RAADSINFORMATIEBRIEF – Nr. 2022-026

Aan de leden van de gemeenteraad

Datum	12 april 2022
Zaaknummer	Z/22/418554 /ADV/22/1089756
Onderwerp	RID - Brief VNG Cyberalert
Portefeuillehouder	H. Winters

Contactpersoon	Rob van Dick
E-mail	R.vanDick@zevenaar.nl
Telefoon	0316-595533

Geachte leden van de gemeenteraad,

Inleiding
Op 28 oktober 2021 stuurde de Vereniging van Nederlandse Gemeenten (VNG) aan alle burgemeesters in Nederland een brief over 'cyberalert'. Onze Regionale ICT-dienst Samenwerking de Liemers (RID) heeft vervolgens een informatiebrief opgesteld voor de gemeenteraden van de deelnemende gemeenten. Hierin geeft de RID aan welke maatregelen genomen moeten worden om risico's op een cybersecurity aanval te verkleinen en wanneer het zich voordoet, de schade te beperken.

Kernboodschap
De VNG ("brief Van Zanen") adviseert vijf belangrijke maatregelen met de hoogste prioriteit in te voeren en bij te houden. RID de Liemers neemt dit advies over.

Het gaat om maatregelen om de kans op een hack met gijzelsoftware te verkleinen en de schade te bepreken mocht het zover komen:

1. *Up-to-date houden van hard- en software*
2. *Twee- of meerfactorauthenticatie (2FA/MFA)*
3. *Strikte netwerksegmentatie*
4. *Robuuste back-ups en het toetsen van het terugzetten van die back-ups*
5. *Testen en oefenen van ICT-crisisplannen*

Context
☐ Actueel maatschappelijk onderwerp/probleem
☐ Collegeprogramma
☐ Motie/amendement/toezegging

X Anders, namelijk VNG-signaal over informatiebeveiling

Inhoudelijke boodschap
Het Dagelijks Bestuur van Samenwerking De Liemers adviseert de vijf maatregelen die door Van Zanen worden genoemd sowieso te nemen en als er al stappen zijn gezet op dit gebied, deze op de juiste manier af te ronden en door te ontwikkelen. Voor het jaar 2022 heeft het Dagelijks Bestuur hiervoor € 101.500,- beschikbaar gesteld en daarnaast structureel vanaf 2023 een bedrag van € 204.500,- in de concept-meerjarenbegroting SDL 2023-2026 laten opnemen.

Uiteraard heeft RID De Liemers in het verleden – met inbegrip van de periode na 28 oktober 2021 – al de nodige stappen gezet rond de vijf door de VNG geadviseerde maatregelen. Maar de tijd heeft intussen niet stil gestaan en de ontwikkelingen dwingen de Liemerse gemeenten tot een vervolg.

Communicatie en vervolgproces

Communicatie naar buiten
Er zal over dit onderwerp niet nader naar buiten worden gecommuniceerd. Mede gezien de aard van het onderwerp en het risico dat kwaadwillende met deze informatie schade kunnen toebrengen aan de gemeente.

Vervolgproces
Zoals aangegeven gaat dit om een continu proces, waarbij gemeenten en RID de Liemers moeten blijven door ontwikkelen. Met het beschikbaar stellen van het budget wordt deze mogelijkheid gecreëerd.

Met vriendelijke groet,
burgemeester en wethouders van Zevenaar,

Danielle Jansen
secretaris

Lucien van Riswijk
Burgemeester

Bijlagen
1. *Informatiebrief RID Cybersecurity mrt28.pdf*
2. *U202100883_70557785.cleaned.pdf (VNG-Cyberalert)*

RID De Liemers

Regionaal ICT en Inkoop dienstencentrum
Gemeenten Duiven, Westervoort en Zevenaar

Datum	21-03-2022
Onderwerp	Cybersecurity/Brief Van Zanen
Opsteller	Wilfred Hekkers, algemeen directeur Samenwerking de Liemers

Geacht College van Burgermeester en Wethouders,

Op 28 oktober 2021 heeft de Vereniging van Nederlandse Gemeenten (VNG) aan alle burgemeesters een brief gestuurd met als onderwerp 'cyberalert'. Mr J.H.C. van Zanen vraagt in de betreffende brief als voorzitter van de VNG aandacht voor de toenemende kans geconfronteerd te worden met zgn. ransomware. Ransomware is kwaadaardige software, die een computer blokkeert of bestanden versleutelt. Pas na betaling van losgeld (ransom) zou de computer weer te gebruiken zijn. Synoniemen voor ransomware zijn 'cryptoware' of 'gijzelsoftware'.

Het verzoek deze brief met bijlage ook ter kennisname naar de Raadsleden te versturen.

Citaat uit de brief Van Zanen
'Het is een kwestie van tijd voor een grotere groep gemeenten tegelijkertijd wordt aangevallen. Veel van de huidige maatregelen om die risico's te beheersen zijn ontoereikend, blijkt uit de recente voorbeelden uit binnen- en buitenland, ook bij gemeenten. Zo'n hack of cyberaanval raakt de dienstverlening van gemeenten en dus inwoners rechtstreeks. Het gevolg: geen uitkeringen, geen vergunningen, geen paspoorten; jaren werk dat verdwijnt en enorme financiële schade om de dienstverlening te herstellen. Gegevens worden gestolen of gemanipuleerd. Openbare voorzieningen komen in gevaar', aldus van Zanen. En even verder: 'Ik vind dit een dermate alarmerend signaal dat ik u in mijn rol als voorzitter van de VNG met klem oproep om met college, raad en ambtelijke organisatie de benodigde tijd, mensen en middelen vrij te maken om de digitale beveiliging van uw gemeente in lijn te brengen met de actuele risico's van ransomware'.
In het verlengde van het bovenstaande adviseert Van Zanen om vijf belangrijke maatregelen met de hoogste prioriteit in te voeren en bij te houden.

Criminelen worden steeds handiger in het gebruik van ransomware; het gaat er geavanceerder en professioneler aan toe dan vroeger. RID De Liemers en de deelnemende gebruikersorganisaties moeten meegroeien met deze ontwikkeling. Dit vraagt om extra inspanningen om de kans op een hack met ransomware verder te verkleinen en de schade te beperken als het zover is. In beide gevallen brengt dit extra kosten met zich mee.

Kortom: de lat moet hoger want de risico's worden steeds groter. In dit verband is aan het Dagelijks Bestuur van Samenwerking De Liemers geadviseerd de vijf maatregelen die door Van Zanen worden genoemd sowieso te nemen en, als er al stappen zijn gezet op dit gebied, deze op de juiste manier af te ronden. Voor het jaar 2022 heeft het Dagelijks Bestuur SDL hiervoor € 101.500,- beschikbaar gesteld en heeft het Dagelijks Bestuur hiervoor structureel vanaf 2023 een bedrag van € 204.500,- in de meerjarenbegroting SDL 2023-2026 laten opnemen.

Gemeente Duiven gemeente Westervoort Gemeente Zevenaar

Uiteraard heeft RID De Liemers in het verleden – met inbegrip van de periode na 28 oktober 2021 - al de nodige stappen gezet rond de vijf door de VNG geadviseerde maatregelen, maar de tijd heeft intussen niet stil gestaan en de ontwikkelingen dwingen de Liemerse gemeenten tot een vervolg.

Met deze brief en bijlagen informeren wij u verder over de te nemen maatregelen.

Met vriendelijke groet,

Wilfred Hekkers
Algemeen directeur Samenwerking De Liemers

Bijlage 1

Vijf belangrijke maatregelen om de kans op een hack met ransomware te verkleinen en de schade te beperken als het zover is.

Maatregel 1 Up-to-date houden van de hard- en software
Op dit moment worden software-updates om efficiency-redenen zoveel mogelijk op 'vaste' momenten geïnstalleerd. Als er sterke aanwijzingen zijn dat de updates daar 'echt-niet-op-kunnen-wachten', wordt eerder gehandeld. Het risico dat er problemen optreden qua werking, wordt door een aangepaste aanpak verder verkleind. Daar wordt extra menskracht en een planningsinstrument voor ingezet.

Maatregel 2 Twee- of meerfactorauthenticatie (2FA/MFA)
Nog niet zolang geleden was één-factorauthenticatie in kantooromgevingen de standaard; naast de gebruikersnaam of mailadres geeft de gebruiker ook een wachtwoord in. Echter: wachtwoorden bieden een prima eerste beveiligingslaag, maar ook niet meer dan dat.
Bij **twee**-factorauthenticatie zijn de risico's al een stuk kleiner. Dit kan bijvoorbeeld in de vorm van een code die naar de smartphone wordt toegestuurd. Maar een vingerafdruk of gezichtsherkenning kan ook een tweede factor zijn. Bij RID De Liemers en de aangesloten gebruikersorganisaties is twee- of meerfactorauthenticatie al bijna volledig ingevoerd. Dus nog net niet helemaal. Er is een relatief beperkte tijdelijke inzet nodig om het laatste stukje 2FA/MFA verder in te voeren. Ook hier is extra menskracht voor nodig.

Maatregel 3 Strikte netwerksegmentatie
Netwerksegmentatie betekent dat een netwerk in meerdere zones wordt verdeeld. Dit voorkomt dat een virus of aanvaller zich kan verspreiden in het gehele netwerk. Afhankelijk van de wijze van implementatie is netwerksegmentatie een maatregel die de gevolgen van ransomware-aanvallen of DDoS-aanvallen beperkt. Bij RID De Liemers wordt hier verder aan gewerkt; een deel van de segmentering is al afgerond en voor het overige deel dient extra menskracht worden ingezet.

Maatregel 4 Robuuste back-ups en het toetsen van het terug zetten van die back-ups
Bij RID De Liemers wordt het 3-2-1-systeem voor back-ups gebruikt. Dit betekent dat er drie kopieën van alle data worden gemaakt. Deze kopieën staan op twee verschillende media, waarbij tenminste één kopie buiten de deur staat. Het terugzetten van back-ups – ook wel: 'restore' - wordt jaarlijks getest. RID De Liemers en de gebruikersorganisaties blijven bij dit alles binnen de geldende normen, maar deze werkwijze is ondertussen wel wat verouderd.
Daarom werken we o.a. aan het verhogen van de back-up frequentie, het volgen van een bepaalde methodiek en het uitbreiden van restore-testen. Ook hiervoor wordt extra menskracht ingezet. Ook de opslagcapaciteit wordt aangepast.

Maatregel 5 Testen en oefenen van ICT-crisisplannen
De crisisplannen van de gebruikersorganisaties en van RID De Liemers moeten (beter) op elkaar afgestemd worden. Anders: het ICT-crisisplan moet complementair zijn aan de overige crisisplannen. Per kritisch proces dienen de gebruikersorganisaties een deelplan op te stellen. Het deelplan moet worden geïmplementeerd en er dienen jaarlijks twee kritische processen geoefend te worden.

Uiteraard brengt dit extra werk met zich mee en moet de beschikbare personeelscapaciteit binnen de RID aangepast worden.

Aan Alle Burgemeesters

Datum
28 oktober 2021
Kenmerk
TPW/U202100883
Telefoonnummer
06 22493064
Bijlage(n)
-

Onderwerp
Oproep aan alle burgemeesters; cyberalert

Beste collega,

Een betrouwbare en veilige overheid vraagt om gedegen beveiliging van de informatie en bescherming van de privacy binnen de gemeentelijke informatiehuishouding. Inwoners vertrouwen ons immers hun identiteit- en persoonsgegevens toe. Veel incidenten kunnen voorkomen worden door het ‘eigen huis op orde’ te hebben en te houden. Dat vraagt om permanente en bestuurlijke aandacht.

Onze Informatiebeveiligingsdienst (IBD) meldt mij desgevraagd dat de kans om slachtoffer te worden van een aanval met ransomware (oftewel gijzelsoftware) sterk is toegenomen. Het is een kwestie van tijd voor een grotere groep gemeenten tegelijkertijd wordt aangevallen. Veel van de huidige maatregelen om die risico’s te beheersen zijn ontoereikend, blijkt uit de recente voorbeelden uit binnen- en buitenland, ook bij gemeenten. Zo’n hack of cyberaanval raakt de dienstverlening van gemeenten en dus inwoners rechtstreeks. Het gevolg: geen uitkeringen, geen vergunningen, geen paspoorten; jaren werk dat verdwijnt en enorme financiële schade om de dienstverlening te herstellen. Gegevens worden gestolen of gemanipuleerd. Openbare voorzieningen komen in gevaar.

Ik vind dit een dermate alarmerend signaal dat ik u in mijn rol als voorzitter van de VNG met klem oproep om met college, raad en ambtelijke organisatie de benodigde tijd, mensen en middelen vrij te maken om de digitale beveiliging van uw gemeente in lijn te brengen met de actuele risico’s van ransomware.

De VNG/IBD adviseert in dit kader de navolgende maatregelen met de hoogste prioriteit in te voeren en bij te houden.

1 **Houd hard- en software up-to-date**: installeer ten minste de meest recente beveiligingsupdates en zorg ervoor dat manieren om deze software van buiten te benaderen tot een minimum zijn beperkt.
Hackers scannen continu het hele internet op zwakke systemen. Zodra een zwakke plek gevonden is, begint een stroom van aanvallen om deze zwakke systemen binnen te dringen.

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

2 **Gebruik meerfactorauthenticatie** (2FA/MFA) waar dat kan en neem extra maatregelen als dat noodzakelijk is.
Alleen gebruikersnaam en wachtwoord zijn inmiddels ontoereikend om ongeautoriseerde toegang tot systemen tegen te houden. Twee- of meerfactorauthenticatie biedt een extra drempel en maakt het voor hackers moeilijker om uw systemen binnen te komen. Wanneer 2FA/MFA niet mogelijk is, bijvoorbeeld wanneer een product deze mogelijkheid niet bevat, dient u extra maatregelen te nemen om toegang tot de systemen af te schermen. Vraag uw CISO u daarover te informeren.

3 **Hanteer een strikte netwerksegmentatie**. Verdeel uw netwerk in meerdere zones die apart beveiligd zijn. Zo kunt u de gevolgen van een aanval beperken.
Criminelen zullen, eenmaal binnen in een systeem, proberen zoveel mogelijk systemen te besmetten of gegevens te stelen. Door systemen van elkaar te scheiden, beperkt u de schade in geval van een hack.

4 **Zorg voor robuuste backups** en toets regelmatig het terugzetten van deze backups.
Uw productiedata zijn uw kroonjuwelen. Voor uw bedrijfscontinuïteit is het essentieel dat u backups maakt en deze bewaart op verschillende locaties. Doe dit zodanig, dat minimaal één niet gekoppeld is aan uw bedrijfsnetwerk of op een andere wijze manipuleerbaar is.

5 **Test en oefen uw ICT-crisisplan(nen)**
Wees voorbereid op een incident en zorg dat u uw (interne en externe) crisisorganisatie direct bijeen kunt roepen in het geval van een incident.
In bijgaande link: Producten - Informatiebeveiligingsdienst *vindt u een handig hulpmiddel (het 'kaartje voor in de meterkast') waarin u direct uw in- en externe contacten bij een daadwerkelijke crisis kunt opnemen. Zet de belangrijke namen en nummers nú in uw agenda.*

Agenda Digitale Veiligheid
Met deze oproep benadrukt het VNG-bestuur het belang van digitale weerbaarheid. In februari van dit jaar deed u dat ook door unaniem de resolutie 'Digitale veiligheid: kerntaak voor gemeenten' aan te nemen. Wij hechten grote waarde aan digitale veiligheid en zien een grote gezamenlijke opdracht. Eerder stelden we de Agenda Digitale Veiligheid op, waarin ook de relaties met openbare orde en veiligheid en de strafrechtketen nader uitgediept worden. Het VNG-bureau is hiermee voortvarend aan de slag. U vindt een en ander op https://vng.nl/rubrieken/onderwerpen/digitale-veiligheid-en-privacy. Uw denkkracht als bestuurder is hierin meer dan gewenst. Wilt u meedenken? Neem dan contact op met teamadv@vng.nl.

De IBD ondersteunt
De hierboven genoemde prioriteiten zijn onderdeel van het normenkader voor de Nederlandse overheid, de Baseline Informatiebeveiliging Overheid. De IBD ondersteunt gemeenten bij de implementatie van deze normen. U vindt een en ander op Producten - Informatiebeveiligingsdienst
Mocht u hierover vragen hebben, dan kunt u contact opnemen met de IBD via info@ibdgemeenten.nl of 070 204 5511. In geval van een spoedeisend incident is dit nummer 24x7 bereikbaar.

Met u voel ik de urgentie om onze digitale veiligheid en weerbaarheid te vergroten. Ik vertrouw erop dat we met elkaar al het juiste doen om een crisis in onze informatiesamenleving en de gemeentelijke informatiehuishouding te voorkomen.

Met vriendelijke groet,
Vereniging van Nederlandse Gemeenten

mr J.H.C. van Zanen
Voorzitter