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
E22.000666

Aan de gemeenteraad van Nijmegen

Datum 19 april 2022
Betreft Voortgang verbeterplan databeveiliging

Geachte leden van de raad,

De auditcommissie van uw raad heeft op 5 oktober 2021 een brief “Advies van de auditcommissie aan de Raad over de Stadsbegroting 2022-2025” geschreven. Een van de speerpunten die in deze brief benoemd werd is het thema databeveiliging, en in het bijzonder de voortgang rondom ‘cyber security’. In reactie daarop heeft het college op 19 oktober 2021 aangegeven later terug te komen op de voortgang van het verbeterplan dat in juli 2021 is opgestart op het vlak van cyber security. In deze brief komt het college daar graag op terug en schetsen we de voortgang langs een tweeluik: de gerealiseerde verbeteracties en de geplande acties. Overigens sluiten deze acties aan bij de interim-bevindingen van de accountscontrole waarover per brief aan u op 7 december jl. is gerapporteerd.

Gerealiseerde verbeteracties
Het informatiebeveiligingsbeleid is het vertrekpunt voor het gesprek over maatregelen en dient als richtlijn om de informatieveiligheid verder te vergroten. Op 8 februari 2022 is een nieuwe versie, vastgesteld door het college, die beter leesbaar is voor de Nijmegenaar. Het nieuwe informatiebeveiligingsbeleid heeft ook meer aandacht voor de verantwoordelijkheid van het bestuur en de toepassing van de 10 bestuurlijke principes van de VNG.

In 2021 zijn ook een aantal andere verbeteracties uitgevoerd. Zo hebben wij bijvoorbeeld een aantal controles uitgevoerd op programma’s die wij gebruiken met betrekking tot de juiste omgang met wachtwoorden. Maar ook is gecontroleerd of functiescheiding wel goed wordt toegepast op die plekken waar gevoelige gegevens verwerkt worden. Deze controles zijn het gevolg van aanscherpingen op het vlak van hoe wij werken met toegang tot gevoelige informatie en programmatuur. Het werken met mobiele apparatuur wordt beter beveiligd, toegang tot gegevens wordt sneller afgesloten als dit niet meer nodig is en wijzigingen aan programmatuur en de toegang daartoe worden altijd geaccordeerd door de eigenaar. Dit akkoord wordt vastgelegd. Om ervoor te zorgen dat medewerkers voldoende kennis en kunde hebben om met de aangescherpte maatregelen om te kunnen

gaan, is er verplichte scholing voor alle medewerkers beschikbaar gesteld. Over de uitgevoerde controles zullen wij ook verantwoording afleggen richting diverse partijen. De eerste set indicatoren waarop dit wordt gebaseerd is ontwikkeld.

Het functioneren van de regionale organisatie tijdens een ICT-crisis is in het afgelopen jaar beschreven en geoefend. Uit de crisisoefening van oktober 2021, en ook de doorstane Log4j crisis[1] rond de kerst, zijn een aantal lessen naar voren gekomen. Deze zijn gevat in een projectopdracht op het vlak van bedrijfscontinuiteit die is intern is uitgezet bij PIF. We versterken daarmee de basis, zonder dat we 100% garanties kunnen afgeven, zoals ook eerder al is toegelicht in de auditcommissie.

Geplande acties
Een aantal acties die in het afgelopen jaar in gang zijn gezet worden in de komende tijd doorgezet, waar mogelijk op basis van een inschatting van het risico dat wij lopen. Zo worden na de meest gevoelige programmatuur ook de minder gevoelige applicaties nagelopen op de omgang met wachtwoorden. Ook het verder toepassen van functiescheiding en controle op toegang wordt uitgebreid. Het monitoren op het gebruik van toegang (logging) vraagt om aanpassingen in de IT-omgeving.

Daarnaast wordt het werken met rollen ook buiten applicaties onderzocht om verder grip te krijgen op toegangsrechten van gebruikers. Meer grip krijgen op de geautomatiseerde omgeving van Nijmegen gebeurt ook door het uitbreiden van het beheer op alle machines en programmatuur. Zo hebben we steeds beter onder controle wat er gebruikt wordt op onze omgeving, wie of wat er verbinding maakt en welke handelingen zij uitvoeren.

Het systeem dat ons moet ondersteunen bij het afleggen van verantwoording over informatieveiligheid wordt verder ingericht en gemeente breed uitgerold. Daarnaast worden ook de indicatoren op basis waarvan wij ons verantwoorden verder ontwikkeld, zodat zij meer inzicht geven. Waar wij van onszelf verwachten dat wij ons steeds beter kunnen verantwoorden over onze informatiebescherming en privacy naleving, verwachten wij dat ook van onze leveranciers en partners. Hen zullen wij steeds meer om verantwoording vragen.

Naast het voorkomen van uitval van dienstverlening, zorgen wij er ook voor dat we voorbereid zijn op de situatie dat digitale dienstverlening niet mogelijk is (door technische oorzaken of een hack). Daarvoor stellen we een project in ten behoeve van het ontwikkelen van continuïteitsplannen, te beginnen bij de meest bedrijf kritische processen.

Wat is nodig
Een groot deel van de genoemde acties vraagt om een intensivering van onze aanpak. Denk daarbij aan het gemeente breed uitvoeren van controles en verbeteracties. Waar dat een vertaling gaat krijgen naar aanvullende formatie en/of middelen, komen we uiteraard tijdig bij uw raad terug.

---

[1] Stilte voor de storm door groot beveiligingsprobleem: 'Dit gaat niet met een sisser aflopen' | NOS

Tot slot willen wij de auditcommissie bedanken voor de opmerkingen en aanbevelingen in de afgelopen periode.

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

mr. drs. A.H. van Hout
gemeentesecretaris

drs. H.M.F. Bruls
burgemeester