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
22 februari 2021

Onderwerp
CSR Adviesbrief inzake het versneld delen van incidentinformatie

Excellentie,

De Cyber Security Raad (hierna de raad) reageert middels dit advies op uw Kamerbrief "Uitkomsten verkenning wettelijke bevoegdheden digitale weerbaarheid en beleidsreacties WODC-rapporten"[1] dd. 3 februari 2021 waarin u onder meer heeft aangekondigd te bezien of een wetswijziging ten gunste van de vorming van een volwassen Landelijk Dekkend Stelsel van informatieknooppunten (LDS) moet plaatsvinden. Het LDS is binnen de raad regelmatig onderwerp van gesprek geweest. Zo heeft de raad hierover in 2017 een advies[2] gepubliceerd. Sinds dat advies zijn er belangrijke stappen gezet in de (verdere) vorming en uitrol van het LDS, zoals de oprichting van het *Digital Trust Center (DTC)*. Momenteel is het LDS nog immer 'in oprichting', en heeft het nog niet de volwassenheid bereikt die de raad graag zou zien. Het verdient aanbeveling om inzichtelijk te maken hoe de verdere uitrol van het LDS vormt krijgt, zodat organisaties zich kunnen voorbereiden op hun rol binnen het stelsel. De raad is van mening dat er vooruitlopend op de door u voorgestelde wetswijziging op korte termijn acties moeten worden ondernomen om dit proces te versnellen ten gunste van een open, vrije en welvarende (digitale) samenleving.

Een van de belangrijkste instrumenten om de cyberweerbaarheid van organisaties en burgers te verhogen, is hen snel te informeren wanneer hun IT-systemen kwetsbaarheden vertonen of gehackt zijn. Ons *Nationaal Cyber Security Centrum (NCSC) is aangewezen als ons nationaal centraal contactpunt* als bedoeld in artikel 8, derde lid van de NIB-richtlijn en ontvangt in die hoedanigheid elke dag duizenden meldingen over Nederlandse IP-adressen waar zich gecompromitteerde systemen bevinden. De incidentmeldingen komen bij het NCSC binnen via geautomatiseerde datastromen van de nationale CERT's van andere landen en via internetbedrijven, non-profitorganisaties, beveiligingsonderzoekers en andere partijen, zowel uit het binnen- als buitenland.
De taak van het NCSC is primair Rijksoverheid en vitale aanbieders te informeren indien zich cybersecurity-kwetsbaarheden in hun systemen voordoen. In aanvulling daarop heeft het NCSC als taak de ontvangen incidentmeldingen door te geven aan 'schakelorganisaties', die vervolgens de incidentmeldingen aan de getroffen partijen in hun achterban kunnen doorgeven. Om een (sluitend) informatiesysteem te creëren is het LDS van cybersecurity-samenwerkingsverbanden ingericht.

[1] Deze inventarisatie heeft geen betrekking op de taken en bevoegdheden van overheidsdiensten in het kader van de strafrechtelijke opsporing van cybergerelateerde delicten.
[2] CSR Advies 2017, nr. 2 'Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime'

In de Nederlandse Cybersecurity Agenda (NCSA) uit 2018[3] is als doelstelling opgenomen het inrichten van het LDS om de slagkracht van publieke en private partijen te vergroten in het tegengaan van digitale dreigingen en incidenten. In de *Wet beveiliging netwerk- en informatiesystemen (Wbni)* en de voorganger *Wet gegevensverwerking en meldplicht cybersecurity (Wgmc)*,[4] zijn enkele bepalingen opgenomen over het delen van informatie door het NCSC buiten de primaire doelgroep. In de praktijk loopt het NCSC nu tegen een aantal situaties aan waarin het, volgens de tot nu toe daarover afgegeven juridische adviezen, toch **geen** incidentinformatie kan delen met de belangrijkste schakelorganisaties, terwijl deze partijen specifiek daartoe in de Wbni zijn aangewezen en vervolgens ook door de belanghebbende private marktpartijen zijn opgezet, ingericht en gecertificeerd. Gevolg van dit alles is dat het NCSC op dit moment geen incidentinformatie deelt met de belangrijkste schakelorganisaties, waardoor kritische incidentinformatie de getroffen bedrijven en burgers[5] **niet** bereikt. Tevens kan deze informatie van belang zijn voor politie en OM. Het delen van incident- dan wel restinformatie met politie en OM kan het veiligstellen van digitale sporen en de opsporing en strafrechtelijke vervolging in algemene zin ten goede komen.
Alle partijen rondom het LDS (inclusief het NCSC) zijn het inmiddels eens dat dit een onwerkbare situatie oplevert en het bereiken van het LDS onmogelijk maakt. Vele duizenden bedrijven en burgers worden nu niet geïnformeerd, terwijl de overheid wel informatie heeft dat zij slachtoffer of kwetsbaar zijn.
Hierna lichten we eerst kort de juridische problematiek toe. Daarna volgt het advies van de raad aan u hoe dit probleem te adresseren.

Juridische aspecten

Krachtens Art. 3 lid 1 uit de Wbni heeft het NCSC primair tot taak om de Rijksoverheid en vitale aanbieders in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen te informeren, adviseren en anderszins bijstand te verlenen. Het NCSC heeft daarnaast tot taak om dreigings- en incidentinformatie, die is verkregen in het kader van de genoemde primaire taak (door het NCSC ook wel 'restinformatie' genoemd), te verstrekken aan bepaalde 'schakelorganisaties' in het LDS, indien daarmee nadelige maatschappelijke gevolgen kunnen worden voorkomen.

Art. 3 lid 2 Wbni beschrijft met welke derden het NCSC deze restinformatie mag delen:

a. organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren (OKTT's);
b. Computer Security Incident Response Teams (CSIRT's);
c. andere computercrisisteams, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie;
d. aanbieders van internettoegangs- en internetcommunicatiediensten ten behoeve van het informeren van gebruikers van die diensten.

In de praktijk loopt het NCSC nu tegen de situatie aan waarin het, volgens de tot nu toe daarover binnen het ministerie van Justitie en Veiligheid afgegeven juridische adviezen, toch geen restinformatie - kan delen met de

[3] Nederlandse Cybersecurity Agenda: Nederland digitaal veilig, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), namens Rijksoverheid, 2018, pagina 19
[4] De Wgmc is op 1 mei 2018 in werking is getreden en is op 9 November 2018 vervangen door de Wbni. De bepalingen die in deze brief worden besproken zijn nagenoeg identiek. Hierna wordt uitsluitend gerefereerd aan de Wbni, maar wordt in feite beide wetten bedoeld.
[5] Burgers krijgen een melding van hun internetaanbieder als een van hun apparaten is geïnfecteerd. Internetaanbieders verzorgen deze melding op basis van informatie die met hen gedeeld wordt over IP-adressen in hun netwerk waarop geïnfecteerde apparaten zijn gesignaleerd. Voor veel internetaanbieders loopt het ontvangen van deze informatie via AbuseHub, de 'abuse information exchange' die is opgericht door aanbieders om hun gebruikers te kunnen informeren en beschermen.

in artikel 3 lid 2 genoemde OKTT's. Dit terwijl deze OKTT's een sleutelrol hebben te vervullen om het LDS te laten functioneren. Er zijn op dit moment vier OKTT's, te weten AbuseHUB, Nationale Beheersorganisatie Internetproviders (NBIP), Cyberweerbaarheidscentrum Brainport (CWB) en Brancheorganisatie Cyberveilig Nederland. Andere organisaties, zoals het DTC van het Ministerie van Economische Zaken en Klimaat, hopen binnenkort als OKTT erkend te worden.

Belangrijkste obstakel voor het NCSC om restinformatie te kunnen delen met de OKTT's, is dat Art. 20 lid 2 van de Wbni bepaalt dat het NCSC met een beperkt aantal derden *vertrouwelijke* gegevens mag delen die herleid kunnen worden tot een aanbieder, uitsluitend voor zover dat dienstig is aan het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. In andere gevallen zal eerst toestemming van de getroffen aanbieder moeten worden gevraagd. De hiervoor genoemde schakelorganisaties waarmee vertrouwelijke gegevens mogen worden gedeeld zonder toestemming van de getroffen aanbieder omvatten vervolgens niet de OKTT's.
Volgens de juridische adviezen, bevat de restinformatie die ziet op kwetsbare of gecompromitteerde systemen in nagenoeg alle gevallen tevens vertrouwelijke, herleidbare gegevens, zoals domeinnamen en IP-adressen waar zich gecompromitteerde systemen bevinden. Deze gegevens zijn *herleidbaar*, immers, de IP-adressen zijn met raadpleging van het RIPE-register eenvoudig te herleiden tot aanbieders tot wie deze IP-adressen behoren. Hetzelfde geldt voor de domeinnamen die via SIDN tot een aanbieder of eigenaar te herleiden zijn. De gegevens zijn ook *vertrouwelijk*, omdat de restinformatie, informatie bevat dat de systemen van deze aanbieders zijn gecompromitteerd. Indien deze informatie niet vertrouwelijk wordt behandeld, kan dit de aanbieder (potentieel slachtoffer) schade toedoen. Vanwege genoemd obstakel van art 20 lid 2 Wbni deelt het NCSC de restinformatie *niet* met de OKTT's. Dit is duidelijk een ongewenste situatie, en zondermeer in strijd met de bedoeling van de Wbni en in ieder geval in strijd met de bedoeling van het LDS.
Het doel van de Wbni/LDS is mogelijk te maken dat het NCSC incidentinformatie doorgeeft aan schakelorganisaties om hen zo in staat te stellen slachtoffers in hun achterban te informeren, dit ter bescherming van deze slachtoffers. Daarvoor is *herleidbare* informatie nodig (hoe anders het slachtoffer te identificeren en notificeren, zodat deze na het verkrijgen van deze informatie ook daadwerkelijk maatregelen kan treffen). Omdat deze incidentinformatie echter *vertrouwelijke informatie* betreft van het slachtoffer, mag deze volgens de gevolgde wetsuitleg niet worden genotificeerd, dit ter bescherming van de vertrouwelijke informatie.
Kortom, het informeren van het slachtoffer met als doel het slachtoffer te beschermen is niet mogelijk, omdat de betreffende informatie vertrouwelijk is. Dit wederom ter bescherming van hetzelfde slachtoffer. Vertaald naar de fysieke wereld: iemands slot op de voordeur is kapot, waardoor iedereen kan binnenlopen, maar we mogen de burger niet via de buurtwacht waarschuwen dat zijn slot kapot is, want dit is vertrouwelijke informatie van deze burger.
Het behoeft weinig toelichting dat dit niet de bedoeling van de Wbni kan zijn geweest en dat een redelijke uitleg van de bepalingen van de Wbni zou dienen te zijn dat deze informatiedeling wel mogelijk dient te zijn. De raad brengt in herinnering dat vóór de inwerkingtreding van deze bepalingen per 1 mei 2018, deze incidentgegevens wel werden gedeeld door het NCSC met getroffen organisaties. De Wbni was bedoeld hiervoor een wettelijke basis te bieden, maar levert hiervoor nu juist een obstakel op.

Alle partijen rondom het LDS (inclusief het NCSC) zijn het inmiddels eens dat vorenbedoeld obstakel onwenselijk is en inmiddels heeft u de kamer geïnformeerd dat u zal bezien of daartoe met urgentie een traject voor specifieke wetswijziging wordt ingezet.

Advies

Op zich ondersteunt de raad uw voorstel voor de wetswijzing. De raad signaleert echter dat daadwerkelijke wetswijziging realistisch gezien waarschijnlijk nog twee jaar op zich zal laten wachten. De raad geeft u in overweging om te onderzoeken of de wetswijziging via een *spoedreparatie* mogelijk sneller kan worden doorgevoerd. Gezien de urgentie van de vorming van het LDS is de raad verder van oordeel dat niet kan worden gewacht met het delen van de incident informatie met de OKTT's totdat de gehele wetswijzigingsprocedure doorlopen is. Er is alle aanleiding de Wbni toe te passen zoals deze is bedoeld.

Om die reden adviseert de raad u om, overeenkomstig de bedoeling van de Wbni en vooruitlopend op de aangekondigde wetswijziging, nu al tot het delen van incidentinformatie met OKTT's over te gaan. Dit komt ten goede aan de bescherming van de belangen van de duizenden bedrijven, organisaties en burgers die nu niet geïnformeerd worden, terwijl de overheid wel informatie heeft dat zij slachtoffer of kwetsbaar zijn.

Uitkijkende naar uw reactie voorafgaand aan onze CSR Vergadering op 25 maart a.s. verblijven wij,

Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR