Digitale Veiligheid

als voorwaarde voor digitale transformatie

CYBERVEILIG NEDERLAND

Digitale veiligheid als voorwaarde voor digitale transformatie

De digitale economie is niet meer weg te denken in Nederland. Het regeerakkoord van het nieuwe kabinet zal dan ook gericht moeten zijn op een versnelling van die transformatie. Alleen dan worden de economische en maatschappelijke mogelijkheden optimaal benut. Het vergroten van de weerbaarheid is een belangrijke randvoorwaarde voor onze internationale positie van digitale mainport.

Immers, discontinuïteit bij organisaties doordat zij slachtoffer zijn van cybercrime is aan de orde van de dag. Diefstal van (intellectuele) eigendommen door statelijke actoren komt steeds vaker voor. Desinformatie ('fake news') en hierdoor de (mogelijke) ondermijning van de democratische rechtsorde is een zorgelijke ontwikkeling.

Aandacht voor cybersecurity is daarom geen luxe, maar noodzaak. Het verkleinen van de digitale kwetsbaarheid van Nederland is een gemeenschappelijke uitdaging die vraagt om een actieve en stimulerende rol van de overheid en politiek. Cyberveilig Nederland geeft haar visie op de rol die cybersecurity speelt in deze digitale transformatie.
De volgende vijf ambities voor het nieuwe kabinet zijn hierin leidend.

IN 2025...

... is het belang van investeren in digitale weerbaarheid breed gedragen en neemt iedereen daar ook de juiste maatregelen voor

... is er centrale overheidsregie binnen de departementen

... is het ontwikkelen van cybersecurityvaardigheden een vast onderdeel binnen het onderwijs

... zijn rollen en verantwoordelijkheden strak gedefinieerd

... staat Nederland bekend om haar innovatieve cybersecurity klimaat

Het belang van investeren in digitale weerbaarheid

Cybersecuritymaatregelen zijn noodzakelijk om schade te voorkomen, beperken of te herstellen die is ontstaan door een storing, uitval of misbruik van een informatiesysteem of computerinfrastructuur. Organisaties moeten hierin meer verantwoordelijkheid nemen. Door de onderlinge verbondenheid hebben incidenten al snel impact op een grotere keten van organisaties.

- Investeer blijvend in programma's en initiatieven die bijdragen aan betere 'awareness', zoals het Digital Trust Centre (DTC) van het ministerie van Economische Zaken en Klimaat. Veel organisaties zijn nog altijd 'onbewust onbekwaam'.

- Informeer organisaties over het belang van investeren in digitale weerbaarheid. Zorg bijvoorbeeld dat iedere organisatie weet waarom het implementeren van basismaatregelen zoals patchen, hardening en autorisaties zo belangrijk is[1]. Neem ook de aanbevelingen van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) over en maak een classificatie van cyberaanvallen, gekoppeld aan specifieke responsmogelijkheden[2]. Ook een meer verplichtend karakter van Coordinated Vulnerability Disclosure bij organisaties kan helpen omdat ethische hackers kunnen bijdragen aan het verbeteren van de informatiebeveiliging[3].

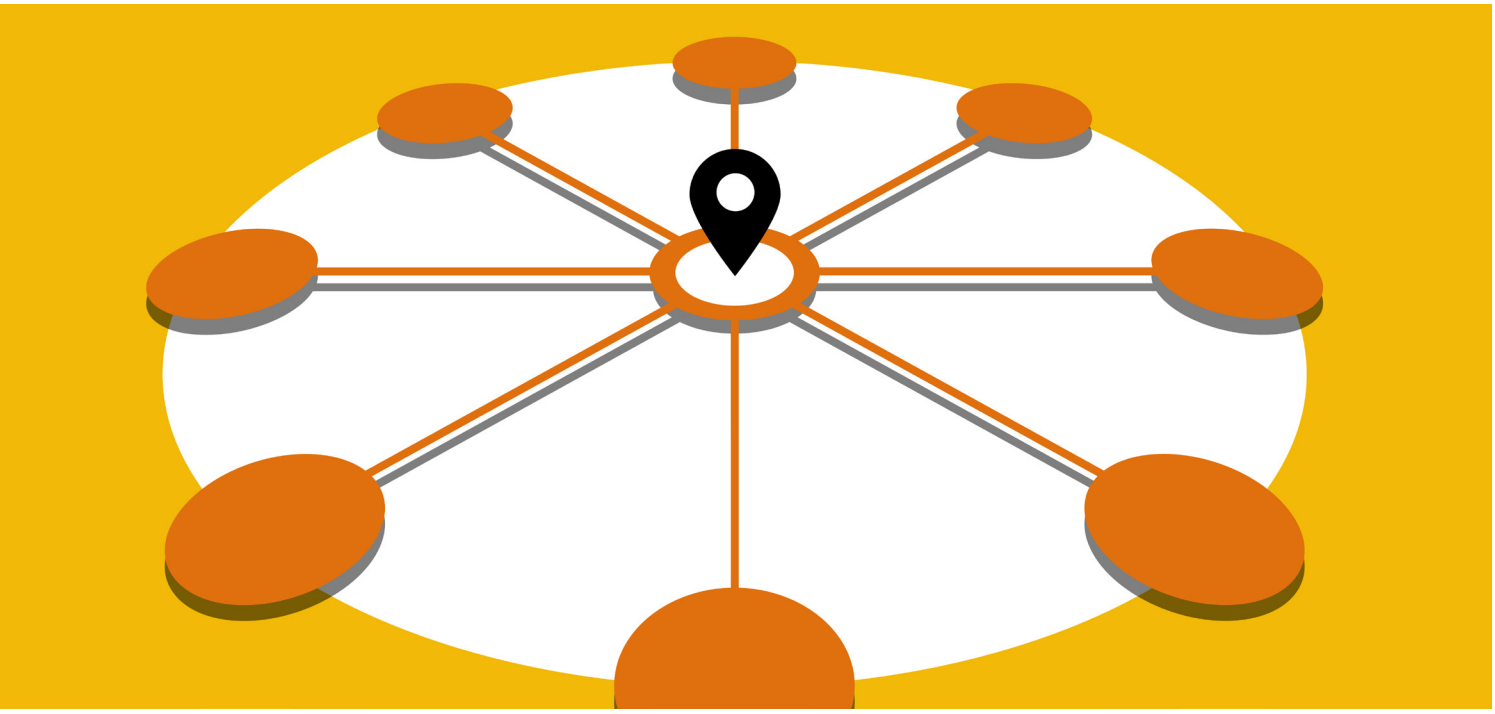
- Onderzoek de mogelijkheden voor fiscale prikkels voor bedrijven die investeren in cybersecuritymaatregelen. Tijdens de bouwcrisis enkele jaren geleden werden investeringen tijdelijk met een lager BTW-tarief belast. Onderzoek ook deze mogelijkheden wanneer bedrijven investeren in hun digitale veiligheid.

[1] Sommige cybersecurity termen zijn lastig te begrijpen voor een niet cybersecurity ingewijde. Daarom heeft Cyberveilig Nederland het initiatief genomen om te komen tot een cybersecurity woordenboek waar deze termen begrijpelijk zijn uitgelegd. Kijk hiervoor op: cyberveilignederland.nl/woordenboek-cyberveilig-nederland.

[2] WRR, Voorbereiden op digitale ontwrichting (2019).

[3] Cyberveilig Nederland heeft een stappenplan ontwikkeld voor het inzetten van Coordinated Vulnerability Disclosure. Zie hiervoor: cyberveilignederland.nl/cyberveilig-nederland-publiceert-stappenplan-bij-hulp-ethische-hackers-voor-bescherming-tegen-cybercrime.

De noodzaak van centrale regie binnen de overheid



De afgelopen jaren zijn er verschillende cybersecurityrapporten, strategieën en roadmaps gepubliceerd. Helaas adresseren zij slechts deelaspecten van de problematiek. Versnippering en gebrek aan ambitie van en tussen de verschillende (beleids)departementen hebben een verlammende werking op de digitale weerbaarheid. Betere samenwerking is essentieel om de kansen van digitalisering volop te benutten.

- Her-evalueer de definitie van de vitale sectoren. Vitale partijen zijn in grote mate afhankelijk van toeleveranciers die vaak niet als vitaal zijn gekenmerkt. Hierdoor ontstaat er een risico in de keten waar nu nog onvoldoende aandacht voor is. Zorg dat organisaties met een hoog cybersecurity volwassenheidsniveau ook binnen het stakeholder-landschap van het Nationaal Cyber Security Centrum (NCSC) worden opgenomen in plaats van bij het DTC. Hiertoe moet meer visie ontwikkeld worden hoe het OKTT[4]-landschap wordt ingevuld en op welke manier het NCSC met deze organisaties gaat samenwerken en (welke) informatie kan en mag delen.

- Onderzoek het aanstellen van een tijdelijke cybercommissaris die departement overstijgend kan handelen en daarbij beschikt over doorzettingsmacht, budget, etc. Deze wordt dan ondersteund door een zogenoemd *Deltaplan Cybersecurity*, waarin onafhankelijkheid, pro-activiteit, integraliteit en strakke coördinatie centraal staan.

- Richt een onafhankelijk 'Cyber Outbreak Management Team' (COMT) in, naar analogie van het OMT tijdens de COVID-19 crisis. Dit onafhankelijke COMT adviseert de regering in het geval van acute en/of maatschappelijke vraagstukken of bij een majeur incident. Het COMT zou moeten bestaan uit een diversiteit aan cybersecurityspecialisten (ethische hackers, privacy-deskundigen, gedragswetenschappers, specialisten, etc).

- Maak het delen van informatie over cybersecurity de norm. Zorg dat opgedane informatie, bijvoorbeeld van datalekken (AP), aangiftes (politie) of incidenten (NCSC) gedeeld en onderzocht worden in een breder publiek - privaat consortium. Op deze manier kan er verder onderzoek worden verricht naar de desbetreffende crimineel/actor en kan deze informatie breder worden gedeeld en ingezet. Bijvoorbeeld het treffen van preventieve maatregelen bij vergelijkbare – vitale – partijen enerzijds en het doen van aangifte (de aangiftebereidheid te verhogen) anderzijds.

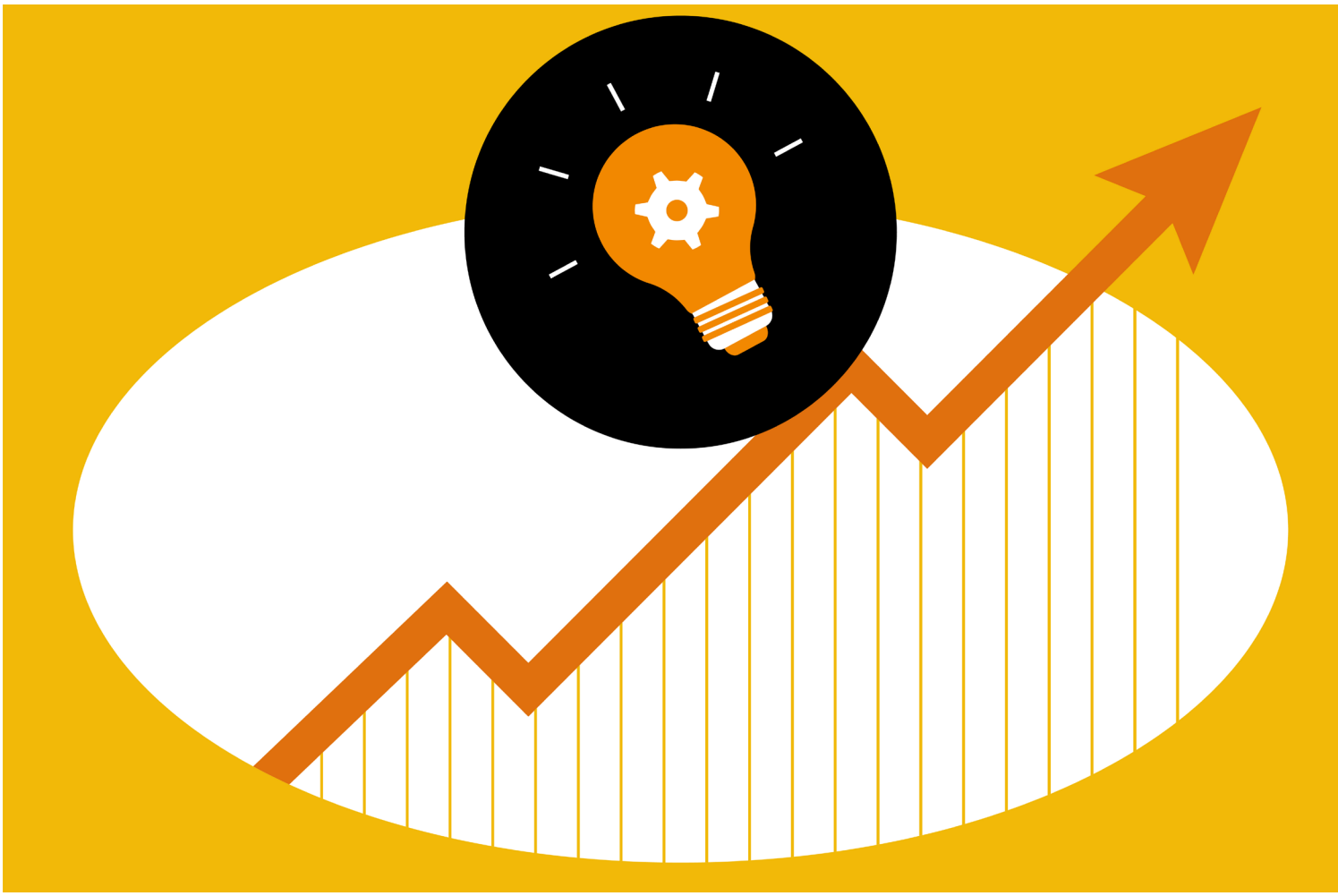
[4] Op basis van de wet Wbni (wet beveiliging netwerk- en informatiesystemen) kan het NCSC informatie delen met organisaties die: "kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten, en computercrisisteams."

De essentie van digitale vaardigheden in het onderwijs

De digitale toekomst van Nederland moet veilig worden gesteld. Hiervoor is het noodzakelijk dat er voldoende cybersecurityprofessionals zijn en dat de Nederlandse jeugd wordt voorbereid op de digitale toekomst. De Nederlandse cybersecuritysector kenmerkt zich als een jonge sector waar een veelheid aan producten en diensten wordt aangeboden en een grote diversiteit aan specialisten hun werk doen: van security analisten, tot juristen tot psychologen. Al deze kennis en capaciteiten zijn nodig en er is een grote vraag naar talent, maar te weinig aanbod.

- Investeer in cybersecurityonderwijs dat aansluit op de praktijk. De steeds grotere behoefte aan gekwalificeerde cybersecurity experts en de beperkte uitstroom uit het onderwijs of bijscholingsmogelijkheden zorgen voor een krapte op de markt waar publieke en private organisaties met elkaar strijden om schaars talent.

- Digitale weerbaarheid is voor een belangrijk deel afhankelijk van het onderwijs. Aandacht voor cybersecurity en privacy is dan ook evident. Cyberveilig Nederland ziet dit nog niet terug in de praktijk. Wij stellen daarom een cyberveiligdiploma voor waarin wordt gemeten en vastgesteld welke minimale vaardigheden een kind op de basisschool zou moeten beheersen om digitaal in redelijke veiligheid te bewegen.

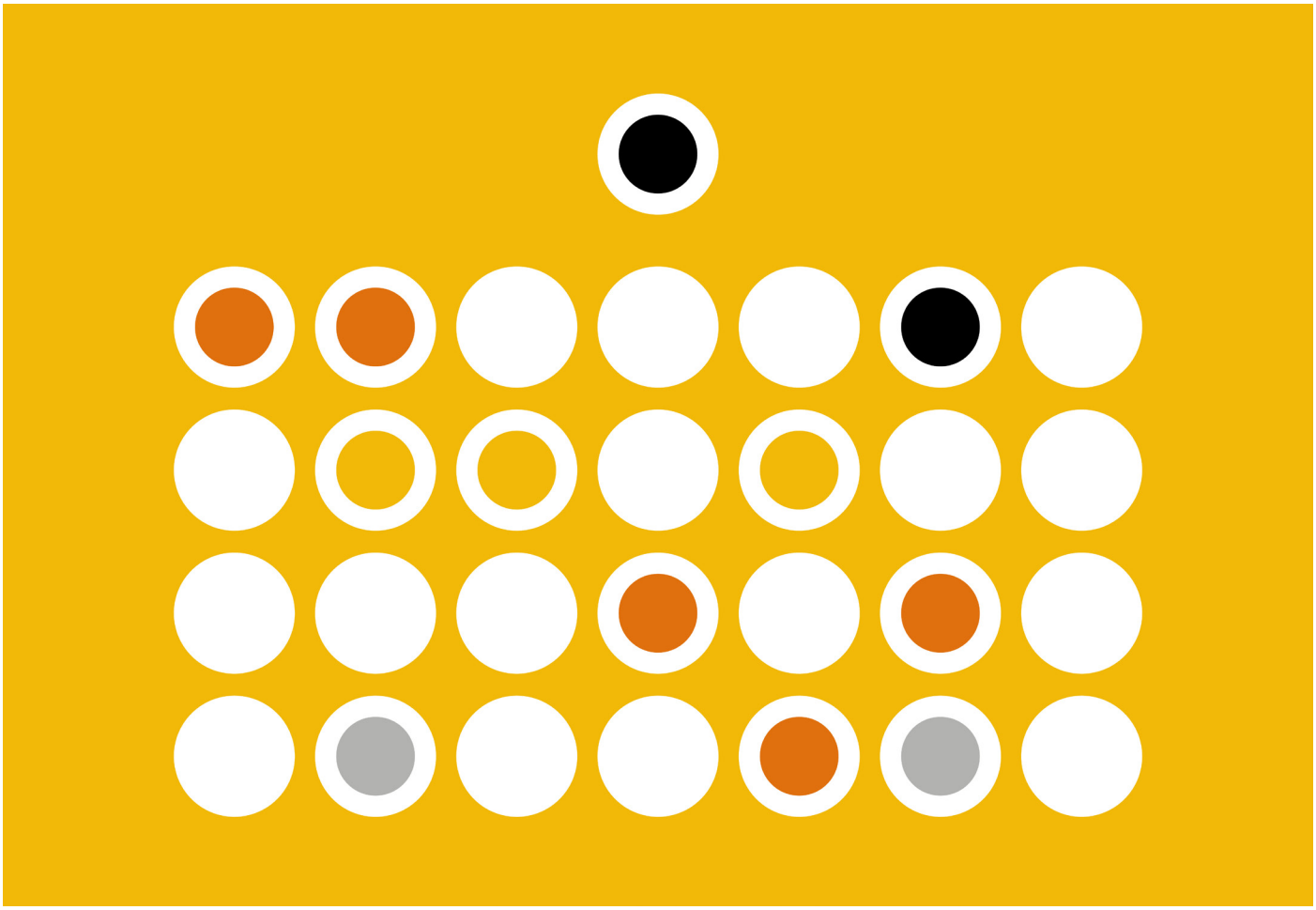


Rollen en verantwoordelijkheden

Waar voor verstoringen in de fysieke wereld uitgebreide wet- en regelgeving en verantwoordelijkheden zijn beschreven, geldt dit niet voor de digitale wereld. Dit brengt kwetsbaarheden met zich mee, die grote gevolgen kunnen hebben voor individuele organisaties, maar door de onderlinge verbondenheid van organisaties ook voor de samenleving als geheel.

- Treed als overheid strenger op tegen organisaties die bewust nalatig zijn in het nemen van cybersecurity maatregelen en handhaaf hierop. De markt lijkt op dit aspect niet goed te functioneren: slechts een beperkte groep afnemers houdt rekening met de veiligheid van hard- en software, terwijl het merendeel van de afnemers dit (o.i. terecht) impliciet aanneemt. Nederland zou een voortrekkende rol in Europa moeten spelen en actief een standpunt moeten bepalen rondom aansprakelijkheidstelling.

- Zorg dat er objectieve kwaliteitscriteria komen die de vakkundigheid en betrouwbaarheid van de cybersecurity dienstverlening op een transparante manier vaststelt. We komen pas tot een digitaal veilig Nederland wanneer afnemers van cybersecuritydiensten snappen welke maatregelen voor hun organisatie het beste werken. Cyberveilig Nederland is met een breed consortium van organisaties betrokken bij het ontwikkelen van een certificeringsysteem voor cybersecuritybedrijven[5].



[5] Het CCV is projectleider om te komen tot een risicomodel en certificering van cybersecurity diensten. Dit project wordt in samenwerking met de volgende organisaties uitgevoerd: VNO NCW, Ministerie van Justitie & Veiligheid, Ministerie van Economische Zaken en Klimaat, CIO Platform, NL Digital, Verbond van Verzekeraars, de Nationale Politie en Partnering Trust.

Onderzoek en innovatie voor een sterkere Nederlandse positie

Het vakgebied van cybersecurity is breder dan dat van techniek alleen en richt zich op mens, techniek en organisatie: van secure softwareontwikkelaars, tot auditors tot gedragswetenschappers. Dit biedt kansen voor innovatie.

- Zorg voor meer overzicht. Het is onduidelijk welke onderzoeken waar gebeuren en wat de relevantie kan zijn voor het cybersecurity bedrijfsleven. Eén aanspreekpunt vanuit de wetenschap waar alle onderzoeksvragen vanuit de sector neergelegd kunnen worden en waar overzicht is wie wat waar doet is een essentiële eerste stap. Hierbij is kennis van zowel de cybersecuritysector, de vraagzijde van cybersecurityontwikkelingen en kennis van het onderzoek domein essentieel. Eén loket waar alle onderzoeksvragen en -behoeften terecht komen.

- Er is weinig samenhang tussen de overheid, de cybersecuritysector en (wetenschappelijk) onderzoek. Door deze samenhang wel te creëren krijg je een duidelijke vraag-allocatie ('waar ben ik mogelijk kwetsbaar voor?') hetgeen tot onderzoeksvragen kan leen en van waaruit nieuwe producten en diensten kunnen worden ontwikkeld. Dit vraagt een versterking van het cyber-ecosysteem.

- Zorg voor meer aandacht voor cybersecurity binnen andere wetenschapsdomeinen. Cybersecurity is een combinatie van mens, organisatie en techniek. Deze moeten meer met elkaar in balans worden gebracht. Hiervoor is het van belang om andere academische domeinen te integreren ('holistische benadering') binnen het cybersecurity domein. Denk hierbij aan gedrag, recht, data-analyse, kunstmatige intelligentie, machine learning, maar ook bij technische studies ten behoeve van bijvoorbeeld security van de Industriële Automatisering & Controle Systemen.

- Versimpel (innovatie) subsidies t.b.v. MKB-bedrijfsleven. De cybersecuritysector in Nederland is grotendeels een MKB-markt. Voor hen is het zeer moeilijk om zicht te krijgen of aanspraak te maken op de verschillende subsidiepotjes die voor innovatie beschikbaar zijn. Dit geldt zowel op provinciaal, nationaal (o.a. DTC/TVO en WBSO), als Europees (Horizon2020) niveau: Ook de vorm waarin de regelingen zich uiten nodigt weinig uit tot deelname. Bij veel regelingen moeten bedrijven naast tijd ook ruime financiële middelen in samenwerkingsprojecten steken. Innovatieve regelingen die beter aansluiten op deze sector zijn daarom nodig.

- Treed als overheid als 'launching customer op' om innovatie in het Nederlandse cyberdomein aan te jagen. Dit versterkt de economische en maatschappelijke kansen van digitalisering en beschermt de nationale veiligheid in het digitale domein. Hiertoe is het noodzakelijk om de essentiële cybersecurity key-capaciteiten vast te stellen en te stimuleren. Voor veel van de (met name technische) oplossingen zijn cybersecurity dienstverleners grotendeels afhankelijk van niet-Europese producten. De huidige mondiale spanningen in acht nemend, kan het voor Nederland verstandig zijn om een meer zelfstandige kennispositie te hebben op verschillende cybersecurity-domeinen.

Over Cyberveilig Nederland

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[6]: tot stand gebracht onder de Cybersecurity Alliantie in samenwerking met 70 publiek-private partners.

[6] Cyberveilignederland.nl/woordenboek-cyberveilig-nederland

Colofon

Dit is een uitgave van Cyberveilig Nederland. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Cyberveilig Nederland kan daarvoor niet aansprakelijk worden gesteld.

Meer informatie over de activiteiten van Cyberveilig Nederland vindt u op *cyberveilignederland.nl*

Contactgegevens
E-mail: *info@cyberveilignederland.nl*
Telefoon: 088 - 118 25 10

Omslagontwerp en opmaak: Cooler Media

CYBERVEILIG NEDERLAND