Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Ministerie van Justitie en Veiligheid
T.a.v. Dhr. prof. mr. F.B.J. Grapperhaus
Postbus 20301
2500 EH Den Haag

Datum
11 september 2020

Onderwerp
CSR Adviesbrief inzake reactie WRR-rapport en Citrix-evaluatie

Excellentie,

De Cyber Security Raad (hierna de raad) reageert middels dit advies op uw *Kamerbrief evaluatie Citrix-problematiek en kabinetsreactie WRR-Rapport: "Voorbereiden op digitale ontwrichting"* dd. 20 maart 2020. In deze brief staat u stil bij de constateringen in het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en wat deze betekenen in uitbreiding, wijziging of aanvulling op het beleid van dit kabinet. Daarbij betrekt u ook de geleerde lessen uit de Citrix-problematiek en zet u uiteen hoe dit kabinet zich voorbereidt op digitale incidenten en welke maatregelen worden genomen voor het verhogen van onze digitale weerbaarheid.

De raad heeft kennisgenomen van de door u voorgestelde maatregelen voor respons bij digitale incidenten en crises met digitale elementen, het voorkomen van dergelijke incidenten en het verhogen van de cyberweerbaarheid. De raad is van mening dat de door u gekozen aanpak een belangrijke stap in de goede richting is. Op een aantal terreinen vraagt uw aanpak volgens de raad om aanscherping en/of uitbreiding van de te nemen maatregelen. Mede dankzij de coronacrisis zijn we versneld in een nieuwe fase van onze digitale samenleving gekomen. Naast dat het virus onze fysieke samenleving voor langere tijd heeft lamgelegd, zorgt het virus er nu voor dat we met elkaar nog intensiever gebruikmaken van onze digitale infrastructuur en alle middelen die hierbij komen kijken. Een groot deel van de Nederlandse bevolking werkt nu op afstand, studeert op afstand en onderhoudt sociale contacten op afstand. Ook het dataverkeer is in de afgelopen periode sterk toegenomen. Onze afhankelijkheid van (aanbieders van) digitale middelen is doordoor structureel aanzienlijk toegenomen en daarmee ook het digitale aanvalsoppervlak dat door kwaadwillenden kan worden misbruikt. Bovendien schetst het onlangs uitgebrachte Cybersecuritybeeld Nederland 2020 een onverminderd zorgwekkend beeld. De cyberweerbaarheid van onze samenleving is daarmee belangrijker dan ooit. We moeten slagvaardig kunnen blijven reageren op misstanden en/of cyberaanvallen en kunnen vertrouwen op de veiligheid en continuïteit van onze digitale infrastructuur, juist nu en in de toekomst. Daartoe moeten doeltreffende maatregelen worden genomen.

Er moet zo snel mogelijk sprake zijn van een volwassen stelsel van informatie-uitwisseling en er moet een cyclus ontstaan van oefening, evaluatie en implementatie van verbeterpunten. Tevens moet er onverminderd ingezet worden op het opsporings- en vervolgingsbelang. Om dit te bereiken acht de raad het noodzakelijk dat er meer regie komt op samenwerking[1].

[1] CSR Urgentieverklaring, Cyber Security Raad, 31 maart 2020

Dekkende informatie-uitwisseling

Dat voorkomen beter is dan genezen blijkt ook in het digitale domein op te gaan. Dit ziet de raad terug in de praktijk; er gaat veel aandacht uit naar het voorkomen van incidenten. Dit valt of staat met accurate, tijdige en begrijpelijke informatieverstrekking; informatie over cybersecurity moet voor alle organisaties in Nederland op eenvoudige wijze toegankelijk zijn en reële handelingsperspectieven bieden. Ondanks eerdere adviezen[2] hierover van de raad en onder meer de WRR[3] en verschillende lopende initiatieven constateert de raad dat er wel aandacht is voor het breed beschikbaar stellen van dreigingsinformatie via het Landelijk Dekkend Stelsel Informatieknooppunten (LDS), maar dat het tempo waarin het stelsel wordt uitgerold, niet in de pas loopt met de toenemende behoefte aan de benodigde informatie waarop organisaties maatregelen kunnen baseren om hun cyberweerbaarheid te vergroten. Dekkende informatievoorziening blijkt een hardnekkig knelpunt te zijn. In belangrijke mate is dit te wijten aan het feit dat het LDS nog steeds in opbouw is, zoals u ook in uw Kamerbrief inzake de evaluatie Citrix-problematiek en kabinetsreactie WRR-Rapport en uw 'Beleidsreactie CSBN 2020 en voortgangsrapportage NCSA' aangeeft. Daarnaast wordt de huidige informatie-uitwisseling gekenmerkt door een zekere mate van vrijheid, omdat het verstrekken van relevante informatie niet altijd verplicht is. Ook is het verstrekken van informatie binnen de vigerende wet- en regelgeving soms niet mogelijk.

De raad acht het noodzakelijk en urgent om de uitrol van het LDS te versnellen en de informatie-uitwisseling tussen slachtoffers, het National Cyber Security Centrum (NCSC), Digital Trust Center (DTC) en de opsporingsinstanties te verbeteren. Vrijblijvendheid en eventuele (juridische) obstakels dienen hierbij weggenomen te worden. We kunnen het ons niet veroorloven dat de informatievoorziening in ons land hapert en onze cyberweerbaarheid in het geding komt. De digitale stroomversnelling waarin we terecht zijn gekomen, maakt de urgentie nog hoger.

Regie op samenwerking

Met de versnelde uitrol van het LDS en verbetering van de informatie-uitwisseling zijn we er nog niet. Zoals de WRR ook concludeert, kunnen we niet alle incidenten voorkomen en pleit de WRR voor een betere voorbereiding op digitale ontwrichting door onder andere adequate bevoegdheden om escalatie te voorkomen. Ook het in het CSBN 2020 geschetste dreigingsbeeld benadrukt het belang van een goede voorbereiding op mogelijke ontwrichting. Daarom is het belangrijk dat organisaties voldoende veerkrachtig zijn; men moet snel kunnen herstellen van een crisis of van de schadelijke gevolgen door cybercriminaliteit. Om cybercriminaliteit effectief te kunnen bestrijden, is het van belang dat de opsporing actief wordt betrokken bij een dergelijk incident. Zoals in het Nationaal Crisisplan-Digitaal reeds wordt geconstateerd, bestaat in de praktijk het risico dat hier een dilemma ontstaat tussen het organisatiebelang - streven naar bedrijfscontinuïteit - en het belang van de opsporing - data veiligstellen, daders opsporen en vervolgen (op basis van aangifte). De raad wijst ook op de vierde aanbeveling van de WRR, en hecht waarde aan een evaluatie van de wettelijke gronden waarbij alle overheidsinstanties aan cybersecurity- en opsporingskant in een duidelijk samenspel worden geplaatst.

Dat dit momenteel nog geen vanzelfsprekendheid is, valt volgens de raad mede te wijten aan versnippering als gevolg van gedeelde verantwoordelijkheden en beperkt mandaat. Gedurende de uitbraak van COVID-19 is dit voor het NCSC deels opgevangen door de kortgeleden doorgevoerde spoedwetgeving[4] die het NCSC mandateert om bij digitale dreigingen en incidenten bijstand te verlenen aan bijvoorbeeld ziekenhuizen,

[2] CSR Advies 2017, nr. 2 'Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime'
[3] Wetenschappelijke Raad voor het Regeringsbeleid (2019) Voorbereiden op digitale ontwrichting, WRR-Rapport 101, Den Haag, pag. 55-60
[4] Kamerstuk 26643, nr. 695: Beleidsreactie CSBN 2020 en voortgangsrapportage NCSA, 29 juni 2020, pagina 2-3

farmaceuten en onderzoekscentra. De raad is van mening dat ook meer in het algemeen (overheids)partijen tijdens incidenten in voldoende mate bijeen moeten worden gebracht, zodat in gezamenlijkheid de nodige acties en maatregelen kunnen worden genomen.

De raad acht het noodzakelijk dat regie op samenwerking voortvarend wordt aangepakt en adviseert u met klem om de overheidspartijen aan cybersecurity- en opsporingskant te voorzien van het benodigde mandaat en voldoende slagkracht om in samenhang op te treden bij incidenten. Zo vindt stroomlijning van de advisering aan en ondersteuning van getroffen organisaties plaats, met evenwichtige aandacht voor het opsporingsbelang en beperking van maatschappelijke schade.

Oog voor overige verbeteringen

In aanvulling op juiste en tijdige informatievoorziening vooraf en tijdens incidenten en een evenwichtige balans tussen het organisatiebelang en het overheidsbelang, waaronder het opsporingsbelang, wijst de raad op de waardevolle lessen die getrokken kunnen worden uit (grotere) incidenten. Daarom gaat de raad in dit advies ook in op de versterking van de processen en mechanismen die in werking treden *nadat* een (groot) digitaal incident heeft plaatsgevonden. In aanvulling op de voorgestelde maatregelen uit uw brief pleit de raad ervoor incidenten met grote impact binnen vitale processen *standaard* goed te evalueren, en leer- en verbeterpunten daadwerkelijk te implementeren. De raad is in dit kader verheugd met de snel tot stand gekomen evaluatie op hoofdlijnen van de Citrix-problematiek en het recente bericht dat de Onderzoeksraad voor Veiligheid de impact van dit incident diepgaander zal evalueren. De raad dringt erop aan erop toe te zien dat de lessen die uit deze evaluaties (zullen) blijken daadwerkelijk worden geïmplementeerd. Echter, de raad constateert ook dat diepgaande evaluaties van incidenten op dit moment nog niet vanzelfsprekend zijn en dit geldt ook voor het implementeren van verbeterpunten. Er is op dit moment geen uniforme wijze beschikbaar voor het evalueren van incidenten op verschillende niveaus en de uitkomsten ervan worden niet altijd onder alle betrokken partijen gedeeld. Daarnaast blijft het doen van aangifte regelmatig uit en dit komt niet ten goede aan een effectieve aanpak voor het bestrijden van cybercriminaliteit. Verbetering op dit punt draagt eveneens bij aan de cyberweerbaarheid van organisaties.

Met de WRR is de raad van mening dat het doen van oefeningen cruciaal is om de digitale paraatheid te verhogen. Dit geldt voor álle organisaties, maar in het bijzonder voor de vitale infrastructuur, waar uitval van digitale systemen snel kan leiden tot maatschappelijke ontwrichting. Overheid en vitale sectoren moeten elkaar snel weten te vinden en de rollen en acties moeten duidelijk zijn. Dit vraagt om een hoge mate van geoefendheid. Het Citrix-incident heeft laten zien dat dit nog niet goed gaat.
Hoewel u in uw reactie op het CSBN 2020 aangeeft dat cyberoefeningen meer en meer de norm worden, acht de raad een structureel oefenprogramma waarbij overheid en vitale sectoren met regelmaat met elkaar oefenen op digitale uitval noodzakelijk. Dit kan en mag niet beperkt blijven tot een enkele oefening zoals Isidoor III. Binnen dit oefenprogramma is het essentieel dat belangrijke verbeterpunten uit verrichte evaluaties worden meegenomen.

Adviezen

De raad adviseert het volgende:

1. Draag zorg voor een versnelling van de uitrol van het Landelijk Dekkend Stelsel van informatieknooppunten en een verbetering van de informatievoorziening zodat eind 2021 alle organisaties in Nederland kunnen beschikken over de informatie die nodig is om cyberweerbaar te zijn. Eventuele (juridische) obstakels moeten uit de weg worden geruimd.
2. Draag binnen een jaar zorg voor voldoende mandaat, slagkracht en regie op samenwerking voor de overheidsinstanties aan cybersecurity- en opsporingskant, opdat zij tijdens grotere incidenten in samenhang kunnen adviseren en optreden met evenwichtige aandacht voor de continuïteit van de organisaties, het opsporingsbelang en het beperken van maatschappelijke schade.
3. Ontwikkel en implementeer binnen twee jaar een cyclus van (jaarlijkse) publiek—private cyberoefeningen, evaluaties van grote incidenten en implementatie van verbeterpunten. Deze cyclus dient in het teken te staan van het lerend vermogen van organisaties en draagt bij aan het versterken van de cyberweerbaarheid van onze samenleving. Cruciale verbeterpunten uit gehouden diepgaande evaluaties en conclusies en aanbevelingen uit onderzoeksrapporten van bijvoorbeeld de Algemene Rekenkamer, adviesraden en/of toezichthouders dienen hierin te worden meegenomen.

Om het bovenstaande te bereiken is, naast regie op samenwerking, ook onderling vertrouwen van groot belang en een open houding van de betrokken partijen, die erop gericht is niet alleen de cyberweerbaarheid van de organisatie, maar binnen de gehele keten(s) te versterken en daarmee ook onze digitale samenleving en de maatschappelijke veiligheid.

Mede op deze wijze verbeteren we de omgang met (digitale) incidenten in Nederland en bouwen publieke en private partijen gezamenlijk aan de versterking van de cyberweerbaarheid en neemt de veerkracht van getroffen organisatie toe.

Zo werken we aan een open, veilig en welvarend digitaal Nederland.

Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR