Commissie Digitale Zaken

**Kapteynstraat 1, SBIC - Building suite 220 / 2201 BB Noordwijk**

**info@cyberveilignederland.nl**
**www.cyberveilignederland.nl**

**KvK 71802525**

**Noordwijk, 4 april 2024**
**Ref.: 314.2-0304**

Betreft: Input Commissiedebat Online Veiligheid en Cybersecurity

Geacht lid van de commissie Digitale Zaken,

De belangrijkste maatschappelijke vraagstukken en ons economisch verdienmodel zijn tegenwoordig mede afhankelijk van de inzet van digitale technologie. Vrijwel alle organisaties doen iets met data of digitalisering en zijn verbonden met het Internet. De kansen die daardoor ontstaan kunnen alleen verzilverd worden wanneer deze hand in hand gaan met cybersecurity. Dit vereist coördinatie, prioritering en planning van overheid, bedrijven én politiek.

De Nederlandse Cybersecurity Strategie 2022-2028 (NLCS) biedt een lange termijn visie op cybersecurity die verder rijkt dan de gewoonlijke kabinetsperiodes. Voor het slagen van de NLCS en haar actieprogramma zijn eigenaarschap en draagvlak in de uitvoering essentieel. Dat betekent nauwe betrokkenheid van stakeholders vanuit de overheid, het bedrijfsleven en de wetenschap. In dit kader geeft Cyberveilig Nederland (CVNL) u voor het Commissiedebat Online Veiligheid en Cybersecurity een aantal aandachtspunten mee op het gebied van:

1. Versterken publiek private informatiedeling
2. Betrekken private organisaties bij de (uitvoering van de) NLCS
3. Versterken kennis over OT-Security/IACS
4. Overbruggen cyberweerbaarheidskloof op langere termijn

**Ad 1. Versterken publiek private informatiedeling**
Om Nederland een onaantrekkelijk doelwit te maken voor digitale aanvallen is het essentieel dat publieke en private partijen sneller (onderling) informatie delen over digitale dreigingen en

incidenten. Hierdoor ontstaat een breed gedragen inzicht in actuele problematiek en wordt handelingsperspectief gecreëerd waardoor incidenten elders kunnen worden voorkomen of de impact wordt verminderd.

Vanuit CVNL hebben we de afgelopen jaren hard gewerkt aan meer transparantie en het delen van informatie uit incidenten. Dat begint bij onderling vertrouwen. Dit stimuleren we niet alleen tussen onze leden onderling, maar ook tussen onze leden en de overheid. Zo is met het NCSC, het Openbaar Ministerie en Politie een vruchtbare samenwerking ontstaan rondom ransomwarebestrijding in het project Melissa. Niet alleen zijn uit deze samenwerking een aantal successen in de bestrijding van cybercrime voortgekomen[1], maar verzamelen we ook kwalitatieve en kwantitatieve cijfers over de impact van ransomware[2] en delen we opgedane kennis via whitepapers.[3] De sleutel in deze samenwerking is een gezamenlijke opgave om Nederland weerbaarder te maken en het besef dat dit alleen lukt als de overheidspartijen en private organisaties ieder hun 'stukjes van de puzzel' beschikbaar stellen en zoeken naar manieren om deze, binnen geldende juridische kaders, met elkaar te delen.

Project Melissa laat zien dat er al veel mogelijk is als kennis bij elkaar wordt gebracht. Het is van belang dat informatie-uitwisseling richting de toekomst nog verder wordt gestimuleerd en dat knelpunten in de informatiedeling waar mogelijk worden opgeheven. Het programma Cyclotron[4] van de Rijksoverheid moet hierin voorzien, omdat deze moet leiden tot een platform waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen in bredere zin. CVNL is al vanaf de start betrokken bij dit programma en deelnemer aan verschillende deelprojecten.

*Cyberveilig Nederland vraagt u om bij de minister van Justitie en Veiligheid te borgen dat het programma Cyclotron wordt doorontwikkeld en de motor gaat vormen voor informatiedeling binnen het cybersecuritydomein.*

**Ad 2. Betrekken private sector bij de (uitvoering van de) NLCS**

De overheid heeft met de NLCS een ambitieuze strategie neergezet waar wij ons als cybersecuritysector grotendeels in herkennen. Hoewel er op hoofdlijnen in de pijlers focus is aangegeven, mist die focus wat ons betreft in de uitwerking van de meer dan 100 (!) actielijnen.
We maken ons zorgen over de prioriteiten en de uitvoerbaarheid van de strategie en daarmee de resultaatgerichtheid van de NLCS. Ook is de koppeling tussen de NLCS en de actielijnen niet altijd duidelijk. Dit is ook beschreven in het rapport van Dialogic dat een evaluatiekader en nulmeting

[1] https://www.politie.nl/nieuws/2023/oktober/3/11-melissa-samenwerkingsverband-ransomwarebestrijding.html
[2] https://cyberveilignederland.nl/actueel/jaarbeeld-ransomware-2023
[3] https://cyberveilignederland.nl/actueel/persbericht-cyberveilig-nederland-publiceert-whitepaper-data-exfiltratie-met-politie-om-en-ncsc
[4] https://www.nctv.nl/onderwerpen/programma-cyclotron

op de NLCS heeft uitgevoerd.[5] Voorts zijn er zorgen of alle acties in de NLCS voldoende (financieel) gedekt zijn bij de verschillende departementen. Het lijkt ons goed als in de verdere uitwerking een heldere roadmap wordt vastgesteld met haalbare doelen en beschikbare middelen voor de kortere termijn én de langere termijn.

In de actiepunten valt op dat op veel plekken in de NLCS nadrukkelijk private organisaties genoemd worden om onderwerpen uit de NLCS (te helpen) op te pakken. De NLCS maakt echter onvoldoende duidelijk welke partijen hiermee precies worden bedoeld en wat de Nederlandse overheid gaat doen om te zorgen dat deze partijen ook daadwerkelijk betrokken worden bij de gewenste acties.

In de praktijk zien we dat in de samenwerking rondom de NLCS hooggespannen verwachtingen zijn van de inzet van private organisaties, maar dat in de samenwerking private organisaties voornamelijk ingezet worden als klankbord en niet zozeer als samenwerkingspartner. Gedeeld eigenaarschap is echter een essentiële voorwaarde voor het slagen van de NLCS. Dat betekent dat in stuurgroepen die rondom de uitvoering van de NLCS ontstaan, waarin nu voornamelijk overheidsorganisaties participeren, ook ruimte komt voor private (koepel)organisaties die gaan helpen de benodigde samenwerking te realiseren.

*Cyberveilig Nederland vraagt u om bij de minister van Justitie en Veiligheid te pleiten om actief private (koepel)organisaties te betrekken in eigenaarschap en draagvlak rondom de uitvoering van de NLCS, niet alleen in de projecten zelf, maar ook in de aansturing (governance) daarvan.*

**Ad 3. Versterken kennis over OT-Security/IACS**

Industriële automatiseringssystemen vormen het fundament van belangrijke fysieke processen, zoals de productie en verwerking van grondstoffen, het zuiveren van drinkwater, de bediening van sluizen en distributie van elektriciteit. De veiligheid van deze systemen is van fundamenteel belang voor de Nederlandse maatschappij en economie. Echter de kennis over cybersecurity in dit domein (vaak benoemd als Operationele Technologie – OT of Industrial Automation & Control Systems – IACS) is beperkt en gefragmenteerd.

CVNL is blij met het initiatief voor het starten van de IACS-coalitie, waarin we actief deelnemer zijn, zowel inhoudelijk als in de besturing, en samenwerken aan (kennis)producten en informatiedeling. Echter, de kennis en kunde op OT-security blijft desondanks significant achter bij de vraag. We verwachten dat met de komst van de NIS2 de behoefte aan expertise op dit gebied nog verder zal toenemen en achter zal blijven op het aanbod.

[5] https://dialogic.nl/projecten/evaluatiekader-en-nulmeting-nederlandse-cybersecuritystrategie/

Een uitbreiding van de IACS-coalitie met meer belanghebbenden vanuit de private sector (zoals de vitale infrastructuur) is naar inzicht van CVNL noodzakelijk om een versnelling te realiseren. Daarnaast is het belangrijk dat cybersecurity wordt meegenomen in het inkoopproces van OT-systemen.

*Cyberveilig Nederland vraagt u bij de minister van Binnenlandse Zaken en Koninkrijksrelaties aan te dringen op stimuleren van het definiëren van aankoopeisen op gebied van cybersecurity bij de investering in nieuwe OT-systemen en bij de minister van Infrastructuur en Waterstaat aan te dringen op een versnelling en uitbreiding van de IACS-coalitie.*

Ook is het van belang dat meer organisaties gaan voldoen aan de standaarden op dit gebied, te beginnen bij de basis zoals deze in de BIACS[6] is geformuleerd. CVNL werkt samen met veel andere organisatie onder leiding van het Centrum voor Criminaliteitsbeheersing en Veiligheid (CCV) om gezamenlijk een keurmerk voor de BIACS te ontwikkelen. Het is het belangrijk dat deze ook wordt ondersteund vanuit de overheid: zowel vanuit de ontwikkeling als de implementatie van het keurmerk bij het inkoopproces.

*Cyberveilig Nederland vraagt u bij de minister van Infrastructuur en Waterstaat en minister van Justitie en Veiligheid te pleiten voor steun voor de ontwikkeling van een BIACS-standaard en daarvoor beperkte financiële middelen ter beschikking te stellen voor het CCV.*

**Ad 4. Overbruggen cyberweerbaarheidskloof op langere termijn**

Het MKB is de ruggengraat van onze economie en onmisbaar voor alle grote maatschappelijke transities. Er zijn op dit moment in Nederland 2.308.165 bedrijven waarvan er 430.410 zijn met twee medewerkers of meer[7]. Een optimaal cyberweerbaar MKB is daarom van belang voor Nederland. Er is een cyberweerbaarheidskloof tussen voorlopers op het gebied van cybersecurity en achterblijvers, veelal MKB-organisaties. Cybersecurity is vaak niet *top of mind* voor MBK-bedrijven en lastig te realiseren door gebrek aan expertise en betaalbare veilige oplossingen.

Op dit moment kiezen we als strategie voor het overbruggen van de kloof vooral voor het versterken van de weerbaarheid van het MKB. De verantwoordelijkheid voor weerbaarheid wordt daarmee voornamelijk bij het eindpunt in de keten belegd: bedrijven zijn primair zelf verantwoordelijk voor hun cybersecurity. De overheid heeft het Digital Trust Center (DTC, (ministerie EZK) ingericht om het MKB hierbij te ondersteunen en stelt subsidies beschikbaar die de weerbaarheid van het MKB moeten versterken.

---

[6] BIACS staat voor Basismaatregelen voor cybersecurity van IACS-systemen in het OT domein. De basis is ontleend uit de CSIR, een normenkader opgesteld door Rijkswaterstaat in samenwerking met de waterschappen. De BIACS is een vereenvoudigde versie van deze CSIR.

[7] CBS, 1e kwartaal 2024

CVNL is van mening dat de verantwoordelijkheid voor cybersecurity zou moeten opschuiven naar andere organisaties in de keten, zodat deze MKB-bedrijven in de toekomst idealiter *vanzelfsprekend veilig* zijn. Er is een systeemaanpak nodig waarbij andere (grotere en volwassener) organisaties meer verantwoordelijkheid gaan krijgen voor cybersecurity en de (kleinere) MKB-bedrijven in de toekomst steeds meer kunnen vertrouwen op de veiligheid van ingekochte producten en diensten.

Dit betekent dat de overheid andere prikkels moet stimuleren: minder subsidies voor weerbaarheidsinitiatieven van het DTC en City Deals (ministerie J&V), en meer aandacht voor het in stelling brengen het totale cybersecurity ecosysteem. Er zijn al positieve voorbeelden die effect hebben op het systeem zoals de aanstaande Cyber Resilience Act (CRA). Deze legt in de toekomst cybersecurityverplichtingen op aan commerciële aanbieders van digitale producten en diensten. Ook het initiatief van KPN, die een 'Extra Veilig Internet'-optie aanbiedt aan haar MKB-klanten, is hierin noemenswaardig.

De Rijksoverheid speelt in deze transitie een belangrijke rol en heeft in de ogen van CVNL een leidende rol als het gaat om het stimuleren van de dialoog over wat er nodig is om een situatie te bereiken waarin MKB-organisaties vanzelfsprekend veilig worden. De uitdagingen op gebied van cybersecurity nemen alleen maar verder toe en daarom moet er nu nagedacht worden over hoe deze op de langere termijn voor MKB-bedrijven het hoofd kunnen worden geboden.

*Cyberveilig Nederland vraagt u om bij de minister van Justitie en Veiligheid, als onderdeel van de uitvoering van de NLCS, en bij de minister van Economische Zaken en Klimaat als verantwoordelijk voor het Digital Trust Center, te pleiten om een dialoog op te starten om in publiek-privaat verband een visie te ontwikkelen op hoe vanzelfsprekende veiligheid voor het MKB op de langere termijn verder moet worden gerealiseerd.*

Indien u nog vragen heeft over deze onderwerpen, dan kunt u zich wenden tot Liesbeth Holterman, strategisch adviseur, via liesbeth@cyberveilignederland.nl of 06-36268957.

**Met vriendelijke groet,**
**Namens Cyberveilig Nederland,**

***Petra Oldengarm***
***Directeur***

Over Cyberveilig Nederland

Cyberveilig Nederland (CVNL) is de belangenvereniging van de cybersecuritysector. In die hoedanigheid maken we ons sterk voor het creëren van meer transparantie en kwaliteit in de markt. Ook behartigen we de belangen van de cybersecuritysector richting stakeholders zoals de overheid, wetenschap en politiek. Onze missie is de digitale weerbaarheid van Nederland te vergroten. Eén van de eisen om dit te bereiken is het actief delen van informatie. Vanuit CVNL stimuleren we dit actief door samen te werken met relevante overheidspartijen en andere belanghebbenden. In die hoedanigheid zijn we ook door het ministerie van Justitie en Veiligheid in 2020 aangewezen als schakelorganisatie onder de wet beveiliging netwerk informatiesystemen (wbni).[8] Daarnaast spelen we een actieve rol in het tot stand komen van een 'landelijk dekkend stelsel van informatieknooppunten'[9], zijn we vanaf de start betrokken bij het Anti Abuse Netwerk (AAN)[10], zijn we actief deelnemer in het Programma Cyclotron[11] en zijn we mede-initiatiefnemer van Project Melissa waarin we (de gevolgen van) ransomware bestrijden.[12]

[8] https://www.ncsc.nl/actueel/nieuws/2020/december/9/intensievere-informatie-uitwisseling-ncsc-en-nederlandse-cybersecuritybedrijven

[9] https://www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel

[10] https://www.abuse.nl/

[11] Cyclotron moet leiden tot een platform waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen. Zie: https://www.nctv.nl/onderwerpen/programma-cyclotron

[12] Project Melissa is een samenwerkingsverband tussen publieke en private partijen om ransomware aanvallen te bestrijden. Vanuit de overheid zijn het NCSC, OM en politie betrokken. Het gezamenlijke doel is om Nederland een onaantrekkelijk doelwit te maken voor ransomware criminelen. Zie: https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf en https://cyberveilignederland.nl/actueel/cyberveilig-nl-politie-om-en-ncsc-werken-samen-aan-ransomwarebestrijding