Collegevoorstel
Openbaar

Onderwerp
Programma informatiebeveiliging iRvN

Opsteller	Niels Loeffen	**Behandeldatum**	7 juni 2022
Programma	Bestuur en Organisatie	**Status**	Openbaar
Portefeuillehouder	P. Molenaar		

Advies

1. Het Advies programma informatiebeveiliging iRvN vast te stellen waarmee we de basis voor informatieveiligheid op orde houden en een extra stap zetten in de richting van monitoring, detectie en preventie.
2. Raadsbrief over het Advies programma informatiebeveiliging iRvN vast te stellen.

Aanleiding
Door de toegenomen digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers, bedrijven en ketenpartners van groot belang. De bedreigingen voor informatieveiligheid voor de (lokale) overheid groeien de afgelopen jaren exponentieel in omvang en volwassenheid. Gemeente Nijmegen heeft de technische uitvoering voor de bescherming daarvan ondergebracht bij ICT Rijk van Nijmegen (iRvN). iRvN heeft daarom een GAP-analyse op basis van wereldwijde veiligheidsnormen laten uitvoeren door het bedrijf Hunt & Hackett, experts in informatiebeveiliging en cybercrime. Op basis van de aanbevelingen uit de analyse heeft iRvN een programma van maatregelen inclusief kostenraming samengesteld waarmee de bescherming van de regiogemeenten meegroeit met de toename van het dreigingsniveau.

De regionale hoofden bedrijfsvoering hebben inhoudelijk ingestemd met het programma van maatregelen zoals voorgesteld door iRvN. Zij hebben zich laten adviseren door de regionale CISO's (chief information security officer) en de informatiecoördinatoren van de betrokken gemeenten.

Beoogde impact
Dit voorstel heeft tot doel om het benodigde budget voor het programma informatiebeveiliging vast te stellen. Het besluit draagt bij aan het programma Bestuur en organisatie waarin het doel is opgenomen dat we een moderne en betrouwbare overheidsorganisatie willen zijn. Het betreft een programma van drie jaar dat elk jaar wordt herijkt op basis van de ontwikkelingen op het gebied van informatieveiligheid. Daarna worden de maatregelen onderdeel van de reguliere dienstverlening van iRvN. Voor het starten van het programma is ook de instemming van de overige regiogemeenten noodzakelijk.

Met het programma van maatregelen houden we de basis voor informatieveiligheid op orde en zetten we een extra stap in de richting van monitoring, detectie en preventie. Hiermee worden aanvallen in een vroeger stadium gedetecteerd en wordt er direct, geautomatiseerd op gereageerd.

Argumenten

1.1. *Aanvallen worden professioneler en het dreigingsniveau neemt exponentieel toe*
Kwaadwillenden werken georganiseerd, internationaal en op hoog technisch niveau. De gebruikte methodes en technieken staan inmiddels op gelijke voet met die van statelijke actoren. Daarnaast valt op dat aanvallers niet alleen gericht overheidsorganisaties aanvallen, maar ook in hoge mate via ketenpartners bij overheden proberen binnen te dringen. In de onlangs ontvangen brief van Jan van Zanen (voorzitter VNG) wordt hier op basis van de digitale agenda Veiligheid aandacht voor gevraagd.[1] Met de voorgestelde maatregelen houden we de technische basis op peil om de informatie en gegevens van Nijmegenaren, bedrijven en ketenpartners te beschermen.

1.2. We ambiëren een professionele bescherming tegen hackaanvallen
In ons digitaal informatiebeleid stellen we onszelf ten doel om onze informatiebeveiliging op orde te houden. Dat vraagt om het blijvend kunnen meebewegen met het toegenomen dreigingsniveau. De maatregelen binnen het programma vergroten onze slagkracht binnen drie aandachtgebieden:
- basishygiëne: aanscherping van monitoring van kwetsbaarheden;
- reactieve maatregelen: eerder kunnen detecteren van (potentiële) aanvallen en geautomatiseerd kunnen reageren;
- proactief acteren: regulier testen van de ICT-infrastructuur waarin handmatig en actief op zoek wordt gegaan naar kwetsbaarheden.

1.3. We blijven voldoen aan wet- en regelgeving voor informatiebeveiliging
De Baseline Informatiebeveiliging Overheid (BIO) is sinds 1 januari 2019 de verplichte standaard voor informatiebeveiliging van Nederlandse overheden. De BIO is een gemeenschappelijk normenkader en beschrijft verplichte maatregelen voor de beveiliging van de informatie(systemen). De maatregelen in het programma sluiten aan bij het normenkader, houden het noodzakelijke beveiligingsniveau op orde en gaan zelfs een stap verder dan het minimaal vereiste niveau.

2.1. Gelet op het belang van informatieveiligheid informeren we de raad.
Hoewel het onderwerp is geagendeerd in de eerste voortgangsmonitor 2022 en de stadsbegroting 2023-2026 informeren we de raad vanwege het belang van het onderwerp en de financiële consequenties.

Kanttekeningen

Risico's worden verminderd, maar 100% informatieveiligheid bestaat niet
Garanties op informatieveiligheid zijn niet te geven. Methoden en technieken voor het uitvoeren van hackaanvallen, en daarmee het dreigingsniveau, ontwikkelen zich in versneld tempo door. Hoewel we weten dat het menselijke handelen het grootste risico op datalekken vormt, zijn binnen het programma met name technische maatregelen opgenomen. De technische maatregelen zijn bedoeld om het beveiligingsniveau te professionaliseren zodat het mee kan blijven bewegen met het continu toenemend dreigingsniveau. Herhaaldelijk herijken en zo nodig bijstellen van het programma en de daarmee samenhangende kosten blijft noodzakelijk.

[1] 28 oktober 2021, Oproep aan alle burgemeesters; cyberalert, J.H.C. van Zanen voorzitter VNG

Er is gekozen voor maatregelen die proportioneel en meest urgent zijn
iRvN kiest er bewust voor om aanbevelingen van expertisebureau Hunt & Hackett als maatregelen op te nemen in het programma. Dat zijn maatregelen uit de middenvariant die aanvullend zijn op bestaande maatregelen. Er is niet voor de hoogste variant gekozen omdat de meerkosten niet opwegen tegen de extra baten of risicobeperking. Gekeken is naar de maatregelen die proportioneel en het meest urgent zijn om het beveiligingsniveau op peil te houden. Deze afweging is ook gemaakt in het licht dat het werkbaar moet blijven voor de organisatie (aspect gebruikersgemak). Nog verdergaande maatregelen kunnen zelfs voor vertraging leiden van onze systemen voor dienstverlening, waardoor de doelmatigheid en efficiency in het geding komen.

Informatieveiligheid vraagt ook aandacht voor houding en gedrag van medewerkers
Het voorgestelde programma betreft technische maatregelen. Daarnaast worden de bewustwordingsmaatregelen voor medewerkers opgepakt door regiogemeenten zelf en ook iRvN organiseert dit separaat voor haar eigen medewerkers.

Financiën
De jaarlijkse exploitatiekosten voor de voorgestelde maatregelen bedragen € 885.500 voor een programma met een looptijd van drie jaar. In overeenstemming met de in MGR verband afgesproken verdeelsleutel neemt de gemeente Nijmegen daarvan 54% voor haar rekening.

De exploitatiekosten voor onze gemeente bedragen € 163.000 in 2022, € 366.000 in 2023, € 407.000 in 2024 en structureel € 480.000 vanaf 2025. De begroting op concernpost I-deel DVO iRvN bij afdeling PIF is daarvoor niet toereikend. Voor deze bijdrage (incl. € 163.000 in 2022) is een melding gedaan in de eerste voortgangsmonitor 2022 en wordt, na instemming door de gemeenteraad, verwerkt in de stadsbegroting 2023-2026.

Vervolg
Na instemming door alle besturen van de regiogemeenten kan het programma informatiebeveiliging uitgevoerd worden. iRvN wil daarmee starten in het derde kwartaal van 2022.

Bijlage(n)
1. Advies programma informatiebeveiliging, iRvN, 7 april 2022
2. Gezamenlijke reactie op ‘’Advies Programma Beveiliging’’, CISO-groep Rijk van Nijmegen, 29 maart 2022