Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 786

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 oktober 2021

Op 20 april 2021 (Handelingen II 2020/21, nr. 70, item 24) heeft uw Kamer de motie van het lid Yesilgöz-Zegerius aangenomen[1]. Deze motie is ingediend naar aanleiding van het Algemeen Overleg Cybersecurity van 9 december 2020 van de Vaste Kamercommissie Justitie en Veiligheid (Kamerstuk 28 684, nr. 645).

Met deze brief geef ik uitvoering aan de motie. De motie stelt dat het aantal organisaties en instellingen dat slachtoffer is geworden van cyberaanvallen sterk is toegenomen en verwijst daarbij in het bijzonder naar de hack op de gemeente Hof van Twente van december vorig jaar. De motie roept op om in samenwerking met de Vereniging Nederlandse Gemeenten (VNG) en de Informatiebeveiligingsdienst (IBD) een cyberverdedigingsprotocol op te stellen, zodat gemeenten een duidelijk handelingskader hebben in het geval van ransomware, DDos-aanvallen en andere ontwrichtende cyberaanvallen.

Ik wil vooropstellen dat enkel een cyberverdedigingsprotocol niet effectief zal zijn, omdat er meerdere factoren bepalend zijn in dit verband. In de eerste plaats is het belangrijk dat een aanval wordt voorkomen en dat overheden effectief reageren als het hen alsnog overkomt. Daarbij is het van groot belang dat er actief wordt ingezet op detectie van cyberdreigingen. In mijn voortgangsbrief informatieveiligheid bij de overheid heb ik uw Kamer op 18 maart 2021 geïnformeerd over de inzet die is gepleegd om informatieveiligheid bij de gehele publieke sector te verhogen.[2] In deze brief zal ik het beleid en de diverse maatregelen die worden getroffen voor de gemeentelijke sector nader duiden.

[1] Kamerstuk 26 643, nr. 753
[2] Kamerstuk 26 643, nr. 749

kst-26643-786
ISSN 0921 - 7371
's-Gravenhage 2021

Inzet VNG en taak gemeenten

De VNG heeft op 12 februari van dit jaar de *Agenda Digitale Veiligheid gemeenten 2020–2024*[3] vastgesteld tijdens de Buitengewone Algemene Ledenvergadering. De agenda richt zich op de gemeentelijke bedrijfsvoering, de gemeentelijke rol in de aanpak van digitale criminaliteit en haar rol bij (ontwrichtende) digitale crises en incidenten. Weerbaarheid van de gemeenten is de kern van de agenda; hierbij is nadrukkelijk aandacht voor cybergevolgbestrijding. Daarbij draait het onder andere om opschaling en samenwerking met de veiligheidsregio's, het in kaart brengen van ketenafhankelijkheden en oefenen met cyberincidenten.

Overheidsorganisaties, zo ook gemeenten, zijn zelf verantwoordelijk voor de wijze waarop het informatieveiligheidsbeleid in hun organisatie gestalte krijgt. Het blijven uiteindelijk afwegingen van het lokaal bestuur die worden getroffen in het kader van risico-gebaseerd werken. Onder risico-gebaseerd werken wordt verstaan dat een overheidsorganisatie haar informatieveiligheid zodanig organiseert dat steeds de afweging wordt gemaakt tussen enerzijds kans, dreiging, gevolgschade en anderzijds de kosten van de maatregelen om deze schade te beperken.

Mijn taak als Staatssecretaris is kaderstellend, voorts ondersteunend, en waar nodig aanjagend naar alle overheidslagen. De gemeenten in het bijzonder worden op tal van manieren ondersteund door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). In de navolgende paragrafen licht ik dat toe.

Kader implementeren/monitoren en detectie van dreigingen

De Baseline Informatiebeveiliging Overheid

Onder leiding van het Ministerie van BZK is de Baseline Informatiebeveiliging Overheid (BIO) opgesteld. De BIO is het normenkader voor informatiebeveiliging binnen de gehele overheid en is sinds 1 januari 2019 van kracht. De BIO dient als basis en bevat de maatregelen die overheden dienen te treffen. Gemeenten hanteren binnen de eigen bedrijfsvoering de BIO als verplichtende standaard voor basismaatregelen en vullen die basis waar nodig risico-gestuurd aan. De BIO bevat een overzicht van alle relevante beveiligingsgebieden waar maatregelen voor moeten worden getroffen.

Eenduidige Normatiek Single Information Audit

Via de methodiek met de naam Eenduidige Normatiek Single Information Audit (ENSIA) wordt de verantwoordingssystematiek op het gebied van informatiebeveiliging en informatiekwaliteit gemonitord. Dit zorgt voor een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor gemeenten. De focus ligt hierbij op verantwoording richting de gemeenteraad over de staat van informatiebeveiliging op basis van de BIO. Parallel hieraan wordt ENSIA gebruikt om verantwoording af te leggen aan de rijksoverheid over het gebruik van landelijke voorzieningen, zoals onder meer DigiD en de Basisregistratie Personen (BRP).

[3] Zie voor de aangenomen Resolutie Digitale Veiligheid: https://www.informatiebeveiligingsdienst.nl/nieuws/resolutie-digitale-veiligheid-aangenomen/

Detectie van cyberdreigingen

De Informatiebeveiligingsdienst (VNG/IBD) is voor de gemeenten het sectorale Computer Emergency Response Team (CERT).[4] De IBD ondersteunt gemeenten bij hun informatiebeveiliging, zowel met waarschuwingen over dreigingen en kwetsbaarheden, als ook door een ondersteunende rol in de eerste response bij incidenten.[5] In het geval van een actieve dreiging, fungeert de IBD in nauwe samenwerking met het Nationaal Cybersecurity Centrum (NCSC) als schakelpunt tussen gemeenten en andere sectoren. Hiervoor heeft de IBD een breed netwerk van vertrouwde contactpersonen bij iedere gemeente.
Cyberweerbaarheid wordt verhoogd door vroege detectie van cyberdreigingen. Gemeenten kunnen hiervoor gebruik maken van producten en diensten uit de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) van de VNG, als onderdeel van de Agenda Digitale Veiligheid.
Hieronder vallen onder meer actieve monitoring en responsediensten voor het bewaken van gedrag en acties op het eigen bedrijfsnetwerk – bijvoorbeeld een Security Operations Centre (SOC) – diverse beveiligingsproducten voor de ICT-infrastructuur en beveilingsexpertise-diensten.

Oefenen en kennisdelen

Overheidsbrede cyberoefening

Oefenen om beter voorbereid te zijn als het een keer onverhoopt dreigt mis te gaan. Dat is het doel van de Overheidsbrede Cyberoefening die door het Ministerie van BZK dit jaar voor de derde keer wordt georganiseerd.[6] Deze oefening, die is bedoeld voor Rijks- en uitvoeringsorganisaties, provincies, gemeenten en waterschappen, laat zich ieder jaar inspireren door recente en actuele dreigingen en cyberaanvallen (zoals op de gemeenten Lochem en Hof van Twente). Aan de hand van een gesimuleerde hackaanval oefenen alle partners in de publieke sector met elkaar, op verschillende niveaus van de organisaties, op crisispreparatie.

Stimuleren oefenen door gemeenten

Om het belang van oefenen met cybersecurity te stimuleren bij gemeenten, heeft het Ministerie van BZK een drietal cyberoefenpakketten gesubsidieerd die ontwikkeld zijn door het Instituut voor Veiligheids-, en Crisismanagement.[7]
De IBD stimuleert het gebruik van deze cyberoefenpakketten door gemeenten aan te sporen gratis gebruik te maken van dit aanbod.

Kennisdelen

Naast oefenen wordt er ook ingezet op kennisdeling binnen de overheid. Zo is de podcastserie *«Lets talk about Hacks»* ontwikkeld waarin slachtoffers, ethisch hackers, wetenschappers en beleidsmakers vertellen over de risico's van cyberaanvallen en vertellen wat je kunt doen om dit te voorkomen. Eveneens worden er in de maand oktober diverse webinars

[4] https://www.informatiebeveiligingsdienst.nl/ibd-cert/
[5] In 2019 heeft het Ministerie van BZK onder de noemer Gemeenschappelijk Overheid Security Operations Center (GOV-SOC) de opbrengsten van hun verkenning overgedragen aan de bestuurslagen die de uitkomsten benutten om de incident response capaciteit van hun eigen bestuurslaag te versterken.
[6] Informatie over de Overheidsbrede Cyberoefening is te vinden op https://www.weerbaredigitaleoverheid.nl/
[7] De gemeentelijke cyberoefenpakketten zijn te vinden op de website van de IBD: https://www.informatiebeveiligingsdienst.nl/project/cyberoefenpakket-vngoefenscenarios-digitale-incidenten/

georganiseerd waarin organisaties als de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de VNG en IBD, de provincie Drenthe en het Platform Crisisbeheersing Waterschappen Midden-Nederland vertellen over uiteenlopende onderwerpen rondom cyberdreigingen. Speciaal voor bestuurders worden er in november een viertal bestuurlijke «cybertafels» georganiseerd, waar bestuurders en topambtenaren met elkaar in gesprek gaan over de gemeente als partner in informatieveiligheid, cyberdilemma's voor bestuurders, cyberweerbaarheid in de watersector en de lessons learned van de GGD-hack. Alle webinars, podcasts, cyberoefening en de belangrijkste opbrengsten van de cybertafels worden samen met verschillende interviews met bestuurders gepubliceerd in een online magazine.

Masterclass ransomware

Omdat ransomware op steeds grotere schaal plaatsvindt, wordt er door het Ministerie van BZK gewerkt aan een speciale Masterclass Ransomware die in december van dit jaar plaatsvindt. Tijdens deze masterclass wordt er met onder andere slachtoffers, cyberexperts, ethisch hackers, het NCSC, Openbaar Ministerie en Politie gesproken over het fenomeen ransomware en wat organisaties kunnen doen om de schade van ransomware zo beperkt mogelijk te houden.

Crisisopschaling en nazorg

Crisisopschaling

In het geval van een cyberincident zijn gemeenten zelf verantwoordelijk voor de veiligheid en continuïteit van de gemeentelijke processen. Wanneer ook andere organisaties betrokken zijn, of het risico op digitale ontwrichting van één of meer regio's ontstaat, is opschaling en samenwerking nodig. Volgens de Gecoördineerde Regionale Incidentbestrijdingsprocedure (GRIP) worden de Veiligheidsregio's betrokken en indien noodzakelijk kan ook snel en flexibel opgeschaald worden naar de nationale crisisstructuur. Om de voorbereiding op en samenwerking tijdens cyber gerelateerde crises verder te versterken wordt onder verantwoordelijkheid van de Minister van Justitie en Veiligheid het bestaande Nationaal Crisisplan Digitaal doorontwikkeld naar een Landelijk Crisisplan Digitaal.[8] Deze doorontwikkeling wordt in nauwe samenwerking met veiligheidsregio's en met betrokkenheid van onder andere aanbieders van vitale processen c.q. essentiële diensten nader vormgegeven.

Nazorgfase IBD

Na afwikkeling worden incidenten ook gebruikt om te leren. De IBD evalueert met de betrokken gemeente het incident om te leren en waar nodig de dienstverlening van de IBD aan te passen. Op basis van deze evaluatie wordt een lessons learned document opgesteld voor brede verspreiding en ondersteund door kennisbijeenkomsten.

Tot slot

Bovenstaande uiteenzetting geeft aan dat er in mijn beleid reeds aandacht wordt besteed aan zowel de preventie van digitale ontwrichting als het bieden van handelingsperspectieven in het geval van een crisis. Daarbij zet ik in mijn beleid niet in op een cyberverdedigingsprotocol voor alle

[8] Kamerstuk 30 821, nr. 129

gemeenten, omdat de ene situatie niet de andere is. Hoe er daadwerkelijk moet worden gehandeld is contextafhankelijk. Het risico-gebaseerd werken en de daaruit volgende getroffen maatregelen verschillen per gemeente. Om die reden richt het beleid zich, in samenwerking met de VNG en IBD, op de implementatie van de BIO, de verantwoording daarover aan het lokaal bestuur, het stimuleren van het gebruik van de GGI, het oefenen met gesimuleerde hackaanvallen, het delen van kennis en zorgt de IBD na elk incident voor de nazorgfase zodat de overheid daarvan kan leren. Kern daarbij is dat we als overheid zoveel als mogelijk proberen aanvallen te voorkomen, maar wel effectief kunnen reageren als we worden geraakt.

De afhankelijkheid van digitale processen is groot en is door de COVID-19-pandemie nog verder toegenomen. Incidenten zoals de problematiek rondom de software van het bedrijf Citrix in januari 2020 en de ransomware bij de gemeenten Hof van Twente, Lochem en de universiteit van Maastricht laten zien dat de afhankelijkheid van digitale dienstverleningsprocessen en systemen ons ook kwetsbaar maakt. Technologie en de bijbehorende bedreigingen lijken zich sneller te ontwikkelen dan dat organisaties adequate beheersmaatregelen kunnen inrichten. Hierbij is het besef gekomen dat men meer en meer moet accepteren dat cyberincidenten niet altijd te voorkomen zijn, maar dat men beter in staat moet zijn deze incidenten te detecteren en beter moet kunnen ingrijpen om de gevolgen te beperken.
Daarom heb ik meer inzet gepleegd op het oefenen met cybersecurity-incidenten bij overheden en op crisisbeheersing in samenwerking met mijn collega, de Minister van Justitie en veiligheid, vanuit zijn coördinerende verantwoordelijkheid voor beleid rond cybersecurity en crisisbeheersing.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops