



Sterkere schakels versterken de keten!

In dit project hebben Cyber Weerbaarheidscentrum Brainport (CWB), Cyber4Z, ASML, Avans Hogeschool en het Regiobureau Integrale Veiligheid Oost-Brabant (RIVOB) de handen ineengeslagen om kleinere ondernemers te helpen hun cyberweerbaarheid te vergroten. Enerzijds door hen 10 uur gratis hands-on ondersteuning te bieden via een Shared Cyberprofessional. Anderzijds door hulpkaarten te ontwikkelen waarmee de ondernemer zelf aan de slag kon. De 16 ondernemers die hebben deelgenomen zijn met name afkomstig uit Zuidoost Brabant en Limburg. Het project is uitgevoerd in de periode april 2022 tot en met april 2023. Het gehele proces is gemonitord door Avans Hogeschool. Het doel is om de cyberweerbaarheid in de hele toeleveranciersketen van de maakindustrie te verbeteren.

Probleem

De keten is zo sterk als de zwakste schakel. Dit geldt ook voor de cybersecurity in de keten van toeleveranciers van grote bedrijven. Grote bedrijven hebben over het algemeen meer financiële middelen en kennis in huis om de informatiebeveiliging op orde te hebben en te houden. Kleinere bedrijven hebben per definitie minder financiële middelen en kennis om dit te doen. Dit leidt tot kwetsbaarheden voor de gehele keten. In dit project is geëxperimenteerd met een methodiek waarbij de grote bedrijven de kleinere toeleveranciers ondersteunen bij het opschrijven van de informatiebeveiliging. Daar plukken de individuele bedrijven – en daarmee de gehele keten – de vruchten van.

Aanpak

In dit project is op twee manieren geëxperimenteerd met het ondersteunen van kleinere bedrijven bij het vergroten van hun cyberweerbaarheid:

- Hands-on ondersteuning vanuit het grote bedrijf bij de kleinere toeleveranciers. De hands-on ondersteuning krijgt vorm door het opstellen van zogenaamde “white papers” door een grote onderneming met kernachtige uitleg over wat de kleine ondernemer kan inregelen om de cyberweerbaarheid te verhogen.
- Eén-op-één ondersteuning van kleinere toeleverancier bij cybersecurity via een Shared Cyberprofessional. Deze cyberprofessional gaat naast de ondernemer zitten om de cybersecurity te vergroten. Hij onderneemt met de ondernemer meteen actie om de cybersecurity te versterken.

Resultaten

De volgende resultaten zijn bereikt:

- Bij 16 bedrijven in de keten is de cyberveiligheid daadwerkelijk vergroot. Bij de meeste bedrijven is een technische test uitgevoerd om te testen of cybercriminelen toegang zouden kunnen krijgen tot het netwerk. Op basis hiervan zijn beveiligingsadviezen geformuleerd. Andere interventies zijn: phishing campagne, VPN, CYRA-assessment, opstellen incident respons plan en NIS2 assessment.
- Gedurende de looptijd van het project zijn er diverse hulpkaarten ontwikkeld. Onderwerpen van deze advies-, nood- en preventiekaarten zijn: phishing, Microsoft 365, back-up, bedrijfswebsite, clean desk & clear screen, it-leverancier, ransomware. Deze zijn hier vrij te downloaden van de website van het CWB.
- Meer inzicht in de werkzame en niet-werkzame elementen van de geteste aanpak bij het ondersteunen van kleinere toeleveranciers.



Tips

Voor gemeentes (of andere partijen) die dit project over willen nemen, hebben we de volgende tips:

- Maak een zorgvuldige keuze bij de Shared Cyberprofessional die je hiervoor in de arm neemt. Het is verstandig om met een organisatie te werken die meerdere expertises in huis heeft. De werkzaamheden lopen dusdanig uiteen dat deze niet in één persoon zitten.
- Tien uur voor de Shared Cyberprofessional is niet genoeg om de organisatie te leren kennen én een interventie te plegen. Mogelijk kan het interessant zijn om gebruik te maken van bestaande (gratis) scans om de situatie alvast in kaart te brengen. En vervolgens de Shared Cyberprofessional in te zetten voor de adviezen die uit de scan komen.

Vervolg

Het project is afgerond met een ontwerpworkshop waarin met diverse stakeholders van elf organisaties is gesproken over de verdere uitwerking van de functie van Shared Cyberprofessional. Op dit moment wordt er vanuit het Cyber Weerbaarheidscentrum gewerkt aan deze verdere uitwerking.



Meer informatie

Meer weten over dit project? Neem contact op met Mieke Zijlstra, projectleider Cyber Weerbaarheidscentrum Brainport, Mieke.zijlstra@cwbrainport.nl.

Het secretariaat van de City Deal Lokale Weerbaarheid Cybercrime wordt gevoerd door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Bekijk de CCV-database voor nog meer interessante cyberprojecten.