Aan de gemeenteraad van Nijmegen

Postadres
Gemeente Nijmegen
Postbus 9105
6500 HG Nijmegen

Bezoekadres
Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactpersoon
Esther Zijlstra
e.zijlstra@nijmegen.nl
T 024 – 329 39 63

Ons kenmerk
E24.000421

Datum 5 maart 2024
Onderwerp Voortgang op informatiebeveiliging en privacy

Geachte leden van de raad,

In juli 2022 is het bestuurlijk rapport van de regionale rekenkamer over informatiebeveiliging en privacybescherming verschenen genaamd ‘Weten wat je moet weten’. Dit rapport bevat verschillende aanbevelingen, waar wij de laatste jaren mee aan de slag zijn gegaan. Eén van de aanbevelingen was om te gaan werken met Kritische Prestatie Indicatoren (KPI’s). Een andere aanbeveling was om bestuurlijk meer aandacht te geven aan deze thema’s binnen onze gemeente.
Middels deze brief willen wij opvolging geven aan deze aanbevelingen door de Raad op de hoogte te brengen van de stand van zaken omtrent informatiebeveiliging en privacybescherming binnen gemeente Nijmegen. Dit doen wij op een drietal manieren. Ten eerste door inzage te geven in de lopende ontwikkelingen te beschrijven aan de hand van de IT-roadmap (hierna: de roadmap). Daarnaast schetsen we een totaalbeeld van compliance op gebied van de BIO en de AVG. Tot slot geven we inzicht in de KPI’s die na afstemming met de Raad geprioriteerd dienen te worden.

IT-roadmap

Om een overzicht te geven van de stand van zaken zullen wij de lopende ontwikkelingen beschrijven aan de hand van de roadmap. Deze roadmap is samen met de accountant ontwikkeld als instrument om over risico’s en maatregelen te rapporteren. Het gaat in de roadmap zowel over maatregelen op het gebied van infomatiebeveiliging, als over maatregelen op het gebied van privacybescherming. In de roadmap zijn aanbevelingen en ambities omgezet in maatregelen die te volgen zijn door de tijd. Onderstaande acties zijn de acties in het kader van de roadmap. Zij vormen geen uitputtend overzicht van de acties die lopen op deze thema’s binnen de gemeente.

In 2023 zijn de volgende acties afgerond:

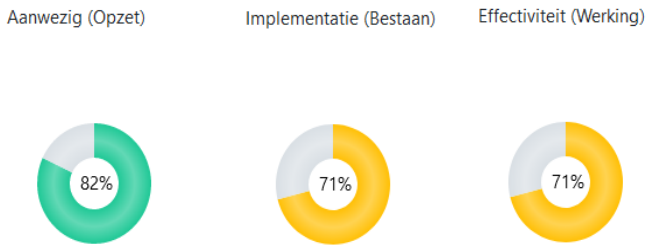
- Implementatie sterker wachtwoordbeleid
- Verhelderen en actualiseren privacybeleid
- Tweemaal jaarlijks de Raad informeren omtrent de stand van zaken op privacybescherming en informatiebeveiliging
- Uitbreiding formatie CISO en FG
- Verhogen bewustzijn medewerkers door middel van een jaarlijks iBewustzijn-plan
- Gebruik generieke accounts zo ver mogelijk terugdringen
- Wijzigingsbeheerproces standaardiseren
- Jaarlijks oefenen met het ICT-crisisteam Nijmegen
- Kritische prestatie indicatoren vastgesteld. Deze worden later in deze brief aangeboden.

De volgende acties lopen op dit moment:

- Het certificeringstraject van iRvN loopt (naar verwachting in 2027 gereed)
- Verdeling van de BIO maatregelen tussen iRvN en Nijmegen is in 2023 gestart en nagenoeg gereed. In 2024 afronden en verwerken in de CyberManager.
- Het bestaande informatiebeveiligingsbeleid moet worden geactualiseerd. Geplande vaststelling begin 2025.
- Continu risicomanagement moet worden ingericht. Op dit moment ligt de focus op het beheer van continuïteit en crisismanagement.
- Verwerkersovereenkomsten en privacy analyses zullen verder moeten worden uitgewerkt en ook getoetst.
- De continuïteitsplannen van de afdelingen zullen regelmatig moeten worden geoefend. Eerste oefening is voor 2024 gepland.
- Van alle privacy gevoelige applicaties zullen autorisatie matrices moeten worden opgesteld, met in acht neming van functie scheiding. Deze zullen regelmatig moeten worden getoetst.
- Meer inzet op iBewustzijn van het college en de raad door scholing aan te bieden, bijvoorbeeld in de vorm van thema sessies en/of eLearning.

Totaalscores vanuit CyberManager

De CyberManager is een applicatie die wij gebruiken als Information Security Management System (ISMS) en als Privacy Information Management System (PIMS). In deze applicatie houden we de voortgang op de naleving van de BIO en de AVG bij. De applicatie geeft voor beide onderwerpen een totaalscore als het gaat om opzet, bestaan en werking van de geïmplementeerde maatregelen op beide vlakken.



Figuur 1 status informatiebeveiliging



Figuur 2 status privacy

Informatiebeveiliging
Zoals hier boven te zien zijn de scores niet 100%. Het feit dat dit niet 100% is heeft te maken met beperkingen in de capaciteit door onze gehele organisatie (eerste, tweede en derde lijn), maar ook bij iRvN, die een deel van de (technische) maatregelen voor de gemeenten in de regio beheert.

Privacy
Ook voor privacy is de score nog niet volledig 100%. De toetsing hiervan is gedaan aan de hand van de AVG borging QuickScan 2.0. De implementatie van de maatregelen is grotendeels afgerond, alleen de naleving kan nog onvoldoende aangetoond worden. In de toekomst zullen we de toetsing doen aan de hand van het AVG Borgingsproduct 3.0. Dat betekent dat in volgende brieven de score kan afwijken.

KPI's om mee te sturen

Nu wij een totaalbeeld hebben geschetst van de informatiebeveiliging en de privacybescherming binnen onze gemeente, gaan we in op de KPI's die in overleg met de Raad zijn uitgekozen om op te sturen. Deze KPI's zijn uitgekozen op basis van aandachtsgebieden die in het bovengenoemde rekenkameronderzoek naar voren kwamen, gecombineerd met prioriteiten die aangegeven werden door raadsleden binnen de domeinen van informatiebeveiliging en privacybescherming. Het maken van keuzes binnen deze domeinen is essentieel om wezenlijke vooruitgang te kunnen boeken en om effectief te kunnen sturen.

E zijn op hoofdlijnen drie aandachtsgebieden vastgesteld:

1. Gegevensbeheer
2. Personeel
3. Toegangsbeveiliging (zowel fysiek als digitaal)

Zoals hieronder te zien kan men op deze gebieden inzoomen op meetbare KPI's. Zie bijlage 1 voor een weergave van de KPI's zoals ze in de Cybermanager te zien zijn. Deze aandachtsgebieden zijn door de raadsleden uitgekozen als thema's die de komende periode extra aandacht verdienen.

1. KPI's vanuit privacy

Gegevensbeheer is het eerste thema. Het heeft zowel componenten van informatiebeveiliging als van privacy in zich. Er zijn twee sub KPI's in het kader van privacy onderdeel van gegevensbeheer, namelijk het uitvoeren van DPIA's en het voldoen aan privacy eisen op het gebied van wetgeving en contracten.

a. Uitvoeren DPIA's

Een Data Protection Impact Assessment (DPIA) is een privacy scan die een gegevensverwerking van start tot eind in beeld brengt. Met de DPIA wordt het hele proces langs gelopen en gecontroleerd of het zo privacy vriendelijk mogelijk is ingericht. We zijn verplicht DPIA's uit te voeren op gegevensverwerkingen met een mogelijk hoog risico.[1]

De huidige score op voor wat betreft DPIA's is als volgt:
Opzet: 100 – het uitvoeren van DPIA's is vermeld in het privacy beleid en er is gemeente breed ruim gecommuniceerd over de verplichting om DPIA's uit te voeren op gegevensverwerkingen met een mogelijk hoog risico.
Bestaan: 100 – we zien dat er steeds meer DPIA's gemaakt worden (afgelopen jaar 26, in totaal 67)
Werking: 75 – jaarlijks worden de DPIA's gecontroleerd op naleving door de Functionaris Gegevensbescherming (hierna: FG). Niet van alle DPIA's komt ook daadwerkelijk een rapportage terug. Het gegeven dat de DPIA's op naleving getoetst worden, is nog niet meegenomen in de CyberManager (zie bijlage).

b. Privacy-eisen wetgeving en contracten

Deze KPI gaat over verwerkersovereenkomsten en andere soorten privacy-overeenkomsten (denk aan privacy protocollen en overeenkomsten onder gezamenlijke verantwoordelijkheid). Deze afspraken dienen in het kader van de AVG gemaakt te worden en worden periodiek gecontroleerd op naleving.
De huidige score op deze KPI is als volgt:

[1] Artikel 35 AVG

Opzet: 100 – het is gemeente breed duidelijk dat er met partners afspraken over gegevensverwerking gemaakt dienen te worden als onderling gegevensuitwisseling plaats vindt.
Bestaan: 100 – er zijn een groot aantal verwerkersovereenkomsten, of anderszins afspraken over gegevensverwerking gesloten. Hoewel het precieze aantal niet bekend is, gaat het waarschijnlijk over meer dan 150 overeenkomsten.
Werking: 50 – de verwerkersovereenkomst en privacy protocollen worden jaarlijks door de FG getoetst op naleving. Wegens het grote aantal, gebeurt dit middels een steekproef. We zien hierbij ook dat we er niet altijd in slagen om aan te kunnen tonen dat de afspraken die we hebben gemaakt ook daadwerkelijke nageleefd worden. De score in de CyberManager geeft de werking nog niet goed weer.

2. KPI's vanuit informatiebeveiliging

Voor **gegevensbeheer** vanuit het perspectief van informatiebeveiliging kijken we vooral naar het veilig verwijderen van gegevens en het risicobewust classificeren van gegevens.

a. Veilig verwijderen van gegevens

Het veilig verwijderen van gegevens heeft betrekking op wat er gebeurt met gegevensdragers op het moment dat deze niet meer gebruikt worden. Het gaat daarbij om bijvoorbeeld gegevensdragers in computers (bijvoorbeeld de "harde schijf"), maar het kan ook gaan om USB sticks (die bijvoorbeeld gevonden worden) of andere dragers. De score in de Cybermanager is:

Opzet: 100 - onze laptops en telefoons, en dus ook de gegevensdragers, zijn van iRvN. Aan het einde van de levensduur, of bij vertrek van de medewerker worden deze weer ingenomen. iRvN heeft een overeenkomst met D-two voor het gecertificeerd wissen en zo mogelijk opnieuw inzetten van apparatuur die door ons niet meer gebruikt wordt. Als dat niet gewenst is wordt de drager vernietigd.
Bestaan: --- Bestaan en werking is niet aangetoond in de CyberManager omdat iRvN deze maatregel beheert en het afgelopen jaar niet toegekomen is aan de administratie van de maatregel in het ISMS. Ze wordt wel uitgevoerd, daarom in de tabel oranje.
Werking: --- Bestaan en werking is niet aangetoond in de CyberManager omdat iRvN deze maatregel beheert en het afgelopen jaar niet toegekomen is aan de administratie van de maatregel in het ISMS. Ze wordt wel uitgevoerd, daarom in de tabel oranje.

b. Classificatie van informatie

Gegevensbeheer is niet mogelijk zonder classificatie van informatie. Bij het classificeren van informatie wordt bepaald welk niveau van vertrouwelijkheid, integriteit en beschikbaarheid bij deze informatie hoort. Het is de enige manier om te kunnen bepalen welke informatie wanneer vernietigd moet worden. De score is op dit moment:

Opzet: 100- Applicaties en de data die daarin gebruikt wordt zijn geclassificeerd volgens de standaard die door de Informatiebeveiligingsdienst voor gemeenten (hierna de IBD) gebruikt wordt. Dit proces is gedocumenteerd en de resultaten zijn goedgekeurd door de eigenaren van de applicaties. Er is ook aandacht voor informatie in mailboxen.
Bestaan: 100- Bij het in gebruik nemen van nieuwe/vervangende applicaties worden deze meteen geclassificeerd. Daarnaast worden bepaalde mailboxen gearchiveerd en is er een campagne geweest om medewerkers te doordringen van het belang van het archiveren van bepaalde documenten. Dit gebeurt steeds meer.
Werking: 100- Het is zo dat hoe minder gevoelig de applicatie is hoe minder aandacht er is, bijvoorbeeld voor het periodiek controleren van de classificatie (risico gestuurd). Dat is de reden dat in de tabel de status nog oranje is. Daarnaast is er steeds meer aandacht voor archiveren en op tijd verwijderen maar kan de consequente toepassing nog niet aangetoond worden.

In de context van de overgang van gemeente Nijmegen naar Microsoft 365 (in de loop van 2024) zal er meer aandacht zijn voor de ongestructureerde data buiten de applicaties.

Personeel is het tweede thema. Hierbij wordt met name gevraagd om aandacht voor het iBewustzijn (2a) van de medewerkers, de basis onder veel maatregelen die afhankelijk zijn van de medewerking van het personeel. Dit heeft ook raakvlakken met privacy.
Medewerkers moeten weten hoe gevoelig de informatie is waar zij mee werken, zij moeten tijdig de nodige trainingen volgen op het vlak van informatiebeveiliging en privacy en daarnaar handelen (2b). De statussen zijn hier:

Opzet: 100- Er is een scholingsprogramma (eLearning, maar ook aanvullende activiteiten) dat medewerkers volgen waarbij zij relevante informatie krijgen over wat gevoelige informatie is en hoe daar mee te werken.
Bestaan: 100 -Medewerkers volgen het scholingsprogramma (meer dan 90% heeft het basisprogramma afgerond, dat is hoog). Het management draagt uit dat het volgen van deze scholing belangrijk is.
Werking: 100 -Het doel van het scholingsprogramma is dat medewerkers zich informatiebewust gaan gedragen. Wij zijn nog op zoek naar manieren om dat te onderzoeken en het effect van onze eLearning en andere interventies te meten. Daarom is dit punt in de tabel nog oranje.

Het derde thema is **Toegangsbeveiliging.** Dit kent twee aspecten: de fysieke toegangsbeveiliging (3a) tot de gebouwen en beveiligde zones binnen de gebouwen. En de digitale toegangsbeveiliging (3b) tot applicaties en data.
De huidige status van de fysieke beveiliging is:

Opzet: 100-De beveiliging van de fysieke ruimte is met de toegangspoortjes erg verbeterd. De afspraken rond toegang tot de beveiligingszones zijn tegen het licht gehouden en waar nodig herzien.
Bestaan: 75-De toegangspoortjes worden gebruikt. De afspraken zijn aan de receptie over gedragen en worden zo veel mogelijk door hen toegepast. Met enige regelmaat is er overleg over de hantering van de afspraken.
Werking: 50-Het blijkt dat erg nog een extra stap nodig is om maximaal van de poortjes te kunnen profiteren. Het is nog te makkelijk om ze te omzeilen en dit gebeurt ook. Daarnaast zijn er dilemma`s die ontstaan door de inrichting en het gebruik van de panden. Consequent juist gebruik van de toegangssystemen is daarom nog niet aan te tonen.

De digitale toegangsbeveiliging is gebaseerd op de juiste omgang met accounts, wachtwoorden en multi-factor authenticatie.

Opzet: 100- Het beheer van toegangsrechten betreft maatregelen die getroffen worden om er voor te zorgen dat alleen medewerkers een account hebben, dat zij alleen toegang hebben tot de applicaties die zij nodig hebben en alleen met de juiste rechten. Om dit goed te kunnen doen moeten verantwoordelijkheden gedefinieerd zijn en de processen moeten bekend zijn bij de betrokkenen.
Bestaan: 100 – Op het functioneren van de processen voor het toekennen van rechten aan gebruikers worden controles op uitgevoerd. Dit gebeurt voor het generieke deel van het proces dat toegang geeft tot de gemeente Nijmegen omgeving. En voor applicaties naarmate het risico hoger is.
Werking: 50- Op deze controles zullen we nog een verbeterslag uitvoeren waarbij de toekenning van rechten voor meer applicaties getoetst zal worden, vandaar het oranje in de tabel.

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

A.P.W. van de Klift
gemeentesecretaris

H.M.F. Bruls
burgemeester

Bijlage 1: KPI`s in tabelvorm en de CyberManager

PRIVACY			
1. Gegevensbeheer	Opzet (1)	Bestaan(2)	Werking (3)
1b. DPIA's			

NL-20.2.4 Uitvoeren DPIA's Opzet: 100% Bestaan: 100% Werking: 0%

NL-20.2.7 Privacy eisen wetgeving en contracten Opzet: 100% Bestaan: 100% Werking: 100%

INFORMATIE BEVEILIGING			
1. Gegevensbeheer	Opzet (1)	Bestaan(2)	Werking (3)
1a. Veilig verwijderen van gegevens			
1b Gegevensbeheer			

8.3.2.2 Veilige verwijdering gegevens Opzet: 100% Bestaan: 0% Werking: 0%

8.2.1 Classificatie van informatie Opzet: 100% Bestaan: 100% Werking: 100%

8.2.1.1 Risico afgewogen classificatie Opzet: 100% Bestaan: 100% Werking: 100%

2. Personeel	Opzet (1)	Bestaan(2)	Werking (3)
2a. i-bewustzijn			
2b. Bescherming bedrijfsinfo en bewustzijn			

7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging Opzet: 100% Bestaan: 100% Werking: 100%

7.2.2.1 Bedrijfsinformatie beschermen Opzet: 100% Bestaan: 100% Werking: 100%

7.2.2.2 Bewustzijn training Opzet: 100% Bestaan: 100% Werking: 100%

3. Toegangsbeveiliging (zowel fysiek als digitaal)		Opzet (1)	Bestaan(2)	Werking (3)
3a	fysiek			
3b	digitaal			

