Digital Trust Center

Veilig digitaal ondernemen

Hand-out versterking cyberweerbaarheid

digital trust center.

Inhoudsopgave

digital trust center.

Subsidieregeling

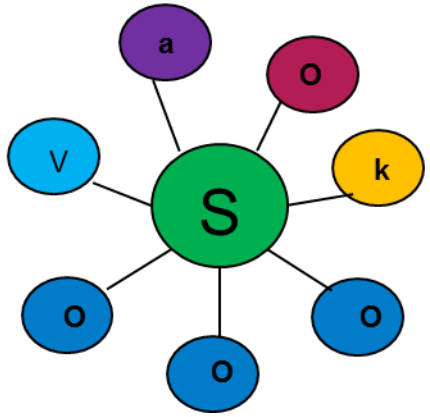
Doel en subsidiabele activiteiten

- Het stimuleren van bewustwording onder niet-vitale ondernemers, waaronder informatievoorziening omtrent cyberdreigingen;
- Het uitvoeren van activiteiten die inzicht geven in digitale kwetsbaarheden;
- Verrichten van diensten om de cyberweerbaarheid binnen specifieke regio's of sectoren te versterken;
- Vormen en in stand houden van een netwerk, alsmede het door derden laten uitvoeren van netwerkactiviteiten;
- Het anderszins versterken van de cyberweerbaarheid van niet-vitale ondernemingen.

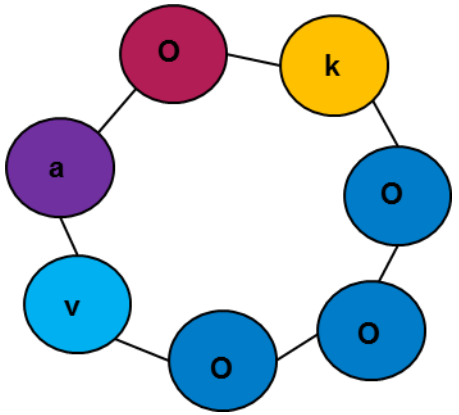
digital trust center.

Subsidieregeling

Wie komt er in aanmerking?



Een rechtspersoon die de cyberweerbaarheid van ondernemingen die in niet-vitale sectoren actief zijn behartigt.



Een samenwerkingsverband van maximaal 8 subsidieontvangers dat de cyberweerbaarheid van ondernemingen die in niet-vitale sectoren actief zijn behartigt.

digital trust center.

Kennisinstelling Aanbieder IT/Cyber Verzekeraar
Samenwerkingsverband Ondernemer Onderwijsinstelling

Subsidieregeling

Beoordelingscriteria

U heeft meer kans op subsidie wanneer u rekening houdt met de volgende punten

Het cyberweerbaarheidsplan moet een grote bijdrage leveren aan het versterken van de cyberweerbaarheid van niet-vitale ondernemingen;

Het netwerk waarbinnen het cyberweerbaarheidsplan wordt uitgevoerd heeft in hoge mate aantoonbaar tot doel, en is door de samenstelling van het netwerk geschikt om, de cyberweerbaarheid van niet-vitale ondernemingen duurzaam te versterken;

Het verband waarbinnen het cyberweerbaarheidsplan wordt uitgevoerd kan een groot netwerk vormen waarbinnen ervaring en kennis over cyberweerbaarheid aanwezig is en wordt uitgewisseld;

Het cyberweerbaarheidsplan is innovatief.

Subsidieregeling

Meer informatie kunt u vinden op de website van RVO:

https://www.rvo.nl/subsidie-en-financieringswijzer/subsidieregeling-cyberweerbaarheid

digital trust center.

Gesubsidieerde samenwerkingsverbanden

Landelijk dekkend stelsel van informatieknooppunten voor ondernemend Nederland op het gebied van cybersecurity

Voordelen samenwerken met DTC

- Mogelijke subsidie;
- Begeleiding en ondersteuning van DTC relatiemanagement;
- Netwerk van samenwerkingsverbanden;
- Informatievoorziening;
  - Actuele nieuwsberichten samengesteld door het NCSC
  - Start of Week
  - Dreigingsinformatie en kwetsbaarheden
- Tools ontwikkeld door het DTC en andere samenwerkingsverbanden;
- Toegang tot de Digital Trust Community en een bijbehorende samenwerkingsruimte;
- 2 netwerkbijeenkomsten per jaar met andere samenwerkingsverbanden;
- Landingspagina op de website van het DTC;
- Co-creatie productontwikkeling.

2020

digital trust
center.

2018

2019

2020

Subsidie 2018

1. Cyber Security Programma NZKG
2. Cybersecurity Center Maakindustrie
3. Cyberweerbaarheid in Limburg
4. NIDV
5. Stichting Cyberweerbaarheid Noord Nederland
6. Groente- Zaadveredelingsbedrijven

Subsidie 2019

7. Cyberweerbaarheidscentrum Brainport
8. NuBNO
9. CYSSEC
10. Cyberweerbaarheidscentrum Drechtsteden
11. Groep Educatieve Uitgeverijen
12. Stichting NBIP
13. Cyberworkplace

Subsidie 2020

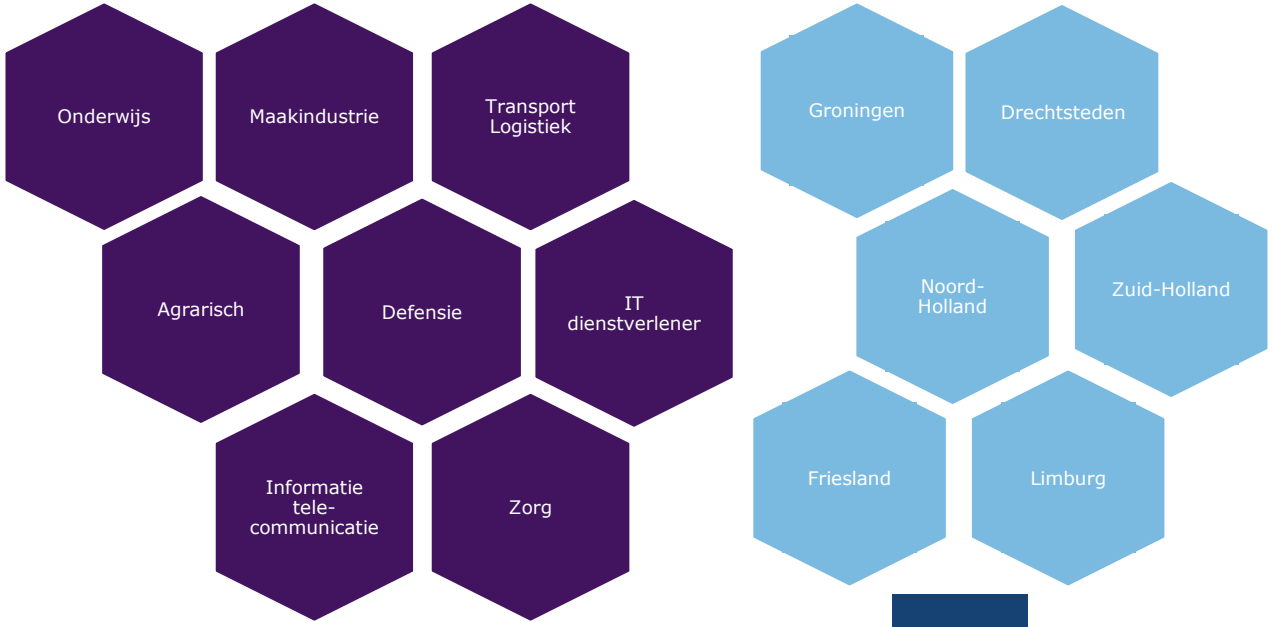
14. Cybernetwerk Zuid Hollandse Eilanden
15. FERM
16. Cyberchain
17. Cyber Heroes
18. Agrifood Cyberweerbaarheid
19. Cyberweerbaarheid in de agrarische sector

Samenwerkingen DTC

20. Connect2Trust
21. Noord Holland Samen Veilig
22. Brancheorganisatie: Transport en Logistiek Nederland
23. Brancheorganisatie: Adfiz
24. Brancheorganisatie: PZO
25. Brancheorganisatie: FHI

26. HI Cybersecurity Network
27. Zorg Cert
28. Brancheorganisatie: NPAL
29. Brancheorganisatie: Bouwend Nederland
30. Brancheorganisatie: Thuiswinkel.org
31. Brancheorganisatie: Techniek Nederland

Huidige dekking, find the gap…



- Dekking van sectoren en regio's binnen Nederland
- Duurzaamheid van het project, financiering na subsidieregeling.
- Producten die opgeleverd worden, aanvulling op bestaande producten.
- Schaalbaarheid van producten, kunnen de producten worden ingezet voor andere ondernemingen in Nederland?

digital trust center.

Cyberweerbaarheid in Limburg

Initiatiefnemer: Platform Veilig Ondernemen Limburg, Brightlands Smart Services Campus, en hun partners

***Sector*:** Sectoroverstijgend, regionaal

Doelstelling: Het project "Cyberweerbaarheid in Limburg" wil een actieve community tot stand brengen waarin ondernemers en andere maatschappelijke organisaties zich kunnen informeren over cybersecurity, verbindingen kunnen leggen met andere bedrijven en ICT dienstverleners, inzicht krijgen in hun individuele situatie door weerbaarheid scans en zelfevaluaties, maar ook met e-learning modules zichzelf en hun medewerkers kunnen trainen.

Activiteiten/Producten: Kennissessies, branche en sectortafels, online forum, nieuwsbrieven, berichtenapplicatie, best practices, service loket, netwerkmogelijkheden, matchmaking (register).

Stap 1: Bewustwording

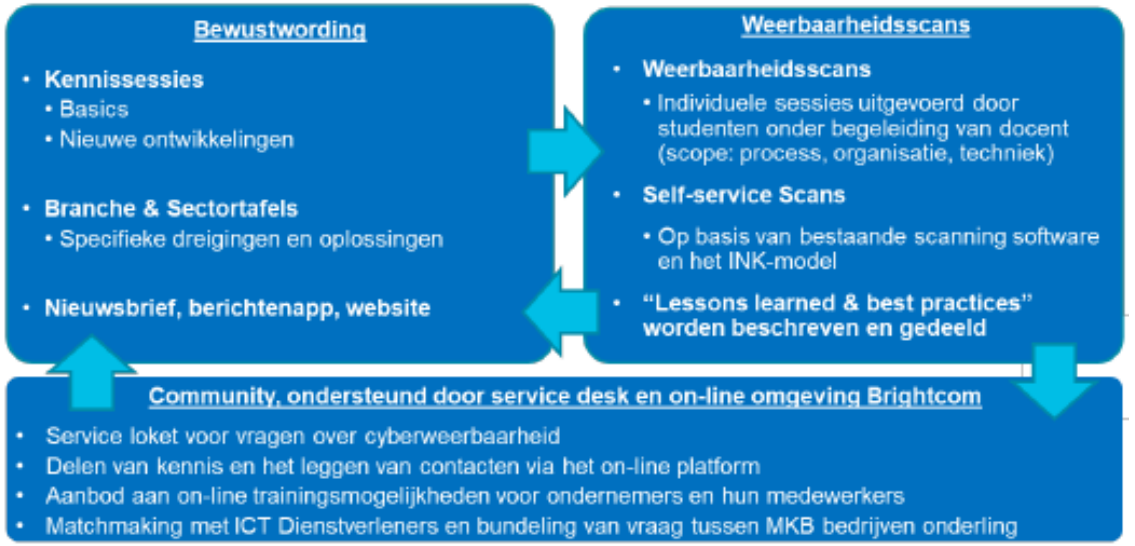
- Algemene kennissessies
- Branche en sectortafels
- Community bouwen via online forum, nieuwsbrief, berichtenapplicatie

Stap 2: Weerbaarheidsscans

- Weerbaarheidsscan (door studenten)
- Self service scan (o.b.v. bestaande software)

Stap 3: Community ondersteuning

- Online omgeving
- Service loket (telefonisch en via mail bereikbaar)
- Trainen en opleiden – ontsluiten van specifieke modules waarmee de ondernemer zichzelf en zijn medewerkers kan trainen
- Match making – koppelen van ondernemers aan ICT dienstverleners uit de regio



digital trust center.

MKB Cyber Campus

Initiatiefnemer: Stichting Cybersafety Noord Nederland, DataDiensten Fryslân, Friesland zorgverze- keraar, Connect.frl, Bedrijvenvereniging west, Samenwerking Noord, Provincie Groningen, Provincie Fryslan, Provincie Drenthe

Sector: Sectoroverstijgend, regionaal

Doelstelling: De stichting wil graag samen met de ondernemers in Noord Nederland werken aan een betere cyber weerbaarheid.

Activiteiten/Producten: Cyber to go roadshow, security scan, security pool, nieuwsbrieven, periodieke bijeenkomsten, cyber escaperoom, 24*7, crisisoefening.

Stap 1: Vormen samenwerkingsverband

Stap 2: Werkpakket 1 – Cyber to Go roadshow
- Voorbereiding
- Uitvoering (continue proces gedurende duur van het programma)

Stap 3: Werkpakket 2 – Security Scan
- Voorbereidingen en selectie
- Pilot uitvoering
- Uitvoering (continue proces gedurende duur van het programma)

Stap 4: Werkpakket 3 – Security Pool
- Voorbereidingen
- Opleiden

Stap 5: Werkpakket 4 – Security Community
- Conferenties
- Netwerkbijeenkomsten
- Kennissessies
- Cyber escaperoom

Stap 6: Werkpakket 5 - Cybercrisis oefening
- Ontwerpen van programma
- Pilot uitvoering
- Uitvoering oefenen
- Analyseren van de gegevens

Stap 7: Werkpakket 6 – Communicatie
- Opstellen plan
- Pilot 24*7 telefonische beschikbaarheid
- Evaluatie pilot over gebruik
- Ontwikkelen middelen (website, app, facebook, twitter, nieuwsbrief)
- Sitrap rapportage politie
- Benaderen bedrijven

Stap 7: Oprichten Cyber Security Expertise Centrum Noord

digital trust center.

Gemeenschap Port of Amsterdam

Initiatiefnemer en deelnemers: Havenbedrijf Amsterdam N.V., Koopman Car Terminal B.V., Tata Steel IJmuiden B.V., Capgemini Nederland B.V. Datacentrum Amsterdam, ICL Fertilizer Europe C.V., Cargill B.V.

***Sector*:** Sectoroverstijgend, regionaal

Doelstelling: Het doel van het programma is het vergroten van de weerbaarheid en gedragsverandering te realiseren door het creëren van bewustwording met betrekking tot Cybersecurity bij bedrijven in het Noordzeekanaalgebied.

Activiteiten/Producten: Optuigen community, table top simulaties, seminars, kick-off bijeenkomsten, trainingsmateriaal (IT, IoT, OT), mailvoorzieningen, oprichten informatieknooppunt, oprichten expertisecentrum (meldpunt), toekomst: CSIRT

Stap 1: Bouwblok 1: Community of practice

- Deelname Port Cyber Summit
- Bijeenkomst 1: creëren van sense of urgency dmv oefenscenario
- Bijeenkomst 2: oefenscenario AMAS en private partijen
- Bijeenkomst 3: Kick-off seminar
- Bijeenkomst 4: bestendigen community of practice

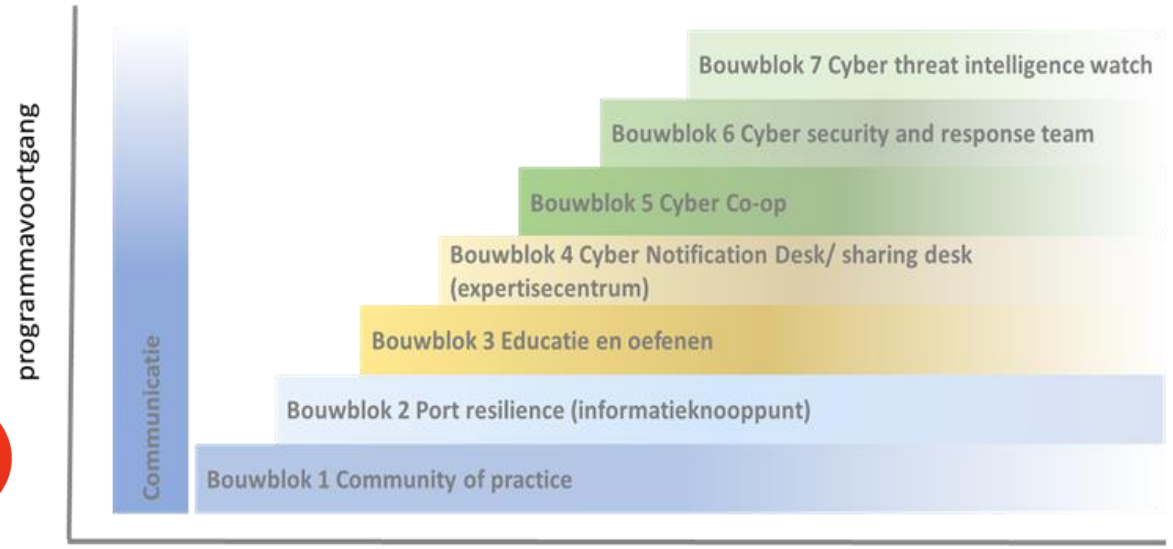
Stap 2: Bouwblok 2: Informatieknooppunt

Stap 3 - Bouwblok 3: Educatie en oefening

Stap 4 - Bouwblok 4: Cybernotificatie

Stap 5: Oprichten van expertisecentrum, dat de basis vormt voor het meldpunt cyberincidenten

- Inrichten Haven Noordzeekanaal ISAC (Q4 2018 optuigen)
- Inrichten meldpunt (eind januari gereed)



digital trust center.

Cybersecurity Center Maakindustrie

Initiatiefnemer: Novel-T, Saxion Hogeschool, Universiteit Twente, CIO Platform, Koninklijke Metaalunie, Ten Hag Advies, BOOST, The Garden, HTSP, Provincie Overijssel

Sector: Maakindustrie gericht op OT

Doelstelling: Bedrijven betrouwbare en onafhankelijke informatie verschaffen over digitale kwetsbaarheden en het geven van concreet handelingsadvies. Het stimuleren van cybersecurity samenwerkingsverbanden tussen bedrijven om van bewust onbekwaam te transformeren naar bewust bekwaam. Eerst Oost en daarna Nederland.

Activiteiten/Producten: Opzetten informatieknooppunt (ISAO), cybersecurityscan, nulmeting, kennissessies.

Stap 1: Kwartiermakersfase

Stap 2: Projectleiding en voorbereiding projectorganisatie

Stap 3: Oprichten ISOA – informatieknooppunt.

- Doelgroep 1: bewust bekwaam
- Doelgroep 2: bewust onbekwaam

Stap 4: Het bieden van handelingsperspectief door kennissessies en security scans/nulmetingen

Stap 5: Het inkopen van cybersecurity uit de markt (gebaseerd op de scan en nulmeting)

- Shared sector SOC
- Ondersteuning van het creëren van bewustwording en gedragsverandering
- Technische advisering bij incidentafhandeling
- Forensisch onderzoek
- Advisering bij woordvoering en interne communicatie
- Ondersteuning van response op dreigingen en incidenten

- Stap 6: Uitrol richting Maakindustrie Nederland

digital trust center.

Cyberweerbaarheid NIDV

Initiatiefnemers: Nederlandse Industrie voor Defensie en Veiligheid

Sector: Nederlandse Defensie & Civiele Veiligheidsgerelateerde Industrie

Doelstelling: Het samenwerkingsverband richt zich op de verbetering van de cyberweerbaarheid van de DVI als geheel, te beginnen met die bedrijven en organisaties die betrokken zijn bij producten en diensten waarbij met Departementaal Vertrouwelijk (DepV) of Staatsgeheim (STG) gerubriceerde informatie gewerkt wordt. De ABDO 2017 is een belangrijk speerpunt.

Activiteiten/Producten: Website, nieuwsbrieven, symposia, kennissessies, ABDO diensten register, communicatiecampagne ABDO register, wijzigingen doorvoeren wet/regelgeving, haalbaarheidsonderzoek ABDO Cloud.

Stap 1: Projectstart

- Website en periodieke nieuwsbrieven
- Monitoring en overleg met NAVO en EDA m.b.t. cybersecurityontwikkelingen.
- Afstemming met andere Digital Trust Centra en NCTV.
- Organiseren van cybersymposia en kennissessies met Nederlandse Defensie en Veiligheidsindustrie

Stap 2: ABDO Register

- Veldonderzoek naar Nederlandse cybersecurity bedrijven en overleg met die bedrijven over voor- en nadelen van opname in het register
- Communicatie met de Nederlandse ABDO bedrijven over het register met Nederlandse cybersecurity bedrijven met hun specialiteiten.
- Communicatie met de plm. 700 Nederlandse ABDO bedrijven over het Register met Nederlandse Cybersecurity bedrijven.
- Haalbaarheidsonderzoek naar mogelijkheid om een "Nederlandse Trusted ABDO Cloud" t.b.v. het MKB op te zetten

Stap 3: Duurzame veranderingen

- Overleg met MIVD over aanpassing regelgeving zodat ABDO2017 autorisatie op aanvraag van Nederlandse bedrijven mogelijk wordt.
- Overleg met MIVD en AIVD over aanpassing regelgeving waar VGB onderzoek.

GroentenZaad veredelingsbedrijven

Initiatiefnemer: Rijk Zwaan Zaadteelt & Zaadhandel, East West Seeds, Pop Vriend Seeds

Sector: Groentenveredelingsbedrijven

Doelstelling: Doelstelling is om op basis van het karakteristieke risicoprofiel van de bedrijven actief in de groenteveredeling een kennisplatform te ontwikkelen, dat als basis kan dienen voor het verbeteren en ontwikkelen voor: risicomanagement en bedrijf continuïteit. Beschermen van IP.

Activiteiten/Producten: Risicoprofielen in kaart brengen, opzetten/aansluiten platform, incident analyses, business continuity plan, response, risicolandschap evalueren.

Stap 1: Opstellen risicoprofiel

Stap 2: Selectie en inrichting kennisplatform

Stap 3: Incident analyses

Stap 4: Bedrijf continuïteit disaster recovery

Stap 5: Response

Stap 6: Evaluatie risicolandschap

Stap 7: Jaarlijkse evaluatie en samenwerking

CYSSEC

Initiatiefnemer: Schiphol

Sector: Sectoroverstijgend, regionaal

Doelstelling: Samenwerkingsverband Schiphol om het algehele cyber weerbaarheids- en volwassenheidsniveau van het Schiphol ecosysteem op een duurzame wijze te verhogen.

Activiteiten/Producten: Informatieknooppunt middels website, nieuwsbrief en LinkedIn. Tools ontwikkelen en delen via online platform. Sessies organiseren. Ambassadeurs werkgroep met CYSSEC campagnes vanuit hun organisaties.

Stap 1: Verzorgen van cybersecurity sessies om kennis te delen en awareness te creëren.

Stap 2: Cybersecurity kennis, nieuws en informatie uitwisselen middels meerdere communicatiemiddelen.

Stap 3: Ontwikkelen, verzamelen en delen van cybersecurity tools en hulpmiddelen.

Stap 4: Door ontwikkelen van het CYSSEC-ambassadeurs netwerk en samen campagnes organiseren.

Stap 5: In samenwerking met onderwijsinstellingen cybersecurity campagnes initiëren.

Stap 6: Cybersecurity (awareness) agenderen bij lokale onderwijsinstellingen.

Stap 7: Verbinden van studenten aan de lokale cybersecurity arbeidsmarkt door stages/(werk)opdrachten/startersfuncties bij organisaties in de community.

Brainport

Initiatiefnemer: ECSG, Brainport Industries, Brainport Development, BDO Accountants & Adviseurs, de Provincie Noord-Brabant en de Metropoolregio Eindhoven

Sector: Bedrijven met 2 of meer medewerkers binnen de hightech industrie

Doelstelling: De belangrijkste doelstelling is het verhogen van de weerbaarheid van de hightech industrie in Nederland tegen cyberaanvallen. Daarbij worden met name de mkb-bedrijven binnen de hightech supply chain ondersteund door dit centrum en via dit centrum door hun corporate klanten.

Activiteiten/Producten: Brainport wil een verhoogde cyberweerbaarheid bereiken door het bieden van een vertrouwde omgeving aan de deelnemers waarin ze kennis, informatie en best-practices met elkaar delen. Deze vertrouwde omgeving bevat tevens een IT-platform waarop realtime nieuw geïdentificeerde risico's, dreigingen en kwetsbaarheden alsmede oplossingen worden gedeeld. Het centrum is zo opgezet dat deelnemers elkaar kunnen ondersteunen bij het voorkomen, detecteren en herstellen van cyberaanvallen.

Cyber Weerbaarheidscentrum Brainport biedt dienstverlening aan binnen de hightech industrie aan hun leden. Dit dienstverlingspakket/lidmaatschap bestaat uit 5 diensten.

1. Identificatie;
2. Bescherming;
3. Detectie;
4. Reactie;
5. Herstel.

Elke dienst bestaat uit basis diensten en additionele diensten die bijgekocht kunnen worden bij het lidmaatschap.

NuBNO

Initiatiefnemer: NuBNO, NAZL Programma Crisisbeheersing en Opleiding Training en Oefening Limburg, Spies Creations,Van Velthuisen Creative

Sector: Zorg- en ziekenhuisinstellingen

Doelstelling: Het doel is om voor zorg- en ziekenhuis instellingen een digitale standaard te ontwikkelen, met bijbehorend awareness- en opleidingsprogramma waardoor zorginstellingen meer cyberweerbaar worden en daardoor kwetsbare patiënten en cliënten minder kans lopen op het mislopen van de juiste zorg op het juiste moment door ontwrichting/uitval van de organisatie.

Activiteiten/Producten: De BNO-tool, een verschuifbare infographic, die als kennisoverdrachtssysteem moet gaan dienen omtrent de organisatorische invulling ten aanzien van digitale veiligheidsrisico's. Kennis en informatie kan hierdoor op een volledig interactieve manier worden verzameld en gedeeld op taak en verantwoordelijkheid vóór, tijdens en ná een digitaal incident. De verkregen informatie, best practices en leermiddelen kunnen vervolgens via de BNO-tool gedeeld worden met de andere deelnemers.

Stap 1: Vooronderzoek en inventarisatie bij zorg en ziekenhuizen Limburg.

Stap 2: Het ontwikkelen van een uniforme infographic naar escalatiemodel van NuBNO/NAZL.

Stap 3: Het ontwikkelen van workshops ten aanzien van Bedrijf Kritische Bedrijfsprocessen.

Stap 4: Het ontwikkelen van een denkkaart volgens model NuBNO/ NAZL.

Stap 5: Het bepalen van de sleutelfiguren en het ontwikkelen van taakkaarten voor elke rol en verantwoordelijkheid.

Stap 6: Het inrichten van de digitale BNO-tool.

Stap 7: Het trainen van een proces verantwoordelijk sleutelfiguur in het gebruik van de Infographic, de BNO-tool en het in stand houden van de cyclus op jaarlijkse of tweejaarlijkse basis.

Groep Educatieve Uitgeverijen (GEU)

Initiatiefnemer: Groep Educatieve Uitgeverijen

Sector: Onderwijs

Doelstelling: De GEU wil de leden ondersteunen bij de volledige invoering en hantering van het certificeringsschema en helpen het beveiligingsniveau van digitale onderwijsmiddelen naar een nog beter niveau te brengen. Daarmee wordt de cyberweerbaarheid van de leden van de GEU verdiept en verstevigd, met als doel dat uiterlijk schooljaar 2022 - 2023 alle GEU-leden deze verdiepingsslag hebben uitgevoerd en nog beter aan scholen kunnen verantwoorden dat de persoonsgegevens die zij verwerken state-of-the art beveiligd zijn.

Activiteiten/Producten: Cyberweerbaarheidsnetwerk, stimuleren bewustwording doelgroep, hulpmiddelen, beveiligingseisen, bedrijfsscan.

Stap 1: Vorming van een cyberweerbaarheidsnetwerk.

De vorming van een cyberweerbaarheidsnetwerk waarin alle leden van de GEU participeren die het privacyconvenant hebben ondertekend en waarin de leden relevant cyber security expertise krijgen aangereikt en kennis en informatie met elkaar delen.

Stap 2: Het stimuleren van bewustwording en het ontwikkelen en beschikbaar stellen van praktisch toepasbare hulpmiddelen.

Het stimuleren van bewustwording van cyberweerbaarheid bij de leden van het cyberweerbaarheidsnetwerk en het ontwikkelen en beschikbaar stellen van praktisch toepasbare hulpmiddelen om de cybersecurity te verbeteren.

Stap 3: Ontwikkelen van een verdieping op de bestaande beveiligingseisen (baseline).

Het ontwikkelen van een verdieping op de bestaande beveiligingsbijlage, met het certificeringschema als basis voor de maatregelen: cyber security baseline.

Stap 4: Uitvoeren van bedrijfsscans.

Het uitvoeren van bedrijfsscans om inzicht te geven in (potentiele) digitale kwetsbaarheden van de leden van het cyberweerbaarheidsnetwerk en om te adviseren over mogelijkheden tot het versterken van de cyberweerbaarheid van de onderneming.

Cyber Netwerk Drechtsteden

Initiatiefnemer: VitrumNet BV, HBO Drechtsteden, Hoek en Blok IT Advisory, IMC Organisatie Personeel Subsidie BV

Sector: Sectoroverstijgend, regionaal

Doelstelling: Het Cyber Netwerk Drechtsteden (CND) is een samenwerkingsverband dat het thema cyberweerbaarheid onder de aandacht wil brengen bij bedrijven in de regio Drechtsteden. Het doel is om bedrijven in de regio bewust te maken van de risico's die digitalisering (van bedrijfsprocessen) en daarmee cyberbedreigingen voor de bedrijfsvoering vormen én hen te voorzien van middelen en tools om die risico's en eventuele economische schade te verkleinen.

Activiteiten/Producten: Nulmeting, cyberweerbaarheidsplan, evenementen, tools, IT afhankelijkheid checklist, weerbaarheidsscan, risico inventarisatie, cursus cyber security, workshops hoe tools in te zetten, publicaties.

Stap 1: Werken aan bewustzijn

- Nulmeting
- Inspiratie dag
- Bijeenkomsten

Stap 2: Tools ter vergroting cyberweerbaarheid

- Pakket aan maatregelen/werkwijzen obv geïdentificeerde risico's
- IT afhankelijke checklist
- Weerbaarheidsscan

Stap 3: Vormen netwerk

Stap 4: Informatie delen

- CND website en DTC platform
- Offline – Events/publicaties/training
- Online – Social media

NBIP

Initiatiefnemer: Nationale Beheersorganisatie Internet Providers (NBIP), Stichting AbuseIO

Sector: Internet Service Providers (ISP's), Hosting Providers, Cloud Providers

Doelstelling: De stichting Nationale Beheersorganisatie Internet Providers (NBIP) en AbuseIO hebben samen met andere stakeholders het plan opgevat om aanbieders van digitale infrastructuur te mobiliseren om meer te gaan doen met het bestrijden van misbruik en cybercriminaliteit in hun netwerken.

Activiteiten/Producten: Platform om informatie te verspreiden naar DSP's.

Stap 1: Het uitbouwen van de informatiedeling functie van www.abuseplatform.nl tot een volledig, functioneel operationeel systeem voor honderden bedrijven.

Stap 2: Het toevoegen van een door TU Delft ontwikkeld meetinstrument voor het meten van de cyberweerbaarheid van de op het platform aangesloten bedrijven, en het gericht verspreiden van die informatie.

Stap 3: Het toevoegen van publieke en andere digitale bronnen met relevante informatie over de netwerken van aangesloten bedrijven.

Stap 4: Het aansluiten van tientallen tot enkele honderden DSP's.

Stap 5: Het geven van inzicht in digitale kwetsbaarheden van niet-vitale ondernemingen.

Cybernetwerk ZHE

Initiatiefnemer: Nemesys Groep, WEA, CompanyCure, Rabobank, De VeiligheidsAlliantie regio Rotterdam, Het Platform Veilig Ondernemen regio Rotterdam, Gemeente Hoeksche Waard, Goeree-Overflakkee, Westvoorne, Brielle, Hellevoetsluis en Nissewaard

Sector: Sectoroverstijgend, regionaal

Doelstelling: Het Cybernetwerk Zuid-Hollandse Eilanden heeft als doelstelling om ondernemers te binden aan een gedegen netwerk. Dit netwerk is van meerwaarde, biedt aanbod op de vraag en weet het verschil te maken.

Activiteiten/Producten: (Fysieke) kennisbijeenkomsten, online Seminars, online trainingen, nulmetingen, nepadvertenties op social media, inforatievestrekking via een online platform, nieuwsbrief, platform.

Stap 1: in de eerste fase wordt basisbewustzijn gecreëerd. Hierin wordt actief basale informatie gedeeld over de risico's van cybercrime voor ondernemers.

Stap 2: nadat de bereidwilligheid is ontstaan om actief maatregelen te nemen, wordt in de tweede fase een verdiepingsslag gemaakt. Naast het aanbieden van handelingsperspectief, wordt hier ook het dialoog aangegaan over complexere onderwerpen als bedrijfscultuur.

FERM

Initiatiefnemer: Havenbedrijf Rotterdam, Gemeente, Rotterdam, Zeehavenpolitie, Veiligheidsregio Rotterdam-Rijnmond, Deltalinqs.

Sector: *West-Nederland, vervoer en logisitek*

Doelstelling: Doel van het programma is het stimuleren van samenwerking tussen bedrijven in de Rotterdamse haven en het verhogen van het bewustzijn met betrekking tot cyberrisico's om zo de best digitaal beveiligde haven van de wereld te worden

Activiteiten/Producten: website, nieuwbrief, Port Cyber Café, acute dreigingen informatie, cyberweerbaarheidsscan, onderlinge anonieme benchmark, vst tarief bij geselecteerde IT en OT security bedrijven voor advies en implementatie, actuele en relevante algemene dreigingsinformatie, jaarlijkse gezamenlijke cyberoefening, jaarlijks Cyber Security Beeld Rotterdamse Haven, collaboratie platform, standaardtraining en -opleiding van praktische kennis

Stap 1: ontwerpen organisatie

Stap 2: inrichten organisatie

Stap 3: begeleiding pilot

Stap 4: roll-out

Stap 5: Schaal en inkoopvoordeel

Cyber Heroes

Initiatiefnemer: *Flavor, Stichting HackShield & Stichting Awareness NL*

Sector: *Sector overstijgend, nationaal*

Doelstelling: *Doelstelling is mkb-ondernemers met de aanpak op inspirerende wijze helpen verder digivaardig te worden en zichzelf te wapenen tegen eventuele gevaren. Hierin spelen kennisdeling, ervaringsuitwisseling, activatie en ons Hero Centred Design een belangrijke rol. Daarbinnen staat de MKB ondernemer als gebruiker centraal, want het draait immers allemaal om de gebruiker meer inzicht te geven hoe hij/zij zichzelf en anderen meer weerbaar kan maken en dus actie te ondernemen.*

Activiteiten/Producten: *Community-activatie door b.v. maandelijkse webinars, HackShield (fan) meet-ups, Inhoudelijke seminars, Netwerk events, Human factor in security award uitreiking, HackShield award-uitreikingen en Metingen en onderzoek.*

Stap 1: Verzamelen en plaatsen content in leerplatform in samenwerking met cyber experts.

Stap 2: Activatie van de eerste brede groep MKB-organisaties via betaand ecosysteem.

Stap 3: Per sector specifiek content aanvullen en uitrollen.

Stap 4: Stap 3 herhaald zich door middel van een verfijning van een blauwdruk sectorspecifieke aanpak. Deze blauwdruk wordt uitgerold per sector. Hierdoor ontstaat er een constante duurzame groei van vakexperts.

Cyberchain

Initiatiefnemer: The Cyber Partners B.V., Demcon Group Boessenkool Machinefabriek B.V., Hollander Techniek B.V. Previder B.V.

Sector: *Sector overstijgend, ketenweerbaarheid*

Doelstelling: De gemeenschappelijke doelstelling van de samenwerkende ondernemingen is om sneller te digitaliseren en de volwassenheid van cyberweerbaarheid in de eigen en de afhankelijke toeleverketen / netwerk te vergroten.

Activiteiten/Producten: *Kick off, Health check; Eerste opzet en iteratie Workshop, Gap analyse (voor de bedrijven), Lezingen / publicaties, Gap analyse, Ontwikkeling self assessment, Ontwikkeling best practices, Embedding in QMS, Workshop: elke 2 maanden, Projectafsluiting.*

Met dit project gaan bedrijven zelf aan de slag vanuit hun eigen behoefte. Door vervolgens de best practices met andere ondernemers te delen, wordt de impact vergroot. Zeker als de deelnemers aan de workshops door hun eigen klanten/partners worden gevraagd om deel te nemen.

Agrifood

Initiatiefnemer: ForFarmers, De Heus, Vion, FrieslandCampina, Nutreco, Eurofins Agro, AgroConnect

Sector: Agrarisch

Doelstelling: Het inperken van de kwetsbaarheid van agrifood-ketens voor cyberaanvallen vraagt om een sectorbrede aanpak. Zeven leidende agribusiness-bedrijven nemen daarom onder begeleiding van de brancheorganisatie AgroConnect het voortouw in het opzetten van een agrifood cybersecurity framework. Losse initiatieven van individuele bedrijven worden gebundeld en versterkt tot een gezamenlijke aanpak van maatregelen die leiden tot een sector standaard.

Activiteiten/Producten: *cybersecurity baseline, assessment tool, workshops*

Cybersecurity baseline

De cybersecurity baseline is bedoeld als een praktische handreiking aan actoren in de agrifood-keten voor het verbeteren van de cyberweerbaarheid.

Cybersecurity assessment tool

Met een assessment tool kan het niveau van de cyberweerbaarheid vastgesteld worden. Als zodanig kan het gezien worden als een momentopname van de ‘as-is’ situatie. Zodra een actor inzicht heeft in het huidige niveau van cyberweerbaarheid, is het relatief eenvoudig vast te stellen wat eventuele tekortkomingen zijn om een hoger niveau van cyberweerbaarheid te bereiken.

Cybersecurity workshops

Tijdens de totstandkoming van de hiervoor genoemde 'deliverables' zullen we regelmatig consultaties houden bij onze achterban in de agrifood-sector. Hiervoor zullen we een reeks cybersecurity workshops organiseren. Tijdens deze workshops is het de bedoeling om zowel input te verzamelen voor het verbeteren en aanscherpen van onze deliverables, als ook het delen van kennis en ervaringen.

Cyberweerbaarheid in de agrarische sector

Initiatiefnemer: LTO Noord, ROC Friese Poort, ROC Friesland College, MKB Cyber Campus

Sector: Agrarisch

Doelstelling: Dit samenwerkingsverband heeft als doel om te bereiken dat de cyberweerbaarheid van de huidige generatie agrariërs aantoonbaar wordt verhoogd. Daarnaast willen ze ervoor zorgen dat de toekomstige generatie agrariërs al eerder kennis krijgen van de risico's van digitalisering. Tevens willen ze dat cyber protectie onderdeel gaat uitmaken van de digitale revolutie (smart farming) van de agrarische sector.

Activiteiten/Producten*: bewustwordingssessies, trainingsmodule, IOT lab, train de trainer*

Via een aantal werkpakketten wil het samenwerkingsverband bereiken dat de cyberweerbaarheid van de huidige generatie agrariërs aantoonbaar wordt verhoogd, maar ook zorgen dat toekomstige generatie agrariërs al eerder kennis krijgen van de risico's van digitalisering. Tevens willen we dat cyber protectie onderdeel gaat uitmaken van de digitale revolutie (smart farming) van de agrarische sector. Ons doel is de agrarische sector cybersafe te maken met behulp van alle spelers in het proces.

1. Bewustwordingssessies Cyber to Go specifiek per sector ontwikkelen;

2. Ontwikkelen Trainingsmodule Cyber in de Agrarische sector;

3. De leveranciers van de agrarische sector centraal;

4. IOT Lab inrichten voor de agrarische sector;

5. Train de trainer voor adviseurs LTO.

https://www.digitaltrustcenter.nl/samenwerkingsverbanden

Contactgegevens

Dennis Huele
Adviseur RVO
cyberweerbaarheid@rvo.nl
088 042 42 42

Jacco van der Kolk
Relatiemanager DTC
j.f.vanderkolk@minezk.nl
06 1104 2315

Rajko Smaak
Relatiemanager DTC
r.smaak@minezk.nl
06 2920 6573

Kim van der Veen
Relatiemanager DTC
k.m.vanderveen@minezk.nl
06 2564 2512