Hoe cyberweerbaar zijn mkb-retailers?

Regio Den Haag

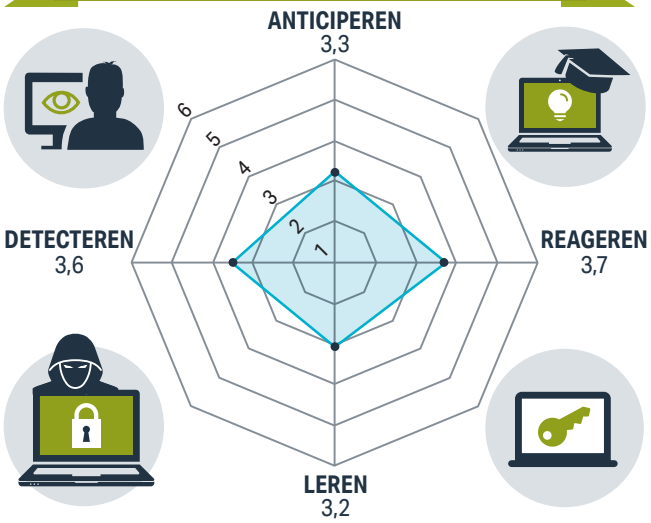
Wat is cyberweerbaarheid?

Cyberweerbaarheid is het vermogen van het mkb om weerstand te bieden tegen bekende en onbekende vormen van cybercriminaliteit en snel te herstellen van een cybercrisis. Dit betekent dat het mkb in staat moet zijn om te anticiperen op bedreigingen en kansen en deze ook moet kunnen detecteren als deze zich voordoen in de organisatie. Ook moet het mkb adequaat kunnen reageren op incidenten en begrijpen wat er heeft plaatsgevonden zodat ervan kan worden geleerd.

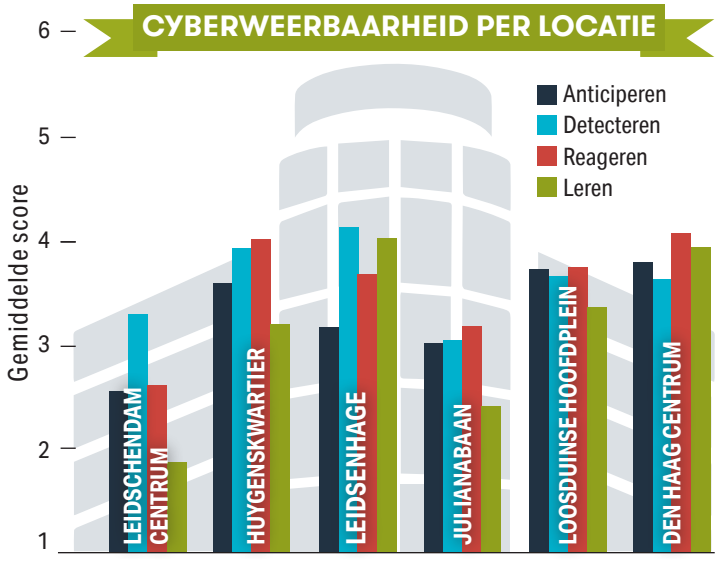
Cyberweerbaarheid gemeten

Cyberweerbaarheid is gemeten met behulp van een vragenlijst met stellingen. Een voorbeeld van een stelling is: 'Medewerkers in ons bedrijf vinden de bestrijding van cybercriminaliteit op het werk belangrijk'. Hoe hoger een bedrijf scoort op deze stellingen, hoe meer cyberweerbaar het bedrijf is. De score loopt van 1 tot en met 6 punten per stelling. De gemiddelde score voor cyberweerbaarheid is 3,46. Het mkb scoort het hoogst op 'reageren' en het laagst op 'leren'.

CYBERWEERBAARHEID OVERALL



CYBERWEERBAARHEID PER LOCATIE



Onderzoeksopzet en respons

In september en oktober 2018 heeft De Haagse Hogeschool in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een pilotonderzoek uitgevoerd in opdracht van de gemeente Den Haag bij mkb-retailers.

Hiermee is een eerste beeld opgehaald over de cyberweerbaarheid van mkb retailers in 6 winkelgebieden in Den Haag en omstreken. In totaal hebben 57 leidinggevenden uit 56 bedrijven een enquête ingevuld.

De volgende cyberdelicten kwamen het meest voor bij de 56 mkb-bedrijven

Slachtofferschap van cybercrime

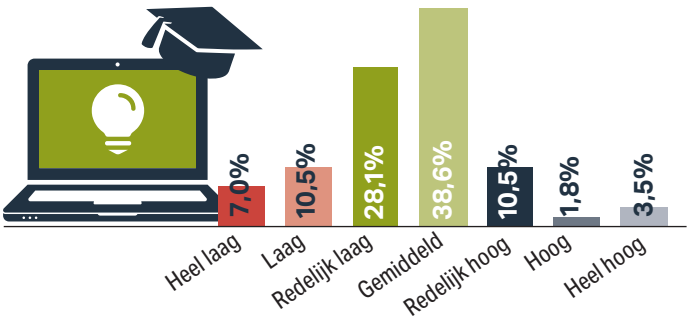
Bijna de helft (48 %) van de retailers geeft aan slachtoffer te zijn geweest van cybercriminaliteit in de laatste 12 maanden. Zeven bedrijven (12 %) hebben ook daadwerkelijk schade hiervan ondervonden. Schade als gevolg van cybercriminaliteit kan zich op verschillende vlakken voordoen. Zo kan een bedrijf financiële schade oplopen. Ook kunnen belangrijke bedrijfsgegevens gestolen of vernietigd zijn. Schade kan ook bestaan uit tijdverlies, doordat de bedrijfsprocessen tijdelijk stilliggen. Daarnaast kan een bedrijf imagoschade oplopen.

Sanctiebeleid cyberonveilig gedrag

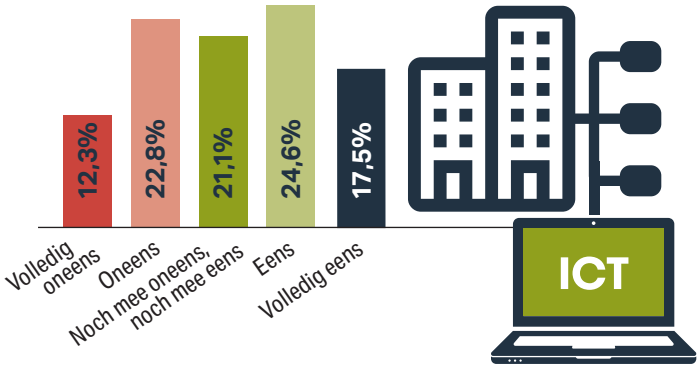
In het onderzoek is ook gevraagd naar het sanctiebeleid dat de mkb-retailers voeren op cyberonveilig handelen van medewerkers. Een sanctiebeleid verschaft duidelijkheid over wat wel of niet wordt geaccepteerd binnen een bedrijf en welke maatregelen er kunnen worden getroffen indien een werknemer zich cyber-onveilig gedraagt. Wat blijkt? Hoe strikter het sanctiebeleid van een bedrijf, hoe méér cyber-weerbaar het bedrijf is.

Gemiddelde IT-kennis personeel

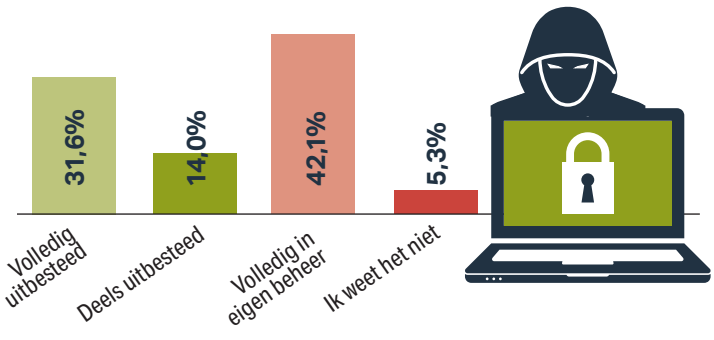
Naarmate de gemiddelde IT-kennis van het personeel hoger is, is een mkb-bedrijf ook méér cyberweerbaar.



Bedrijfsprocessen afhankelijk van ICT?



Is de IT-beveiliging uitbesteed?



Conclusies

Dit onderzoek laat zien dat de cyberweerbaarheid van de mkb-retailers in de regio Den Haag omhoog kan. Vooral het vermogen om te leren van cyberincidenten kan worden versterkt. IT-kennis van het personeel en een strikt sanctiebeleid op cyber onveilig gedrag kunnen bijdragen aan meer cyberweerbaarheid van het mkb.

Contact:

Dr. Rick van der Kleij
Lectoraat Cybersecurity in het mkb
De Haagse Hogeschool

@ **r.vanderkleij@hhs.nl**

DE HAAGSE HOGESCHOOL