gemeente Westervoort

Kennisgeving aan de gemeenteraad

Documentnummer: 201558170 Zaaknummer: Z/22/093193

Portefeuillehouder(s): burgemeester

Voor vragen
Naam: Piet Hoogstraten
Telefoon: 06-1175494
E-mail: p.hoogstraten@1stroom.nl

Komt wel terug tot besluitvorming in de raad bij de besluitvorming over de zienswijze bij de Meerjarenbegroting van de SDL.

Onderwerp: Reactie RID de Liemers op brief VNG - Cyberalert

Aanleiding voor deze kennisgeving

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 om geconfronteerd te worden met een ransomware-aanval. 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’.
In het verleden is bijvoorbeeld de gemeente Hof van Twente slachtoffer geworden van een aanval met gijzelsoftware. Ook de oorlog in de Oekraïne heeft mogelijk consequenties op digitaal gebied. Het Nationaal Cyber Security Centrum (NCSC) sluit eventuele gevolgen en aanvallen in Nederland in de toekomst niet uit.

Relevant beleidskader
Informatiebeveiliging

Inhoud van mededeling

Citaat uit de brief Van Zanen (voorzitter van de VNG)
‘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. Dit bedrag is vrijwel gelijk aan de onderbesteding van 2021. Dit bedrag wordt terugbetaald aan de deelnemende gemeenten. Verder heeft het Dagelijks Bestuur hiervoor structureel vanaf 2023 een bedrag van € 204.000,- in de meerjarenbegroting SDL 2023-2026 laten opnemen. De meerjarenbegroting van de SDL zal voor een zienswijze nog worden voorgelegd aan de gemeenteraad.

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.

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

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 hardware en menskracht te worden ingezet.

Maatregel 4 Robuuste back-ups en het toetsen van het terugzetten 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 gezegd: het ICT-crisisplan moet complementair zijn aan de overige crisisplannen. Per kritisch proces dienen de gemeenten een deelplan op te stellen. Het deelplan moet worden geïmplementeerd en er dienen jaarlijks minimaal twee kritische processen geoefend te worden. Uiteraard brengt dit extra werk met zich mee en moet de beschikbare personeelscapaciteit binnen de RID aangepast worden.

Westervoort, 5 april 2022.

Burgemeester en wethouders van Westervoort

M. Sluiter MA	drs. A.J. van Hout
secretaris	burgemeester

Bijlagen:

Registratienummer:	*Omschrijving:*
1. 201558177	Brief VNG - Cyberalert