OpStap naar weerbaarheid

Samenwerking in cyberweerbaarheid in branches en tussen ketenpartners

Jacco van der Kolk
Digital Trust Center

Alexis Barron
Cyberweerbaarheidscentrum Brainport

Zaalvoorzitter: Rob Augustinus, Agentschap Telecom

#OpStap2019

Veilig Digitaal Ondernemen

Op naar een cyberweerbaar bedrijfsleven

Symposium Telekwetsbaarheid

07-11-2019

digital trust center.

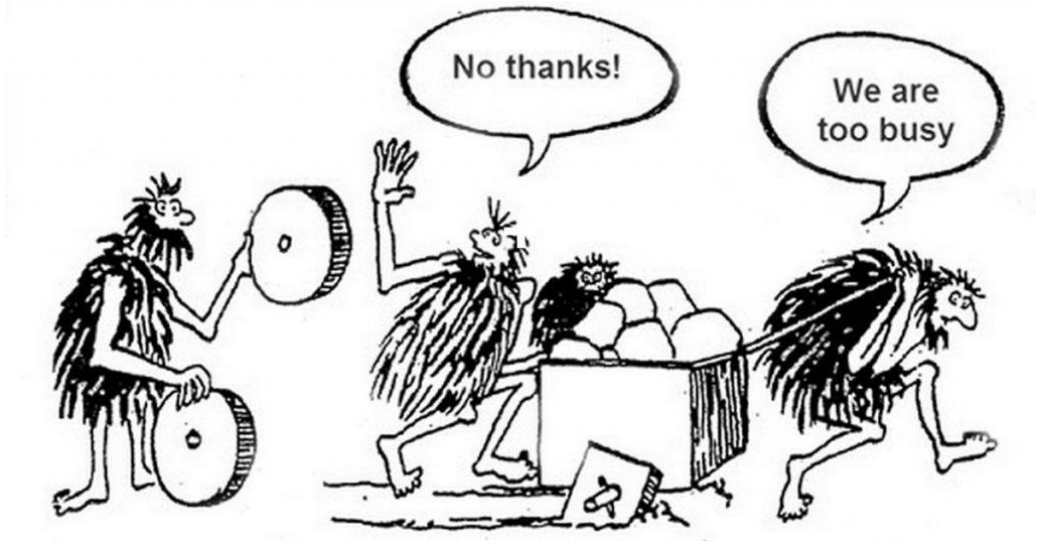
Wat gaan we vertellen?

1. **Wat is het Digital Trust Center (DTC)?**
2. **Waarom stimuleren we samenwerken?**
3. **Hoe kunnen wij jullie helpen?**
4. **Hoe hebben anderen dit aangepakt?**
5. **Hoe willen jullie het aan gaan pakken?**

digital trust center.

Het DTC stelt ondernemend Nederland in staat om haar digitale veiligheid te vergroten.

Ondernemers die samenwerken maken meer mogelijk



WAAROM
MOEILIJK DOEN

ALS
HET SAMEN KAN

Loesje

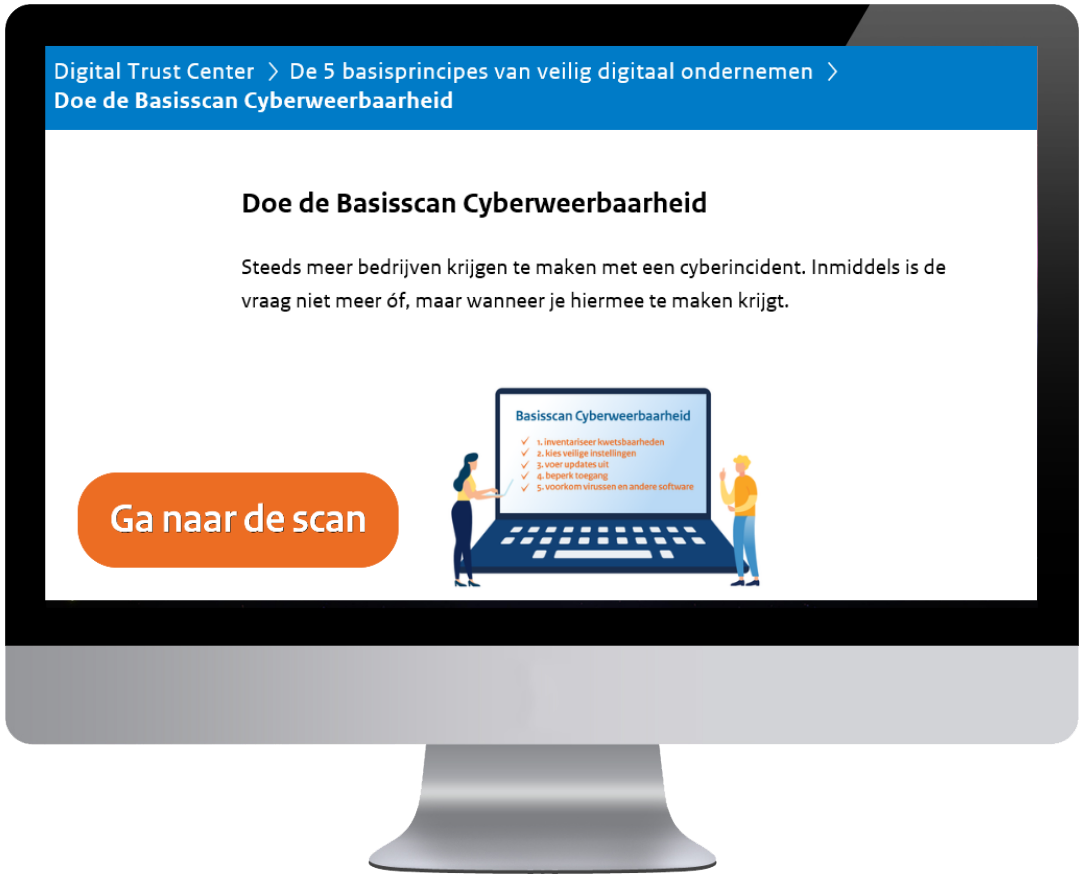
Het DTC kan jullie helpen om ondernemers digitaal veiliger te maken

digital trust
center.

… door subsidie beschikbaar te stellen die samenwerking stimuleert

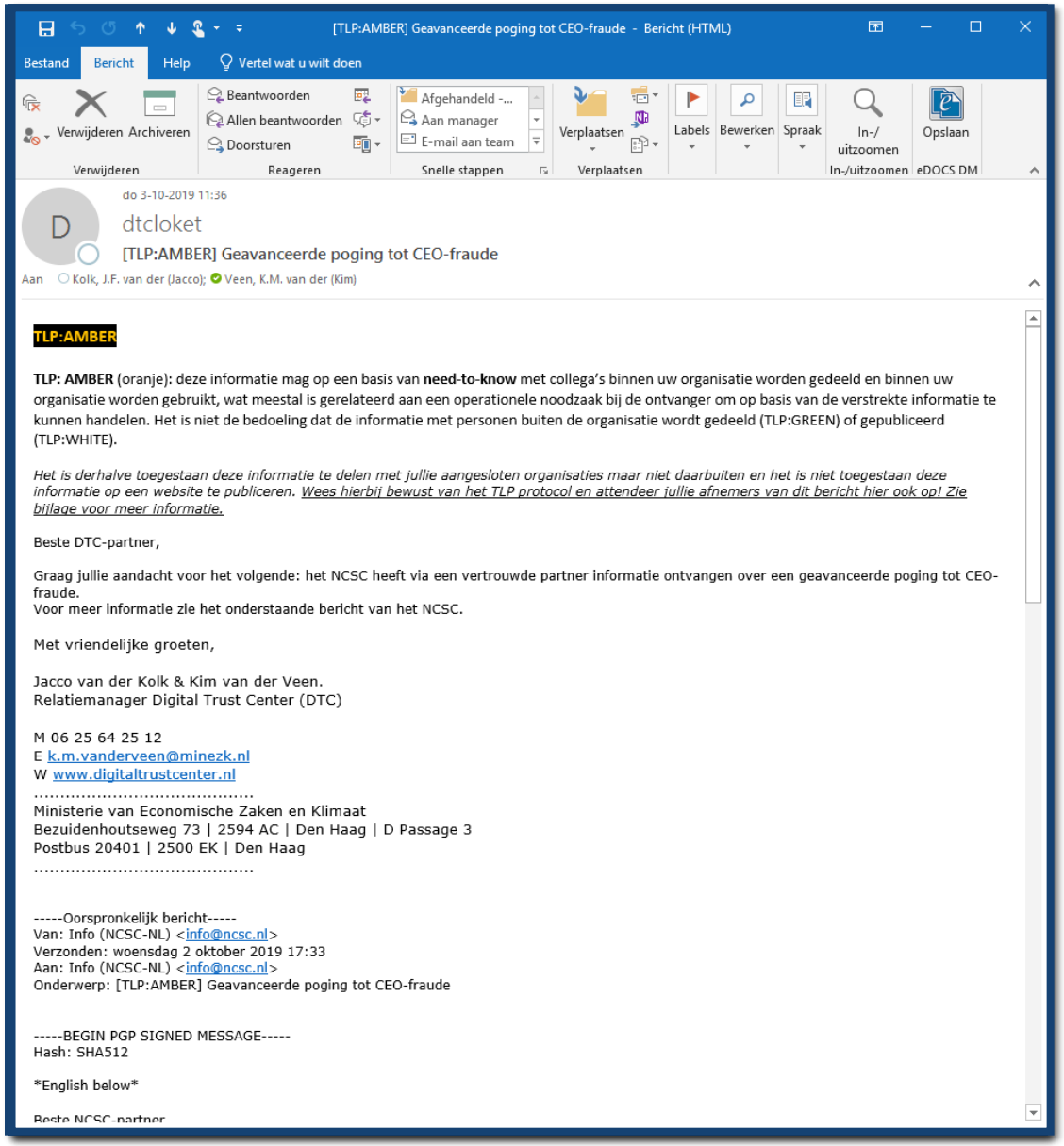
digital trust center.

… door onze kennis beschikbaar te stellen



digital trust center.

… door jullie te voorzien van specifieke informatie



[TLP:AMBER] Geavanceerde poging tot CEO-fraude - Bericht (HTML)

Bestand | Bericht | Help | Vertel wat u wilt doen

Verwijderen | Archiveren | Beantwoorden | Allen beantwoorden | Doorsturen | Afgehandeld -... | Aan manager | E-mail aan team | Verplaatsen | Labels | Bewerken | Spraak | In-/uitzoomen | Opslaan

Verwijderen | Reageren | Snelle stappen | Verplaatsen | In-/uitzoomen | eDOCS DM

do 3-10-2019 11:36

dtcloket

[TLP:AMBER] Geavanceerde poging tot CEO-fraude

Aan Kolk, J.F. van der (Jacco); Veen, K.M. van der (Kim)

TLP:AMBER

TLP: AMBER (oranje): deze informatie mag op een basis van **need-to-know** met collega's binnen uw organisatie worden gedeeld en binnen uw organisatie worden gebruikt, wat meestal is gerelateerd aan een operationele noodzaak bij de ontvanger om op basis van de verstrekte informatie te kunnen handelen. Het is niet de bedoeling dat de informatie met personen buiten de organisatie wordt gedeeld (TLP:GREEN) of gepubliceerd (TLP:WHITE).

Het is derhalve toegestaan deze informatie te delen met jullie aangesloten organisaties maar niet daarbuiten en het is niet toegestaan deze informatie op een website te publiceren. Wees hierbij bewust van het TLP protocol en attendeer jullie afnemers van dit bericht hier ook op! Zie bijlage voor meer informatie.

Beste DTC-partner,

Graag jullie aandacht voor het volgende: het NCSC heeft via een vertrouwde partner informatie ontvangen over een geavanceerde poging tot CEO-fraude.
Voor meer informatie zie het onderstaande bericht van het NCSC.

Met vriendelijke groeten,

Jacco van der Kolk & Kim van der Veen.
Relatiemanager Digital Trust Center (DTC)

M 06 25 64 25 12
E k.m.vanderveen@minezk.nl
W www.digitaltrustcenter.nl
.....
Ministerie van Economische Zaken en Klimaat
Bezuidenhoutseweg 73 | 2594 AC | Den Haag | D Passage 3
Postbus 20401 | 2500 EK | Den Haag
.....

-----Oorspronkelijk bericht-----
Van: Info (NCSC-NL) <info@ncsc.nl>
Verzonden: woensdag 2 oktober 2019 17:33
Aan: Info (NCSC-NL) <info@ncsc.nl>
Onderwerp: [TLP:AMBER] Geavanceerde poging tot CEO-fraude

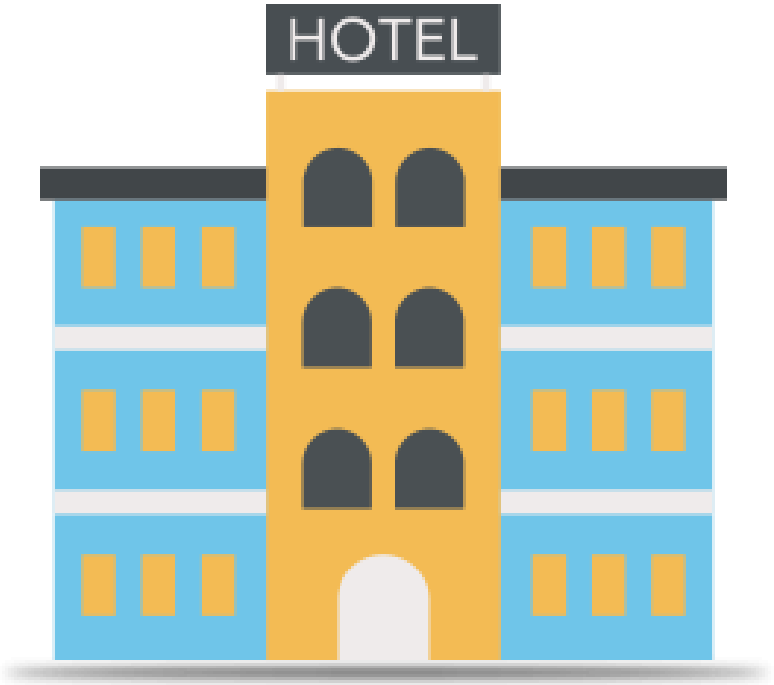
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

English below

Beste NCSC-partner

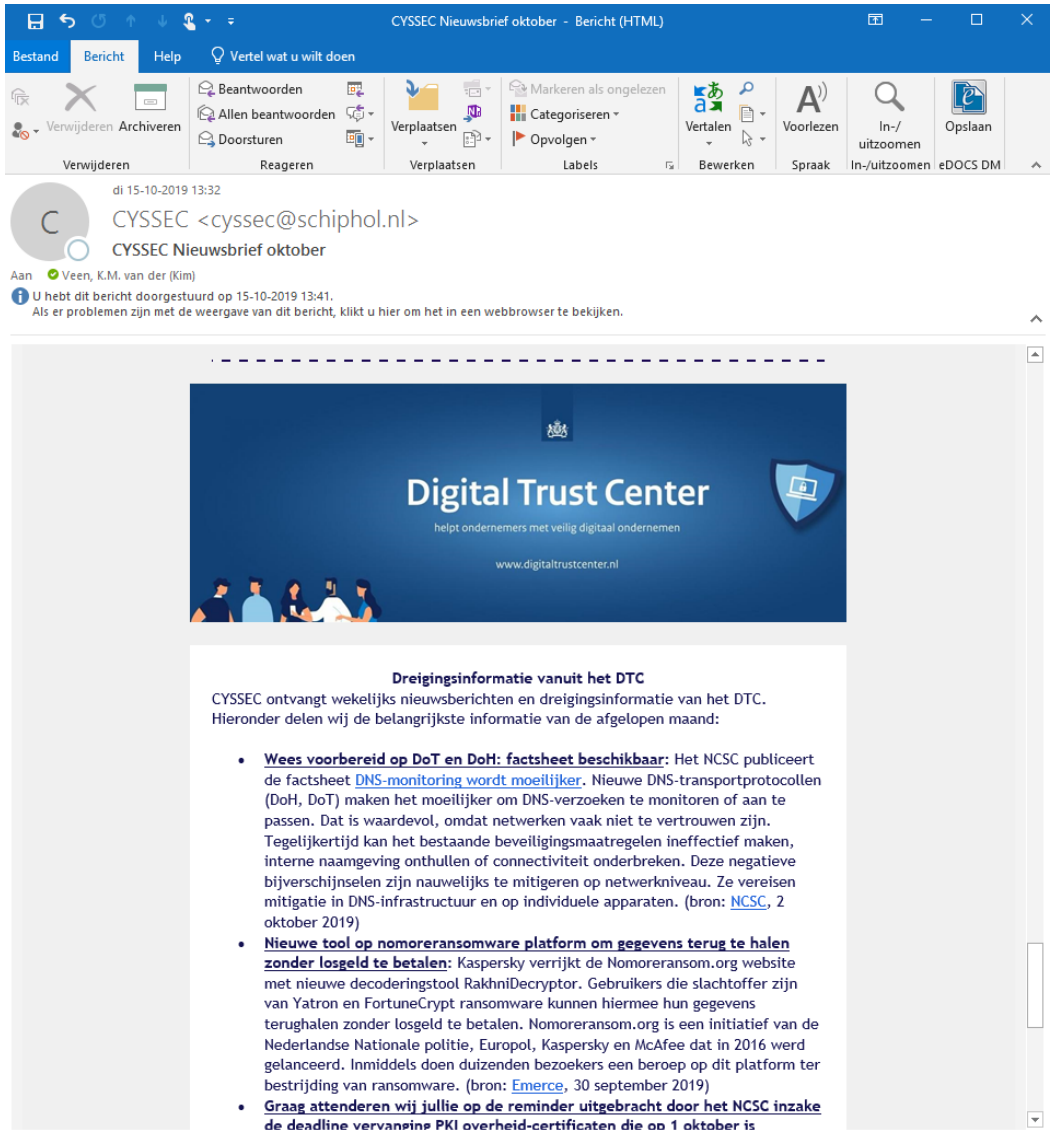
digital trust center.

… door jullie toegang te geven tot de Digital Trust Community



Waarom moeilijk doen als het samen kan?

digital trust
center.



Ter inspiratie

Samenwerkingsverband CYSSEC

GEZOCHT: BEDRIJVEN DIE ETHISCH GEHACKT WILLEN WORDEN

CYBERSECURITY: DE BASIS OP ORDE

Ruim 40 procent van de bedrijven in de logistiek heeft wel eens te maken gehad met cybercriminaliteit. Volgens onderzoek van de Haagse Hogeschool zal dit in de toekomst vaker voorkomen.

Nederland is een logistieke hotspot met zijn geografische ligging en infrastructuur. Digitalisering is daarbij een belangrijke factor. Nederland moet daarom vooroplopen op het gebied van digitale security om nu en in de toekomst aantrekkelijk te blijven. Het Digital Trust Center (DTC) – een initiatief van het ministerie van Economische Zaken en Klimaat – kan hierbij helpen. Het DTC is er om het Nederlandse bedrijfsleven weerbaarder te maken tegen cyberdreigingen. Dit voorziet ondernemers van praktische informatie en advies via www.digitaltrustcenter.nl.

BASISPRINCIPES EN SCAN

Het DTC heeft vijf basisprincipes opgesteld die ondernemers helpen de basisbeveiliging voor veilig digitaal ondernemen op orde te krijgen. Ondernemers die deze basisprincipes opvolgen, vergroten hun weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren. De basisprincipes zijn zo opgesteld dat iedere ondernemer, van zzp'er tot mkb'er, ermee uit de voeten kan. De maatregelen zijn toegankelijk en praktisch en staan opgesomd in illustratie bij dit artikel. Om ondernemers in korte tijd inzicht te geven in hun digitale veiligheid, kunnen zij ook gebruikmaken van een nieuwe cybersecurityscan die het DTC heeft ontwikkeld. Het is ook een goed middel om bedrijven aan te sporen tot het nemen van concrete acties om hun digitale weerbaarheid te vergroten. Met de 'basis op orde'-scan kunnen ondernemers direct aan de slag. Hiermee worden zij geholpen om inzicht te verkrijgen in waar de onderneming staat op het gebied van cybersecurity, maar de scan genereert naast praktische tips ook een uitgebreid adviesrapport over hoe een ondernemer de digitale veiligheid binnen zijn organisatie kan vergroten. De scan is te vinden op de website van het DTC: www.digitaltrustcenter.nl.

ONDERZOEK VIA HACK

Bedrijven kunnen ook op een andere manier hun digitale veiligheid vergroten, namelijk door mee te doen aan een zogenoemde ethische hack in het kader van een onderzoek door TNO samen met andere organisaties in de logistiek. Dit betreft een onderzoek naar de IT-security van bedrijven in de logistieke keten, dat moet leiden tot praktische handvatten voor logistieke bedrijven om de meest kritieke problemen in de keten te verhelpen en de cybersecurity te verbeteren. Het project wordt mede gefinancierd uit de Toeslag voor Topconsortia voor Kennis en Innovatie (TKI's) van het ministerie van Economische zaken. Voor het onderzoek is TNO op zoek naar logistieke bedrijven die zicht willen krijgen op hun IT-security via de uitvoering van een ethische hack – een gesimuleerde cyberaanval – door specialisten. Daarvoor is een tool in ontwikkeling die onderzoekt welke systemen door malware, bijvoorbeeld het 'WannaCry'-virus, aangetast kunnen worden. Deze tool, die bijna klaar is, wordt op het interne netwerk uitgevoerd. Vanzelfsprekend brengt de tool geen daadwerkelijke schade toe aan de systemen.

RESULTATEN

Na de ethische hack ontvangt het deelnemende bedrijf een overzicht van de resultaten. Het overzicht bevat ook een interpretatie van de resultaten om een duidelijk beeld te krijgen van de impact die een dergelijk incident op het interne netwerk kan hebben. De verworven informatie kan dus gebruikt worden om de security te verbeteren. Mogelijke uitkomsten zijn bijvoorbeeld dat de bestanden binnen het TMS niet meer beschikbaar zijn, er geen toegang meer is tot de vrachtbrieven of dat de voorraden in het voorraadsysteem niet meer inzichtelijk zijn.
De resultaten van de 'ethische hack' worden door TNO anoniem verwerkt voor het onderzoek dat het consortium met TNO uitvoert. Naast de 'ethische hack' neemt een TNO-medewerker een interview af om inzicht krijgen hoe de cybersecurity is georganiseerd.

PRAKTISCHE HANDVATTEN

De ethische hacks worden uitgevoerd door deskundige IT-securityspecialisten van Reqon Security. Zij ontwikkelen de tool en testen deze grondig. Uiteraard zijn zij bereid om een geheimhoudingsverklaring (NDA) te ondertekenen. Dat geldt ook voor de

DE DOOR EEN ETHISCHE HACK VERWORVEN INFORMATIE KAN WORDEN GEBRUIKT OM DE SECURITY TE VERBETEREN

Ter inspiratie

Brancheorganisatie Transport Logistiek Nederland

Ter inspiratie

Brancheorganisatie Adfiz

Hoe kan het DTC jullie verder helpen om ondernemers digitaal weerbaarder te maken?

digital trust
center.

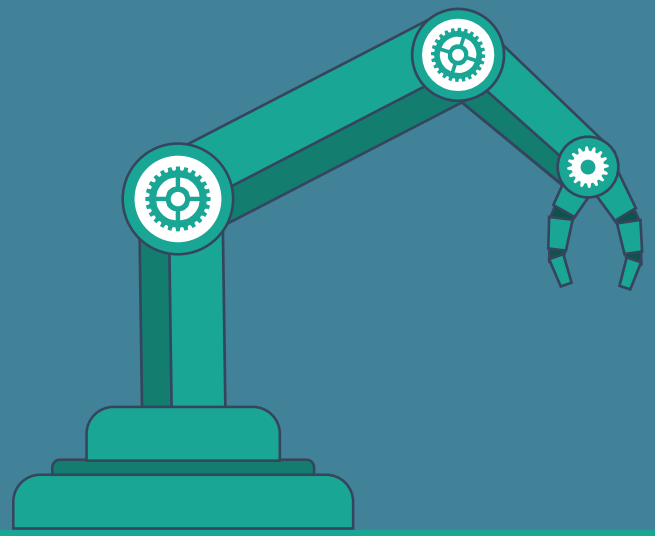
Vragen??

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

digital trust center.



Cyber Weerbaarheidscentrum Brainport

CYBER
WEERBAARHEIDSCENTRUM
BRAINPORT
voor de hightech industrie in Nederland

Cyber Weerbaarheidscentrum Brainport

Met elkaar, voor elkaar, door elkaar

Alexis Barron

Work Experience

2019
Cyber Weerbaarheidscentrum
Directeur

2012 – 2019
ASML Netherlands
Security Awareness Manager

Background

UK born

Security (awareness) & Communication

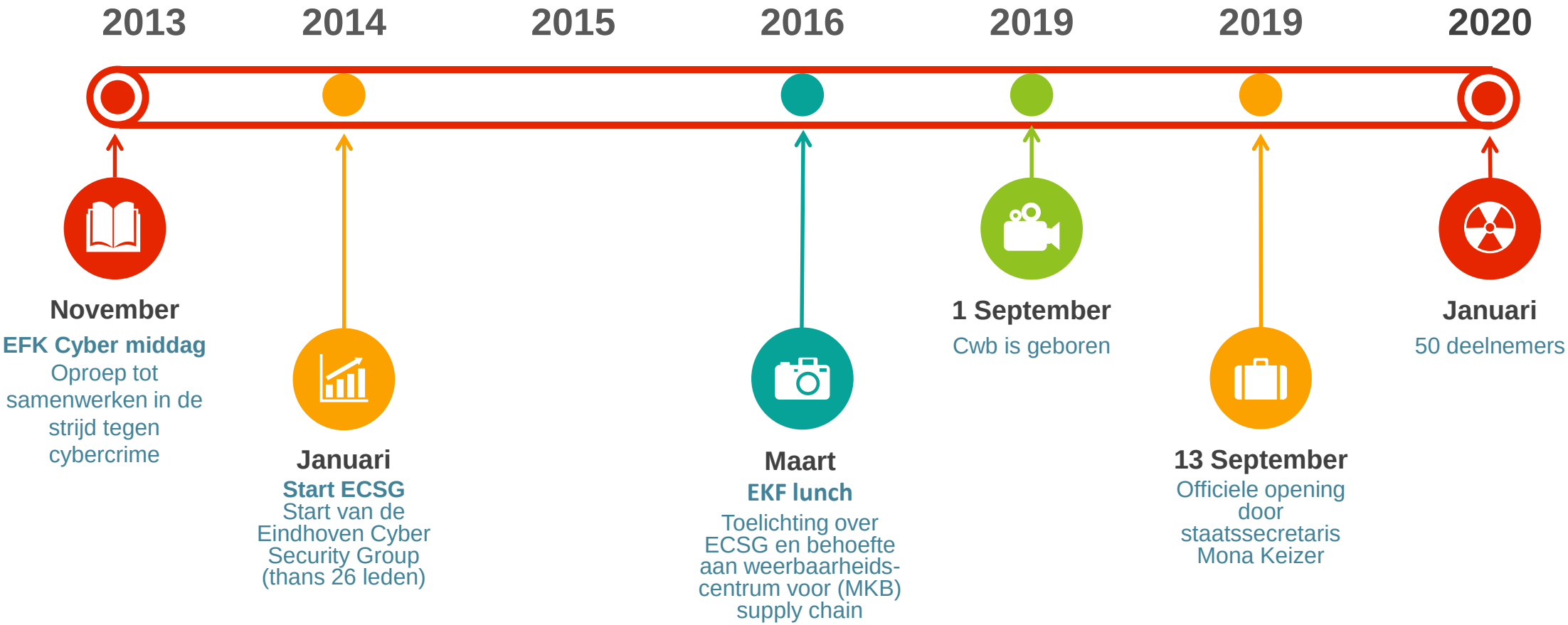
01 Hoe zijn we begonnen

02 Hoe werken we samen

03 Wat doen we

04 Waar gaan we naartoe

Timeline


2013
2014
2015
2016
2019
2019
2020
November
EFK Cyber middag
Oproep tot samenwerken in de strijd tegen cybercrime
Januari
Start ECSG
Start van de Eindhoven Cyber Security Group (thans 26 leden)
Maart
EKF lunch
Toelichting over ECSG en behoefte aan weerbaarheids-centrum voor (MKB) supply chain
1 September
Cwb is geboren
13 September
Officiele opening door staatssecretaris Mona Keizer
Januari
50 deelnemers

Waarom het MKB

Digitalisering brengt economische en maatschappelijke kansen

Maar ook bedreigingen, onder meer door spionage en sabotage

Informatie-uitwisseling en samenwerking is de sleutel naar cyber weerbaarheid

Voor het MKB is het niet/nauwelijks mogelijk dit zelfstandig te organiseren

Maar wel noodzakelijk om je ‘license to operate’ te behouden

Niets doen is geen optie !

Pilot

12 first users uit de high-tech industrie

Digital Trust Center

TNO

Requirements

Naar een meer volwassen informatie-uitwisseling binnen de keten van toeleveranciers voor de leden

Deelname voor (mkb) toeleveranciers - de supply chain van de leden

Gebruik makend van regionale kennis en ICT/Consultancy bedrijven

Bron voor beveiligingsadvies en kennisoverdracht

- Structureel delen van threat intel (code rood)
- Ontvangen van code Amber informatie

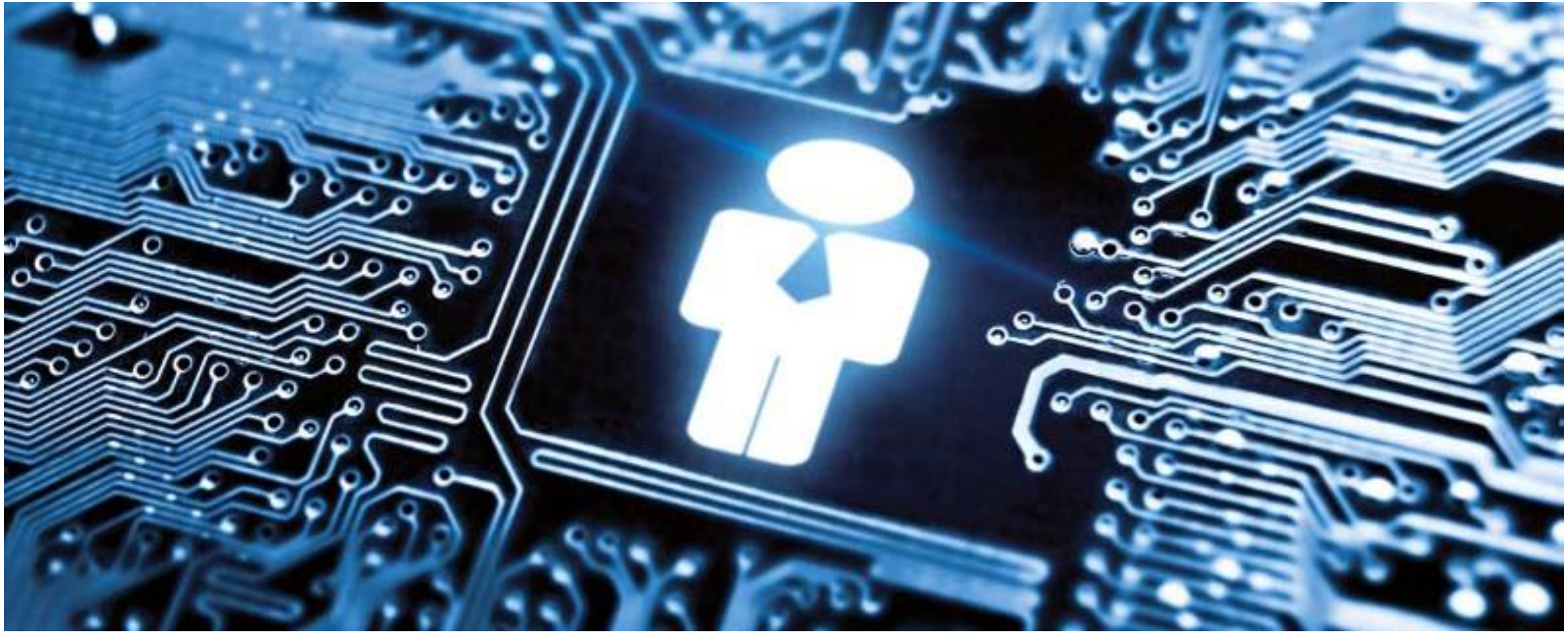
Ondersteuning

- Hulp bij creëren van bewustwording
- Hulp bij reactie op dreigingen en incidenten
- Hulp bij analyse kwetsbaarheden
- 24-uurs hulp bij ICT-beveiligingsincidenten / forensisch onderzoek

Actieve monitoring van ICT systemen

Collectieve inkoop cyber security producten / cyber security diensten

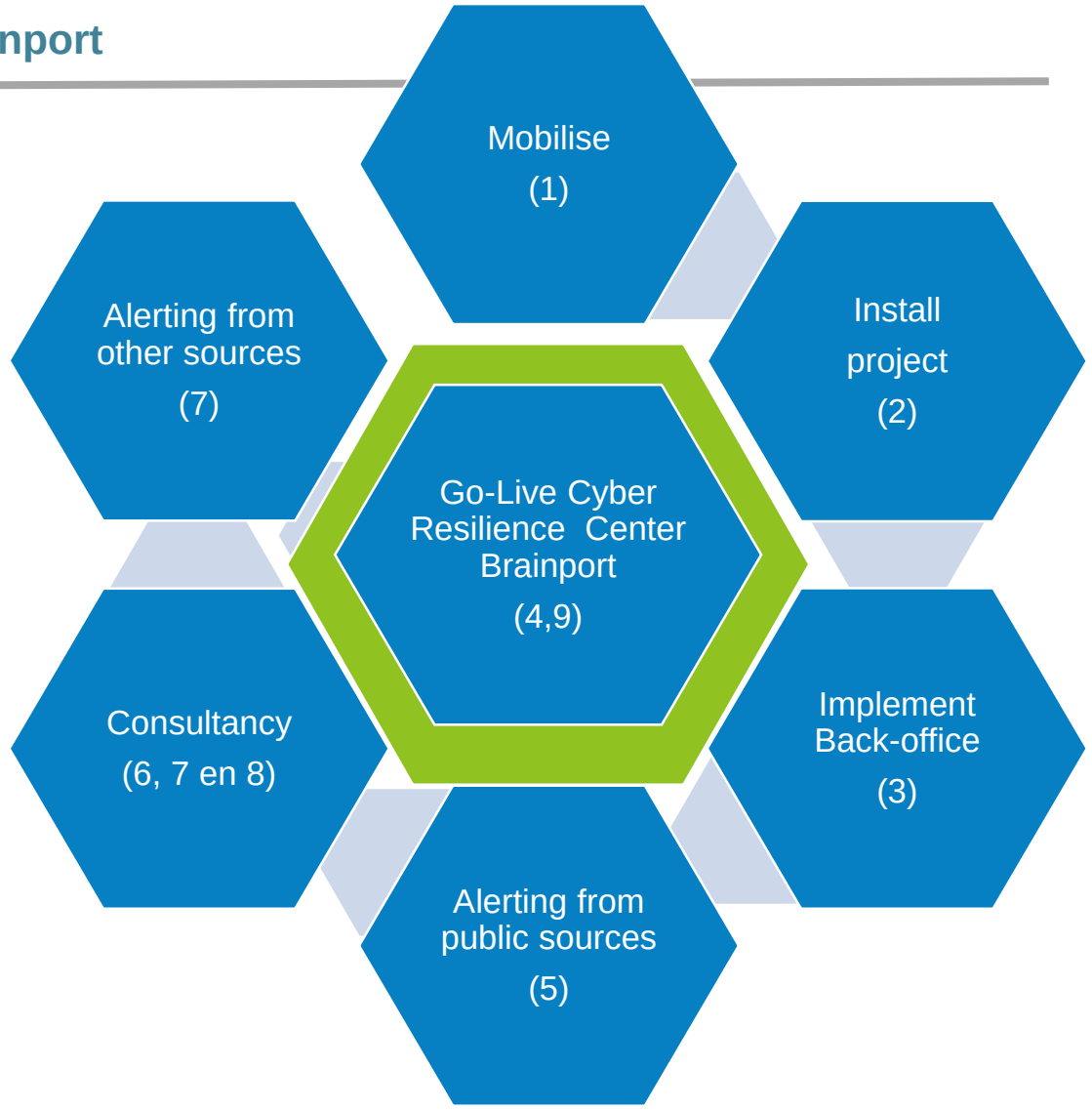
Blauwdruk voor alle cyber weerbaarheidscentra in NL



10-stappen Benadering

In 10 stappen naar een ‘Cyber Weerbaarheidscentrum Brainport

1. Mobiliseer stakeholders & regel startbudget
2. Eerste gebruikersgroep & projectgroep installeren
3. Back-office implementeren (database)
4. Ontwerp duurzame business case
5. Waarschuwingen uit openbare bronnen implementeren
6. Consultancy implementeren
7. Meldingen van andere bronnen implementeren
8. Crisismanagement implementeren
9. Ga live-centrum, lever plannen en blauwdruk op
10. Begin met uitrollen naar supply chains



Ministerie van Economische Zaken en Klimaat

BRAINPORT EINDHOVEN

BDO

Digital Trust Center

Provincie Noord-Brabant

Brainport Industries

METROPOOL REGIO EINDHOVEN

Het Cyber Weerbaarheidscentrum is daarna mede opgericht als stichting met deze partners met als doel:

Het verhogen van de weerbaarheid van het MKB tegen cyber criminaliteit van de high-tech industrie in Nederland

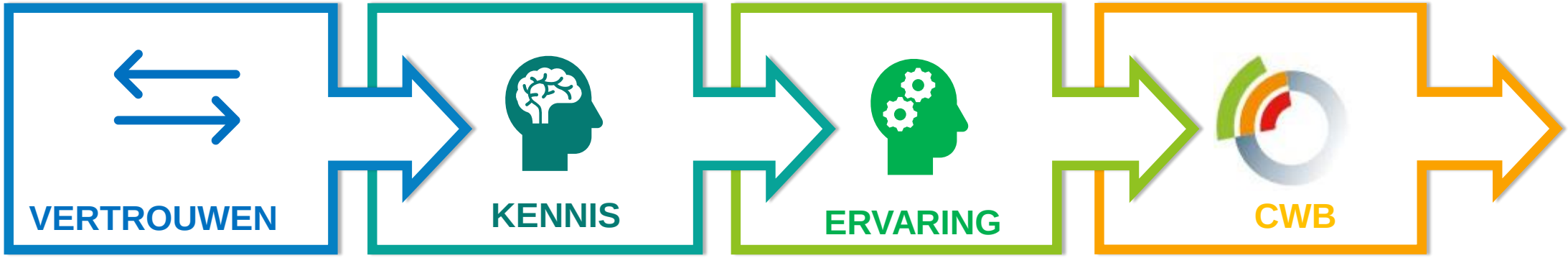
Wat doet het CWB?

IDENTIFICATIE	BESCHERMING	DETECTIE	REAKTIE & HERSTEL

- Intake (healthcheck)
- Delen van threat intelligence van elkaar
- Delen van threat intelligence van het Digital Trust Center (DTC)
- Delen van threat intelligence van het NCSC
- Delen van best practices
- Delen van contactgegevens
- Intervisiegroepen
- Jaarlijks sectoraal dreigingsbeeld
- Verwijzing naar geschikte leverancier

IDENTIFICATIE	BESCHERMING	DETECTIE	REAKTIE & HERSTEL

Groeimodel



VERTROUWEN

- Netwerk met onderling vertrouwen
- Faciliteren van expert sessies
- Vergroten van bewustwording
- Elkaar ondersteunen
- Ad-hoc kennis uitwisselen

KENNIS

- Alles van 1 plus:
- Structureel (digitaal) delen van dreigingen informatie
- Delen van operationele alerts voor hightech maakindustrie
- Digitaal portaal met kennis, best practices

ERVARING

- Alles van 1 en 2 plus:
- Digitaal portaal en ervaringen en aanbevelingen..

CYBER WEERBAARHEIDSCENTRUM BRAINPORT

- Gezamenlijke security diensten voor ketenpartners
- (112 functie)

Samenwerkingsverbanden

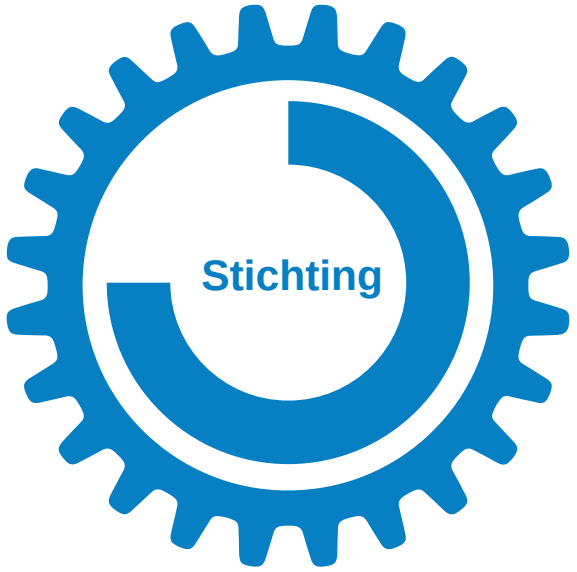
O.a.

- Cyber Security Center Maakindustrie
- Cyberweerbaarheid Ned. Defensie & Veiligheidsindustrie (DVI)
- Cyber Security Awareness Havengemeenschap Port of Amsterdam
- Vergroting Cyberweerbaarheid Groentezaadverdelingsbedrijven
- Cyberweerbaarheid door samenwerking in Noord-Nederland

Organisatie Model

Zeer compacte (flexibele) support organisatie

- Directeur (dienstverlening, marketing & sales)
- Front office (IT, marketing & sales)
- Back office (Communicatie, organisatie & administratie)



- Stichting
- Eén directeur
- Raad van Toezicht met 3 leden

Waarom aansluiten?

Uw bedrijf is onderdeel van de high-tech industry in Nederland

Uitval van ICT systemen (op specifieke moment- en) kan exceptionele ge -volgen hebben voor de omzet en/of bedrijfsvoer ing van uw organisatie

Uw klant eist een (aant oonbare) mate van info rmatie-beveiliging

U wilt verlies van Intellectueel Eigendom voorkomen en u ziet interesse in uw Intellectuele Eigendo m bij andere partijen

U wilt uw kennis delen maar ook leren van de kennis en ervaring van anderen.

WEERBAAR DOOR SAMENWERKING!

Thank You

Cyber Weerbaarheidscentrum Brainport

Voor de hightech industrie in Nederland

Stichting Cyber Weerbaarheidscentrum Brainport

Opgericht door Brainport Development in samenwerking met Provincie Noord-Brabant, MRE, Brainport Industries, BDO Advisory, Ministerie van Economische Zaken en Klimaat en het Ministerie van Justitie & Veiligheid.

Alexis Barron, Directeur
alexis.barron@cwbrainport.nl
www.cwbrainport.nl

CYBER WEERBAARHEIDSCENTRUM BRAINPORT
voor de hightech industrie in Nederland