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
E24.003954

Datum 19 november 2024
Onderwerp Voortgang op informatiebeveiliging en privacy

Geachte leden van de raad,

Middels deze brief geven wij verder opvolging aan de aanbevelingen om te werken met Kritische Prestatie Indicatoren (KPI's) en bestuurlijk meer aandacht te geven aan de thema's informatiebeveiliging en privacy binnen onze gemeente. Wij doen dit door dezelfde indicatoren die wij in onze brief van 5 maart 2024 besproken hebben opnieuw te behandelen.
Ten eerste geven wij inzage in de lopende ontwikkelingen door deze 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 zijn afgestemd met de Raad en inmiddels bevestigd zijn door de Auditcommissie. Deze KPI's verdienen prioriteit. Hierbij gaan we in op eventuele verschillen ten opzichte van maart 2024.

IT-roadmap
Om een overzicht te geven van de stand van zaken beschrijven 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 informatiebeveiliging, 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. Dit is geen uitputtend overzicht van de lopende acties binnen onze gemeente.

In 2024 zijn tot en met oktober de volgende acties afgerond:
- Tweemaal jaarlijks de Raad informeren omtrent de stand van zaken op privacybescherming en informatiebeveiliging
- Uitbreiding capaciteit CISO en FG door inzet budget
- Verhogen bewustzijn medewerkers door middel van het uitvoeren van het iBewustzijn-plan (inclusief onderzoek door Hogeschool Saxion)
- Vergrendelen scherm bij het verlaten van de werkplek

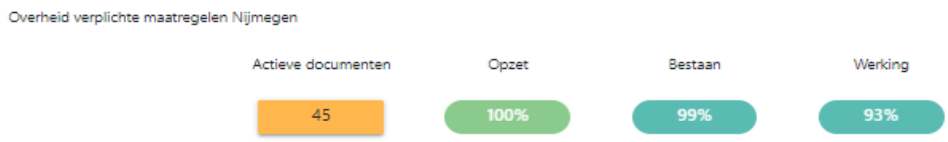
- Kritische prestatie indicatoren doorgezet
- Terugkoppeling autorisatiecontrole naar CISO is ingericht.
- Verbeterslag op ISMS is uitgevoerd.

De volgende acties lopen op dit moment:

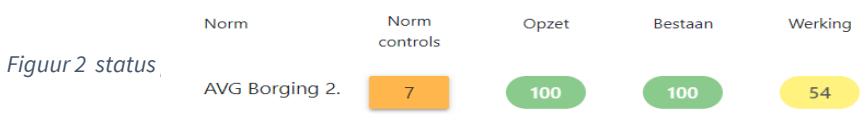
- Continuïteitsplannen per afdeling worden aangepast, meer oefeningen worden gepland. Plannen voor meer processen worden opgesteld
- Verdeling van de BIO maatregelen tussen iRvN en Nijmegen is in 2023 gestart en nagenoeg gereed. Eind 2024 wordt dit afgerond
- Het bestaande informatiebeveiligingsbeleid wordt geactualiseerd. Geplande vaststelling volgt begin 2025
- Verwerkersovereenkomsten en privacy analyses zullen verder worden uitgewerkt en ook getoetst
- Van privacygevoelige applicaties worden autorisatie matrices opgesteld, met inachtneming van functiescheiding. Verbeteringen in het proces worden toegepast voor de rondes van 2025.
- Meer inzet op iBewustzijn van het college zal dit jaar nog van start gaan. De verplichting voor het bestuur om aantoonbaar voldoende kennis verkregen te hebben zal in gaan in 2025.

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

Informatiebeveiliging

Zoals hierboven te zien zijn de scores voor opzet en bestaan (bijna) 100%, maar is dit voor werking nog niet zo. Het is wel belangrijk om hier een aantal kanttekeningen bij te maken.

De toetsing voor deze score is gedaan aan de hand van het geldende BIO normenkader 1.04. Daarbij zijn alleen de verplichte overheidsmaatregelen meegenomen. Het feit dat opzet en bestaan van deze maatregelen bijna 100% zijn, betekent dat we bij de maatregel beschreven hebben hoe we deze uitvoeren (opzet) en een voorbeeld kunnen laten zien dat dit ook zo is gebeurd (bestaan). De werking is nog geen 100%, want dat zou betekenen dat het proces altijd goed wordt uitgevoerd. En dat is nog niet zo. In deze toetsing werken we risicogestuurd, wat wil zeggen dat we de opzet het meest kritisch beoordelen bij de meest risicovolle processen. Dit 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. En dus moeten we keuzes maken. Dit betekent dat er met name als het gaat om werking voor de gemeente nog verbetering mogelijk is bij processen die niet tot de meest kritische, maar wel gevoelige, processen behoren. Ook deze processen maken ons kwetsbaar.

Daarbij is de verwachting dat de implementatie van de nieuwe Cyberbeveiligingswet (Cbw) in Q3 van 2025 zal betekenen dat de scores zullen verslechteren. Hoe dat er precies uit komt te zien is nog onduidelijk. Het aantal verplichte maatregelen zal toenemen als ook het bereik van de maatregelen. De lat komt hoger te liggen. Vanaf de tweede raadsbrief in 2025 maken we dat voor u inzichtelijk.

De hier boven beschreven actualisatie van het informatiebeveiligingsbeleid, onder andere ten behoeve van de Cbw, is ter hand genomen door de CISO. Een aantal adviseurs van Bureau Informatiemanagement en Automatisering dragen bij door het huidige beleid te vergelijken met de lopende ontwikkelingen en aanpassingen te doen waar nodig. Hierbij zal ook de relatie met de beleidsstukken van ICT Rijk van Nijmegen (iRvN) worden uitgewerkt.

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. Wat we wel zien is een lichte stijging ten opzichte van de brief in maart. Dat heeft te maken met het feit dat we de Cybermanager hebben geüpdatet op het onderdeel DPIA's. We houden elk jaar in november en/of december een interne audit om het algehele beschermingsniveau op gebied van privacy te kunnen duiden. Daarom valt te verwachten dat in de eerste brief van 2025 er een grotere verandering te zien is dan in deze brief. Bovendien zullen we vanaf 2025 de toetsing doen aan de hand van het AVG Borgingsproduct 3.0. We streven ernaar dit product minimaal 3 jaar gebruiken, zodat getoetst wordt op dezelfde criteria en de trend goed wordt weergegeven. Dat betekent wel dat in de 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. In de tabel in de bijlage staan de bevindingen van de CISO en privacy officer op opzet, bestaan en werking. Deze komen niet altijd overeen. De hierboven genoemde aandachtsgebieden zijn door de raadsleden uitgekozen als thema's die de komende periode extra aandacht verdienen.

Bij elke KPI worden aparte scores gegeven voor de mate waarin de beschrijving van de procedure voldoet aan de norm (opzet), de mate waarin de uitvoering van het proces voldoet aan de beschrijving (bestaan) en de mate waarin het proces consequent uitgevoerd wordt (werking). Deze scores worden apart weergegeven zodat zichtbaar is waar het eventueel aan schort.

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. Tot op heden zijn er dit jaar 22 DPIA's afgerond. Naar verwachting komen er dit jaar nog 5 tot 10 bij. De cyclus opzet, bestaan, werking fungeert nu goed bij DPIA's. Het is duidelijk wanneer DPIA's gedaan moeten worden en ze worden ook daadwerkelijk uitgevoerd. De score is daarom in de Cybermanager 100%. Het betekent echter niet dat we klaar zijn met DPIA's: er zijn nog steeds processen waarbij we geen DPIA hebben, terwijl die er wel zou moeten zijn. Die achterstand zijn we aan het inhalen. Daarom staat er in de tabel in de bijlage bij werking nog een oranje kleur. De huidige score op DPIA's is in de Cybermanager 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.

Werking: 100 – jaarlijks worden de DPIA's gecontroleerd op naleving door de Functionaris Gegevensbescherming (hierna: FG). Afdelingen moeten evidence based aantonen dat zij de maatregelen uit de DPIA hebben genomen.

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). Dit jaar worden alle privacy-overeenkomsten getoetst op naleving door de FG. Dat is nog niet meegenomen in de huidige score, maar zal volgend jaar te zien zijn in het controlplan van de FG. We hopen daarmee de werking van deze KPI aan te kunnen tonen en dus een hogere score te behalen. De huidige score op deze KPI is in de Cybermanager als volgt, maar geeft nog geen realistisch beeld van de werking:

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: 100 – de verwerkersovereenkomst en privacy protocollen worden jaarlijks door de FG getoetst op naleving. Dit jaar worden alle verwerkersovereenkomsten op naleving getoetst. Afgelopen jaren is er getoetst middels steekproeven. Daarbij zagen we dat we er niet altijd in slagen om naleving aan te tonen. 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: 100 - Bestaan en werking is aangetoond in de CyberManager. iRvN beheert deze maatregel.

Werking: 100 - Bestaan en werking is aangetoond in de CyberManager. iRvN beheert deze maatregel.

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. De overgang naar Microsoft 365 heeft de aandacht hiervoor versterkt.
Werking: 100- Voor de kritische applicaties wordt de classificatie onderhouden. 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. Het opruimen van de ongestructureerde informatie in het kader van Microsoft 365 zal naar schatting nog 2 jaar duren.

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). Ook hier geldt dat een score van 100% niet betekent dat alle medewerkers een perfect iBewustzijn hebben.

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. Het management draagt uit dat het volgen van deze scholing belangrijk is.
Werking: 100 – Het scholingsprogramma wordt consequent uitgevoerd en medewerkers nemen hier aan deel. Voor een deel levert het zichtbaar resultaat (schermen vergrendelen bijvoorbeeld). Daarentegen daalt de deelname voor de vervolgtrainingen. Het doel van het scholingsprogramma is dat medewerkers zich informatiebewust gaan gedragen. Wij hebben een onderzoek uitgevoerd naar het meten van factoren die het effect van onze

eLearning en andere interventies bepalen. Dit punt in de tabel is oranje omdat we het geleerde nog effectief moeten gaan toepassen.

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: 100-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. De techniek is verbeterd door de lezers te updaten.
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. Ook de passen zelf hebben een update nodig.

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 ervoor 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: 97 – 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: 90- Op deze controles zullen we nog een verbeterslag uitvoeren waarbij de toekenning van rechten voor meer applicaties getoetst zal worden en de terugkoppeling bij afwijkingen vollediger zal worden uitgevoerd, 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