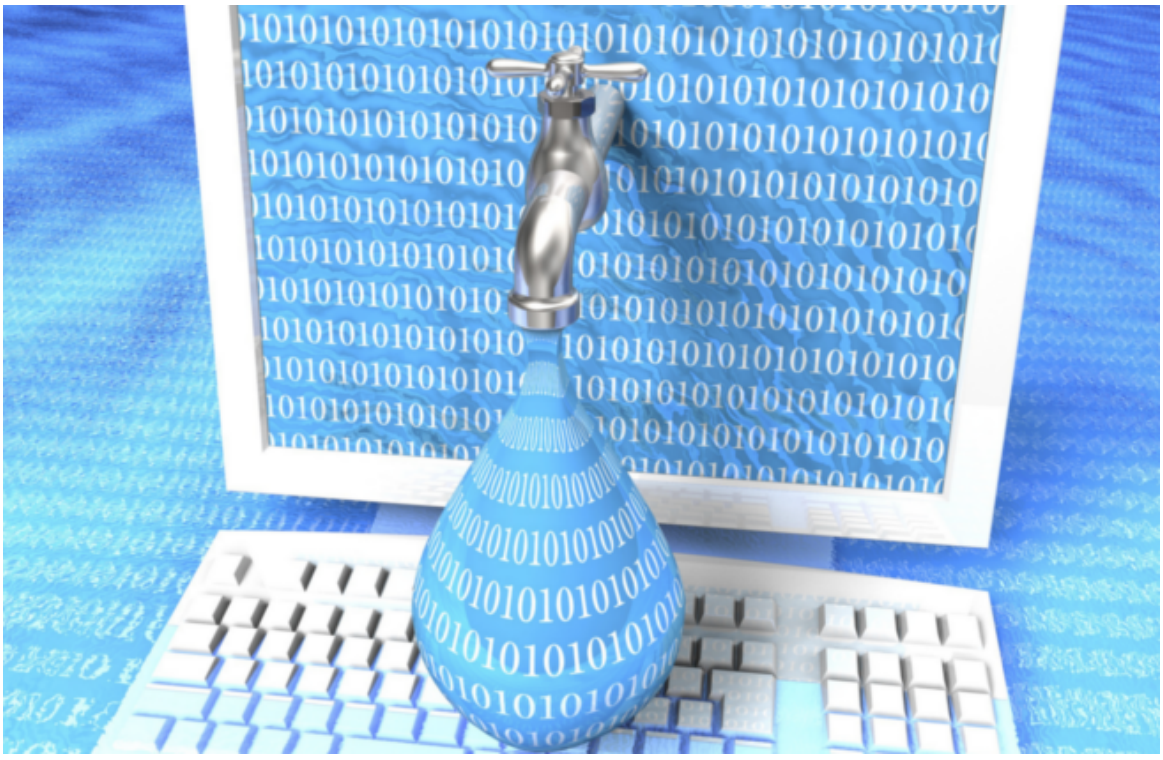
Nijmegen

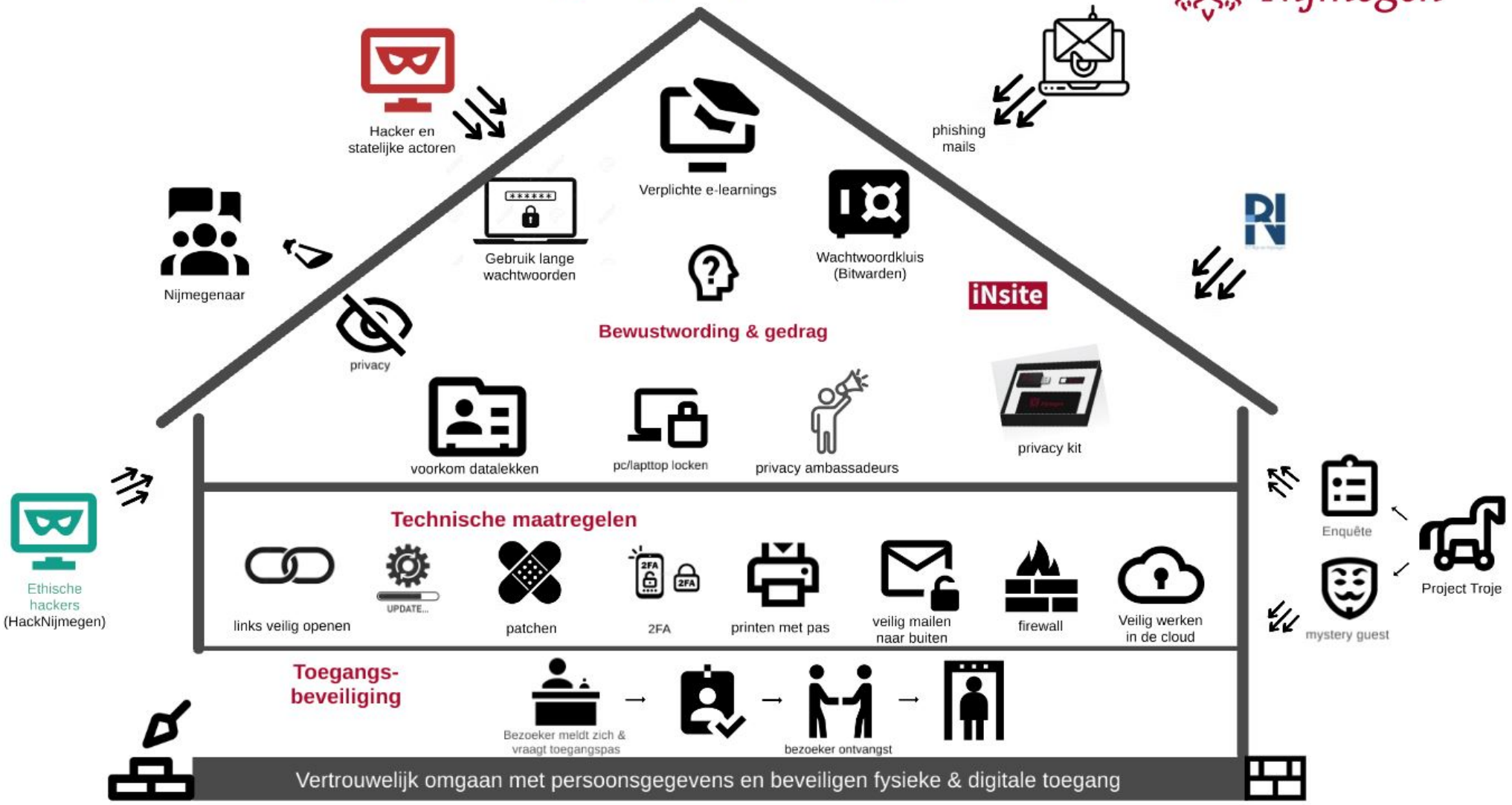


Rapportage Informatiebeveiliging en Privacy 2022

CISO gemeente Nijmegen, december 2022

Informatiebeveiliging & privacy 2022

Nijmegen



Inhoudsopgave

1. Doel & wettelijk kader

Doel

In dit rapport informeert gemeente Nijmegen 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 2023 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 is onderdeel van onze onderbouwing bij de collegeverklaring ENSIA, waarin het college aangeeft in welke mate gemeente Nijmegen voor DigiD en Suwinet aan de eisen voldoet. Bij de collegeverklaring horen verantwoordingsrapportages, waaronder dit jaarrapport maar ook verantwoordingsrapportages voor BAG, BGT en BRO, BRP, RNI en de WOZ, die door het college van B&W vastgesteld worden.

Wettelijk kader

Een periodieke rapportage aan alle managementlagen over de stand van zaken rond informatiebeveiliging is onderdeel van de Baseline Informatiebeveiliging Overheid (BIO). Met de passage over informatiebeveiliging in de jaarrekening en het onderbouwende rapport dat voor u ligt, verantwoordt het college zich aan de gemeenteraad over informatiebeveiliging in brede zin. In opvolging van de aanbevelingen van het regionale rekenkameronderzoek “Weten wat je moet weten” zal de rapportage ook beschikbaar gesteld worden aan de raad.

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:

- de maatregelen die wij op verschillende terreinen treffen om ons huis veilig en sterk te houden
- een aantal partijen waar wij mee samenwerken om ons huis te versterken
- een aantal dreigingen die proberen binnen te dringen.

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

3. Ambitie

De gemeente Nijmegen wil haar volwassenheidsniveau[1] 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 weet welke (passende) maatregelen we nemen
- weet wie waar verantwoordelijk voor is
- zorgt voor een controleerbare planning van maatregelen die genomen moeten worden
- de planning van de implementatie van maatregelen bewaakt
- weet in hoeverre de maatregelen effectief zijn
- de risico`s die overblijven accepteert.

Deze ambitie hoort bij het zijn van een professionele gemeente. Een ambitie die in 2021 nogmaals door de Nederlandse gemeenten bekrachtigd is, door af te spreken hier de benodigde middelen voor vrij te maken. Het regionale rekenkameronderzoek “Weten wat je moet weten” wijst ons er op dat gemeente Nijmegen zwaarder zal moeten inzetten op het verwezenlijken van deze ambitie om volwassenheidsniveau drie te halen.

Het team Stadscontrol binnen de gemeentelijke organisatie, met hier in ondergebracht de CISO en de FG, brengt de oordeelsvormende rol binnen de gemeente meer voor het voetlicht. 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 iRvN werkt aan professionalisering. Zij zijn gestart met een externe partij die hen naar certificering begeleidt. Hiermee geven zij gehoor aan de wens van gemeente Nijmegen tot meer transparantie en verantwoording ook naar andere partners toe.

[1] Het volwassenheidsniveau is gebasseerd op zowel de Norea handreiking als de BIO-SA (die gebaseerd is op de Capacility Maturity Model Integration). Daarin zijn meerdere modellen geïntegreerd tot één model. Volwassenheidsniveau 1: ad-hoc / informeel. Volwassenheidsniveau 2: beheerst. Volwassenheidsniveau 3: **vastgesteld / control gedefinieerd**. Volwassenheidsniveau 4: voorspelbaar. Volwassenheidsniveau 5: geoptimaliseerd.

4. Terugblik

4.1 Wat wilden we bereiken?

In 2022 gebruiken we het meerjarenplan, ambitiedocument en activiteitenoverzicht met daarin opgenomen de planning van de opvolging van alle maatregelen en aanbevelingen als leidraad voor onze activiteiten. De benodigde acties zijn gestart, onderweg dan wel afgerond. Er zijn acties die langer dan een jaar door lopen.

De inrichting van de **CyberManager** heeft in 2022 het stadium bereikt van het verder betrekken van de organisatie. Voor het verkrijgen van inzicht in de risico's die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen zijn de implementatie acties bij de afdelingen zelf uitgezet. In 2022 zijn zij aan de slag gaan met de maatregelen implementatie, een dreigingen analyse en continuïteitsplannen.

Alle afdelingen hebben het uitvoeren van **het AVG-proof plan** opgepakt. 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. Bij afronding van het AVG-proof project wordt duidelijk dat nog niet iedereen klaar is. Om een goed beeld te krijgen van de stand van zaken op het vlak van informatiebeveiliging en privacy bij onze gemeente hebben wij in 2022 meegedaan met het Project Troje van provincie Gelderland. Om zicht op de stand van zaken te houden is er een voorstel gedaan voor het werken met KPI`s.

Om meer gestructureerd aandacht te besteden aan **iBewustzijn** is verplichte scholing onderdeel van de jaarlijkse plannen. Vanaf de zomer is het jaarplan iBewustzijn acties uitgevoerd.

Naar aanleiding van het rapport van Cuccibu met betrekking tot de regionale crisisoefening wilden we aan de slag met continuïteitsplannen en het aanpassen van het **regionale crisisproces**. Dit crisisproces kent een nu verbeterde versie die in de eerste helft van 2023 vastgesteld zal worden.

4.2 Wat hebben we bereikt?

4.2.1 De gemeente Nijmegen

Activiteiten over de hele gemeente

- Het AVG-proof project is bij een drietal afdelingen afgerond.
- Het Continuïteitsproject heeft een eerste versie van de continuïteitsplannen opgeleverd. Er ligt een voorstel om de plannen verder uit te werken en te oefenen bij het GMT.
- Er is een eerste dreigingsanalyse opgesteld met het GMT. Vervolgstappen worden gecombineerd met het uitbreiden van de continuïteitsplannen.
- Er is door het jaar heen een i-Bewustzijn campagne geweest aan de hand van het opgestelde plan. Dit behelsde voorlichting via iNsite, aanwezigheid op medewerkersevenement waar privacy kits zijn verstrekt, en de introductie van de Dodo (als herkenbare personificatie van IB/privacy).
- Informatieveiligheid, Privacy en Informatiebeheer cursussen zijn beschikbaar gesteld via Studytube en voor iedere medewerker verplicht. Het aandeel afgeronde modules ligt op ruim 70%
- Het regionale ICT crisisproces is geactualiseerd. De aangepaste versie moet nog regionaal worden vastgesteld.
- Het HackNijmegen evenement heeft een aantal verbeterpunten opgeleverd (o.a. op het terrein van netwerkinrichting en wachtwoorden). De evaluatie met de studenten en iRvN was positief.

- iRvN is aan de slag met het beveiligingsproject evenals het traject naar certificering op basis van de BIO.
- Binnen de afdeling Juridische Zaken is een tweede Privacy Officer toegevoegd ter ondersteuning van de PO.
- 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, het begeleiden van prestatie dialogen en het toetsen van maatregelen, bijvoorbeeld door het uitvoeren van audits met behulp van de CyberManager door de FG en de CISO.

Er waren een aantal opvallende gebeurtenissen in het afgelopen jaar. Zo was er de oplevering van het rapport inzake het **regionale rekenkameronderzoek**. Gemeente Nijmegen heeft deelgenomen aan het **Project Troje** van de provincie Gelderland. En er was het **HackNijmegen** evenement.

Er is in het afgelopen jaar ook een melding gedaan die onder de responsible disclosure[2] regeling valt. Deze is niet gedaan via de website van gemeente Nijmegen maar via een collega.

In 2022 zijn er 56 beveiligingsincidenten gemeld, 21 daarvan waren datalekken. Van de datalekken zijn er 6 bij de Autoriteit Persoonsgegevens gemeld. Als het gaat om beveiligingsincidenten dan gaat de verkeerd verstuurde mail nog steeds aan kop. Wat afgelopen jaar opviel was het gestegen aantal meldingen van relaties aan ons dat zij gecompromitteerd waren. Daarnaast werden we voor het eerst gewaarschuwd (door de IBD) voor expliciet op de burgemeester gerichte social engineering.

Invoering van de CyberManager gaat door

Implementatie taken die zijn uitgezet bij de afdelingen werden door de ene afdeling beter afgehandeld dan de andere afdeling. Hier liggen een aantal factoren aan ten grondslag die in 2023 zullen worden aangepakt zodat de informatie over de status van de maatregelen steeds waardevoller wordt. Dit gebeurt in overleg met de afdelingen omdat hier capaciteit voor vrijgemaakt moet worden. We hebben overzicht gekregen van de status door in de CyberManager een interne audit uit te voeren op de BIO maatregelen.

In de CyberManager is nu 64% van de maatregelen actief. Dit betekent dat er over het geheel genomen weinig verschil is met het voorgaande jaar. De verklaring hier voor is dat er veel energie gestoken is en wordt in het beleggen van maatregelen bij de juiste eigenaren en het toetsen van de uitvoering van maatregelen. Zo blijkt bijvoorbeeld het implementeren van toegangspoortjes wel beveiligingswinst te hebben opgeleverd maar de uitvoering is nog niet sluitend. Hier zal het komende jaar een verbeterslag op plaats vinden. Dit leidt wel tot verbeterde beveiliging maar niet tot een hoger percentage in CyberManager.

In de CyberManager is ook een interne audit uitgevoerd op privacy op basis van het IBD AVG borgingsproduct. Hiermee is op organisatieniveau een meer en actueel inzicht verkregen over de status van doorgevoerde maatregelen. De uitkomsten van de audit zullen het komende jaar een vast onderdeel gaan vormen van de control cyclus.

Resultaten uit het regionale rekenkamer onderzoek

Het rapport over dit onderzoek is in juli 2022 naar de raden van de deelnemende gemeenten gestuurd. Na de zomer hebben de betreffende gemeenten ieder bepaald hoe ze met de aanbevelingen om willen gaan. Nijmegen omarmt de aanbevelingen maar erkent ook dat het belangrijk is de uitvoering er van efficiënt te organiseren omdat we niet alles tegelijk kunnen. Onze capaciteit is beperkt gezien onze andere opgaven. De

[2] Een beveiligingsonderzoeker, -organisatie, ethische hacker of een toevallige bezoeker een fout of kwetsbaarheid ontdekt in een product of een dienst.

complexiteit en dreiging op het vlak van informatiebeveiliging en privacy neemt toe. Om hier het hoofd aan te bieden is niet alleen techniek nodig maar ook een verandering in organisatie cultuur.

De volgende acties zijn onderweg:

- Eind eerste kwartaal 2023 wordt een hernieuwd strategisch privacy beleid aan de raad voorgelegd (aanbeveling 3).
- Een externe organisatie voert een risicoanalyse uit. Deze komt in de tweede week van januari ambtelijk in concept gereed (aanbeveling 5).

Ondertussen werken we in dit kader ook aan:

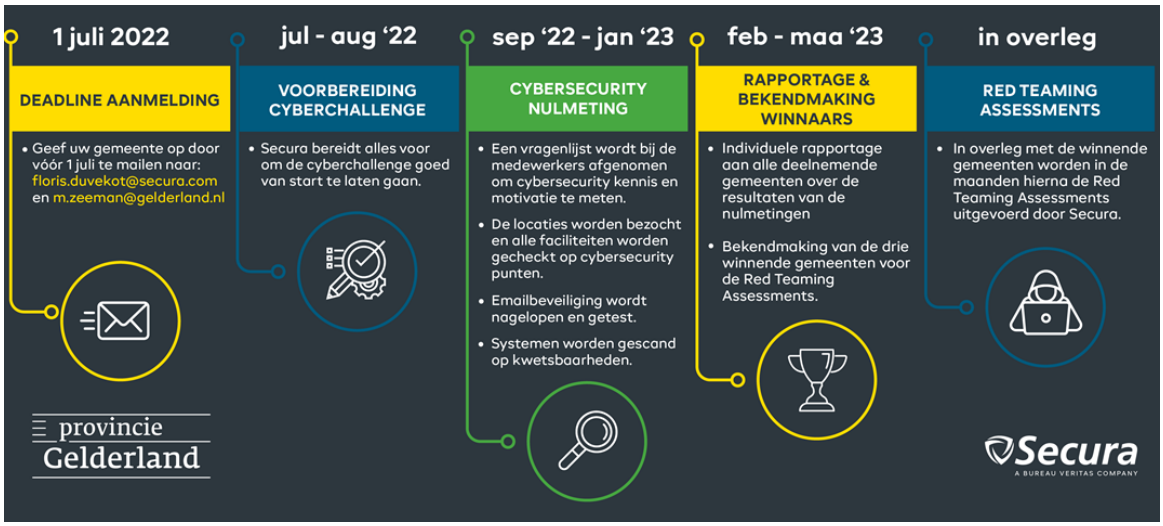
- Het met de iRvN uitvoeren van het meerjarige investeringsplan. Dit plan omvat het uitvoeren van maatregelen gericht op preventie, monitoring/bewaking en maatregelen die ertoe leiden dat in geval van dreiging of uitval, de functionaliteit snel hersteld is (curatie). Aanleiding voor dit plan was de analyse tussen de huidige situatie en gewenste situatie rond informatieveiligheid (ook bekend als GAP-analyse). Voor deze maatregelen is oplopend tot 2025 extra geld in de begroting opgenomen.
- Het jaarlijks oefenen en verbeteren van ons i-crisis protocol zodat we gesignaleerde kwetsbaarheden van passende maatregelen voorzien en we daarmee alert blijven op cybercriminaliteit.
- De ontwikkeling en beheer van continuïteitsplannen die we in kunnen zetten als er onverhoopt uitval van systemen door cybercriminaliteit of andere oorzaken plaatsvindt.
- Onszelf in de praktijk van alledag uitdagen door ons te laten bezoeken door een mystery guest.
- Onze systemen testen op kwetsbaarheden tijdens HackNijmegen.

Wat en wanneer we iets doen, hangt sterk samen met het (na te streven) volwassenheidsniveau. Het rekenkameronderzoek maakt duidelijk dat er nog genoeg te doen is om volwassenheidsniveau 3 te behalen. In de afweging tussen de waarden betaalbaarheid, uitvoerbaarheid en veiligheid bij de inzet van digitale middelen is niveau 3 het niveau waarvan wij, maar ook instanties die ons toetsen, de inschatting maken dat dit het meest passende doel is om na te streven. Om hier effectief op te kunnen toe zien zullen we in samenwerking met sturende organen zoals de raad, indicatoren en rapportage vormen ontwikkelen.

Resultaten uit Project Troje

De Gemeente Nijmegen heeft meegedaan met fase 1 van de Cyberchallenge van het Project Troje. Deze meting wordt aangeboden door de Provincie Gelderland en uitgevoerd in samenwerking met gedragswetenschappers en cybersecurityspecialisten van Secura. Deelname aan fase 1 bestond uit de volgende onderdelen

- Kennis en motivatie vragenlijst medewerkers
- Faciliteitenchecklist CISO
- Technische scan van buiten af
- Locatie bezoek (mystery guest) bij gemeente Nijmegen in oktober



De terugkoppeling van het complete resultaat verwachten wij in maart 2023. Wij doen niet mee aan fase 2 van dit project in verband met de belasting voor de iRvN en de relatief geringe toegevoegde waarde bovenop de al uitgevoerde tests in onze omgeving.

Desondanks zijn er nu al belangrijke resultaten naar voren gekomen uit het locatie bezoek dat in oktober heeft plaatsgevonden, als het gaat om het gebruik van de toegangspoortjes. Toegangspoortjes zijn een goed middel tegen ongewenste toegang tot het pand als je ze op de goede manier gebruikt. Naar aanleiding van de resultaten is er een GMT voorstel gedaan om een aantal verscherpingen en aanvullingen te doen op het Toegangsbeleid en het gebruik van de toegangspoorten.

Resultaten uit HackNijmegen

In november 2022 vond in het Stadhuis Nijmegen het HackNijmegen evenement plaats. Dit evenement was door gemeente Nijmegen en iRvN in samenwerking met Hunt&Hackett en het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen, georganiseerd. De studenten van de RU testten samen met studenten van Fontys Hogeschool Eindhoven, de technische informatiebeveiligingsmaatregelen van gemeente Nijmegen. Het doel van dit evenement was het verhogen van de weerbaarheid van gemeente Nijmegen doordat de gevonden kwetsbaarheden worden opgelost.
De studenten vonden een aantal kwetsbaarheden. Deze bestonden onder andere uit apparatuur die benaderbaar was, kwetsbare software en wachtwoorden die niet voldoende tegen de hackers bestand bleken. De bevindingen zijn deels technisch van aard maar raken ook aspecten van beleid.
De technische punten zijn opgepakt of bij de leverancier aangekaart. Zo is de configuratie van de apparatuur die benaderbaar bleek aangepast. Voor de kwetsbaarheden waar inrichtingskeuzes aan ten grondslag liggen zijn voorstellen gemaakt en gesprekken gepland. De verbeteringen zullen in zo snel mogelijk in 2023 worden uitgevoerd.

IT Audit observaties van de Accountant over 2022

Op het vlak van Algemene IT beheersmaatregelen en Cybersecurity concludeert de accountant over 2022 dat de gemeente de bevindingen oppakt uit de verschillende audits en ook opvolgt. Daarnaast zijn er verschillende plannen die de gemeente uitvoert. Hierin worden stappen gezet waarmee verbetering bereikt wordt, bijvoorbeeld op het vlak van contractmanagement en toegang tot systemen. Maar het ontbreekt aan executiekracht om alle plannen tijdig uit te voeren. Het is niet alleen zo dat de IT-

beheersing naar een hoger niveau getild moet worden. Tegelijker tijd vinden er ook veranderingen op het vlak van applicaties plaats die veel capaciteit vragen, zoals het project rond Coda. De accountant vraagt aandacht voor dit punt en adviseert het opstellen van een integraal plan om meer inzicht te krijgen in acties en tijdslijnen.

Resultaat van de ENSIA Cyclus 2022

Deze zelfevaluatie, gebaseerd op de BIO, is tijdig afgerond. Alle vragenlijsten zijn ook dit jaar op tijd ingeleverd. Bij de definitieve audit wordt voor DigiD aan de normen voldaan. Voor Suwinet blijkt dat de interne beheersingsmaatregelen nagenoeg aan de normen voldoen, op een tweetal normen voor het onderdeel DKD inlezen na. Voor deze normen is een verbeterplan opgesteld.

Een kanttekening bij het verantwoordingsproces is dat bij het aansturen van de leveranciers er strenger gemonitord moet worden op het tijdig opleveren van de Third Party Memoranda.

Daarnaast is een aanbeveling om de bezetting in de organisatie en de overdracht van taken die te maken hebben met de zelfevaluatie en de DigiD/Suwinet audit beter te bewaken. Dit met name ook met het oog op de toetsing van werking (met ingang van 2024), waar het tijdelijk niet uitvoeren van monitoring taken tot grotere problemen zal leiden bij de audit dan nu.

Zie de figuur hier onder waarin onze ENSIA auditor de ontwikkeling naar het toetsen van werking uit legt.

Figuur 1 Opbouw van opzet naar werking

Wij rapporteren als gemeente Nijmegen op één moment in het jaar over de status van onze informatieveiligheid, via ENSIA. Deze Rapportage IB en Privacy is daar een onderdeel van. Vanuit de gemeente brede 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 – BRO en WOZ bij de collegeverklaring over ENSIA. Een korte samenvatting per stelsel vindt u hier onder.

Stelsel	Samenvatting
DigiD	Er zijn een aantal wisselingen van de wacht geweest waardoor de overdracht en de opvolging van aandachtspunten vertraging op liep. Gemeente Nijmegen voldoet op alle punten en we zullen in het komende jaar extra aandacht besteden aan overdracht en opvolging ook in verband met de komende toetsing op werking.
Suwinet	Bij Z&I heeft in het afgelopen jaar een reorganisatie plaatsgevonden. Door geconcentreerde inzet van het team kwaliteitsmedewerkers is de verantwoording via ENSIA goed afgerond. De punten uit het verbeterplan van 2021 zijn allemaal aangepakt.
BRP	1. ENSIA: De verantwoording over informatieveiligheid. Het thema “organisatie van de beveiliging”, is met 110 punten afgenomen. Vanwege de lopende opleidingstrajecten binnen de afdeling is er voor gekozen medewerkers in 2022 niet extra te belasten met de i-bewustzijn trainingen. Deze staan gepland voor 2023. Daarnaast speelde in 2022, dat niet bij alle medewerkers, die BRP -werkzaamheden verrichten, naar een verklaring omtrent gedrag is gevraagd. Wel is een plan (en overeenkomst met KPN) beschikbaar in een situatie dat internet/telefonie uitvalt om de bedrijfscontinuïteit te garanderen. Het thema “toegang” (-sbeveiliging), is verbeterd doordat de prestaties van leveranciers op het gebied van informatiebeveiliging jaarlijks beoordeeld worden op vooraf vastgestelde prestatie-indicatoren. Het thema “naleving” is ongewijzigd, goed. 2. KWALITEITSMONITOR: toetsing van de kwaliteit van de processen op basis van afgesproken normen. In de tabel, blijkt uit onderdeel 2, een stijgende lijn, een goede score. 3. RNI: Register Niet Ingezetenen. De score bij toegang (-sbeveiliging) nam af wegens problemen bij de leverancier, voor het leveren van aangevraagde autorisatiepassen. * De in 2021 behaalde RNI-score bij thema “bijhouding”, ten opzichte van de maximaal te behalen score van het thema komt, doordat in 2022 een verschuiving van vragen in de thema’s “bijhouding” en “verstrekking gegevens”, plaats vond. Het geeft zowel in 2021 als in 2022 een goede score.

1. ENSIA BRP	Max te behalen	Behaald in 2021	Behaald in 2022
Organisatie beveiliging	400	400	290
Toegang	400	375	385
Naleving	400	360	360
2. Kwaliteitsmonitor			
Bijhouden BRP	400	331	385
Verstrekken gegevens	300	300	300
Aanbeveling	100	61	92
3. RNI			
Organisatie beveiliging	100	100	100
Toegang	40	40	15
Naleving	40	40	34
Bijhouding van de BRP	150	155	150 *
Verstrekking gegevens	50	45	50 *
Aanbeveling	20	20	20

Reis-documenten

Zowel in de informatiebeveiliging (ENSIA) als in de aanbevelingen binnen processen (kwaliteitsmonitor) is ten opzichte van 2021 een lichte afname in de score te zien. De verklaring is vrijwel hetzelfde als de verklaring bij de BRP (hierboven). Een verbetering van de toegangsbeveiliging staat gepland.

1. ENSIA reisdocumenten	Max te behalen	Behaald in 2021	Behaald in 2022
Organisatie beveiliging	400	400	330
Toegangsbeveiliging	400	370	340
Naleving	400	400	315
2 Kwaliteitsmonitor			
Aanvraag-en uitgifteproces	400	400	400
Overig proces	300	300	300
Aanbeveling	100	100	75

BAG

2022: Voor een groot aantal verblijfsobjecten is gecontroleerd of ze aan de juiste panden zijn gekoppeld en indien nodig is de koppeling in de registratie verbeterd. Medewerkers van de WOZ controleren aan het begin van het jaar de voortgang van de bouw van de verleende vergunningen. Hiervoor is een jaarlijks terugkerend proces ingericht. Ook hebben we net als in 2021, de techniek van 3D-mutatiesignalering ingezet om aan- en verbouw aan bestaande panden en nieuwe panden te constateren waarvoor geen omgevingsvergunning is verleend. Die constateringen zijn geregistreerd in de BAG. Door interne samenwerking zijn deze wijzigingen ook geregistreerd in de BGT en in de registratie voor de Woz-heffing.

2023:
De controle van de koppeling van verblijfsobjecten aan de juiste panden wordt voltooid en indien nodig wordt de koppeling in de registratie verbeterd. We zullen in 2023 strenger controleren op het proces om de kwaliteitsnorm voor de verwerkingstermijn van het verwerken van definitieve pandgeometrie te halen. Tevens verschilt bij een aantal verblijfsobjecten de geregistreerde "gebruiksoppervlakte" tussen de BAG en de Woz-registratie. Om die verschillen op te lossen wordt in 2023 een nieuw proces ingericht.
Een regel van de wet BAG geeft aan dat van de gemeente wordt verwacht dat afwijkingen ten opzichte van de vergunde situatie worden getoetst op legitimiteit volgens de Wabo-regelgeving. In 2023 gaan we deze gewenste toetsing op legitimiteit bespreken met de gemeentelijke verantwoordelijken van het Vergunningverlenings-, Toezicht en Handhavingsbeleid (VTH-beleid) om te (laten) beoordelen of op dit onderwerp actie is gewenst en eventueel een nieuw proces moet worden ingericht.
Naast de bovenstaande verbetermaatregelen zal de geplande invoering van de Omgevingswet (Ow) en de Wet kwaliteitsborging voor het bouwen (Wkb) op 1 juli 2023 van invloed zijn op het bijhouden van de BAG. Om de juiste informatievoorziening te borgen voor het tijdig kunnen registreren in de BAG zal de ODRN met de gemeente in processen en systemen moeten gaan inrichten.

BGT

In 2022 is de capaciteit op BGT-beheer uitgebreid. De terugmeldingen zijn allemaal op tijd afgedaan, er staan echter nog drie meldingen open die extra aandacht behoeven. De BGT-processen zijn beschreven in een document en de acties die voortkomen uit de kwaliteitsdashboards en Tableau zijn grotendeels verwerkt.
Voor 2023 richten we ons op de drie terugmeldingen ouder dan achttien maanden en op de vijftien BGT-panden, waarvan de pandgeometrie verschilt met de overeenkomstige bag-panden. Verder gaan we onderzoeken waardoor er jaarlijks piekwerkzaamheden optreden in het bijhouden van de BGT. Door hier inzicht in te krijgen kunnen we wellicht besparen op inhuur.

BRO

De BRO wordt nog maar erg beperkt gebruikt in onze organisatie. We coördineren het gebruik van de BRO vanuit het bureau Basis- en Geo-informatie. Dat houdt in dat we de collega's toegang geven om relevantie informatie via de BRO te ontsluiten en of te raadplegen.
De komende periode gaan we ons verder verdiepen in de landelijke ontwikkelingen van de BRO en de impact die dit voor de organisatie heeft. Waar nodig voeren we deze veranderingen door in onze organisatie.

WOZ

Het afgelopen jaar is het project omzetting gebruiksoppervlakte afgerond. Hierbij is de data ook gesynchroniseerd met de BAG. Door middel van mutatiedetectie zijn vergunningsvrije bouwwerken in beeld gebracht en verwerkt in zowel de WOZ als BAG. Het aanleveren van bestanden aan de Waarderingskamer verloopt nu ook via XML berichtenverkeer. Samen met GouwIT is in 2022 de pilot gerealiseerd 'aanpassen taxatieverslag woningen'. Met ingang van 2023 worden alle woningen voorzien van dit nieuwe taxatieverslag. Afgelopen jaar is ook de aanbesteding printservice uitgevoerd. Met ingang van februari 2023 worden deze werkzaamheden uitbesteed aan Data B.
Komend jaar wordt in samenspraak met de Waarderingskamer een plan van aanpak gemaakt inzake het optimaliseren van de data. Een voorbeeld is het controleren van eventueel aanwezige kelders en de tuinen bij etagewoningen. De grond toekenning bij woningen zal ook verder onderzocht worden.

Resultaat op het vlak van privacy

Afhandeling klachten

In 2022 zijn er in totaal negen klachten ingediend door burgers en medewerkers betreffende een onrechtmatige verwerking van hun persoonsgegevens. Op 1 klacht na betrof het in alle gevallen ongegronde klachten. Zo bleek bij een aantal klachten de gemeente Nijmegen niet verantwoordelijk voor de gegevensverwerking of betrof het een rechtmatige verwerking van persoonsgegevens. 1 klacht was gegrond. Dit betrof een verwerking van persoonsgegevens vanuit een onbevoegde verantwoordelijkheid.

Rechten van betrokkenen

In 2022 zijn er bij de gemeente 53 verzoeken ingediend. Dit betrof allen inzageverzoeken. Het aantal van 53 betreft een behoorlijke stijging ten opzichte van het aantal verzoeken in 2021. De stijging is echter te verklaren doordat middels het AVG inzageproces een groot aantal BRP inzageverzoeken zijn ingediend. De BRP kent echter in de vorm van de Wet BRP een eigen wettelijk kader gericht op inzage in de BRP. Deze verzoeken zijn dan ook doorgezet naar de afdeling Publiekszaken.

Uitvoering van de plannen van aanpak ‘elke afdeling privacy-proof’

Medio 2022 zijn de afdelingen begonnen om de uitvoering van de “elke afdeling AVG-proof” plannen weer op te pakken. De afdeling Inkomen, zorg en Leerrecht is de eerste afdeling waarmee begonnen is. Het traject voor deze afdeling liep van juli 2020 tot juli 2022. Eind 2022 is gestart met de afronding van het project binnen de afdeling Financiën, Publiekszaken en de afdeling Vastgoed, Sport en Accommodaties. De overige afdeling zijn in uitvoering of net gestart.

DPIA als continu bijstuurproces

Het instrument DPIA is nog teveel een momentopname van de privacyrisico’s die spelen bij een gegevensverwerking. Ook wordt het instrument onvoldoende ingezet als monitoring op de implementatie en de borging van de ingezette maatregelen op de langere termijn. Hier schuilt dan ook nog steeds een kwetsbaarheid in. Door de ombuiging van implementatie naar beheer / controle wordt de DPIA een blijvend onderdeel van de (interne) verantwoordingsplicht. In 2022 zijn in totaal 23 DPIA’s uitgevoerd op (bestaande) grote complexe gegevens verwerkingen binnen het fysiek, sociaal en veiligheidsdomein. In de jaarlijkse controle wordt getoetst in hoeverre uitvoering en borging wordt gegevens aan de risico’s en maatregelen zoals opgenomen in de DPIA’s .

Naleving WPG

In 2022 heeft de (verplichte) externe audit op naleving van de WPG plaatsgevonden. De resultaten hiervan zijn verstuurd aan de Autoriteit Persoonsgegevens.

Inmiddels is er een traject gestart om de noodzakelijke verbeteringen in dit traject op te pakken en vorm te geven. In het najaar is er reeds een interne (tweede) audit geweest op dit domein door een interne auditeur, die hiervoor in de organisatie benoemd is.

Naleving AVG

In 2022 heeft de Functionaris voor de gegevensbescherming een interne controle uitgevoerd op naleving van de AVG door de gemeentelijke organisatie. Object van onderzoek was:

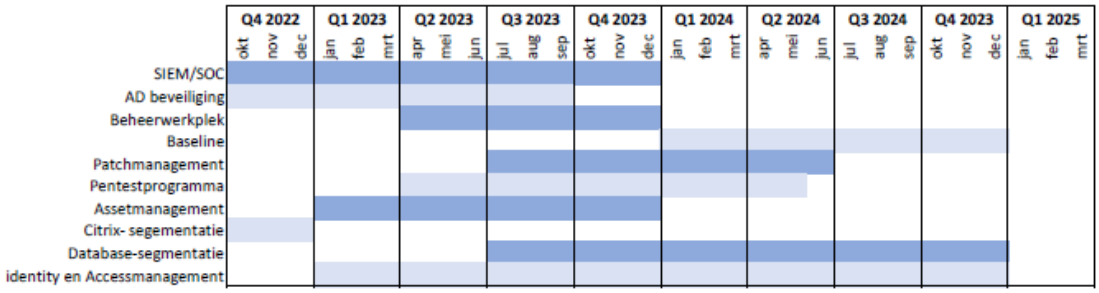
- voortgang ‘Mijn afdeling AVG-proof’;
- registraties datalekken, klachten en incidenten zoals opgenomen in de CyberManager;
- naleving van afspraken gemaakt in de DPIA en in de beoordelingen daarvan;
- naleving van privacy protocollen en tenslotte:
- naleving van de afspraken gemaakt in verwerkersovereenkomsten (getoetst middels een steekproef van 10 overeenkomsten over de afdelingen verspreid).

Ondanks dat er grote stappen zijn gezet op het vergroten van het informatiebewustzijn en het werken conform de AVG zijn er een drietal belangrijke constateringen op te maken:

- Er is voortgang op het traject mijn afdeling AVG—proof. Inmiddels hebben drie afdelingen dit traject afgerond (van de 10). Vier afdelingen zijn goed op weg en naderen de afronding. Drie afdelingen zitten (nog steeds) in de startfase. Hier zal extra effort geleverd moeten worden.
- Naleving van de DPIA's gaat al beter dan voorgaande jaren. Evidenced based aanleveren (aantoonbaar laten zien dat het werkt zoals afgesproken) is nog geen gemeengoed. Hier moet de organisatie nog een duidelijke stap in maken.
- de uitvoering van verwerkersovereenkomsten wordt onvoldoende getoetst op naleving bij leveranciers. Bij navraag vanuit de toezichthoudende rol gebeurt dit wél, echter als onderdeel van de normale bedrijfsvoering is dit géén gemeengoed.
- Er is nu een eerste inventarisatie geweest van de aanwezigheid van privacyprotocollen in de organisatie. Dit geeft al een goed beeld. Naleving maakt onderdeel uit van het controlplan 2023.

4.2.2 iRvN

In reactie op de aanbevelingen van de accountant en gebeurtenissen als de hack van de universiteit van Maastricht is iRvN het veiligheidsproject gestart. Dit project verkeert in de afrondende fase. Een van de doelen had betrekking op het inrichten van een separaat beheernetwerk. Dit project is gepauzeerd vanwege technische problemen (Microsoft heeft het concept teruggetrokken). Om de doelen van dit project (verbeteren van de beveiliging rond beheer) toch te kunnen verwezenlijken is het project herijkt en wordt dit nu in aangepaste vorm doorgezet.
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 implementatie heeft in 2022 gelopen en wordt in 2023 voortgezet.



Figuur 2 planning projecten iRvN

Op dit moment lopen er 4 concrete zaken:

- Aanbesteding Siem/SOC
- Segmentatie, en dan specifiek de Citrix-omgeving
- AD beveiliging
- Beheerwerkplek

Als het gaat om de segmentatie van de Citrix omgeving is het doel dat na de zomer iedere gemeente gesegmenteerd is. De aanbesteding van het SIEM/SOC is inmiddels gepubliceerd en de verwachting is dat er in mei gestart zal kunnen worden met implementeren. Het CSIRT dat is opgezet om informatiebeveiligingsincidenten op te pakken, functioneert goed en zal verder verbeteren met de

lessons learned uit onder andere de Log4j crisis. De gemeente blijft eindverantwoordelijk en legt in die hoedanigheid ook over de bij iRvN belegde maatregelen verantwoording af via ENSIA. In deze context is iRvN vanaf 2022 begonnen met het aanleveren KPI`s die ondersteunen bij het verkrijgen van inzicht. Deze zullen in 2023 verder worden ontwikkeld.

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. 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, privacy protocollen 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. De FG besteedt de komende tijd extra aandacht aan het opvolgen van verwerkersovereenkomsten. De CISO adviseert over passende maatregelen in de inkoopfase.

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 hebben een eigen verantwoordelijkheid voor hun verwerkingen en kunnen gemeente Nijmegen bevragen op de voortgang van de implementatie van maatregelen die wij als gastheer voor onze rekening nemen. Hiervoor is nog geen standaard proces afgesproken.

Het Werkbedrijf Rijk van Nijmegen (WBRN) de beschikking gebruikt een eigen Suwinet aansluiting voor haar werkzaamheden ten behoeve van het uitvoeren van de participatiewet. 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. Daarnaast rapporteert de WBRN in het kader van verwerkingsrelaties zoals die bijvoorbeeld geldt voor de “Doe je mee” regeling.

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.

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. Dit naast aanbevelingen die uit andere onderzoeken naar voren komen.

IT toetsing bij de jaarrekeningcontrole

Voorafgaande aan de controle van de jaarrekening 2022 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 en worden uitgevoerd zoals geformuleerd in onze meerjaren ambitie. Hierbij adviseert de accountant het college kritisch te kijken naar het tijdspad van de aangegeven ambities en daarbij de beschikbare capaciteit en middelen in ogenschouw te nemen. 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.” Het ambitiedocument en de meerjarenplanning zijn daarbij de sturingsinstrumenten. Verbeteracties en status worden 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.

- Het traject dat iRvN in gegaan is richting certificering op basis van de BIO is een belangrijke stap in het verhogen van het volwassenheidsniveau inclusief verantwoording aan de gemeente.
- Rondom riskmanagement werkt gemeente Nijmegen op basis van het ISMS. De implementatie hiervan moet afgerond worden en integraal risicomanagement moet verder ontwikkeld worden.
- De verdere uitwerking en verheldering van beleid en het samenbrengen van activiteiten en ambities in een plan met concrete acties en tijdlijnen is van groot belang om meer zicht te krijgen op de benodigde capaciteit en budget in relatie tot het tijdspad.
- Contractmanagement dient verder opgebouwd te worden zodat het ondersteunend werkt bij het invullen van de verantwoordelijkheden van proceseigenaren.
- De beheersing rondom de rechtenstructuur binnen applicaties en de controle op functiescheiding in kritieke processtappen moet verder verbeterd worden. Hier onder valt ook het tijdig afnemen van toegang tot systemen. Deze aanbeveling is deelt technisch van aard (nieuw ID systeem) en deels gebonden aan gedrag.

Aanbevelingen van de IT-auditor (ENSIA)

Bij de controle ten behoeve van het rapport dat de IT-auditor (2Control) afgeeft bij de collegeverklaring ENSIA zijn er dit jaar geen afwijkingen geconstateerd.

Wel formuleert de IT-auditor een advies met betrekking tot de controle.

- De opbouw en overdracht van controle dossiers moet beter bewaakt worden.
- Daarnaast is het van belang tijdig de leveranciers aan te spreken op de stukken die zij moeten leveren.

5.2 Komend jaar

Gezamenlijk stippelen Stadscontrol en de Informatiemanagers het groeipad uit voor de organisatie naar meer volwassenheid. Hierbij moeten we aandacht hebben voor focussen en prioriteren zoals ook in de reactie op het regionale rekenkameronderzoek en de directiebrief worden weergegeven. Door de juiste speerpunten te kiezen en efficiënte combinaties te maken binnen de opgave “digitale transformatie” verwachten belangrijke stappen vooruit te kunnen zetten op het vlak van informatieveiligheid.

In 2023 staan de volgende stappen gepland:

- Het inrichten van het iVeiligheidsteam om prioriteiten aan te kunnen brengen in de werkzaamheden binnen de afdelingen op het vlak van Informatiebeveiliging.
- Opstellen van een integrale roadmap met alle activiteiten op het vlak van informatiebeveiliging
- Aanbevelingen regionaal rekenkameronderzoek oppakken
- Maatregelen die volgen uit de AVG afdelingsplannen plannen en uitvoeren
- Maatregelen op het vlak van risico analyse/bedrijfscontinuiteit (n.a.v. rapport Cuccibu) inplannen en uitvoeren
- Technische maatregelen uit de accountantscontrole/ENSIA/HackNijmegen
- Organisatorische maatregelen in het kader van de accountantscontrole/ENSIA

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 iRvN in 2022 heeft afgerond zijn een aantal acties uitgevoerd. In 2023 groeit het Veiligheidsproject door in het Hunt & Hackett project waarin een aantal maatregelen worden genomen, gebaseerd op de gap analyse die zij hebben uitgevoerd.

Het controleplan van de FG en van de CISO zal onder andere gevoed worden door informatie over de implementatie status van de normen zoals dat is opgebouwd in de CyberManager. Daarnaast zal gebruik gemaakt worden van informatie verkregen van de afdelingen en toetsingen door het jaar heen.

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. Ook zijn deze thema`s een cruciaal onderdeel van de opgave “digitale transformatie”. Het verhogen van ons volwassenheidsniveau naar niveau drie zal een aantal jaren in beslag nemen waarbij verschillende aspecten van de organisatie geraakt zullen worden. Organisatorische processen, technische maatregelen maar ook de bedrijfscultuur. Dit proces zal gemonitord worden en er zal over gerapporteerd worden.

Het verhogen van de volwassenheid beslaat een aantal sporen. De CyberManager zal verder ingevoerd worden, waarbij alle niveaus van de organisatie betrokken zullen zijn. Van het invoeren van informatie in de lijn tot het sturen op de geproduceerde informatie door het management en het bestuur. Het ondersteunen van en bijdragen aan initiatieven op het vlak van iBewustzijn spelen een centrale rol. Denk hierbij aan een periodieke enquête van medewerkers en gesprekken met concernmanagers. Maar ook investeren in meer kennis en het veranderen van gedrag. Alle voortgangsinformatie wordt gebruikt in de controleplannen van de FG en de CISO om inzicht te geven. In de komende jaren zullen controle mechanismen verder toegepast worden op de toetsing van informatiebeveiligingsmaatregelen, intern maar ook bij externe relaties. 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

Als het gaat om de eenduidige toetsing door de rijksoverheid dan werken wij in 2023 toe naar de toetsing van werking in 2024. De voorbereiding hier op is in 2019 bij iRvN begonnen. Binnen gemeente Nijmegen is deze ontwikkeling wel aangekondigd maar beraden de applicatie eigenaren zich nog op de gevolgen voor de lijn. Op dit moment beperkt de toetsing zich formeel tot opzet en bestaan. 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. Het ministerie van Binnenlandse Zaken heeft aangekondigd dat het streven is om informatieveiligheid bij de overheid een wettelijke basis te geven. Dit moet gebeuren via een zorgplicht waaraan meer regelgeving kan worden gehangen, zoals de BIO. Door het wettelijk verplichten van de BIO is de vrijblijvendheid voorbij. Bij het toezicht zal niet alleen zal worden gekeken naar de naleving van algemene regels zoals de BIO. Er wordt ook toezicht gehouden op specifieke regels die aanvullend worden gesteld door de verschillende ministeries. Naast de binnenlandse wetgeving komt er ook steeds meer wetgeving op het terrein van digitale veiligheid vanuit Europa. Denk hierbij aan NIS2 wat gaat over de bescherming van vitale infrastructuur waar ook overheden onder vallen. Maar er zit nog veel meer in de pijplijn. Dit alles voert terug naar het aantoonbaar serieus nemen van digitale veiligheid en daarom de basis op orde hebben.

Contact met de Nijmegenaar 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. Er zal in de komende jaren gewerkt worden aan een centraal klantportaal “mijn Nijmegen” en aan de beschikbaarheid van verschillende kanalen voor de burger om contact op te nemen met onze gemeente “omni channel”. Dit moet op een veilige en eenduidige manier mogelijk gemaakt worden.

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:

Van implementatie naar beheer / controle

De inrichting van de CyberManager voor informatiebeveiliging, privacy en de WPG heeft in 2022 een volgend stadium bereikt door het invoeren van normenkaders en het daaraan koppelen van maatregelen om naleving te monitoren. Voor het verkrijgen van inzicht in de risico’s die we lopen op het vlak van informatiebeveiliging en de status van de te treffen maatregelen is het nu nodig dat de afdelingen zelf aan de slag gaan met de risico analyses en de implementatie van maatregelen.

De check op de “in control-maatregelen” (= de onderdelen van het controlplan) willen we als volgt invullen:

- Via het systeem CyberManager kunnen we zien welke maatregelen getroffen zijn en welke nog niet. Hier kan een actie uit voortkomen. Dit betreft informatie die voorradig is in het systeem (werkwijze: check melding in systeem en opvolging daarvan).
- Via gerichte vragen kunnen we nagaan of met name ‘nalevingen’ plaatsvinden i.c. wordt ook datgene gedaan wat we afgesproken hebben. Dit gaat met name over houding en gedrag. Deze vragen worden aan de afdelingshoofden - als gegevensverantwoordelijke – gesteld (medium = vragenlijst).

Tenslotte gaan we via gerichte steekproeven “checken” wat de kwaliteit van maatregelen is.

Het is noodzakelijk het komend jaar verder aan de slag te gaan met de ingezette lijn. Dat betekent dat de volgende stappen staan gepland:

- Het gebruik van de CyberManager verder uitrollen;
- maatregelen die volgen uit de AVG afdelingsplannen op basis van het project “mijn afdeling AVG proof”;
- maatregelen op het vlak van de kwaliteit van data (in de context van datagestuurd werken) zullen per bron worden opgepakt;
- Implementeren van de aanbevelingen van de Functionaris voor de Gegevensbescherming op basis van het uitgevoerde controleplan over 2022 (denk aan proces aanpassingen in leveranciers management)
- Het sturen op ‘spontane naleving’. Dat wil zeggen dat de aspecten (zoals kennis en kunde, kosten/baten, mate van acceptatie etc.) ten behoeve van spontane naleving terugkomen in de aansturing van medewerkers; denk aan afspraken rond opleiding.

Bewustwording en weerbaarheid

Op het gebied van bewustwording hebben in 2022 een aantal acties plaatsgevonden. Zo heeft (in het kader van Project Troje) een ‘mystery guest’ bezoek plaatsgevonden. Uit elke test op dit vlak blijkt dat de balans tussen gastvrijheid en waakzaamheid zoeken blijft. In de bewustwordingscampagnes zal er blijvend aandacht worden besteed aan deze balans en hoe dit toe te passen in ons werk. I-bewustzijn blijft een belangrijk thema voor de Nijmegen School ook na 2022. De digitale opleidingsmodules zijn verplichte leerlijnen opgenomen over Privacy en Informatiebeveiliging opgenomen voor alle nieuwe medewerkers, stagairs en anderen werkzaam voor gemeente Nijmegen. In de toekomst zullen aanvullend modules worden aangeboden, maar er zal ook een mix zijn met andere interventies om de medewerkers meer bewust en weerbaar te houden.

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.