Gooimeer 4-15
1411 DC Naarden

088-1182510
info@cyberveilignederland.nl

Aan: Vaste Kamercommissie voor Justitie en Veiligheid

Datum: 16-10-2019
Betreft: Input Cyberveilig Nederland ten behoeve van AO Cybersecurity dd. 31-10-2019

Geachte heer/mevrouw,

Op donderdag 31 oktober aanstaande staat het Algemeen Overleg Cybersecurity gepland. Cyberveilig Nederland wil u graag enkele suggesties meegeven voor dit overleg.

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. Maar vooral: we doen! We zijn initiatiefnemer en uitvoerder van het Cybersecurity Woordenboek: tot stand gebracht onder de Cybersecurity Alliantie in samenwerking met 70 publiek-private partners. Zie: https://cyberveilignederland.nl/woordenboek/. Cyberveilig Nederland heeft ruim 50 leden.

Belang van digitalisering voor Nederland

Nederland is een digitale koploper in de wereld en één van de '*most connected countries in the world*'. Steeds meer bedrijven, burgers en overheden zijn in toenemende mate afhankelijk van informatie- en communicatietechnologie en digitaal met elkaar verbonden. Deze digitalisering brengt economische kansen met zich mee, én vraagt om het verhogen van de weerbaarheid tegen cyberdreigingen. Discontinuïteit door cybercrime en diefstal van (intellectuele) eigendommen door statelijke actoren is een realiteit. Desinformatie ('fake news') en de ondermijning van de democratische rechtsorde ontwikkelen zich snel. Aandacht voor cybersecurity is daarom geen luxe, maar noodzaak. Het verminderen van digitale kwetsbaarheid is een gemeenschappelijke uitdaging waar het ministerie van Justitie en Veiligheid een belangrijke rol in speelt.

Suggesties Cyberveilig Nederland voor AO Cybersecurity

Voor het komende Algemeen Overleg Cybersecurity heeft Cyberveilig Nederland enkele suggesties die ertoe zullen bijdragen dat de digitale weerbaarheid van Nederland wordt verhoogd:

1. Het delen van informatie over cybersecurity-incidenten gebeurt nog veel te weinig en moet nu echt de norm worden. Dit betreft zowel voor informatie afkomstig uit bijvoorbeeld meldplichten (van met name het Nationaal Cyber Security Centrum en de Autoriteit Persoonsgegevens) als cybersecurity gerelateerde informatie waarvoor geen wettelijke basis is. Met deze informatie kunnen organisaties beter hun risico's inschatten, kan de impact van specifieke dreigingen worden verminderd en kunnen methodieken om

dreigingen op te sporen worden verbeterd. De overheid dient te stimuleren dat organisaties informatie over incidenten (anoniem) melden en delen, ook indien daarvoor geen wettelijke basis bestaat. Zo wordt momenteel door maar weinig organisaties aangifte gedaan van cybercrime. Deels komt dit voort uit schaamte en uit angst voor reputatieschade, maar ook door beperkte kennis en capaciteit bij de (lokale) politie. Hierdoor heeft de overheid slechts een beperkt beeld van de impact en omvang van cyberincidenten. De leden van Cyberveilig Nederland hebben veel relevante kennis over cybersecurity-incidenten. Deze zijn zeer welwillend om deze te delen met bijvoorbeeld het NCSC of het AP zodat een beter beeld ontstaat over de impact van cyber-incidenten en mogelijke oplossingsrichtingen.

Beschikbare informatie over cybersecurity-incidenten moet breder worden gedeeld, waarbij de overheid zelf het goede voorbeeld moet geven én moet stimuleren dat andere organisaties ook hun ervaringen over cybersecurity-incidenten breder gaan delen, desnoods anoniem.

2. Organisaties nemen nog steeds veel te weinig hun verantwoordelijkheid op het gebied van cybersecurity. Steeds meer organisaties zijn onderling verbonden en cybersecurity-incidenten hebben daardoor al snel impact op een grotere keten. Organisaties die nalatig zijn in het nemen van afdoende cybersecuritymaatregelen komen hiermee weg, omdat dit verder geen gevolgen voor hen heeft. Hierin moet de overheid verantwoordelijkheid nemen, bijvoorbeeld door het vaststellen van minimale zorgplichten van organisaties, denk aan een soort digitaal rijbewijs. Vertrouwen op zelfregulering is hierbij veel te beperkt. Achteraf boetes uitdelen is bovendien niet voldoende: de overheid moet aan de voorkant afdwingen dat organisaties maatregelen nemen om cyberincidenten tegen te gaan. Denk daarbij aan het promoten van een baseline voor kritieke infrastructuur, vergelijkbaar met de richtlijnen voor fysieke veiligheid (gevaarlijke stoffen, brandveiligheid, etc), het ontwikkelen van een baseline voor Internet of Things (IoT) devices die de veiligheid en privacy van burgers beter moet waarborgen en bijvoorbeeld aan het besteden van meer aandacht en het toevoegen van een verplichtend karakter aan Coordinated Vulnerability Disclosure (CVD, voorheen Responsible Disclosure) waarbij de gemeenschap van ethische hackers wordt ingezet om het internet veiliger te maken. Cyberveilig Nederland publiceerde in 2018 voor organisatie al een handzaam stappenplan voor CVD (zie https://cyberveilignederland.nl/cyberveilig-nederland-publiceert-stappenplan-bij-hulp-ethische-hackers-voor-bescherming-tegen-cybercrime/)

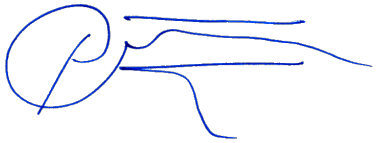
Cyberveilig Nederland vindt dat organisaties veel meer verantwoordelijkheid moeten nemen om digitaal weerbaar te worden. Ze roept de overheid op hier instrumenten voor te ontwikkelen en deze een verplichtend karakter te geven.

3. In het WRR rapport *Voorbereiden op digitale ontwrichting* kwam het al ter sprake: we hebben in Nederland momenteel geen idee hoe digitaal kwetsbaar we zijn. Omdat het aanvalsoppervlak grotendeels onbekend is, of juist bij zeer veel verschillende partijen (in zowel het publieke als private domein) kunnen kwetsbaarheden niet goed worden verholpen. Er moet inzichtelijk worden gemaakt welke processen, ketens en netwerken impact hebben op vitale processen. Daarbij moeten relevante maatregelen worden ontwikkeld om het aanvalsoppervlak te verkleinen.

Cyberveilig Nederland is van mening dat er onvoldoende adequate maatregelen genomen worden om de digitale weerbaarheid van Nederland te vergroten zolang niet duidelijk is waar en hoe we kwetsbaar zijn. Breng dit in kaart.

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