CYBER WEERBAARHEIDSCENTRUM BRAINPORT

voor de hightech maakindustrie in Nederland

ISACA bijeenkomst 28 januari 2019

Robert Jan Marringa - projectleider Cyber Weerbaarheidscentrum Brainport – Partner Two For Innovation

Ewoud Smit – lid projectteam Cyber Weerbaarheidscentrum Brainport – Manager Cyber Defense Operations - ASML

Onderwerpen

- Waarom een Cyber Weerbaarheidscentrum Brainport?
- De aanpak
- De propositie (in ontwikkeling)
- Leerervaringen tot nu toe

Advies Cyber Security Raad: Verbeter informatie-uitwisseling

Constatering:

- Urgentie is hoog
- Tijdig beschikken over de juiste informatie is van groot belang voor de digitale weerbaarheid van organisaties
- Digitale weerbaarheid is één van de pijlers van een welvarend Nederland

Advies: Verbeter informatie-uitwisseling door uitbreiden van Information Sharing & Analysis Centers (zoals ECSG)

Eindhoven Cyber Security Group

Regionale ISAC in regio Eindhoven (met flinke focus op Hightech maakindustrie)

1. In Eindhoven zijn we in november 2013 gestart met een regionale ISAC
   - met steun van Top Management bedrijven
   - als publiek-private samenwerking met de regionale accountmanager van de AIVD
   - met gesloten beurzen
2. Gezamenlijke problematiek:
   - IP bescherming is top priority voor High Tech sector
   - Bedrijven zijn veelal afhankelijk van (regionale) toeleveranciers
   - Kleinere bedrijven kunnen zich (nog) niet zelfstandig beschermen; Samen sterk!
3. Primaire doel ECSG:
   - informatie uitwisselen over kwetsbaarheden, incidenten en best-practices om zodoende elkaars Intellectuele Eigendommen voldoende veilig te stellen
   - samen de cyberweerbaarheid van de regionale toeleveringsketen te vergroten
4. Ambitie: uitgroeien naar een professionele Cybersecurity ‘ISAC’organisatie voor:
   - Top Sector High Tech Systemen & Materialen
   - Brainport regio

BDO

Hoe pakken we dat aan?

- We richten een organisatie in met een **coöperatieve filosofie**
- We zorgen **samen** voor cyberweerbaarheid in de Nederlandse hightech maakindustrie te beginnen in de Brainport regio Eindhoven
- We **delen** informatie met elkaar
- We zorgen dat we **toegang** krijgen tot alle voor ons relevante informatie

Waarom een Cyber Weerbaarheidscentrum Brainport?

Waar geloven we in?

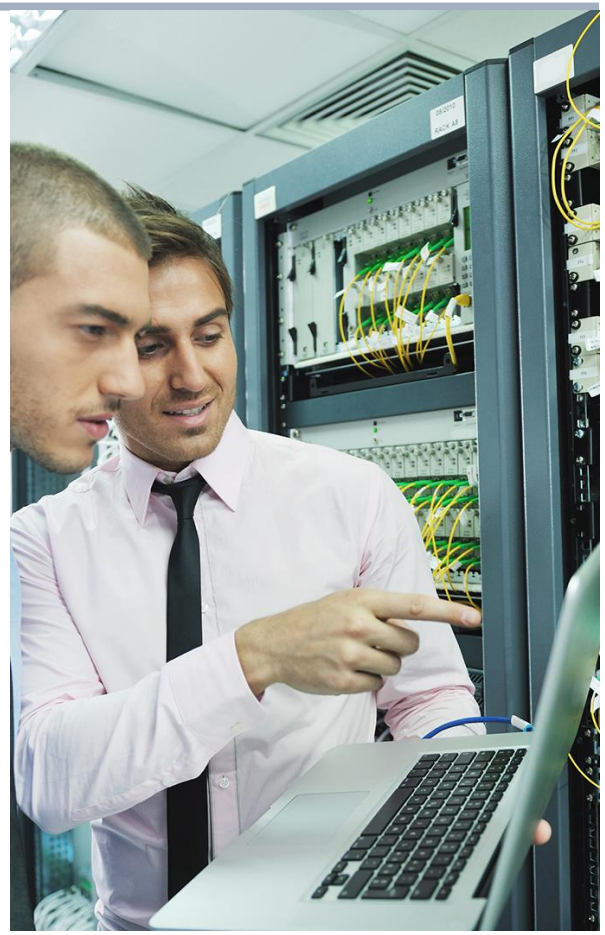
- Digitalisering brengt economische en maatschappelijke kansen
- Maar ook bedreigingen, onder meer door spionage en sabotage
- Informatie-uitwisseling en samenwerking is de sleutel naar cyber weerbaarheid
- Voor het MKB in de hightech maakindustrie is het niet/nauwelijks mogelijk dit zelfstandig te organiseren
- Maar wel noodzakelijk om je ‘license to operate’ te behouden

Niets doen is geen optie !

Waarom lid worden?

Redenen om bij het Cyber Weerbaarheidscentrum Brainport aan te sluiten

- U bent onderdeel van de hightech maakindustrie in Nederland en
  - Uw klant eist een (aantoonbare) mate van informatiebeveiliging
  - Uitval van ICT systemen (op specifieke momenten) kan exceptionele gevolgen hebben voor de omzet en/of bedrijfsvoering van uw organisatie
  - U wilt verlies van Intellectueel Eigendom voorkomen en u ziet interesse in uw Intellectuele Eigendommen bij andere partijen
  - U wilt er zeker van zijn dat de software in uw eindproduct geen malware of andere kwaadaardige software bevat waarmee uw klant ongemerkt haar ICT systemen kan besmetten

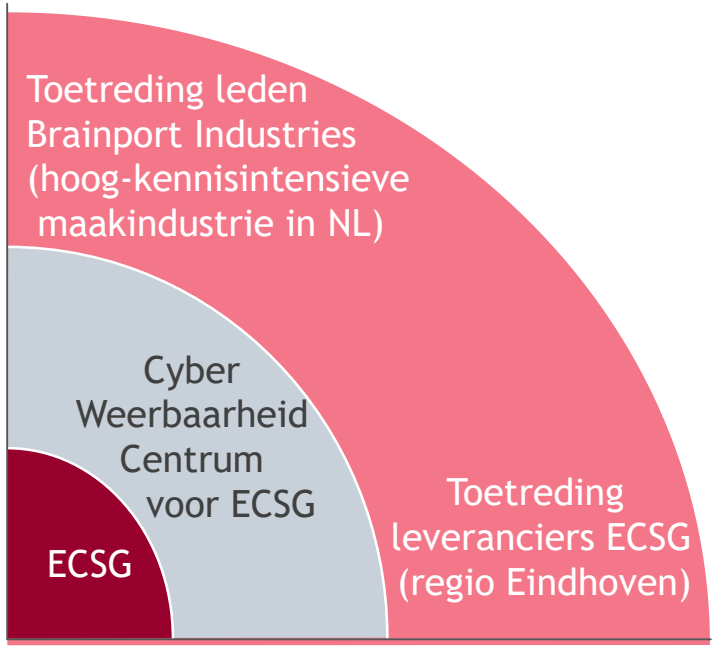


Groeimodel naar Brainport Cyber Weerbaarheidscentrum

Van TRUST naar DELEN VAN KENNIS naar WEERBAARHEID

Logische stappen :

1. Elkaar leren kennen en vertrouwen (netwerken bouwen)
2. Elkaar durven bellen en hulp vragen / good practices delen
3. Good-practices database met tips& tricks
4. Threat-intell uit andere open en gesloten bronnen
5. Aansluiting op NCSC – AMBER informatiestroom (formele CERT)
6. Ondersteuning en training preventief en na verstoring
7. Gezamenlijke monitoring / SOC diensten (zonder marktverstoring)
8. Vragen creëren en bundelen



Bouwen van regionale netwerken: TRUST

- Bouwen en faciliteren van expert overleggen
- Elkaar leren kennen en vertrouwen
- Awareness verhogen
- Elkaar helpen in de keten / regio
- Ad-hoc Kennisoverdracht

Informatiedeling: KENNIS

- Bijhouden van lijst met threat intelligence
- Centraal punt met kennis en good-practices
- Structureel delen van threat intel
- Ontvangen code AMBER NCSC info
- Kenniscentrum van good-practices
- Opstellen en delen van beveiligingsadvies
- Versturen van operationele alerts en dreigingeninformatie bij gerichte aanvallen op de branches waar de leden zich in bevinden
- Ondersteuning bij Awareness campagnes
- Tips & Tricks
- Training

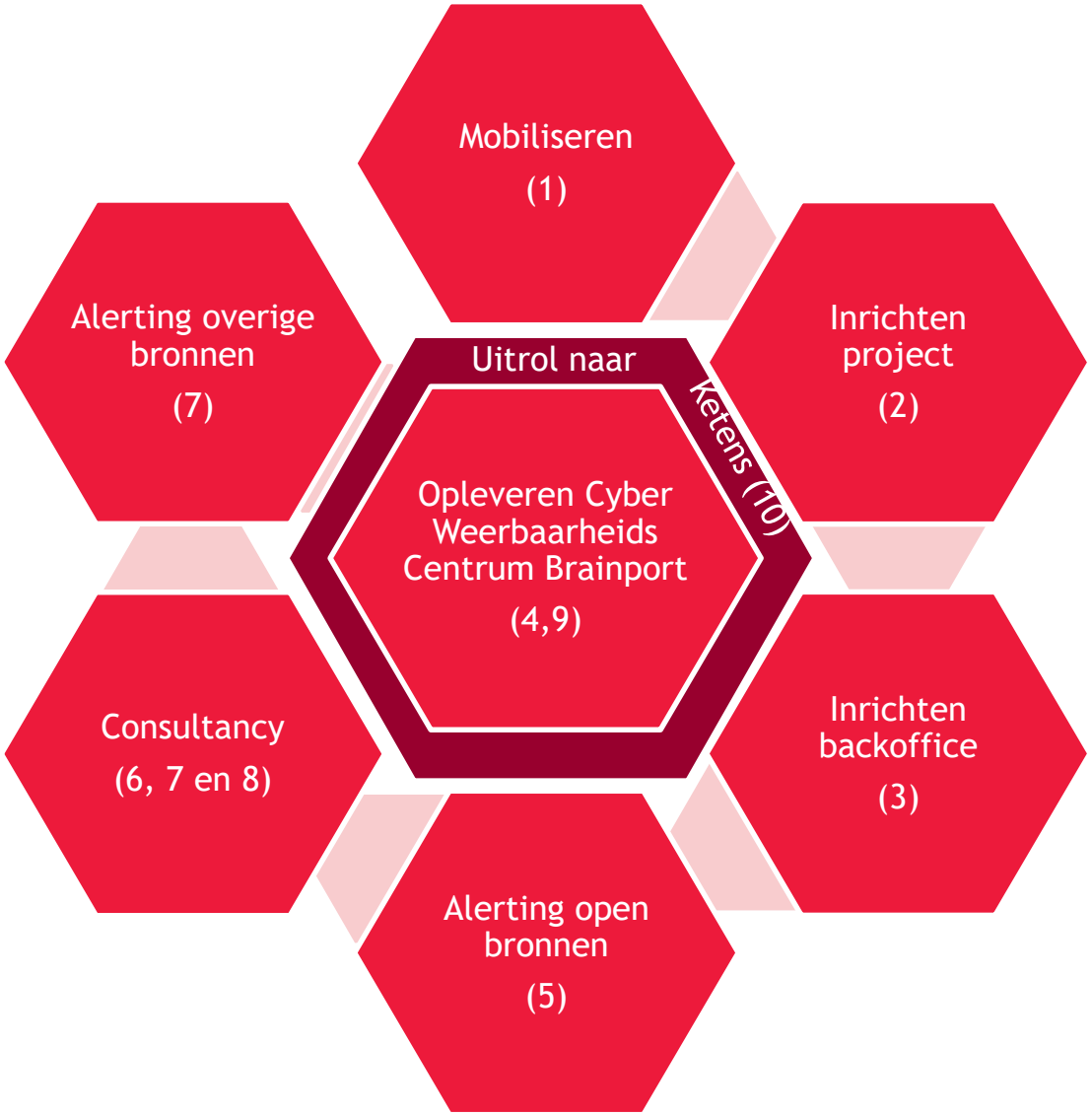
WEERBAARHEID

- Ondersteuning Forensisch onderzoek
- Technische advisering bij incidenten
- Ondersteuning Woordvoering / Pers
- Ondersteuning bij response op dreigingen en incidenten
- Gezamenlijke monitoring diensten (zoals SOC) voor ketenpartners

Planning op hoofdlijnen

In 10 stappen naar ‘Cyber Weerbaarheidscentrum Brainport’

1. Mobiliseren stakeholders & Aanloopsubsidie
2. Inrichten First user group & project groep
3. Inrichten back-office (database)
4. Ontwikkelen duurzame business case
5. Inrichten alerting met opvraagbare informatie
6. Inrichten consultancy
7. Inrichten alerting vanuit andere bronnen
8. Inrichten crisisbeheersing
9. Opleveren centrum, plannen, blauwdruk
10. Start uitrollen naar ketens



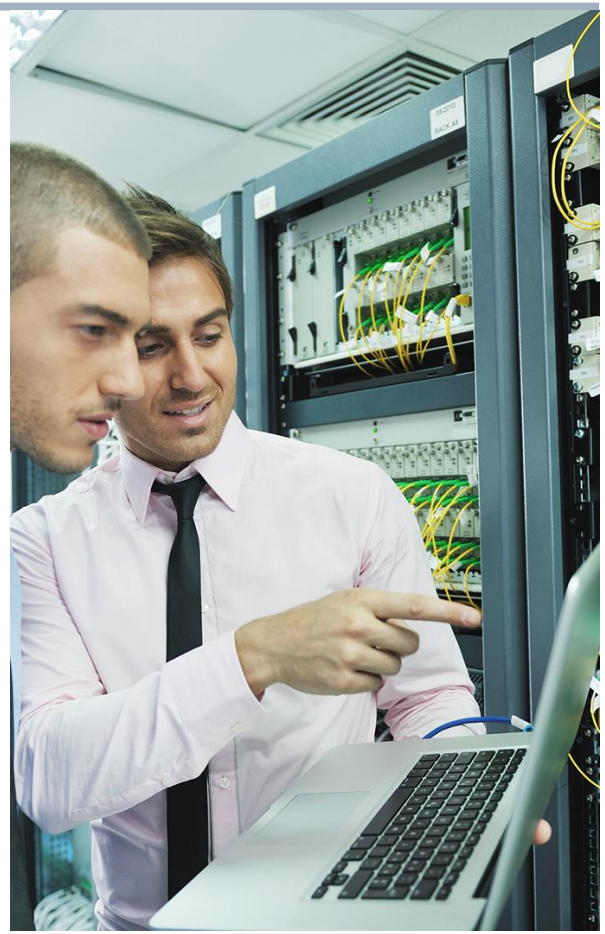
Diensten Cyber Weerbaarheidscentrum Brainport

Vijf kernthema's

Wat gaan we doen en leveren?

5 kernthema's

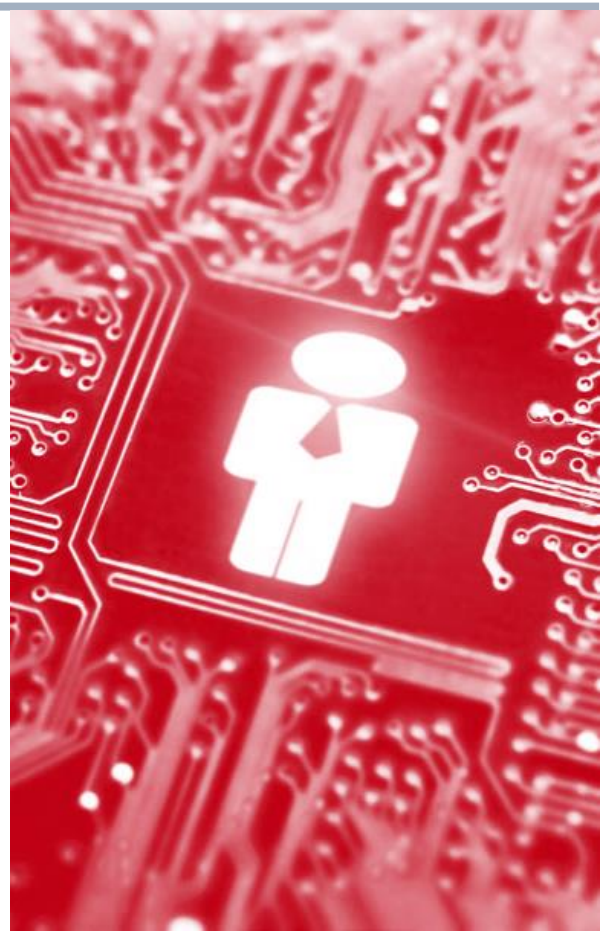
- Identificatie: We geven inzicht in welke mate op dit moment cybersecurity risico's worden beheerst waarbij we kijken naar ICT systemen, mensen, middelen, data en mogelijkheden
- Bescherming: We helpen beschermende maatregelen te nemen om kritieke diensten zeker te stelen
- Detectie: We helpen je vast te stellen of er sprake is van een dreiging en we kunnen de dreiging voor jou duiden
- Reactie: In geval van een cybersecurity incident helpen we je actie te ondernemen om de impact beperkt te houden
- Herstel: We helpen plannen voor cyber weerbaarheid op te stellen en diensten en ICT systemen te herstellen die beschadigd zijn door een cyberincident.



Cybersecurity Health Check

Intake voor nieuwe leden

- Uitvoering door externe partij (keuze uit 2 of 3 – CWCB wijst aan)
- Vergoeding € 1.500 excl. btw
- Basis is Security Health Check van Cyber Security Raad
- Kwaliteitsgarantie door eis in lijn met ISO27001 en ISO27002



Resultaat

- Algemene uitspraak: voldoende op orde om baat bij lidmaatschap te hebben
- Uitspraak per onderdeel over mate van in control zijn en hoe de belangrijkste gevonden risico's aan te pakken. De onderdelen zijn:
  - Security Governance
  - Human Resources
  - Facilities
  - ICT

Diensten Cyber Weerbaarheidscentrum Brainport

Diensten vanuit het Cyber weerbaarheidscentrum Brainport zelf - binnen het basis lidmaatschap

IDENTIFICATIE	BESCHERMING	DETECTIE	REACTIE	HERSTEL
▶ Intake (Healthcheck)	▶ Delen van best-practices ▶ Delen contactgegevens ▶ Intervisiegroepen	▶ Ontvangen threat intelligence van elkaar ▶ Ontvangen public threat intelligence ▶ Ontvangen betaalde threat intelligence	▶ Verwijzing naar de voor jou geschikte leverancier	▶ Delen threat intelligence met DTC ▶ Jaarlijks Sectoraal Dreigingsbeeld ▶ Verwijzing naar de voor jou geschikte leverancier

Diensten Cyber Weerbaarheidscentrum Brainport

Diensten aanvullend op het basis lidmaatschap - af te nemen via het Cyber Weerbaarheidscentrum Brainport

IDENTIFICATIE

- Risicoanalyse op IT, OT, productsoftware en/of de supply chain
- Risicomanagement strategie
- Kwetsbaarhedenscan & penetratietesten

BESCHERMING

- Basis security op orde (n.a.v. Intake)
- Awareness en training
- Support bij implementatie voor IT en OT met o.a.
  - Identity & Access Mgt
  - Data protectie
  - ISMS
  - Roadmap

DETECTIE

- Managed Intrusion Detection System
- Security Operations Center

REACTIE

- Computer Emergency Response
- Forensisch onderzoek
- Support bij communicatie
- Verbeterplan
- Support bij implementatie

HERSTEL

- Support bij herstel

De propositie & basisfee

De “ruil” en de collectieve investering

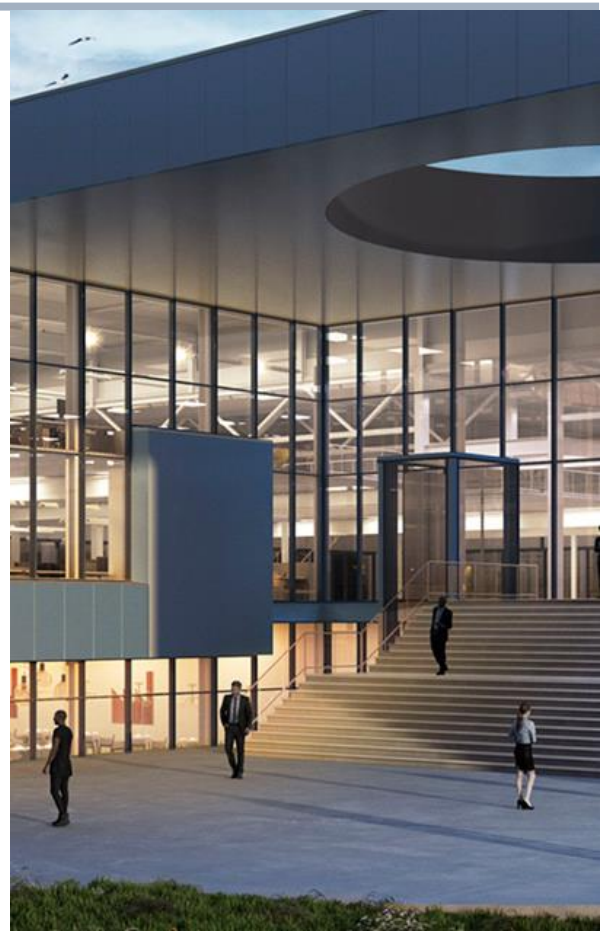
- Voor de jaarlijkse basisfee krijg je:
  - De basis dienstverlening
  - Toegang tot de (voor jou) beste leveranciers en inkoopvoordeel
  - Gebruik van het “merk” lid van Cyber Weerbaarheidscentrum Brainport als kwaliteitsborging (de basis op orde)

- Basis- en entreefee (op basis van contract voor 3 jaar)
  - 2019: 1.500 euro (basis) en 1.500 (entree)
  - 2020: 1.750 euro en 1.500 euro
  - 2021: 2.000 euro en 1.500 euro
  - 2022: 2.500 euro en 1.500 euro

Toekomstig organisatiemodel

Een stichting met het DNA van een coöperatie

- Adres op Brainport Industries Campus (in Eindhoven)
- Zeer compacte (flexibele) support organisatie
  - Moderator voor gezamenlijke portal
  - Front office (dienstverlening, marketing & sales)
  - Back office (IT, organisatie en administratie)
- Rechtsvorm en besturing
  - Stichting
  - Eén directeur bestuurder
  - Raad van Toezicht met 7 leden
    - 4 vertegenwoordigers uit het “ledenbestand”
    - 3 inhoudelijke specialisten (Cyber, Accounting en Marketing)



De leerervaringen tot nu toe

- Startkern
- Urgentie
- Ontwikkelen met de doelgoep
- Aan de slag / Doen

Vragen?

Robert Jan Marringa – marringa@24innovation.nl - 06 23 85 40 43

CYBER WEERBAARHEIDSCENTRUM BRAINPORT

voor de hightech maakindustrie in Nederland