Gooimeer 4-15
1411 DC Naarden

088-1182510
info@cyberveilignederland.nl

Aan: Commissie Digitale Zaken
Datum: 1 april 2022
Betreft: Input Cyberveilig Nederland ten behoeve Commissiedebat Online veiligheid en cybersecurity

Geachte Kamerleden,

Op 7 april vergadert u over Online Veiligheid en Cybersecurity. Cyberveilig Nederland wil u graag enkele suggesties meegeven voor dit debat.

Belang van digitalisering voor Nederland
De digitale economie is niet meer weg te denken binnen onze maatschappij. De huidige corona-pandemie heeft deze transformatie alleen maar versneld. Een keerzijde van deze digitale afhankelijkheid is dat we kwetsbaar zijn voor cyberincidenten. Discontinuïteit bij slachtoffers van cybercrime is aan de orde van de dag. De huidige geopolitieke context zorgt voor een toenemende dreiging voor Nederland, waarbij niet alleen vitale sectoren doelwit zijn, maar ook het verwerven van hoogwaardige kennis een belangrijke doelstelling is. Naast de IT infrastructuur wordt ook steeds meer de ICS-infrastructuur (‘operationele technologie omgeving) kwetsbaar voor aanvallen en verstoring. Tenslotte is desinformatie (‘fake news’) en hiermee samenhangend de (mogelijke) ondermijning van de democratische rechtsorde een zorgelijke ontwikkeling. Aandacht voor cybersecurity is daarom geen luxe, maar noodzaak. Daarom delen we een aantal aandachts- en zorgpunten graag met u.

Achterblijvende investeringen Coalitieakkoord
Vanuit het Coalitieakkoord worden er extra middelen toegekend voor cybersecurity. Echter de toegezegde middelen van €300 mln., waarvoor het gros voor de AIVD, MIVD en NCSC, zijn bij lange na niet afdoende om het toenemende dreigingslandschap waar Nederlandse organisaties zich in bevinden, tegen te gaan. Om de paar maanden zijn nieuwe kwetsbaarheden die een grote impact hebben (log4j, Spring), de geopolitieke situatie vraagt om extra aandacht en veel organisaties zijn nog *onbewust onbekwaam* wat betreft hun digitale weerbaarheid. Dit vraagt om extra investeringen in de volle breedte. De Cybersecurity Raad (CSR) heeft hiertoe een eerste aanzet gemaakt die wij vanuit Cyberveilig Nederland breed steunen en nogmaals onder de aandacht willen brengen.[1] In aanvulling op dit rapport hebben we nog een enkele additionele aandachtspunten die we u willen meegeven voor het debat.

Informatiedelen met het NCSC en DTC
Recente cyberincidenten zoals bij Solarwinds[2] of kwetsbaarheden als log4j[3] laten zien dat de huidige digitale infrastructuur dusdanig is verknoopt dat een hackaanval of kwetsbaarheid bij één specifieke organisatie grootschalige gevolgen kan hebben voor andere organisaties. De digitale wereld maakt geen onderscheid tussen vitaal en niet-vitaal, maar is verbonden via ketens van toeleveranciers, met onderlinge afhankelijkheden, kritische systemen en processen, etc. De vitale sectoren zijn dus in grote

[1] https://www.cybersecurityraad.nl/actueel/nieuws/2021/04/06/csr-adviseert-%E2%82%AC833-miljoen-voor-een-integrale-aanpak-voor-cyberweerbaarheid
[2] https://www.nu.nl/tech/6097701/waarom-de-hack-bij-solarwinds-ministeries-en-grote-bedrijven-treft.html
[3] https://www.ncsc.nl/onderwerpen/log4j

mate afhankelijk van en daardoor de-facto net zo kwetsbaar als niet-vitale sectoren. Om vergaande gevolgen van aanvallen op deze ketens te voorkomen, is snel en proactief handelen cruciaal.
Wij beschouwen transparantie over cyberincidenten als een randvoorwaarde voor het creëren van vertrouwen rond de inzet en gebruik van IT. Het delen van informatie en leren van Incidenten Is daar onderdeel van. Cyberveilig Nederland is eind 2020 aangewezen als OKTT[4], waardoor we als schakelorganisatie informatie mogen uitwisselen met het Nationaal Cybersecurity Centrum (NCSC). Hierin zijn de laatste maanden forse stappen gezet, waarbij de samenwerking met het NCSC door de sector als zeer positief wordt ervaren.

Zo is er rondom de kwetsbaarheid van log4j direct (op een zondagochtend!) en snel vanuit het NCSC geschakeld met (de achterban van) Cyberveilig Nederland. Dreigingsbeelden werden gedeeld en aangevuld met informatie vanuit de cybersecuritysector. Momenteel wordt (dreigings)informatie gedeeld tussen het NCSC en (de leden van) Cyberveilig Nederland via verschillende platforms. Cybersecurity bedrijven kunnen daardoor snel hun klanten informeren over een (mogelijke) kwetsbaarheid of aanval en andersom helpt de sector met het duiden én delen van informatie richting het NCSC. Daarnaast werken we samen aan gezamenlijke kennisproducten met het NCSC, zoals whitepapers over ransomware.[5] Met het DTC starten we een pilot om ook met de doelgroep van het DTC tot informatie-uitwisseling over kwetsbaarheden te komen. Door de NIS 2.0, die momenteel binnen Europa wordt besproken, wordt het steeds belangrijker dat organisaties snel informatie ontvangen over (mogelijke) kwetsbaarheden en hier handelend op kunnen treden.

Cyberveilig Nederland vindt het goed dat deze vorm van samenwerking op gang is gekomen. Het is van belang dat deze breder wordt doorgezet. Hierin is het nodig dat de overheid een centrale rol pakt en het delen van informatie, zoals informatie over incidenten, nog breder invulling geeft zodat de weerbaarheid van Nederland substantieel én structureel wordt verhoogd.

Opschaling bij cyberincidenten
Recente kwetsbaarheden rondom log4j en de huidige geopolitieke situatie hebben vooralsnog niet geleid tot grootschalige ontwrichting van onze digitale infrastructuur. Echter waakzaamheid is geboden. De ontwikkelingen met betrekking tot Oekraïne roepen vragen op en hebben invloed op het dreigingslandschap. Ook en met name hebben we zorgen over de beschikbare capaciteit op gebied van incident respons in geval van een grote crisis. Bij Log4j pakte het NCSC een goede coördinerende rol, maar als het was uitgelopen op een grootschalige crisis waar veel organisaties (gelijktijdig) getroffen zouden zijn door ransomware of een andere kwetsbaarheid, dan zouden er onvoldoende specialisten (publiek en privaat) beschikbaar zijn om iedereen te helpen of ondersteunen.

Hoe ga je als overheid zorgen dat de kritieke infrastructuur en andere belangrijke organisaties alle hulp krijgen die nodig is en daar prioriteiten in stellen? Momenteel ontbreekt het aan een "opschalingsmodel" in Nederland bij dergelijke (potentiële) grootschalige crises. Cyberveilig Nederland vraagt de minister om hier snel een strategie op te ontwikkelen en zo'n opschalingsmodel in te richten.

Uiteraard zijn we zeer bereid om hierover mee te denken, aangezien een substantieel deel van de incident respons capaciteit van Nederland binnen ons ledenbestand te vinden is.

[4] Organisatie Kenbaar Tot Taak.
[5] https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf

Belang van een innovatief Nederlands cybersecurity klimaat
Het beschermen van onze digitale infrastructuur ligt ten grondslag aan het beschermen van onze open, vrije en welvarende maatschappij en dit vraagt onze continue aandacht. Nieuwe technologische ontwikkelingen creëren nieuwe kansen, maar introduceren gelijktijdig ook kwetsbaarheden. Bij het versterken van onze cyberweerbaarheid spelen nieuwe technologieën én hun toepassingsgebieden een steeds belangrijkere rol. Daarnaast maakt de geopolitieke situatie en onze afhankelijkheid van niet-Europese cybersecurityproducten ons kwetsbaar, wat vraagt om betere en gestructureerde samenwerking op innovatie- en kennisontwikkeling én het vasthouden van cybersecurity talent. Vanuit Cyberveilig Nederland zijn we nauw betrokken bij het innovatieplatform dcypher. Hierin wordt tussen de overheid, private sector en onderzoeksinstellingen samengewerkt.

Cyberveilig Nederland vindt het belangrijk dat er wordt geïnvesteerd om de Nederlandse en Europese capaciteiten op het gebied van kennisontwikkeling en innovatie te versterken. Een sterke Nederlandse cybersecuritysector is belangrijk om talenten te ontwikkelen en vast te houden. Hierbij is het belangrijk dat er vanuit de overheid cybersecurity vraagstukken zo veel mogelijk interdepartementaal worden opgepakt in brede programma's met een multidisciplinair karakter en het launching customerschap wordt gestimuleerd.

Twee loketten met dreigingsinformatie voor Nederlandse bedrijfsleven is niet optimaal
Cyberveilig Nederland vindt het moeilijk uitlegbaar dat er binnen de Nederlandse overheid twee verschillende loketten zijn waar bedrijven terecht kunnen met informatie over het vergroten van hun digitale weerbaarheid. Voor vitaal is er het NCSC en voor de rest het DTC. Voor vitaal is er het NCSC en voor het overige bedrijfsleven het DTC. Waarbij die laatste overigens aanzienlijk minder waardevolle informatie beschikbaar stelt dan het NCSC in dit kader. Wie heeft nu welke taak (NCSC vs DTC)? Met name vanuit de Wet bevordering digitale weerbaarheid van bedrijven, die in 2021 vanuit het Ministerie van Economische Zaken en Klimaat in consultatie is geweest, wordt deze vraag urgent. Cyberveilig Nederland is van mening dat hier het risico bestaat dat organisaties vanuit verschillende organisaties (DTC, NCSC, OKTT) geïnformeerd worden. Bij grootschalige incidenten mag geen tijd verloren gaan aan het (onnodig) schakelen tussen organisaties met overlappende doelstellingen en doelgroepen.

Worden organisaties bij een incident door verschillende overheidsinstanties geïnformeerd? Is het voor iedereen duidelijk waar zij terecht kunnen? Hoe is de samenwerking tussen het DTC en NCSC geborgd?

Tot slot zijn twee organisaties met een eigen backoffice, website, personeel (schaarste aan cybersecurity professionals), etc., terwijl veelal dezelfde informatie wordt gedeeld is volgens ons inefficiënt.

Belang van encryptie
Nederland was één van de eerste landen die zich duidelijk uitsprak over het belang van encryptie.[6] Desondanks blijven er vanuit de overheid plannen komen om encryptie te verzwakken. Cyberveilig Nederland begrijpt dat er vanuit de opsporings- en inlichtingendiensten wensen zijn om toch toegang te krijgen tot versleutelde informatie. Echter het verzwakken van encryptie kan nooit de oplossing zijn en brengt te veel risico's met zich mee. Zo gaat Cyberveilig Nederland ervan uit dat ook malafide partijen uiteindelijk gebruik kunnen maken van de 'achterdeur' die wordt gecreëerd. Ook zal het innovatie belemmeren en brengt het grote risico's met zich mee wat betreft het waarborgen van privacy.

[6] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015

Cyberveilig Nederland dringt aan dat het encryptiestandpunt uit 2016 gehandhaafd blijft.

Ik hoop u hiermee voldoende te hebben geïnformeerd. Mocht u nog vragen hebben, dan kunt u contact opnemen met de Beleidsadviseur van Cyberveilig Nederland, Liesbeth Holterman op 06-36268957 of via liesbeth@cyberveilignederland.nl.

Met vriendelijke groet,

Petra Oldengarm
Directeur

Cyberveilig Nederland is dé belangenorganisatie voor cybersecurity bedrijven in Nederland. We brengen transparantie aan in de sector door de ontwikkeling van een gedragscode en keurmerk. We nemen actief deel aan het publieke debat en zien cybersecurity niet alleen als een risico, maar juist ook als een kans om Nederland te positioneren als een land dat veilige producten en diensten voortbrengt. We gaan het gesprek aan met de overheid en andere strategische partners om onze kennis en kunde van het cybersecurity werkveld voor het grotere belang in te zetten. We brengen verbindingen tot stand, tussen cybersecurity bedrijven onderling, maar ook brengen we vragers en aanbieders samen. We praten met de overheid en politiek om (toekomstige) knelpunten weg te nemen die de digitale weerbaarheid van Nederland in de weg staan. Maar vooral: we doen! We zijn initiatiefnemer en uitvoerder van het Cybersecurity Woordenboek en hebben recent een buyers guide securitytesten gepubliceerd:
https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/
https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Buyersguide_Security_Testen_final2.pdf.