Gooimeer 4-15
1411 DC Naarden

088-1182510
info@cyberveilignederland.nl

Aan: Vaste Kamercommissie voor Veiligheid en Justitie

Datum: 21-06-2018
Betreft: Input Cyberveilig Nederland ten behoeve van AO Cybersecurity dd. 28-06-2018

Geachte heer/mevrouw,

Op donderdag 28 juni aanstaande staat het Algemeen Overleg Cybersecurity gepland. Cyberveilig Nederland wil u graag enkele suggesties meegeven voor dit overleg.

Cyberveilig Nederland is recent opgericht en 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.

Belang van digitalisering voor Nederland

Digitalisering is één van de belangrijkste drijvers van economische groei en biedt kansen voor het oplossen van maatschappelijke uitdagingen. In een digitale samenleving moeten we kunnen rekenen op het ongestoord functioneren van ICT-systemen en continue toegang tot betrouwbare informatie. Digitale veiligheid is echter niet vanzelfsprekend. Cybercriminaliteit is de snelst groeiende vorm van criminaliteit waarbij steeds vaker MKB-bedrijven slachtoffer worden van cyberincidenten. Het recent verschenen Cyber Security Beeld Nederland 2018 laat zien dat de afhankelijkheid van digitale middelen dusdanig groot is dat uitval of verstoring een grote impact zal hebben op alle facetten in de samenleving. Cyberveilig Nederland heeft een aantal praktische suggesties die nodig zijn om cybersecurity incidenten effectief aan te pakken en de digitale weerbaarheid van Nederland te vergroten.

Onderzoek fiscale mogelijkheden rondom cybersecurity maatregelen

Cybersecurity roept onveiligheid op, maar angst is een slechte raadgever. Cyberveilig Nederland vraagt meer aandacht voor de kansen van cybersecurity. Economische prikkels om producten veiliger te maken zijn te weinig beschikbaar. Met name binnen het dossier (on)veilige Internet of Things, een onderwerp dat terecht hoog op de agenda van de verschillende Kamerleden staat, is voor veel producenten de *time to market* en de prijs van een product belangrijker dan het toepassen van *security-by-design*. Meer aandacht moet komen voor slimme bedrijven die het digitaliseren combineren met investeringen in digitale veiligheid en ‘security’ toepassen in de verbetering van hun producten en dienstverlening. Omdat de vraag naar veilige producten en diensten wereldwijd toeneemt kan Nederland voorop lopen op het gebied van digitale veiligheid. Om dit te stimuleren zou het goed zijn dat het voor bedrijven financieel aantrekkelijk wordt om in een hogere mate van cyberveiligheid te investeren. Het versneld kunnen afschrijven van investeringen die de digitale weerbaarheid vergroten, fiscale stimuleringen voor bedrijven die hun hard- en software veilig ontwikkelen en het stimuleren van cybersecurity innovaties middels onder andere SBIR-regelingen zijn enkele voorbeelden.

Cyberveilig Nederland vraagt de mogelijkheden van fiscale prikkels rondom cybersecurity investeringen voor bedrijven te onderzoeken. Op deze manier wordt cybersecurity vanuit de kansen-kant geredeneerd en ontstaan er positieve incentives om te investeren in maatregelen rondom digitale veiligheid.

Stimuleer Informatiedeling bij de overheid

Een belangrijke randvoorwaarde voor het verzilveren van deze kansen is het verhogen van de digitale weerbaarheid. Opeenvolgende Nationale Cyber Security Strategieën en Agenda's en nieuwe meldplichten als gevolg van onder andere de AVG hebben onder andere tot doel de digitale weerbaarheid te vergroten door meer informatie te verzamelen over de oorzaken en effecten van cyber-incidenten. Echter, de maatschappij profiteert onvoldoende van de kennis die binnen onder andere binnen de (rijks)overheid wordt opgebouwd. Een meldplicht zou volgens Cyberveilig Nederland gepaard moeten gaan met een verplichting van de overheid om kwalitatief hoogwaardige informatie terug te geven aan de maatschappij. Goede informatie uit meldplichten kan organisaties helpen om betere risico-afwegingen te maken op basis van feiten. De overheid moet hierin het goede voorbeeld geven. Het delen van informatie over cybersecurity incidenten zou de norm moeten worden en kan bijdragen aan de ambitie om een landelijk dekkend stelsel van informatieknooppunten op te bouwen. Hierbij kan standaardisatie een goed middel zijn om expertise op te bouwen, bestaande standaarden te hergebruiken en richting te geven in het vertalen van richtlijnen naar concrete toepasbaarheid.

Diverse meldplichten leveren bij het Nationaal Cyber Security Centrum, de Autoriteit Persoonsgegevens en de sectorale toezichthouders informatie op over cybersecurity-incidenten. Cyberveilig Nederland vraagt aan de overheid een 'pas toe of leg uit'-principe met betrekking tot deze informatie. Wij willen dat alle beschikbare informatie over cybersecurity incidenten binnen de overheid omgezet wordt in kwalitatief hoogwaardige informatie die gedeeld wordt.

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