Gooimeer 4-15
1411 DC Naarden

088-1182510
info@cyberveilignederland.nl

Aan: Minister van Economische Zaken en Klimaat
Datum: 19 augustus 2021
Betreft: Input Cyberveilig Nederland ten behoeve van internetconsultatie Wet bevordering van de digitale weerbaarheid van bedrijven

Zijne excellentie,

U heeft de Wet bevordering van de digitale weerbaarheid van bedrijven 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. Daarom Cyberveilig Nederland dan ook zeer verheugd met de wettelijke borging van het Digital Trust Centre (DTC) van het Ministerie van Economische Zaken en Klimaat in de wet bevordering van de digitale weerbaarheid van bedrijven.

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

DTC organisatie vs doelgroep DTC

Het DTC is medio 2017 opgericht. De missie van het DTC is: om Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen. Alles van zzp'ers tot en met het grootbedrijf. Dit zijn alle bedrijven in Nederland die tot de niet-vitale sectoren behoren. Volgens de laatste cijfers van het CBS zijn er momenteel 1.955.515 bedrijven in Nederland.[1] Een klein deel daarvan behoort tot de vitale infrastructuur en valt hiermee onder verantwoordelijkheid van het Nationaal Cybersecurity Centrum

[1] Op basis van tweede kwartaal 2021. Zie: https://www.cbs.nl/nl-nl/cijfers/detail/81589NED

(NCSC). De rest valt binnen de missie van het DTC. Wat betekent deze uitbreiding van de taak voor de capaciteit van het DTC en kan het DTC met de huidige capaciteit aan de verantwoordelijkheid voldoen om de doelgroep te informeren. Oftewel hoe tijdig en ten alle tijden (24/7?) is het DTC in staat om de doelgroep te informeren met de huidige bezetting?
In de Memorie van Toelichting lees ik dat er genoemde taken een minimale capaciteit is voorzien van 9 fte resp. 3 fte en een materieel budget van € 400.000 voor ICT en communicatie. Incidenten houden zich niet aan kantoortijden. Gezien de enorme omvang van de missie lijkt ons het genoemde budget en het aantal fte verre van toereikend om op een passende wijze aan de wet te voldoen. Ik verwijs in deze graag naar het CSR rapport 'Integrale aanpak cyberweerbaarheid', waarin staat: "Voor het optimaliseren en onderhouden van een Landelijk Dekkend Stelsel van Informatieknooppunten, en ook het bewerkstellingen van een structurele (juridische) oplossing voor het delen van dreigingsinformatie wordt aangenomen dat structureel 5 fte nodig zijn.
Investeer daarnaast structureel € 8 miljoen in het DTC ter versterking van de uitbouw van de informatiedienst en van het netwerk van samenwerkingsverbanden met bedrijven om te komen tot een landelijk dekkend stelsel van informatieknooppunten voor cybersecurity."[2]

Vitaal vs Niet-Vitale bedrijfsleven

Cyberveilig Nederland vindt de onderscheid tussen vitaal en niet-vitaal achterhaald. Vitale aanbieders zijn overheidsorganisaties en privaatrechtelijke rechtspersonen die diensten aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving (bijvoorbeeld drinkwaterbedrijven. Recente cyberincidenten zoals bij Solarwinds[3] en bij Kaseya[4] laten zien dat de huidige digitale infrastructuur dusdanig is verknoopt dat een hack-aanval bij een niet-vitale organisatie grootschalige gevolgen kan hebben voor een vitale organisatie. Cyberveilig Nederland pleit er dan ook voor om verder te kijken dan naar alleen vitaal / niet-vitaal: maak op basis van economische en nationale veiligheid een afweging wie tot de doelgroep van het NCSC en het DTC behoort. Neem hierbij ook mee: supply chain, onderlinge afhankelijkheden, leveranciersafhankelijkheden, kritische systemen en processen, ect. Kijk hierbij ook naar het cybersecurity volwassenheidsniveau van organisaties. Het DTC kan zich focussen op organisaties met een lager volwassenheidsniveau en het initiëren van nieuwe weerbaarheidsinitiatieven.

Twee loketten voor Nederlandse bedrijfsleven is niet optimaal

In aanvulling op het voorgaande punt:
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 beveiliging netwerk- en informatiesystemen die momenteel vanuit het ministerie

[2] https://www.cybersecurityraad.nl/actueel/nieuws/2021/04/06/csr-adviseert-%E2%82%AC833-miljoen-voor-een-integrale-aanpak-voor-cyberweerbaarheid. Pagina 23.
[3] https://www.nu.nl/tech/6097701/waarom-de-hack-bij-solarwinds-ministeries-en-grote-bedrijven-treft.html
[4] https://dutchitchannel.nl/676931/kaseya-topman-tot-vijftienhonderd-bedrijven-getroffen.html

van Justitie en Veiligheid 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? 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 Wbdw.

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.

Risico-informatie vs dreigingsinformatie

In de internetconsultatie van de wet bevordering digitale weerbaarheid van bedrijven staat in de taakstelling het volgende beschreven:
a. het analyseren en het onderzoeken van gegevens over kwetsbaarheden, dreigingen en incidenten die betrekking kunnen hebben op netwerk- en informatiesystemen van bedrijven; b. het informeren en adviseren van bedrijven over kwetsbaarheden, dreigingen en incidenten die betrekking kunnen hebben op hun netwerk- en informatiesystemen;
c. indien relevant het verstrekken van ingevolge onder a verkregen gegevens aan bedrijven. Het is Cyberveilig Nederland niet duidelijk of hierbij ook dreigingsinformatie wordt bedoeld: te weten technische informatie over kwaadwillende actoren inclusief IP-adressen en het DTC hiertoe wordt aangesloten aan het Nationaal Detectie Netwerk (NDN). Het is Cyberveilig Nederland niet duidelijk of het DTC ook dit onderscheid kan en gaat maken ten behoeve van haar taakstelling. Wil het DTC de digitale weerbaarheid van bedrijven helpen vergroten dan is het, naar onze mening, niet alleen nodig om bedrijven alleen te informeren wanneer, bijvoorbeeld, hun IP naar voren komt als mogelijk gecompromitteerd, maar dat bedrijven ook informatie krijgen over dreigingen die nog niet zijn vastgesteld.
Verder staat genoemd onder art. 1 lid 1 (onder b) genoemd dat de minister de verantwoordelijkheid heeft om bedrijven te adviseren over "kwetsbaarheden, dreigingen en incidenten". Het is niet duidelijk of die advisering ook best practices, maatregelen en handelingsperspectief omvat, of alleen een bericht dat sprake is van een van de genoemde zaken. Ons sterke advies is om in de taakstelling van het DTC ook op te nemen dat zij bij het communiceren en adviseren (zeker met minder volwassen doelgroepen) ook een duidelijk handelingsperspectief geven.

Gegevens vallen onder de Wob?

Binnen de wet beveiliging netwerk informatiesystemen (wbni) is geregeld dat vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder niet onder de Wet openbaarheid van bestuur (Wob) vallen. In het voorstel voor de wet bevordering digitale weerbaarheid van bedrijven lijkt geen uitzonderingspositie te zijn opgenomen voor de Wob. Het DTC zal mogelijk gaan beschikken over bedrijfsvertrouwelijke en anderszins gevoelige informatie. In de evaluatie van het DTC[5] wordt nadrukkelijk genoemd dat "er terughoudendheid zal zijn in het delen van informatie, omdat bedrijven vrezen dat informatie van het platform kan worden opgevraagd via een Wob-verzoek." Cyberveilig Nederland zou graag willen zien dat ook voor het DTC een uitzonderingsgrond voor de wob ingeregeld krijgt zoals het NCSC dat heeft geregeld binnen de Wbni.

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,

[redacted]
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.

[5] https://www.rijksoverheid.nl/documenten/rapporten/2020/01/20/evaluatie-programma-digital-trust-center#:~:text=Dit%20rapport%20evalueert%20het%20programma,de%20vitale%20infrastructuur%20en%20Rijksoverheid