geen onderdeel uitmaken van het “normale” kantoorautomatiseringsnetwerk. Voorbeelden hiervan zijn klimaatbeheersingsapparatuur die via het internet verbonden zijn, zodat de leverancier op afstand kan monitoren en beheren.
ISO-27001/2	De wereldwijde standaard ten aanzien van informatiebeveiligingsprocessen. Deel 1 (ISO27001) beschrijft het ISMS proces. Deel 2 (ISO27002) beschrijft de mogelijke maatregelen. De BIO standaard voor de overheid is hiervan afgeleid.
ISMS	‘Information Security Management System’. Dit is een managementsysteem voor informatiebeveiliging en gaat uit van de zogenaamde PDCA-cyclus (Plan, Do, Check, Act). Generieke stappen daarin zijn vast te stellen wat bedrijfskritiek is en het uitvoeren van een risicoanalyse (Plan), vaststellen wat moet je verbeteren (Do), verifiëren of er voldoende maatregelen zijn (Check) en hoe acteer je op eerdere stappen, verbeter je de organisatie, het proces, de techniek en het handelen van medewerkers (Act)? Continu anticiperen en verbeteren is het uitgangspunt om goed te kunnen acteren op steeds veranderende dreigingen.
Key2Control	De applicatie, die door de gemeente Velsen wordt gebruikt voor het aantoonbaar maken van het “In Control” zijn, oftewel compliant. Hierin zijn onder andere de ENSIA, de BIO-nulmeting rapportage en de AVG/Privacy status vastgelegd.
NCSC	Het Nationaal Cyber Security Center (NCSC) zorgt als onderdeel van het ministerie van Justitie en Veiligheid voor de overkoepelende bewaking van vitale onderdelen van de Nederlandse maatschappij en brengen onder andere jaarlijkse het Cybersecuritybeeld Nederland uit.

NIST Cybersecurity Framework	Vanuit de Amerikaanse overheid opgezette organisatie die een Cybersecurity raamwerk heeft ontwikkeld, wat verder gaat dan de standaard processen vanuit informatiebeveiliging, door ook proactieve en herstelprocessen in het raamwerk op te nemen.
Nulmeting	Nulmetingen geven door het toetsen tegen een algemeen bekend raamwerk een eerste inzicht in de compliance status ten opzichte van het raamwerk. Veelal wordt dit gebruikt bij de BIO, ISO27K e nadere generieke raamwerken, waardoor duidelijk wordt wat al op orde is, en waar de prioriteiten liggen ter verbetering vanuit een totaaloverzicht.
PDCA	Bij veel raamwerken bestaat de naleving uit een cirkel proces, met de onderdelen: plan, do, check en act (PDCA). Hiermee wordt gezorgd, dat naast het opstellen van een plan en de uitvoering ervan, ook een controle slag plaatsvindt op de werking van de implementatie. Daarna kan op basis van de controle weer bijsturing plaatsvinden.
P&C Cyclus	Binnen overheidsland is dit proces ingericht om vergelijkbaar met de PDCA en ISMS processen een cyclus in stand te houden, waarbij uitkomsten en resultaten weer worden gebruikt om te verbeteren.
Pentesten / Vulnerability Scans	Twee vormen van technische testen, waarbij met tools en testen wordt onderzocht of een applicatie/systeem of website fouten in de configuratie heeft, waar eventueel gebruik van gemaakt kan worden om ongeoorloofd informatie te bemachtigen, aan te passen of te verwijderen. Pentesten of penetratietesten worden voornamelijk gebruikt om vanaf het Internet te testen of inbraakpogingen mogelijk zijn of vaak websites/webapplicaties. Vulnerability scans worden vaak gebruikt aan de interne kant van de organisatie om vast te stellen of de laatste patches zijn doorgevoerd, of een technische configuratie voldoet aan minimumeisen of een baseline.
Phishing mail	Een phishing mail wordt door hackers gebruikt om via een normaal lijkend verzoek via email nietsvermoedende gebruikers inloggegevens of andere details te ontfutselen, zonder dat dit onderkend wordt.
PPOT	Combinatie van de niveaus waarop beveiligingsmaatregelen genomen kunnen worden, waarbij de afkorting is opgebouwd uit de eerste letters van • People (Personeel) Bewustzijn van betrokken medewerkers, • Process (Proces) Ingeregelde beveiligingsprocedures zoals toegangsbeveiliging, • Organization (Organisatie)

	Verdeling van taken en bevoegdheden zoals het instellen van een beveiligingsfunctionaris en een functionaris gegevensbescherming (eis AVG) en • Technology (Techniek) Technische maatregelen zoals toegangssystemen, firewalls etc.
Privacy Officer / Adviseur	Net als de FG, een vanuit de AVG ontstane functie die binnen de organisatie vooral de uitvoering en inrichting verzorgt van processen en procedures noodzakelijk vanwege de Algemene Verordening Gegevensbescherming.
Ransomware	Software dat er voor zorgt dat gegevens op een server/laptop of harddisk versleuteld wordt, en niet door de eigenaar zelf te ontsleutelen is. Slechts door het betalen van “losgeld” (ransom) kan via een code in te voeren de versleuteling worden teruggedraaid.
Risico management	Het proces dat zorgdraagt voor een totaaloverzicht van mogelijke risico’s gekoppeld aan een vooraf afgebakend onderwerp (scope). In een aantal stappen wordt vanuit de mogelijke dreigingen en kwetsbaarheden, bepaald welke risico’s niet acceptabel zijn, en waarvoor derhalve maatregelen moeten worden getroffen, zodat het risico kan worden teruggebracht naar een acceptabel niveau. Door dit regelmatig te doen, worden veranderingen, incidenten en nieuwe dreigingen en kwetsbaarheden die mogelijk leiden tot risico’s steeds opnieuw afgewogen.
SaaS	Een vorm van een cloud omgeving, waarbij de volledige omgeving (applicatie) als een dienst wordt geleverd en de afnemer hiervoor niets zelf hoeft te doen, zoals een implementeren van patches en testen op beveiligingsrisico’s. De afkorting staat voor Software As A Service.
OGD	Afkorting voor de voornaamste ICT-dienstverlener van de gemeente Velsen, die de werkplekken, netwerken, IT-servers/systemen etc. beheerd voor de gemeente.
SUWINET	Suwinet is een digitale infrastructuur die is ontwikkeld door en om ervoor te zorgen dat, de Suwinet-partijen (UWV, SVB en gemeenten) gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld voor zover daar een wettelijke grondslag voor is.