Gooimeer 4-15
1411 DC Naarden

088-1182510
info@cyberveilignederland.nl

Aan: Minister van Justitie en Veiligheid
Datum: 19 augustus 2021
Betreft: Input Cyberveilig Nederland ten behoeve van internetconsultatie Wet beveiliging netwerk- en informatiesystemen

Zijne excellentie,

U heeft de Wet Wet beveiliging netwerk- en informatiesystemen voorgelegd voor een internetconsultatie. Cyberveilig Nederland wil u graag enkele suggesties meegeven.

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 cyber-incidenten. Discontinuïteit bij slachtoffers van cybercrime is aan de orde van de dag. De huidige geopolitieke context zorgt voor een machtsstrijd tussen landen, waarbij het verwerven van hoogwaardige kennis een belangrijke doelstelling kan zijn voor economisch gewin. Dit kan, voor een innovatief land als Nederland een directe aantasting betekenen voor ons innovatie- en concurrentievermogen. Een aantal van onze leden ziet dan ook een sterke toename van incidenten waarbij mogelijk statelijke actoren, danwel *state sponsored* actoren betrokken. Ook 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. Het verkleinen van de digitale kwetsbaarheid is een gemeenschappelijke uitdaging. Cyberveilig Nederland beschouwt 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. Vanuit Cyberveilig Nederland heeft u, als minister van Justitie en Veiligheid, in december onze vereniging de OKTT-status gegeven. We zijn dan ook zeer verheugd met voorgestelde wijziging van de Wet beveiliging netwerk- en informatiesystemen.

We hebben wel een aantal aandachts- en zorgpunten die wij graag met u willen delen in deze internetconsultatie.

Hoge urgentie van digitale dreigingen vraagt om snel delen

Recente cyberincidenten zoals bij Solarwinds[1] en bij Kaseye[2] laten zien dat de huidige digitale infrastructuur dusdanig is verknoopt dat een hack-aanval 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 de supply chain, onderlinge afhankelijkheden, , kritische systemen

[1] https://www.nu.nl/tech/6097701/waarom-de-hack-bij-solarwinds-ministeries-en-grote-bedrijven-treft.html
[2] https://dutchitchannel.nl/676931/kaseya-topman-tot-vijftienhonderd-bedrijven-getroffen.html

en processen, etc. De vitale sectoren zijn dus in grote mate afhankelijk van en daardoor de-facto net zo kwetsbaar als niet-vitale sectoren. Om daarom vergaande gevolgen van aanvallen op deze ketens te voorkomen, is snel en pro-actief handelen cruciaal. Cyberveilig Nederland pleit er dan ook voor om alvast, voorouitlopend op de goedkeuring van het wetsvoorstel, informatie te delen vanuit het NCSC met de in de wbni bedoelde organisaties.

OKTT als doorgeefluik van informatie

In hoofdstuk 1, alinea 3 van de memorie van toelichting staat het volgende: “De voorgestelde wijziging van artikel 20,tweede lid, Wbni maakt het mogelijk dat het NCSC deze gegevens ook kan delen met organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT’s). Hierdoor kunnen aanbieders in de doelgroepen van de OKTT’s door tussenkomst van die OKTT’s komen te beschikken over de voor hen relevante dreigings- en incidentinformatie.” Het lijkt hier dat OKTT’s tussen NCSC en organisaties worden geplaatst en doorgeefluik worden voor belangrijke dreigingsinformatie en incidenten. Het is hier van belang dat de betreffende OKTT’s geen filter gaan vormen, waardoor mogelijk belangrijke informatie niet bij belanghebbende organisaties terecht gaat komen, simpelweg omdat een OKTT beslist sommige informatie niet door te sturen. Een filterende werking zal dan ook kunnen leiden naar een situatie van schijnveiligheid, omdat organisaties op basis van onvolledige informatie beslissingen gaan nemen. Daarnaast is het van belang dat het informeren over meerdere schijven niet leidt tot vertragingen in de informatievoorziening die tot gevolg hebben dat organisaties significant langer dan via directe informatievoorziening moeten wachten op voor hen belangrijke informatie over bijvoorbeeld kritische kwetsbaarheden of aanvallen.

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 momenteel vanuit het Ministerie van Economische Zaken en Klimaat in consultatie is, wordt deze vraag urgent. Worden organisaties bij een incident door verschillende overheidsinstanties geïnformeerd? Is het voor iedereen duidelijk waar zij terecht kunnen? In de consultatie staat dat ‘Informatie enkel met “anderen” wordt gedeeld mits zij niet een OKTT of samenwerkingsverband hebben.’ In hoeverre is het NCSC bekend met de achterban van de OKTT’s en samenwerkingsverbanden? Cyberveilig Nederland is van mening dat hier het risico bestaat dat organisaties vanuit verschillende organisaties (DTC, NCSC, OKTT) geïnformeerd worden. Wanneer we naar het buitenland kijken, waarbij het NCSC UK wat ons betreft het beste voorbeeld is, zie je dat daar vrijwel overal de trend is om dit soort zaken te consolideren onder één organisatie, één duidelijk loket. Bij grootschalige incidenten mag geen tijd verloren gaan aan het (onnodig) schakelen tussen organisaties met overlappende doelstellingen en doelgroepen.
Wanneer wij kijken naar de aankomende NIS2 in relatie tot de huidige vernieuwingsslag van de Wbni, verdwijnt het onderscheid tussen AED’s en DSP’s. Classificatie van de individuele asset owners zal

plaatsvinden op basis van belangrijkheid waarbij nieuwe criteria gaan gelden. Hierop kan met de Nederlandse wetgeving worden voorgesorteerd door dit alvast mee te nemen in de aanpassingen die volgen uit deze consultatieronde voor de Wbni.

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.

"Bijzondere gevallen"

De hierboven beschreven (kunstmatige) splitsing tussen vitaal en niet-vitaal of NCSC en DTC lijkt er ook toe te leiden dat u in het wetsvoorstel de noodzaak voelt om het delen van informatie alleen in "bijzondere gevallen" mogelijk te maken. In de conceptwijziging of MvT wordt verder niet goed toegelicht wanneer iets een bijzonder geval is of niet, maar er wordt wel de opmerking gemaakt dat deze inperking nodig is omdat het NCSC alleen vitaal en overheid als doelgroep heeft. Hier lijkt dus al gelijk bij het aanpassen van de wet een nieuw obstakel te ontstaan: dat maar in een deel van de incidenten of dreigingen informatie gedeeld zal worden. Wij pleiten er daarom voor om niet alleen in bijzondere gevallen te delen ("delen mits"), maar altijd te delen tenzij daar grote bezwaren tegen zijn ("delen tenzij").

Herleidbare informatie

In paragraaf 2.2.2, alinea 1 wordt gesproken over: "In verband met het hiervoor omschreven probleem, dat in de afgelopen periode ook aandacht heeft gekregen in de media3 en politiek4, wordt voorgesteld om in artikel 20, tweede lid, Wbni OKTT's toe te voegen aan de opsomming van organisaties waaraan vertrouwelijke herleidbare gegevens met betrekking tot aanbieders kunnen worden verstrekt.

Hoe wordt erop toegezien dat binnen de OKTT's deze tot personen herleidbare informatie op de juiste wijze wordt behandeld en op welke wijze de vertaalslag plaats vindt naar niet herleidbare informatie voordat deze wordt uitgestuurd naar de bij de OKTT aangesloten organisaties?

Aantal OKTT's

Verder wordt in de daaropvolgende alinea gesproken over: "Met bovenbedoelde wijziging wordt naar mijn oordeel de kring van organisaties waaraan de in artikel 20, tweede lid, Wbni bedoelde informatie kan worden verstrekt, niet te groot." Aangezien de OKTT's nog moeten worden aangewezen, kunnen hier helemaal nog geen uitspraken over worden gedaan. Het is immers nog niet bekend hoeveel OKTT's er uiteindelijk zullen komen.

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,

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.