De Onderzoeksraad voor Veiligheid
T.a.v. Dhr. Prof. dr. mr. S. Zouridis
Postbus 95404
2509 CK 'S-GRAVENHAGE

Datum
22 december 2022
Kenmerk
TPW/U202200882
Telefoon
[redacted]

Bijlage(n)
-

Onderwerp
Reactie aanbevelingen rapport Kwetsbaar door software

Geachte heer Zouridis,

Op 14 december 2021 overhandigde uw Raad het rapport 'Kwetsbaar door Software' aan de VNG. Wij danken de Onderzoeksraad voor de Veiligheid voor dit rapport, dat we met veel interesse gelezen hebben.

Het rapport duidt de gebeurtenissen rond het beveiligingslek in het softwarepakket Citrix tijdens de jaarwisseling 2019/2020. Dit leidde ook bij een aantal gemeenten tot verstoring van de dienstverlening. Het rapport is voor de VNG een heldere weergave van de gebeurtenissen in die periode. We reageren daarom graag inhoudelijk op het rapport ‘Kwetsbaar door Software’.

De conclusies en daaruit voortvloeiende aanbevelingen zijn herkenbaar en verdienen de volle aandacht. In het rapport stelt de Raad zeven aanbevelingen, waarvan een aantal geheel of gedeeltelijk relevant zijn voor VNG en voor gemeenten.

Zo onderkennen we de noodzaak om potentiële slachtoffers te waarschuwen, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid. De VNG-Informatiebeveiligingsdienst IBD is het aangewezen sectorale Computer Emergency Response Team, of Computer Security Incident Response Team (*CERT*/CSIRT) voor gemeenten. De VNG/IBD waarschuwt gemeenten en gemeenschappelijke regelingen en ondersteunt hen op vraag bij incidenten. We stellen vast dat het advies van de Raad om veiligheidseisen te stellen bij inkoop van software ook voor gemeenten als gebruikers van software relevant is. Dat geldt ook voor de constateringen van de Raad over het delen van expertise en de naadloze samenwerking tussen publieke en private organisaties op het gebied van digitale veiligheid. We onderschrijven de aanwijzing voor een wettelijke basis voor de beheersing van digitale veiligheid. Gemeenten werken nu vijf jaar met een systematiek van enkelvoudige en eenduidige verantwoording over de informatieveiligheid, ENSIA, welke aansluit op de planning- en controlcyclus.

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

In deze brief lichten we inhoudelijk toe op welke wijze we de relevante aanbevelingen ter harte nemen.

Waarschuw potentiële slachtoffers van cyberaanvallen, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid.

De VNG/IBD voorziet gemeenten en partners van informatie en methoden voor informatiebeveiligings- en privacy-risicoanalyse[1]. Naast advies over preventieve beveiligingsmaatregelen en ondersteuning bij digitale verstoring, werken IBD en VNG met gemeenten en veiligheidsregio's aan verbetering van de voorbereiding op mogelijke maatschappelijke ontwrichting. In 2021 en in de eerste maanden van 2022 heeft een aantal (grote) incidenten plaatsgevonden, waar de IBD betrokken organisaties ondersteunde: de gemeente Hof Van Twente, Senzer, IJmond Werkt, VoornePutten Werkt en begin april de gemeente Buren. Ook tijdens het Log4J-incident adviseerde en ondersteunde de IBD gemeenten. De IBD werkt de incidenten uit in lessen en aanbevelingen voor gemeenten[2]. De aanbevelingen zijn van toepassing op zowel overheid als niet-overheidsorganisaties[3].

De geleerde lessen over het belang van een transparante en open uitwisseling van dreigingsinformatie werpen dit moment hun vruchten af. Dit zagen wij terug in de respons op het Log4j-incident[4], van zowel NCSC, de overheidsorganisaties, als ook het bedrijfsleven. De VNG/IBD heeft geen formele rol in de relatie tussen leveranciers en gemeenten. Op basis van de goede relatie kon de IBD wel informatie ophalen en namens gemeenten sturen op een oplossing bij leveranciers. Gemeenten en leveranciers hebben baat bij een gezamenlijke aanpak en een eenduidig beeld bij een oplossing. De collectieve aanpak van VNG richting ICT-leveranciers van gemeenten is breder dan alleen het thema informatiebeveiliging en privacybescherming.

De VNG/IBD publiceerde op 19 oktober 2022 het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2023 -2024[5]. De IBD ziet naast een toename in ransomware aanvallen ook steeds meer en ernstiger kwetsbaarheden in software. De gemeenten zetten stappen, echter de dreiging neemt harder toe. Het beeld biedt handelingsperspectief voor de gemeentesecretaris om deze situatie te kunnen keren. Het programma Nieuwsuur heeft aandacht besteed aan het onderwerp[6]. Het Dreigingsbeeld bevat concrete succesfactoren waar gemeenten mee aan de slag kunnen om de 'basis op orde te krijgen'. De VNG heeft deze publicatie afgelopen oktober overhandigd aan de VGS. De VNG geeft bestuurlijke duiding aan het Dreigingsbeeld IBD met 'Digitale veiligheid en de gemeentelijke bestuurder - Bestuurlijke prioriteiten bij het IBD-dreigingsbeeld 2023-2024'[7]. Hierin worden vijf bestuurlijke prioriteiten op bij het Dreigingsbeeld IBD uitgewerkt in concrete aanbevelingen. Het realiseren van de maatregelen en aanbevelingen uit het dreigingsbeeld vraagt om stevige bestuurlijke aandacht en support. We raden de gemeentebestuurders onder meer aan om digitale veiligheid op te nemen in het Integraal Veiligheidsplan (IVP) en de regie op leveranciers te versterken.

[1] https://www.informatiebeveiligingsdienst.nl/irpa-tool/

[2] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/06/20200310-Lessen-Citrix-Crisis-TLP_WIT.pdf
[3] https://www.informatiebeveiligingsdienst.nl/?s=lessen

[4] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2022/02/20220207-Lessen-Log4J-TLP_WIT.pdf
[5] https://www.informatiebeveiligingsdienst.nl/nieuws/ibd-dreigingsbeeld-groeiende-dreiging-ransomware-aanvallen/
[6] https://nos.nl/nieuwsuur/artikel/2449019-aantal-cyberaanvallen-op-gemeenten-verdubbeld
[7] https://vng.nl/sites/default/files/2022-11/VNG_Digitale_Veiligheid_bestuurlijke%20prioriteiten.pdf

Interbestuurlijk uniforme veiligheidseisen als onderdeel van inkoopvoorwaarden

In de door de VNG vastgestelde uniforme gemeentelijke inkoopvoorwaarden voor ICT, de GIBIT[8], zijn de inkoopeisen cybersecurity overheid al opgenomen. De handreikingen en adviezen van de Informatiebeveiligingsdienst van de VNG bouwen voort op de richtlijnen voor veilig inkopen van hard- en software, opgesteld door de ministeries van BZK en EZK. Het is evenwel van belang dat niet alleen bij aankoop aandacht is voor digitale veiligheid. Goed opdrachtgeverschap is van groot belang. Liefst treden hierin de diverse overheidslagen gezamenlijk op.

De VNG dringt er bij het rijk op aan, dat de richtlijnen voor alle overheden - en vanuit alle departementen - eenduidig zijn en blijven. Transparantie en democratische verantwoording over geopolitieke afwegingen ten aanzien van de inzet van technologie gelden ook voor lokaal bestuur[9]. Er is te allen tijde behoefte aan een duidelijk afwegingskader opdat gemeenten gemotiveerd invulling kunnen geven aan richtlijnen vanuit het rijk[10]. We merken daarbij op dat inkoopeisen gepaard dienen te gaan met goed (collectief) opdrachtgeverschap en sterk leveranciersmanagement bij gebruik van de software.

Gelijke informatiepositie verstevigt verantwoording, transparantie en incidentbestrijding

De VNG deelt de opvatting van de Raad dat kwetsbaarheden, incidenten en cyberaanvallen van de afgelopen jaren hebben laten zien dat een gezamenlijke aanpak, met alle betrokken partijen, urgent en noodzakelijk is. Zoals het rapport stelt: 'De kloof tussen digitale afhankelijkheid en dreiging enerzijds en de weerbaarheid van de samenleving anderzijds groeit. Snel en fundamenteel ingrijpen is nodig om te voorkomen dat de maatschappij ontwricht raakt'. Om die kloof te dichten vindt de VNG het van belang om het onderscheid tussen vitale en niet-vitale organisaties te laten vervallen, in ieder geval waar het gaat om de geopolitieke duiding vanuit de inlichtingendiensten en het delen van dreigingsinformatie. Deze indeling dient te worden vervangen door een helder afwegingskader waaraan iedere organisatie de adviezen kan toetsen aan de eigen situatie.

De VNG ziet, dat vanuit het rijk en inlichtingendiensten nog wel een betere informatiedeling kan plaatsvinden. Daarmee zou de transparantie en democratische verantwoording over (geopolitieke) afwegingen ten aanzien van de inzet van technologie, voor alle bestuurslagen kunnen verbeteren. Wij dringen daarom aan op een gelijke informatiepositie voor alle overheden, hun leveranciers en het bedrijfsleven ten aanzien van het delen van dreigingsinformatie, niet alleen tijdens landelijke incidenten.

Integrale digitale en fysieke veiligheidsaanpak: geen onderscheid tussen vitaal en niet-vitaal

Een gelijke informatiepositie is met name van belang om als lokaal bestuur grip te krijgen op maatschappelijk relevante processen, ook als deze niet-vitaal zijn. Ook digitale verstoringen bij organisaties die nu niet als ‘vitaal’ gedefinieerde zijn, kunnen immers tot maatschappelijke ontwrichting leiden. Tegelijkertijd bevinden alle vitale elementen zich ook op gemeentelijk grondgebied. Bij digitale verstoring daarvan zijn de fysieke gevolgeffecten voor de gemeenten en de Veiligheidsregio’s. Op basis van een helder afwegingskader kunnen deze maatschappelijk relevante organisaties, processen en elementen in de regionale veiligheidsplannen opgenomen worden.

[8] https://vng.nl/projecten/gibit
[9] https://vng.nl/nieuws/gemeenten-maken-zich-hard-voor-verantwoord-gebruik-cameras
[10] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022Z04018&did=2022D08224

Het is van belang dat de burgemeester als bevoegd gezag in positie is om de verantwoordelijkheid voor de (digitale) openbare orde en veiligheid te blijven waarborgen. De VNG werkt met gemeenten en de veiligheidsregio's aan verbetering van de preparatie op mogelijke maatschappelijke ontwrichting. Een digitaal veiligheidsstelsel, in samenhang met het fysieke veiligheidsstelsel is noodzakelijk om de continuïteit van de samenleving bij digitale verstoringen zowel lokaal, regionaal als ook nationaal te kunnen borgen.

Op 10 oktober stuurde de minister van Justitie en Veiligheid de Nederlandse Cybersecurity Strategie (NLCS) met actieplannen naar de Tweede Kamer[11]. NLCS actieplannen bevatten al lopende plannen, zoals: het Landelijk Dekkend Stelsel (LDS), het Landelijk Crisisplan Digitaal (LCP-Digitaal) en de uitwerking van Europese cybersecurity regelgeving (NIB-2) in een herziening van de Wet beveiliging netwerken en infrastructuur.

Wat ons betreft zijn complimenten voor de minister voor de NLCS op zijn plaats. Het betreft een ambitieuze en omvattende strategie waarvan wij verwachten dat deze Nederland concreet digitaal veiliger gaat maken. De VNG heeft in het verleden meermaals aangedrongen op een duidelijke regierol van het rijk ten aanzien van dit dossier en ook hierin worden belangrijke stappen vooruit gezet. De NLCS wordt integraal onderdeel van de werkagenda van staatssecretaris voor Digitalisering. Hiermee wordt mede uitvoering gegeven aan de aanbevelingen die het rapport van de Raad stelt, bijvoorbeeld ten aanzien van de inkoopvoorwaarden voor cybersecurity in hard- en software voor de overheid.

In de NLCS en in de actieplannen zien we echter, dat dit vooral een rijks strategie is en er te weinig rekening is gehouden met de gemeentelijke uitvoeringscapaciteit om bij te dragen aan de doelen ervan. Daardoor zien wij op lokaal niveau drie systeemuitdagingen die zullen moeten worden aangepakt als de ambitie is om werkelijk tot een digitaal veilig Nederland te komen:

1. Een digitaal veiligheidsstelsel is nodig in samenhang met het fysieke veiligheidsstelsel, met uitwerking van bevoegdheden en verantwoordelijkheden:
2. Een (doorlopend) situationeel beeld is nu niet op te maken over de digitale veiligheid van de gemeentelijke organisatie, over de digitale veiligheid van de leefomgeving of over cyberbeelden ten aanzien van digitale criminaliteit.
3. Er is structurele financiering op lokaal niveau noodzakelijk om uitvoering te geven aan deze plannen, met ingang van 2024 (Prinsjesdag 2023)

Tegelijkertijd manen wij de minister van Justitie en Veiligheid en de staatssecretaris voor Digitalisering om richting medeoverheden haast te maken met het bieden van duidelijkheid over nieuwe wet- en regelgeving, zoals de NIB-2. De vereisten rond zorgplicht, meldplicht en toezicht worden door verschillende vakministers uitgewerkt, zoals de ministers van Volksgezondheid, Welzijn en Sport en voor Infrastructuur en Waterstaat. Eenduidigheid hierin is van groot belang. In die uitwerkingen van de NIB-2 en het toezichtstelsel dat dit vraagt, zien we de noodzaak om verdergaand te standaardiseren. Een wettelijke grondslag onder de BIO zou standaardisering en daarmee de eenduidige verantwoording over informatiebeveiliging kunnen versterken.

Wij hebben recent een convenant opgesteld [12] met de minister van Justitie en Veiligheid en met de staatssecretaris voor Digitalisering. Met de samenwerking in het convenant kunnen we borgen dat lokaal bestuur mede sturing geeft aan de actieplannen NLCS en dat de fundamentele uitdagingen de komende jaren ook geadresseerd en aangepakt worden. Dit convenant is op 21 december 2022 ondertekend.

[11] https://www.rijksoverheid.nl/actueel/nieuws/2022/10/10/kabinet-presenteert-nieuwe-cybersecuritystrategie

[12] https://vng.nl/nieuws/convenant-ondertekend-over-lokale-cybersecuritystrategie

Eenduidige verantwoording over beheersing van digitale veiligheidsrisico's.

Gemeenten verantwoorden zich over informatiebeveiliging en kwaliteit middels ENSIA, dat staat voor Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen. ENSIA is een initiatief van de VNG en de ministeries van Binnenlandse Zaken, Sociale Zaken en Werkgelegenheid en van Infrastructuur en Waterstaat. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid. In de afgelopen vijf jaar zijn naar behoefte van gemeenten en toezichthouders, steeds meer stelsels aan ENSIA toegevoegd. Inmiddels structureert ENSIA naast de Baseline Informatieveiligheid Overheid (BIO) de verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), Waardering Onroerende Zaken (WOZ) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid. De verantwoording over informatieveiligheid sluit aan bij de gemeentelijke planning- en controlcyclus.

Op de VNG-ledenvergadering van juni 2022 namen de leden een motie aan voor meer structurele aandacht en financiering voor informatieveiligheid op lokaal niveau. Ondertekenaars van de motie vroegen de VNG ook zo spoedig mogelijk in gesprek te gaan met BZK over de processen rondom de BIO- en ENSIA-veiligheidsaudits. Die toetsen nu of het vereiste instrumentarium aanwezig is voor beveiliging, maar niet of het ook wordt gebruikt en in hoeverre dit structureel bijdraagt aan daadwerkelijke informatieveiligheid voor inwoners, ondernemers en (gemeentelijke) processen. We dringen bij de staatssecretaris van Digitalisering aan op een uitvoerbaar toezicht stelsel op grond van de BIO om daarmee aan de NIB-2 regelgeving te kunnen voldoen. Tegelijkertijd ontwikkelen we met de gemeenten werkwijzen om hun inzicht in feitelijke informatieveiligheid op lokaal niveau te vergroten.

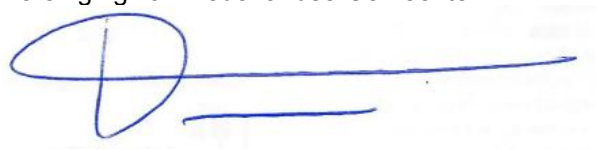
Tot slot

Wij danken de Raad hartelijk voor dit onderzoeksrapport. De aanbevelingen voor het versterken van de digitale veiligheid nemen we graag ter harte en zoals aangegeven pakken we de geleerde lessen gelijk op richting onze leden. De inspanningen die nodig zijn om de fundamentele uitdagingen op lokaal niveau aan te pakken zullen we bij de betreffende bewindspersonen onder de aandacht blijven brengen. Daarbij zullen we de aanbevelingen uit uw rapport in het oog houden.

We nodigen de Raad uit om met ons in gesprek te gaan over de wijze waarop de aanbevelingen door gemeenten opgepakt worden.

Mocht u naar aanleiding van deze reactie vragen hebben, dan kunt u daarvoor contact opnemen met [redacted]

Met vriendelijke groet,
Vereniging van Nederlandse Gemeenten



mr L.K. Geluk
Algemeen Directeur