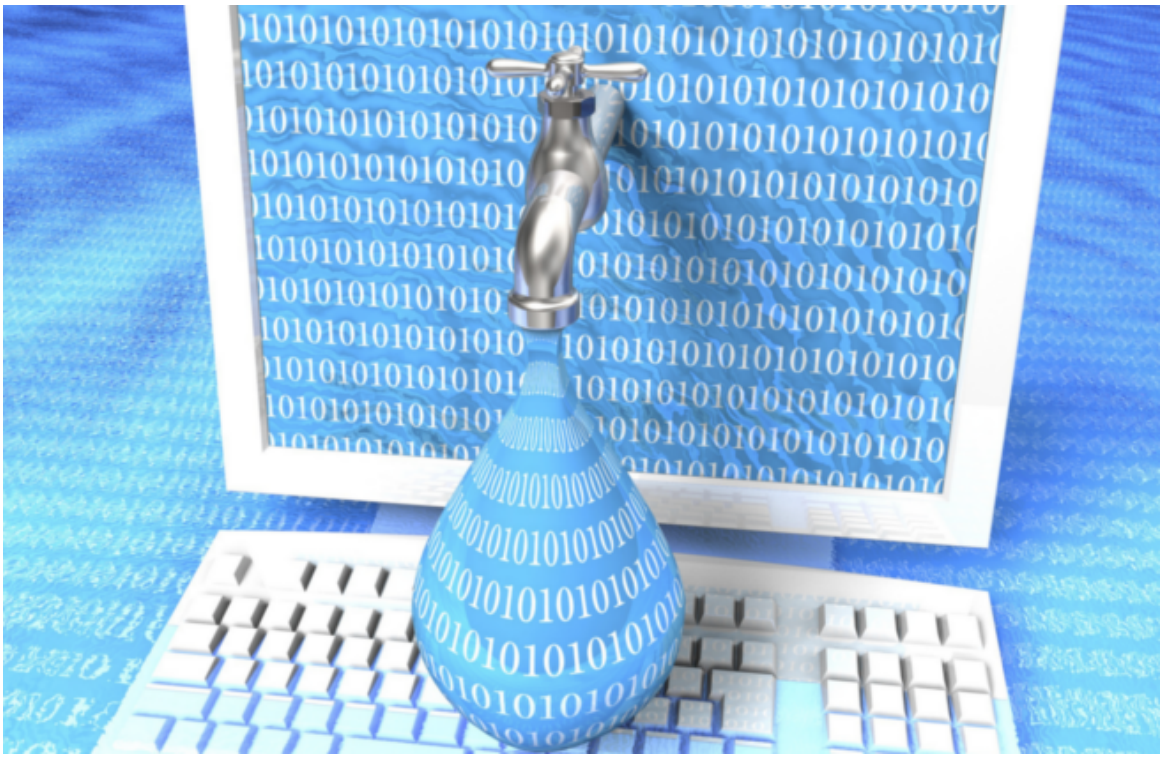
Nijmegen



Rapportage Informatiebeveiliging en Privacy 2020

CISO gemeente Nijmegen, december 2020

Informatiebeveiliging & privacy 2020

Resultaten

Beheersmaatregelen geïmplementeerd
(baseline informatieveiligheid)



Incidenten
29x



12
Data-lekken

Inzage-verzoeken burgers



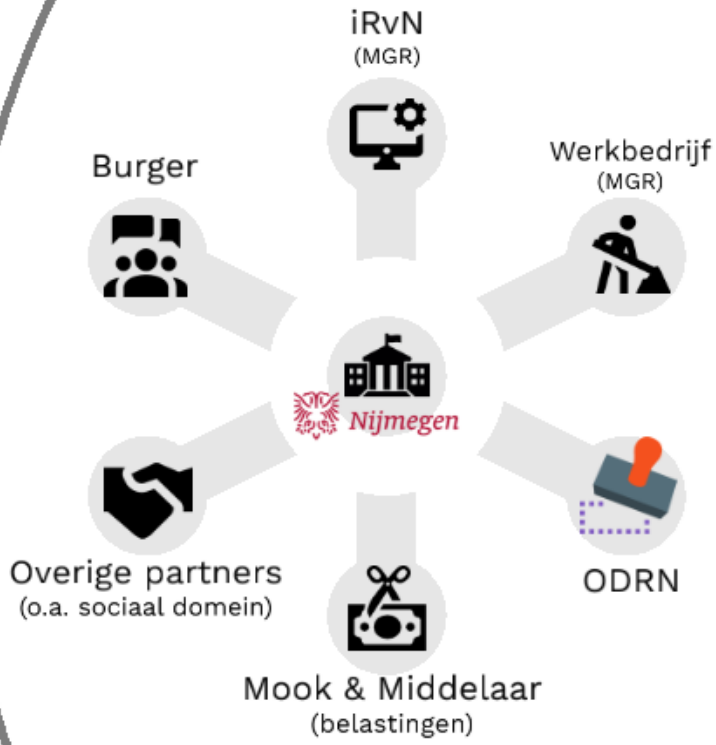
Persoonsgegevens verstrekt aan derden





Verwerkersovereenkomst
(over verantwoord gebruik gegevens burgers/medewerkers)

Ons speelveld



Uitdagingen

Borging in processen
(incl. AVG-proof)



I-bewustzijn



Bij medewerkers
Inzet ambassadeurs

Crisis-oefening





In de regio

Inhoudsopgave

1. Doel & wettelijk kader 4
2. Leeswijzer 4
3. Ambitie 4
4. Terugblik 6
   4.1 Wat wilden we bereiken? 6
   4.2 Wat hebben we bereikt? 6
5. Vooruitblik 11
   5.1 Aanbevelingen uit externe toetsing 11
   5.2 Komend jaar 12
   5.3 Meerjarig 13
Bijlage: achtergrond & begrippen 15

1. Doel & wettelijk kader

Doel

In dit rapport informeren we u over de ontwikkeling van de informatiebeveiliging bij de gemeente Nijmegen. We blikken terug op het afgelopen jaar en kijken vooruit naar de ontwikkelingen in 2021 en de jaren daarna. Dit rapport is onderdeel van de regelgeving rond de Eenduidige Normatiek Single Information Audit (hierna: ENSIA).
ENSIA is een systeem van zelfevaluaties op het vlak van informatiebeveiliging. Een belangrijk document wat hieruit voortkomt is een collegeverklaring. Hiermee legt het college verantwoording af aan de raad en aan landelijke toezichthouders. De voorliggende rapportage Informatiebeveiliging en Privacy rapportage is onderdeel van onze onderbouwing bij de collegeverklaring ENSIA, waarin het college aangeeft in welke mate gemeente Nijmegen voor DigiD, Reisdocumenten, de BRP en Suwinet aan de eisen voldoet. De Chief Information Security Officer (belast met informatiebeveiliging) stelt de rapportage op, met bijdragen van de Functionaris Gegevensbescherming (belast met privacy), collega`s van control, informatiemanagement, collega`s betrokken bij informatieveiligheid en de iRvN. Het rapport wordt vastgesteld door het college.

Wettelijk kader

Gemeenten hebben in de VNG-resolutie ‘Informatieveiligheid, randvoorwaarde voor de professionele gemeente’ uit november 2013 onder meer afgesproken dat in de jaarstukken – in het onderdeel jaarverslag - een aparte passage over informatiebeveiliging wordt opgenomen. Een periodieke rapportage aan alle managementlagen is onderdeel van de Baseline Informatiebeveiliging Overheid (BIO). Met deze passage en het onderbouwende rapport verantwoordt het college zich aan de gemeenteraad over informatiebeveiliging in brede zin.

2. Leeswijzer

Het eerste deel van dit rapport wijden we aan het schetsen van het onderwerp. Wat is het en hoe verhoudt de gemeente Nijmegen zich hiertoe. Daarna blikken we terug op het afgelopen jaar over de vooraf gestelde doelen en de behaalde resultaten. In eerste instantie voor de gemeente zelf en daarna waar het gaat om onze partners. We sluiten af met een vooruitblik naar de toekomst, het komende jaar en de langere termijn.

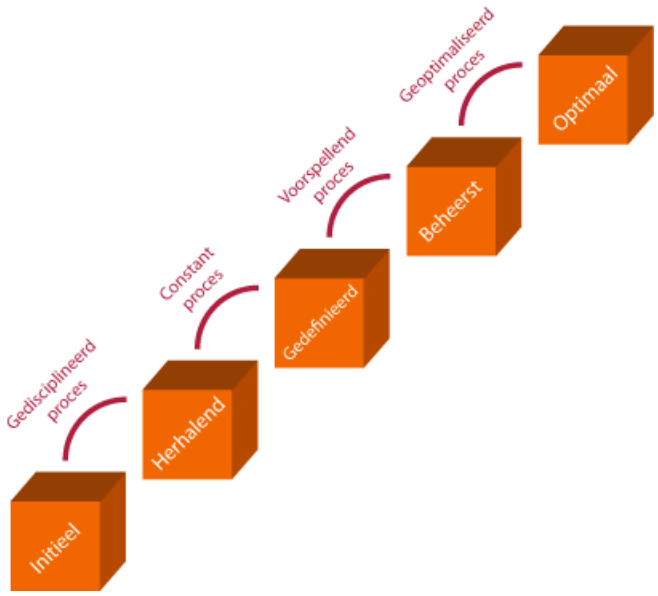
Ter ondersteuning vindt u voorin een infographic waarin de volgende onderwerpen zijn gevisualiseerd: 1) het speelveld waarin we ons begeven rondom het uitwisselen van gegevens, 2) de resultaten die we in 2020 boekten en 3) de uitdagingen waar we in de toekomst voor staan.

In de bijlage vindt u achtergrondinformatie over informatiebeveiliging & privacy inclusief een toelichting op veel gebruikte begrippen.

3. Ambitie

De gemeente Nijmegen wil haar volwassenheidsniveau van de informatiebeveiliging verhogen. Wij streven er naar om “in control” te zijn en daarover op professionele wijze verantwoording af te leggen, onder andere via de voorliggende rapportage. ‘In control’ betekent in dit verband dat de gemeente weet welke risico's en onzekerheden er bestaan op het terrein van de informatiebeveiliging. Daarbij weten we welke (passende) maatregelen we nemen. We zorgen voor een controleerbare planning van maatregelen die genomen moeten worden en we bewaken deze. En tot slot weten we in hoeverre de maatregelen effectief zijn en welk risico’s er over blijven.

Deze ambitie is integraal onderdeel van de professionele gemeente, zoals benoemd in de VNG Resolutie waar eerder naar verwezen is.



Figuur 1 Capability Maturity Model vertaald

De mate van 'in control zijn' kan uitgedrukt worden in volwassenheidsniveaus in het CMM model[1], zoals ook de accountant doet. De gemeente streeft naar niveau 3 in dit model. Dit is het niveau waarop processen zodanig goed gedefinieerd zijn dat ze ook goed functioneren als omstandigheden veranderen (bijvoorbeeld als medewerkers van functie veranderen). De kwaliteit van het proces meten we objectief gemeten.

Met de oprichting van het team Stadscontrol binnen de gemeentelijke organisatie en het hierin onderbrengen van de CISO en de FG is de controlerende en oordeelsvormende rol binnen de gemeente meer voor het voetlicht gebracht. Door meer aandacht te geven aan eigenaarschap, opvolging en verantwoording neemt het volwassenheidsniveau van processen toe. Risico gestuurd werken zorgt er voor dat dit zo efficiënt mogelijk wordt ingevuld.

Ook het iRvN en de WBRN werken aan professionalisering. Zij hebben verzoeken ingediend om in 2020 een aantal processen door gemeente Nijmegen te laten toetsen. Hiermee geven zij gehoor aan de wens van gemeente Nijmegen tot meer transparantie en verantwoording ook naar hun andere partners toe.

[1] https://www.ictloket.nl/kennisbank/mkb-marketing/marketingmodellen/capability-maturity-model-integration-cmmi/

4. Terugblik

4.1 Wat wilden we bereiken?

In 2020 ging veel aandacht uit naar het inrichten van de CyberManager. Dit is een programma dat de gemeente ondersteunt bij het verkrijgen van inzicht in de risico's die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen. Onderdeel van de invoering van de CyberManager was de overgang naar het nieuwe normenkader BIO, waarin eigenaarschap en risicomanagement een veel grotere rol spelen dan in het vorige, meer normgerichte kader.

Daarnaast was het zoeken naar wat er mogelijk was tijdens de Corona pandemie. Afdelingen zijn gestart met het uitvoeren van het AVG-proof plan. Dit plan is een manier om het eigenaarschap voor het voldoen aan de privacyregels en het verbeteren van de informatiebeveiliging bij de afdelingen zelf te beleggen, zoals de BIO ook vraagt.

Het blijvend aandacht besteden aan iBewustzijn is onderdeel van de jaarlijkse plannen evenals het opvolgen van de aanbevelingen van de accountant, IT-auditor en de resultaten van andere toetsingen. De Citrix crisis bleek daarbij een goede aanleiding om de crisisorganisatie van de gemeente te evalueren. Dit heeft geleid tot nieuwe proces afspraken. Daarnaast wilden we in de regio aan de slag met collegiale toetsing en het (ethisch) laten hacken van de iRvN. Dit hebben we moeten uitstellen tot 2021.

4.2 Wat hebben we bereikt?

4.2.1 De gemeente Nijmegen

Activiteiten over de hele gemeente

- Het AVG-proof project van Zorg en Inkomen, en Publiekszaken, heeft in 2020 een goede start gemaakt onder een voortvarende projectleider. Een stuurgroep is aan de slag gegaan met de gemeentebrede implementatie van de AVG maatregelen. Hierdoor is er meer zicht op de stand van zaken en de voortgang.
- De Functionaris Gegevensbescherming zal de implementatie van de maatregelen gemeentebreed monitoren door de uitvoering van het controleplan dat hij dit jaar heeft opgesteld.
- Het in- en uitstroomproces van medewerkers is herzien.
- Bitwarden is als standaard wachtwoord manager ingevoerd.
- De CISO's hebben regionaal een phishing mail campagne uitgevoerd.
- Per 1 juli zijn de betreffende strategisch adviseurs van Stadscontrol tot Functionaris Gegevensbescherming en CISO benoemd. Het team Stadscontrol ziet toe op het opvolgen van bevindingen en het nemen van de juiste maatregelen. Dit gebeurt door het voeren van advies gesprekken en het toetsen van maatregelen, bijvoorbeeld door het uitvoeren van audits met behulp van de CyberManager.

Invoering van de CyberManager uitgelegd

Om compleet en actueel inzicht te hebben in hoe de gemeente er op het vlak van informatiebeveiliging, en het voldoen aan de AVG, voor staat is er een systeem nodig waarin we de status van de maatregelen die we nemen bijhouden. Een dergelijk systeem is een Information Security Management System (ISMS). Tot en met 2019 gebruikten we hier voor een product van SEP[2]. In 2020 zijn we overgestapt op

[2] https://sep.nl/isms/

een ander product, de CyberManager[3]. Tijdens deze invoering hebben we de informatie die in het oude systeem zat overgezet naar het nieuwe normenkader dat in 2020 verplicht werd, de Baseline Informatiebeveiliging Overheid (BIO).

Omdat de manier waarop de systemen werken erg verschilt hebben we de overzetting van de informatie uitgevoerd door in de CyberManager een “interne audit” uit te voeren op de status van de BIO maatregelen. Hierbij hebben we samen met de leverancier handmatig alle informatie uit het SEP systeem overgenomen en ingevoerd in de CyberManager.

De CyberManager drukt de implementatiestatus uit in aparte scores voor of iets beschreven is of dat er bewezen kan worden dat iets feitelijk ook zo werkt. De SEP implementatie statussen zijn vertaald naar de CyberManager statussen. Voor de SEP status “Geaccepteerd risico” is in de CyberManager de norm “Niet van toepassing” verklaard met de toelichting “Geaccepteerd risico” gebruikt.

De resulterende situatie is dat de status en historische informatie nu beschikbaar is in de CyberManager en kan dienen als uitgangspunt voor verdere implementatie van de BIO.

In de infographic voorin kunt u zien dat in de CyberManager nu 70% van de maatregelen actief is. De voortgang bij het implementeren van de maatregelen zal van 2020 op 2021 goed meetbaar zijn via de CyberManager. Met de omzetting is een eerste begin gemaakt met het verhogen van het volwassenheidsniveau van de gemeente.

IT Audit observaties van de Accountant over 2020

De jaarlijkse accountantscontrole heeft een aantal positieve ontwikkelingen laten zien en legt ook een aantal kwetsbaarheden bloot. Deze zijn na te lezen in het IT rapport van de accountant. Positief is dat we meer grip hebben gekregen op het loggen van meldingen uit systemen, het in- en uitdienst proces en de controle op autorisaties. We kunnen betrouwbaar afwijkingen zien in processen. Dit hoort bij CMM volwassenheidsniveau 2 voor detectie (zie hoofdstuk 3). In het afgelopen jaar zijn we op het vlak van het reageren op afwijkingen (response) naar niveau drie opgeklommen. Het lukt dus om incidenten telkens goed af te handelen onafhankelijk van wie het oppakt.

De accountant is minder te spreken over het niet evalueren van het informatiebeveiligingsbeleid en monitoring door KPI’s en het niet volledig betrekking van de eigenaren van Nijmegen in het wijzigingsproces. Hiervoor is een verbetertraject opgestart samen met de iRvN en met advies van de accountant. Kijkend naar de accountantsrapportage zit de gemeente voor het merendeel op niveau een en twee, het niveau waar we afhankelijk zijn van de expertise van specifieke medewerkers. Voor governance en response zitten we nu op niveau drie.

Resultaat van de ENSIA Cyclus 2020

De zelfevaluatie is in gebaseerd op de BIO. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd.

Wij rapporteren als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid, via ENSIA. Dit rapport is daar een onderdeel van. Vanuit de gemeentebrede zelfevaluatie wordt eveneens de verantwoording aan de stelselhouders bij de rijksoverheid afgeleid, de zogenaamde verticale verantwoording. Zo vindt u naast dit rapport ook bijlagen over DigiD, Suwinet, BRP, Reisdocumenten, BAG, BGT en BRO bij de collegeverklaring over ENSIA. Een zeer korte samenvatting per stelsel vindt u hier onder.

[3] https://www.cybermanager.nl/software/

Stelsel	Samenvatting
DigiD	Strengere handhaving op normen betekent voor DigiD dat van de 25 normen per aansluiting bij twee van de vier aansluitingen er een niet voldoet. De auditor geeft wel aan dat wij elk jaar onze zaken beter op orde hebben.
Suwinet	Bij Suwinet is aan de twee toepassingen die wij al kenden er een toegevoegd. Het blijkt dat Gemeente Nijmegen verantwoordelijk is voor DKD inlezen functionaliteit zoals die gebruikt wordt door de Decos Inkomensassistent. Daarnaast is het zo dat er van de veertien normen die gelden voor de twee andere toepassingen bij er Suwinet-Inkijk een niet voldoet.
BRP	Over het algemeen zijn de uitslagen van het jaar 2020 goed. Wij voldoen aan de wettelijke eisen. Aan de verbeterpunten uit 2019 is in 2020 gewerkt zoals bijvoorbeeld aan het punt van functiescheiding.
Reis-documenten	De uitslagen van het jaar 2020 zijn goed.
BAG	Over het jaar 2020 voldoen wij aan de norm score voor de BAG. In 2020 is de samenwerking tussen het bureau Gemeentebelastingen (WOZ) en het bureau Basis- en GEO-informatie (BGT en BAG) sterk verbeterd op het gebied van het (verplicht) gebruik van gegevens. Hiermee zijn de verschillen in de gegevens verder teruggebracht wat de actualiteit en kwaliteit verhoogt.
BGT	Over het jaar 2020 voldoen wij aan de norm score voor de BGT. In 2020 hebben we veel tijd en aandacht besteed aan verschillende projecten om daarmee de kwaliteit van de data in de basisregistraties BGT, BAG en WOZ meer gelijk te krijgen. Daarnaast hebben we de reguliere opdrachten allemaal kunnen verwerken in de BGT. Dit betekent dat we bij zijn conform de wettelijke vereisten in het verwerken van de veranderingen die in de stad zijn gedaan.
BRO	Over het jaar 2020 voldoen wij aan de norm score voor de BRO. Begin 2020 zijn er vervolgstappen gezet om de organisatie rond de BRO verder vorm te geven. Er zijn presentaties gegeven en gesprekken gevoerd met de afdelingen Stadsontwikkeling, Stadsrealisatie en –beheer. Ook is er in maart een vervolggesprek geweest met de projectleiders van bureau Vastgoed.

Resultaat op het vlak van privacy

Als het gaat om het treffen van maatregelen om de persoonsgegevens te beschermen is een aantal stappen gezet. Het bijhouden van het verwerkingen register en het uitvoeren van gegevensbeschermingseffectbeoordelingen behoren op dit moment tot de kerntaken van de tweedelijns adviseur voor privacy, de Privacy Officer. De gegevens rond de verwerkingen ziet u in de infographic. Het aantal registraties met geldige overeenkomsten stijgt. Omdat inkopen decentraal gebeurt vraagt het een hoge mate van bewustzijn om elke verwerking in het systeem opgenomen te krijgen. Het verwerkingenregister wordt in het kader van Open en Weerbaar manifest gepubliceerd. Het publiceren van het register van verwerkingen is geen wettelijke verplichting.

Burgers kunnen in het kader van de AVG een aantal rechten uitoefenen, zoals het recht op inzage in welke gegevens de gemeente van hen verwerkt. Daarnaast worden de datalekken geregistreerd. Het aantal incidenten en datalekken is terug te zien in de infographic.

Het aantal incidenten is gedaald terwijl het aantal meldingen bij de AP is gestegen. Er zijn opvallend minder telefoons verloren in het afgelopen jaar. Dit is wellicht een gevolg van de lockdowns. Daarnaast

zijn er in het afgelopen jaar meer meldingen gemaakt in het zorgdomein ten opzichte van 2019. Meldingen in het zorgdomein leiden vrijwel altijd tot een melding bij de AP. Dit verklaart het hogere aantal meldingen daar. Een aantal opvallende meldingen betreffen gesprekken rond casussen die gemeld werden in het sociaal domein. Binnen de gemeente zal bepaald moeten worden hoe om te gaan met zorgen rond collega`s zonder hun privacy te schenden. Ook zijn er een aantal meldingen gedaan door Publiekszaken. Vanwege de gegevens die bij Publiekszaken verwerkt worden volgt ook hier vrijwel altijd een melding bij de AP. De meldingen bij Publiekzaken leidden daar tot een project waarin het proces herzien wordt om de kwetsbaarheid die ontstaat door het omgaan met papieren dossiers verder te beperken.

Het aantal meldingen wordt sterk beïnvloed door de meldingsbereidheid van de medewerker. Daarbij is zorg ontstaan voor mogelijke sancties voortkomend uit een melding. In het komende jaar is het belangrijk om in het kader van iBewustzijn aandacht te besteden aan het feit dat melden altijd belangrijk is en niet afgestraft zal worden met sancties, om te voorkomen dat de meldingsbereidheid af neemt.

4.2.2 iRvN

In reactie op de aanbevelingen van de accountant en gebeurtenissen als de hack van de universiteit van Maastricht is de iRvN het veiligheidsproject gestart. Dit project omvat een aantal doelen:

- een aanval voorkomen
- een aanval zo snel mogelijk ontdekken (detecteren)
- een gedetecteerde aanval inperken en zo snel mogelijk stoppen

Dit betekent dat het netwerk verder opgedeeld is in een apart netwerk voor beheerstaken en een kantoornetwerk. Er worden ook verschillende accounts gebruikt voor deze netwerken. Zo komen de accounts met beheerdersrechten niet op het kantoornetwerk wat voorkomt dat een aanvaller veel rechten krijgt. Veel maatregelen die te maken hebben met het ontdekken van problemen via het detectiesysteem (EWS) en het beheersysteem voor mobiele apparaten (MDM) zijn in 2020 ingevoerd. De aansluiting met de kopgroep op het landelijke detectiesysteem (SIEM) is ook tot stand gebracht. Daarnaast worden de laptops opnieuw ingericht met meer beperkingen op toegang zodat problemen voorkomen kunnen worden. De gemeente blijft eindverantwoordelijk en legt in die hoedanigheid ook over de bij de iRvN belegde maatregelen verantwoording af via ENSIA.

4.2.3 Overige samenwerkingen

Afspraken met externe partijen

Om haar doelstellingen op een zo effectief en efficiënt mogelijke manier te kunnen behalen maakt de gemeente voor een aantal taken gebruik van samenwerkingsverbanden of externe relaties. Zie voor het speelveld rond gegevensuitwisseling ook de infographic. Om deze samenwerkingen tot een succes te maken worden data en informatie uitgewisseld. Dit betekent dat er afspraken gemaakt moeten worden die vastgelegd worden in dienstverleningsovereenkomsten en verwerkersovereenkomsten. Afhankelijk van de inschatting van het risico dat de gegevens lopen zullen wij waar nodig deze ‘verwerkers’ intensiever beoordelen op hun verantwoordingsplicht vanuit de AVG. Dit is met name ook een aandachtspunt van de FG. De CISO zal zich met name richten op de collegiale toetsing van de informatiebeveiligingsmaatregelen zoals verwerkers die moeten invoeren om de gemeente te ondersteunen. In 2020 is een begin gemaakt met de collegiale toetsing bij de ODRN.

In het kader van het gastheerschap vult de gemeente Nijmegen voor de Meervoudige Gemeenschappelijke Regeling (MGR) en de Omgevingsdienst Rijk van Nijmegen (ODRN) een aantal maatregelen in. Het betreft maatregelen die te maken hebben met voorzieningen op het gebied van

facilitair, personeel en juridische zaken. Denk daarbij aan maatregelen op het vlak van contractbeheer, toegangsbeleid en telewerken.

De ODRN en de MGR blijven verantwoordelijk en kunnen gemeente Nijmegen bevragen op de voortgang van de implementatie. Hiervoor is nog geen standaard proces afgesproken.

Midden 2018 heeft het Werkbedrijf Rijk van Nijmegen (WBRN) de beschikking gekregen over haar eigen Suwinet aansluiting. De IT-auditor geeft voor de regio gemeenten die deelnemen aan de WBRN een verklaring af over het gebruik van de Suwinet aansluiting volgens de geldende normen.

Op het vlak van Belastingen voert gemeente Nijmegen voor gemeente Mook en Middelaar taken uit. Over het gedeelde gebruik van de applicatie Gouw in deze context geeft de IT-auditor een verklaring af die de gemeente Mook en Middelaar in haar verantwoording gebruikt.

Ook met een partij als Samen Sterker wisselt de gemeente gevoelige gegevens uit in het kader van de uitvoering van WMO en Jeugdzorg taken. Hier over zijn convenanten afgesloten met de betrokken partijen. Over de toetsing op de uitvoering van deze convenanten is nog geen overeenstemming bereikt. Stadscontrol is bezig met het ontwikkelen van een standaard toetsingsproces.

5. Vooruitblik

5.1 Aanbevelingen uit externe toetsing

De externe controle door de accountant en de IT-audit in het kader van ENSIA leveren elk jaar weer aanbevelingen op die we meenemen in de ontwikkelingen van dat jaar.

IT toetsing bij de jaarrekeningcontrole

Voorafgaande aan de controle van de jaarrekening 2020 heeft de accountant onze (bedrijfs)processen beoordeeld. In een boardletter zijn deze bevindingen gerapporteerd en voorzien van aanbevelingen. De accountant ziet dat verbeteringen zijn ingezet, maar constateert dat deze nog niet volledig geïmplementeerd zijn. Hierbij adviseert hij prioriteit te geven aan de geautomatiseerde gegevensverwerking, het fundament van onze (bedrijfs)processen. Voor de accountant is deze nog niet betrouwbaar genoeg om op te kunnen steunen. Dit vergt nu nog extra controles op de gegevens uit onze financiële administratie.
Ons college heeft bij het aanbieden van de boardletter aan de raad aangeven dat “de bevindingen worden erkend en (waar nodig) passende verbetermaatregelen zullen worden ingevoerd.” Ambtelijk wordt actief hierop gestuurd en worden de bevindingen en verbeteracties drie keer per jaar geagendeerd in het Gemeentelijk Management Team (GMT).

Aanbevelingen van de accountant

In een praatplaat waarin de thema’s uit de boardletter zijn gevisualiseerd, komt IT als volgt terug.



- Op aanraden van de accountant gaan we een meerjarenplan opstellen rondom IT. Specifiek op de toegangsbeveiliging is ons streven om rechten toe te kennen op basis van rollen in plaats dit per persoon te doen. Daarbij adviseert de accountant om rechten ook periodiek te beoordelen.
- Rondom Cybersecurity lag de focus binnen het informatiebeveiligingsbeleid op de AVG. Hoewel dit begrijpelijk is, wordt geadviseerd om de scope te verbreden.
- Om onderbouwd te kunnen steunen op de iRvN wordt aangeraden om toe te werken naar een certificering van de iRvN, door een onafhankelijke partij, over de betrouwbaarheid van hun processen. Met dit als vergezicht, is ons voornemen om als tussenstop interne audits uit te voeren met behulp van de CyberManager.
- Afsluitend willen we het ‘mobile device management’ rondom het gebruik van persoonlijke apparaten (o.a. smartphones en tablets) uitbreiden. Het formuleren van beleid (soms regionaal) maakt hier een onderdeel van uit.
- Tot slot raadt de accountant ons aan om meer gebruik te maken van geprogrammeerde controles en data-analyses en deze met name ook te gebruiken in de vorm van bijvoorbeeld KPI’s bij het evalueren van de effectiviteit van het informatiebeveiligingsbeleid.

Aanbevelingen van de IT-auditor (ENSIA)

Bij de controle ten behoeve van het rapport dat de IT-auditor (2Control) afgeeft bij de collegeverklaring ENSIA bevestigden zij een aantal afwijkingen voor DigiD en Suwinet.

In de verklaring die het college jaarlijks af geeft over het voldoen aan de wettelijke normen voor het gebruik van DigiD en Suwinet staat voor 2020 dat wij voor een aantal normen niet voldoen. Dit betekent voor DigiD dat van de 25 normen per aansluiting bij twee van de vier aansluitingen er twee niet voldoen. Voor Suwinet betekent dit dat aan de twee toepassingen die wij al kenden er een is toegevoegd. Daarnaast is het zo dat er van de veertien normen die gelden voor de twee bekende toepassingen er een niet voldoet.

- De Suwinet toepassing die wij niet kenden wordt verzorgd door een van onze leveranciers. Het bleek dat wij niet voldoende op de hoogte waren van het gebruik van inkomensgegevens door deze leverancier, onder onze verantwoordelijkheid.
- De tweede Suwinet opmerking heeft betrekking op hoe wij de controle op het gebruik van Suwinet in onze eigen organisatie hebben geregeld met name voor nieuwe toepassingen in het Zorg domein.

Alle aanbevelingen zijn onderdeel van het verbeterplan voor het komende jaar.

5.2 Komend jaar

Gezamenlijk stippelen Stadscontrol en de Informatiemanagers het groeipad uit voor de organisatie naar meer volwassenheid. Dit gebeurt op basis van de visie die de organisatie heeft op het vlak van bijvoorbeeld data gestuurd werken en het weerbaarder maken van de organisatie en de burger. Daarnaast spelen de aanbevelingen van de toetsende instanties natuurlijk ook een belangrijke rol.

In 2021 staan de volgende stappen gepland:

- Implementatie van de CyberManager afronden
- maatregelen die volgen uit de AVG afdelingsplannen
- maatregelen van de mystery guest van juni 2019
- technische maatregelen uit de accountantscontrole/ENSIA
- organisatorische maatregelen in het kader van de accountantscontrole/ENSIA
- maatregelen op het vlak van de kwaliteit van data (in de context van datagestuurd werken) zullen per bron worden opgepakt.

Het informatiebeveiligingsplan van de MGR laat zien hoe zij de gemeente Nijmegen ondersteunt door het implementeren van maatregelen voor de kritische systemen en het nemen van generieke maatregelen om de IT omgeving voorspelbaarder te maken. Met name in de context van het Veiligheidsproject dat de iRvN in 2020 heeft uitgevoerd, en dat in 2021 afgerond zal worden.

Het controleplan van de FG zal onder andere gevoed worden door informatie over de implementatie status van de normen zoals dat is opgebouwd in de CyberManager.

5.3 Meerjarig

5.3.1 Informatiebeveiliging

Toetsing van onszelf en onze partners wordt uitgebreid

Informatiebeveiliging en privacy vormen een essentieel onderdeel van de jaarplannen van Stadscontrol. Het ondersteunen van en bijdragen aan initiatieven op het vlak van iBewustzijn spelen een centrale rol. In de komende jaren zullen controle mechanismen verder toegepast worden op de toetsing van informatiebeveiligingsmaatregelen, intern maar ook bij externe relaties. De verdere invoering van de CyberManager zal betekenen dat deze tool om een gemeentebreed overzicht te krijgen van de toestand van de informatiebeveiliging steeds meer sturingsinformatie zal opleveren, bijvoorbeeld voor het management van de afdelingen. Bovendien levert het de basisinformatie voor het controleplan van de FG en het ondersteunt collegiale toetsing intern maar ook bij partners in de MGR. Daarnaast faciliteert het onze eigen verantwoording richting andere partijen zoals de accountant. Op deze manier maken wij onze partners sterker en kunnen wij vertrouwen geven aan relaties die gegevens aan ons toevertrouwen, dan wel van ons afnemen.

ENSIA blijft het ijkpunt voor informatiebeveiliging

Wat de ontwikkelingen zullen zijn op het vlak van ENSIA is niet bekend. De ontwikkelingen in de stelsels zoals BIO (Baseline Informatiebeveiliging Overheid) en de DSO (Digitaal Stelsel Omgevingswet) zullen gevolgen hebben voor de toetsing. De verwachting is ook dat in de komende jaren de scope van de ENSIA audit breder zal worden, en dat er naast opzet en bestaan ook werking getoetst zal worden. De voorbereiding hier op is in 2019 bij de iRvN begonnen. Op dit moment beperkt de toetsing zich formeel tot opzet en bestaan, al zal er wel een eerste proef plaats vinden op het toetsen op werking. Toetsen op werking zal de volwassenheid van de gemeente Nijmegen ten goede komen. Een dergelijke ontwikkeling zal ook gevolgen hebben voor de eisen die wij stellen aan de partijen waar wij mee samen werken.

Contact met de burger verbeteren

In het contact met de burger zijn de ontwikkelingen dat er steeds meer verwacht wordt van de digitale mogelijkheden om diensten te verlenen en te communiceren. Zie bijvoorbeeld de ontwikkelingen rond manieren om je als burger te identificeren, zoals DigiD, IRMA en Eidas. Anderzijds is het zo dat er geen “one size fits all” burger is. Voor de gemeente is het van belang rekening te houden met burgers die om redenen van ongeletterdheid of geestelijke dan wel lichamelijke beperkingen, niet de mogelijkheid hebben om gebruik te maken van de digitale voorzieningen. Websites en achterliggende procedures moeten hier op onderhouden worden. Het ontstaan, dan wel vergroten, van een kloof tussen diegenen die mee kunnen komen met de ontwikkelingen en degenen die dat niet lukt moet voorkomen worden. Het bieden van alternatieve voorzieningen moet indien nodig meer aandacht krijgen om te voorkomen dat sommige burgers belemmerd worden in hun toegang tot voorzieningen en het uitoefenen van hun rechten.

5.3.2 Privacy

De uitdagingen op het terrein van privacy en informatiebeveiliging zijn ook in de komende jaren onverminderd groot. Om daarop in te spelen wordt verder ingezet op:

Voorlichting en advies zijn onontbeerlijk

Een terugkerende vraag is hoe vanuit professie om te gaan met het gebruik van social media kanalen zoals Whatsapp en Signal of Facebook, naast het gebruik van reguliere kantoor applicaties zoals (versleutelde) mail. De Citrix crisis heeft laten zien dat er bij het gebruik van social media kanalen vragen ontstaan op het vlak van archivering, wat een eis is voor zakelijk gebruik. Daarnaast ontstaat er door de Corona crisis steeds meer vraag naar applicaties die samenwerken op afstand ondersteunen, zoals bijvoorbeeld Miro. Telkens moet hier de afweging gemaakt worden tussen gebruiksgemak en de waarborgen voor het veilig omgaan met persoonsgevoelige informatie. Deze afweging maakt de organisatie zelf bij het formuleren van beleid, maar ook de medewerker maakt deze afwegingen dagelijks bij het uitvoeren van werkzaamheden de keuzes rond de te gebruiken gereedschappen en de te delen informatie.

Evaluatie als continu proces

In het kader van risicomanagement voeren wij Data Privacy Impact Assessments (DPIA) uit op nieuwe en bestaande gegevensverwerkingen. Dit zijn analyses aantonen wat de risico`s van de gegevensverwerking zijn voor de privacy van de betrokkenen (meestal burgers). Deze analyses zijn op dit moment nog te vaak een momentopname van de privacy-risico's die spelen bij een gegevensverwerking. Afdelingen die een DPIA hebben uitgevoerd doen dit meestal maar een keer en gebruiken het niet als terugkerend evaluatie-instrument bij proceswijzigingen. De DPIA kan ook gebruikt worden om het invoeren van de ingezette maatregelen te monitoren en te borgen. Ook dat zien we nog niet. Door de DPIA ook in te zetten bij beheer / controle zal het nadrukkelijk een onderdeel vormen van de (interne) verantwoordingsplicht.

Leren van wat wij doen

Zoals bij elk thema gaan er ook wel eens dingen verkeerd. Het niet functioneren van maatregelen wordt in het ergste geval aangetoond door een datalek. Het bewust worden van de organisatie is het meest gediend als we daar een leermoment van kunnen maken. Juist door het leren van onze ervaringen ontstaat de mogelijkheid om beter te worden. Het breder uitdragen van deze geleerde lessen kan helpen in de bewustwording en daarmee weerbaarder maken van medewerkers en bestuurders

Dit heeft onder andere geleidt tot een voorstel tot het benoemen van iBewustzijn als belangrijk thema voor de Nijmegen School vanaf 2021.

In het kader van leren van wat we doen ondersteunt Stadscontrol het iBewustzijn programma met aanvullende activiteiten op het vlak van gedrag en cultuur.

Bijlage: achtergrond & begrippen

Wat is Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor een pakket aan maatregelen, die getroffen worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te garanderen, en te beschermen tegen bedreigingen. Het begrip 'informatiebeveiliging' heeft te maken met:

- *beschikbaarheid / continuïteit*: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid:* het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Er is ook een sterke samenhang met de archiefwet. In het Informatiebeveiligingsbeleid van gemeente Nijmegen wordt daarom in deze context ook verwezen naar duurzame opslag:

- *duurzaamheid:* het zorg dragen voor de tijdige archivering van informatie zodat ook in de toekomst verantwoording en geschiedschrijving mogelijk blijft. Dit aspect komt voort uit de archiefwet.

Informatie is één van de belangrijkste bedrijfsmiddelen van de gemeente. Toegankelijke en betrouwbare informatie is essentieel voor een gemeente. Gemeente Nijmegen wil zich verantwoordelijk gedragen, aanspreekbaar en servicegericht zijn. Gemeente Nijmegen wil bovenal transparant en proactief verantwoording afleggen aan burgers en raadsleden en met minimale middelen maximale resultaten behalen. De bescherming van waardevolle informatie is datgene waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

Wat is Privacy

De Algemene Verordening Gegevensbescherming (AVG), is mei 2018 van kracht geworden. Er is in 2017 een Functionaris Gegevensbescherming (FG) aangesteld alsook een Privacy Officer (PO). Het Privacy beleid van gemeente Nijmegen legt de nadruk op:

- Transparantie en communicatie
- Ethiek en minimalisatie
- Privacy by Design
- Rechten van de betrokkene
- Relatie met informatieveiligheid

Wat zijn de kaders & hoe toetsen we daarop?

De AVG spreekt van het beschermen van persoonsgegevens met afdoende technische en organisatorische maatregelen. De BIO is het normenkader dat voor een gemeente (overheid) bepaalt of technische en organisatorische maatregelen afdoende zijn.

De standaard voor het toetsen van deze normen kaders is geformuleerd door de beroepsvereniging van register auditors in Nederland, de NOREA.

Deze normenkaders en de toetsing van de toepassing daarvan door middel van de vragen die geformuleerd zijn door de NOREA zijn de basis voor de inhoud van ISMS en PIMS systemen zoals de CyberManager die door gemeente Nijmegen gebruikt wordt.

Waar liggen de bevoegdheden?

De functie van CISO is verplicht gesteld via de BIO. De CISO is verantwoordelijk voor het beveiligen van de informatie om in de beschikbaarheid, integriteit en vertrouwelijkheid te kunnen voorzien die nodig is voor de dienstverlening. De CISO heeft een derdelijns toetsende rol maar geeft ook advies.

De functie van FG is verplicht gesteld (voor een gemeente) via de AVG. Is verantwoordelijk voor de bescherming van de privacy van burgers en medewerkers van gemeente Nijmegen. Het accent van de derdelijns FG rol ligt meer op toetsing en minder bij advies.

In het normenkader van de BIO is het College van B&W eindverantwoordelijk voor de risico`s die aanvaard worden en de maatregelen die getroffen worden. Deze verantwoordelijkheid begint bij de eigenaren in de lijn die voor hun processen bepalen welke keuzes zij willen maken bij het bereiken van hun doelen. Aangezien het college van B&W eindverantwoordelijk is zijn zij de enige die risico`s kunnen accepteren.

Afkortingen

Afkorting	Uitleg
AVG	Algemene Verordening Gegevensbescherming. In werking getreden op 25 mei 2018. Sinds dat moment geldt in de gehele Europese Unie dezelfde privacywetgeving.
BAG	Basisregistratie Adressen en Gebouwen bevat gemeentelijke basisgegevens van alle adressen en gebouwen in een gemeente.
BGT	Basisregistratie Grootschalige Topografie is een digitale kaart van Nederland waarop gebouwen, wegen, waterlopen, terreinen en spoorlijnen eenduidig zijn vastgelegd.
BIO	Baseline Informatiebeveiliging Overheid. Van kracht sinds 1 januari 2020. Een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid gebaseerd op de internationaal erkende en actuele ISO-normatiek.
BRO	Basisregistratie Ondergrond bevat gegevens over geologische en bodemkundige opbouw van de Nederlandse ondergrond.
BRP	Basisregistratie Personen bevat persoonsgegevens van inwoners van Nederland en van personen die Nederland hebben verlaten
CISO	Chief Information Security Officer verantwoordelijk voor het informatiebeveiligingsbeleid. Dit betreft zowel het implementeren van beleid als het toezicht houden op de uitvoering ervan
CMM	Capability Maturity Model. Amerikaans model dat gebruikt wordt om het stadium van volwassenheid van een proces (organisatie) uit te drukken.
DigiD	Digitale Identiteit s een systeem waarmee Nederlandse overheden op internet iemands identiteit kunnen verifiëren, een soort digitaal paspoort voor overheidsinstanties.
DKD	Digitaal Klantdossier gegevens die ingelezen kunnen worden vanaf het Inlichtingenbureau met betrekking tot werk en inkomen.
DPIA	Data Protection Impact Assessement oftewel gegevensbeschermingseffectbeoordeling is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
ENSIA	Eenduidige Normatiek Single Information Audit heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door toezicht te bundelen en aan te sluiten op de gemeentelijke P&C cyclus
EWS	Early Warning System. Systeem voor het analyseren van log informatie en het voeden van het SIEM systeem

Afkorting	Uitleg
FG	Functionaris voor de Gegevensbescherming is een onafhankelijke deskundige op het gebied van gegevensbescherming die binnen een organisatie (of een aantal organisaties) wordt aangewezen om te adviseren, informeren en toezicht te houden op de naleving van de AVG.
ISMS	Information Security Management System is een verzameling van alle (onderling gerelateerde) informatiebeveiligingselementen van een organisatie die ervoor moet zorgen dat beleid, procedures en doelstellingen samenhangend kunnen worden gecreëerd, geïmplementeerd, gecommuniceerd en geëvalueerd om de algehele veiligheid van de informatie van een organisatie beter te garanderen.
MDM	Mobile device management. Het (op afstand) beheren van mobiele apparaten zoals laptops, smartphones en tablets.
NOREA	Nederlandse Orde van Register EDP-Auditors is de beroepsorganisatie van IT-auditors in Nederland.
PIMS	Privacy Information Management System ondersteunt in het managen van een aantal registraties (Datalekken, Verwerkingsregister, Data Protection Impact Assessments (DPIAs), Risico's, Maatregelen, Verzoeken, Toestemmingen) om AVG compliant te zijn.
PO	Privacy Officer is degene die de eerste lijn van advies dient, tot op casus niveau, op het vlak van privacy en het voldoen aan de AVG.
RMC	Regionale Meld- en Coördinatiefunctie voortijdig schoolverlaten richt zich op jongeren tussen 18 en 23 jaar, met het doel voorwaarden te scheppen zodat zij een passende onderwijs- en/of arbeidsmarktpositie kunnen bereiken.
SIEM	Security Incident and Event Monitoring. Systeem voor het analyseren van log informatie vanuit verschillende gemeenten zodat informatie over gebeurtenissen snel gedeeld kan worden.
SUWI	Wet Structuur Uitvoering Werk en Inkomen. Suwinet is de elektronische infrastructuur gebruikt voor de uitvoering van de taken in het kader van de wet SUWI, en sommige ook niet-SUWI taken.