CYBERWEERBAARHEID

VAN DE INDUSTRIËLE SECTOR VAN HET MKB

ONDERZOEKSOPZET

In het huidige onderzoek stond de volgende vraag centraal: "*hoe cyberweerbaar is de industriële sector van het mkb en welke factoren spelen hierbij een rol?*". Cyberweerbaarheid is de mate waarin een bedrijf in staat is zelfbeschermend gedrag te vertonen, oftewel tegenstand te bieden tegen cybercriminaliteit. Aan de hand van veertien interviews met mkb-bedrijven is geprobeerd hier een antwoord op te vinden. De resultaten lieten zien dat er qua cyberweerbaarheid nog veel winst te behalen valt.

IT–INFRASTRUCTUUR

- Uit het onderzoek kwam naar voren dat een groot deel van de bedrijven hun server laat beheren door een externe IT-leverancier. De voornaamste reden hiervoor is een gebrek aan (interne) kennis. Opvallend is het vertrouwen dat men heeft in de externe IT-leverancier. Zij vertrouwen erop dat deze IT-leverancier alles regelt op het gebied van informatiebeveiliging en daarmee ook alle (technische) maatregelen treft. Dit laat zien dat men de noodzaak van andere (meer organisatorische) maatregelen niet voldoende inziet.

- Een ander belangrijk onderdeel van de IT-infrastructuur, is het gebruik van privé apparatuur voor bedrijfsdoeleinden. Het onderzoek heeft laten zien dat regels hieromtrent vaak ontbreken. Het risico hiervan is dat medewerkers malafide software, dat op een mogelijk onbeveiligd thuisnetwerk is gedownload, meenemen naar het bedrijfsnetwerk.

CYBERSECURITY MAATREGELEN

- Cybersecurity maatregelen kunnen worden onderverdeeld in technische en organisatorische maatregelen. Meest getroffen technische maatregelen zijn de spamfilter, een firewall en het maken van (dagelijkse) back-ups van de systemen.

- Organisatorische maatregelen, welke zich richten op het gedrag van personeel binnen een organisatie, zijn vaak onvoldoende aanwezig. Zo had bijna geen enkel bedrijf een beleid met daarin regels omtrent online gedragingen van het personeel. Ook bieden weinig bedrijven (structureel) trainingen/cursussen aan, waarin medewerkers bewust worden gemaakt van de risico's van online gedragingen, alsook hun rol binnen de organisatie als het gaat om informatiebeveiliging. Een groot deel van de bedrijven geeft dan ook aan dat dit bewustzijn onder medewerkers (vaak) onvoldoende aanwezig is.

PREVALENTIE SLACHTOFFERSCHAP

Zes van de veertien bedrijven hebben te maken gehad met een cyberincident:

Hacking
1/6

Phishing
2/6

Datalek
1/6

Ransomware
2/6

RISICOPERCEPTIE

- Bedrijven schatten hun kans op slachtofferschap over het algemeen niet hoog in. Een veel gehoord argument is dat zij niet over interessante data beschikken, waardoor men niet weet wat een cybercrimineel bij hen te zoeken heeft.

- Ook de potentiële impact van een incident wordt laag gewaardeerd. Dit kan wellicht verklaart worden vanuit het feit dat de bedrijven die te maken hebben gehad met een incident, hier nauwelijks schade van hebben ondervonden. Zij zijn zich in dat opzicht niet (voldoende) bewust van de schade die met een incident gepaard kan gaan.

AANBEVELINGEN

- Het onderzoek laat zien dat bedrijven met name moeten investeren in het creëren van bewustzijn. Echter, hierbij moet niet alleen gedacht worden aan de trainingen voor personeel, er moet ook meer aandacht komen voor het bewustzijn onder het bestuur van een organisatie. Indien zij - in lijn met het huidige onderzoek - vinden dat zij als organisatie niet aantrekkelijk zijn voor een eventuele cybercrimineel, zullen zij geen tijd en geld investeren in het creëren van bewustzijn onder personeel. Ook het aantal getroffen beveiligingsmaatregelen zal dan (mogelijk) beperkt blijven.

- Middels voorlichting moeten bedrijven gewezen worden op hun gebrek aan weerbaarheid, teneinde hen handvatten aan te reiken om deze weerbaarheid te vergroten.

"ONE OF THE MAIN CYBER–RISKS IS TO THINK THEY DON'T EXIST"

Voor vragen neem contact op met:
Romée Boer | r.boer@ispbv.nl

INTERNATIONAL SECURITY PARTNERS
We solve