Inleiding: Cyber Weerbaarheidscentrum Brainport (CWB) is een stichting zonder winstoogmerk en betreft een samenwerkingsverband gevestigd in Eindhoven met als doel het meer cyberweerbaar maken van de landelijke hightech maakindustrie (inclusief ketenpartners). CWB maakt deel uit van het Landelijk Dekkend Stelsel. De stichting werd in september 2019 officieel gelanceerd. Sinds augustus 2020 heeft CWB de OKTT-status en delen we dreigingsinformatie van het Nationaal Cyber Security Centrum (NCSC) met participanten. Met het certificeringssysteem CYRA® heeft het CWB bovendien een standaard ontwikkeld voor bedrijven om stapsgewijs maatregelen door te voeren en te laten certificeren. Per 1 augustus 2022 zijn een kleine 90 organisaties aangesloten bij CWB.

Is het voor een specifieke organisatie die getroffen wordt door bijvoorbeeld een cyberaanval ook duidelijk welke crisisstructuur er is en wat verwacht wordt?
Nee, dit is niet duidelijk. Er zijn inmiddels veel initiatieven op het vlak van cyberweerbaarheid maar een duidelijke plek waar ondernemers terecht kunnen en overall coördinatie ontbreekt. Wij zijn dan ook van mening dat er meer coördinatie nodig is en er één onafhankelijke, centrale plek zou moeten zijn waar men terecht kan voor hulp en advies/begeleiding bij een cyberincident. Ideaal zou uitbreiding van de dienstverlening van 112 zijn.

Het CWB heeft een hulpmiddel Cyber Rating (CYRA®) geïntroduceerd wat in de vorm van een self assesment organisaties inzicht geeft in wat te doen om cyberweerbaarheid te verhogen met mogelijkheid tot certificatie. Het zou goed zijn als er één landelijke standaard komt als hulpmiddel (weten waar men staat en hoe te komen tot een volgend niveau) en certificeringsmiddel (op basis waarvan organisaties hun niveau van cyberweerbaarheid (aan bijv. hun afnemers) kunnen tonen) en CYRA® zou deze landelijk standaard kunnen zijn.

Of een individuele onderneming weet wat te doen in geval van een cyber aanval ligt helemaal aan het volwassenheidsniveau van de cyberweerbaarheid van die organisatie. Binnen de doelgroep high tech maakindustrie helpt het CWB hierbij. Wie zich bewust is van de risico's en maatregelen neemt, is soms bekend met de noodzaak om tenminste een Incident Response Plan te hebben (of breder: een Business Continuity Plan). CWB hamert er op om preventiemaatregelen te nemen én om voorbereid te zijn, onder meer door minimaal één document te hebben waarop alle (nood)nummers staan.

Helaas bleek in oktober 2021 nog uit onderzoek dat 1 op de 3 security managers geen formeel reactieplan heeft voor cyberbeveiligingsincidenten [bron: Data Security Report 2021 van GetApp]. Ruim 1 op de 5 heeft geen protocollen om een vermoedelijke cyberaanval te melden.
We hebben de indruk dat hier nog veel winst te behalen valt. Iedereen zou zich bewust moeten zijn van de minimale voorbereiding op een incident (vergelijkbaar met – verplichte - brand- c.q. bhv-oefeningen).
De informatie over 'Wat te doen bij een cyberincident' is op uiteenlopende plekken te vinden, zonder dat duidelijk is hoe actueel deze informatie is en welke waarde die heeft. Er is een toolbox Cyberincident op de website Digitale Overheid, de vraag wordt beantwoord op de site van het Digital Trust Center en er is een hackhelpdesk.nl van Platform Veilig Ondernemen/Centrum voor Criminaliteitspreventie en Veiligheid. Ondernemers zijn zich hiervan vaak niet bewust. Zijn ze dat wel, dan moeten ze een keuze maken, wat lastig is als men niet goed op de hoogte is.

Hoe wordt er gehandeld bij een cyberincident?
Deze vraag is niet eenduidig te beantwoorden, want dat is zeer afhankelijk van de situatie en het type incident. Wel bestaat de indruk dat men de impact onderschat totdat men het aan den lijve ondervindt. De indruk bestaat ook dat men (te) veel tijd verliest door eerst zelf te proberen een incident op te lossen, terwijl dat vaak specialistische (forensische) kennis en ervaring vergt. Die kennis en ervaring is zeer beperkt

beschikbaar, versplinterd en kostbaar. Er zijn relatief weinig bedrijven die voldoende kennis in huis hebben.

Uiteraard zijn er organisaties die een uitgewerkt Incident Response Plan hebben en dat ook (regelmatig) oefenen om adequater te reageren op een cyberincident. Net zoals er organisaties zijn die volledig afhankelijk zijn van een IT-leverancier of van een 24/7 noodnummer van een verzekeraar of cyber dienstverlener. Dit zijn de twee uitersten, daar tussenin zijn nog allerlei reacties mogelijk.
Een groot probleem is dat de kennis van cyberincidenten en ervaring met het oplossen ervan nauwelijks wordt gedeeld. Terwijl dat algemeen goed zou moeten zijn. Net als de Universiteit van Maastricht zou men het aan de grote klok moeten hangen en elkaar waarschuwen voor de risico's op dat moment (meldplicht). Concurreren op cyberweerbaarheid/veiligheid is wat ons betreft *not done*.

Welke lessen hebben cyberoefeningen (bijvoorbeeld ISIDOOR) opgeleverd en hoe wordt daardoor mee omgegaan?
CWB heeft geen ervaring met ISIDOOR, waarschijnlijk mede omdat de stichting zich richt op een niet-vitale sector. Echter, CWB heeft wel participanten die op grond van NIS 2.0 tot de essentiële bedrijven behoren en te maken gaan krijgen met meld- en zorgplicht.
Terwijl de geleerde lessen mogelijk gedeeld moeten worden met organisaties die onderdeel uitmaken van het Landelijk Dekkend Stelsel, zoals CWB, heeft de stichting in juni 2022 haar eerste eigen cyberoefening gehouden in de vorm van een cyber crisis simulatie. Het meest enthousiast waren de deelnemers over de werking van een crisisteam aan de hand van BOB: Eerst Beeldvorming – dan Oordeelsvorming – tot slot Besluitvorming. Deze aanpak verschafte duidelijk handvatten. Verder werd duidelijk dat in- en externe communicatie van groter belang is dan menigeen vooraf denkt.

Een moeilijkheid bleek het verschil in kennis te zijn. Begrip van basisterminologie verhoogt het effect van de oefening, die altijd onder tijdsdruk moet plaatsvinden, wil er sprake zijn van een simulatie. Overigens vormt de 'taalbarrière' een ander aandachtspunt. Want beslissers hebben moeite om IT-mensen te begrijpen en vice versa.

Wat zijn nog belangrijke zorgpunten?
Het gebrek aan besef en kennis, net als het gebrek aan gekwalificeerd personeel. Er wordt nog te vaak gedacht dat alles wel in orde is en komt als de IT is uitbesteed. Daardoor heerst een vals gevoel van veiligheid;
De moeilijkheidsgraad van communicatie over cyberweerbaarheid en cyberveiligheid. Jip en Janneke-taal lijkt een onmogelijke opgave, maar is wel vereist om door te dringen tot iedereen;

1. Er zijn zoveel initiatieven – mede in het kader van het Landelijk Dekkend Stelsel – maar er is geen coördinatie. We zouden elkaar moeten versterken, maar iedereen lijkt zijn eigen ding te doen. Als mogelijke oplossing heeft het CWB mede het online hulpmiddel CYRA® (kort voor Cyber Rating) ontwikkeld dat potentie heeft om dienst te doen als landelijke standaard voor uiteenlopende branches;
2. De gevolgen van NIS 2.0. Zowel de vertaling naar de Wbni, als voor ondernemingen die te maken krijgen met zorg- en meldplicht en de kosten die daarmee gepaard gaan;
3. De angst van ondernemers om te delen wat hen is overkomen en hun angst voor reputatieschade, terwijl hen helemaal geen blaam hoeft te treffen, want het kan de beste overkomen. Hoe kunnen we hen bewegen om lessons learned te delen?
4. Het gebrek aan een landelijke crisisstructuur. Bij brand kun je de brandweer bellen, bij een verkeersongeval de politie en ambulance, maar bij een cyberincident 'moet' je een commerciële partij inschakelen (al assisteert te politie wel).