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