**THEMA'S:** CYBERCRIME VEILIG ONDERNEMEN
**RUBRIEK:** ONDERZOEK & ANALYSE

# CYBERCRIMINALITEIT LEEFT NIET ONDER RETAILERS

Foto: Liesbeth Dingemans

DEEL PRINT DIT ARTIKEL NAAR HOME

4 maart 2019

**AUTEURS:** RICK VAN DER KLEIJ , IRIS DE BRUIN , SUSANNE VAN 'T HOFF-DE GOEDE , MICHELLE ANCHER , RUTGER LEUKFELDT

**Mkb-retailers in de regio Den Haag zijn nauwelijks weerbaar tegen cybercriminaliteit, blijkt uit onderzoek in opdracht van de gemeente Den Haag. Zij zien het niet als een belangrijk bedrijfsrisico. Hoe krijgen we het midden- en kleinbedrijf zover dat zij zich beter beschermen tegen cybercriminaliteit?**

In de Nederlandse economie speelt informatie- en communicatietechnologie (ICT) een steeds belangrijkere rol. Dit brengt nieuwe kwetsbaarheden met zich mee. Criminelen kunnen gericht bedrijven digitaal aanvallen, bijvoorbeeld door bedrijfsprocessen die gebruikmaken van ICT te hacken. Ook kunnen bedrijven te maken krijgen met gedigitaliseerde traditionele criminaliteit, zoals online oplichting. Zo legde in 2017 een ransomware-aanval door cybercriminelen gericht tegen machinefabriek Almi, de volledige bedrijfsvoering plat. Omdat alle bedrijfsprocessen geautomatiseerd waren, was de schade van de cyberaanval aanzienlijk: minstens 60.000 euro.

## IMPACT VAN CYBERCRIME

Het midden- en kleinbedrijf (mkb) heeft, in tegenstelling tot grootbedrijven, vaak onvoldoende kennis en hulpbronnen om zichzelf te weren tegen cybercriminaliteit. Onderzoek laat zien dat 2 op de 5 mkb'ers in 1 jaar tijd te maken hebben gehad met cybercriminaliteit. 1 op de 5 heeft bovendien schade hiervan ondervonden.

Schade kan bestaan uit financiële schade, reputatieschade of verstoring van de bedrijfsprocessen

Schade kan bestaan uit financiële schade, reputatieschade of verstoring van de bedrijfsprocessen. Cybercriminaliteit kan zodoende een grote impact hebben op het mkb. Het mkb vormt de ruggengraat van de Nederlandse economie. Daarom is het van belang inzicht te krijgen in hoe het zich beter kan weren tegen cybercriminaliteit.

## ONDERZOEK NAAR CYBERWEERBAARHEID

In deze bijdrage vatten we de resultaten samen van een eerste exploratief onderzoek in opdracht van de gemeente Den Haag naar cyberweerbaarheid onder mkb-retailers in de regio Den

Haag. Er is gekozen voor onderzoek onder retailers omdat de bedrijfssector waarin zij werken, namelijk de detailhandel, een risicogroep vormt. Ons onderzoek laat zien dat de cyberweerbaarheid van deze groep gering is. Mkb-ondernemers achten zichzelf veelal niet interessant voor cyberaanvallen en zien cybercriminaliteit niet als een van de belangrijkste bedrijfsrisico's.

Bedrijven met medewerkers die relatief veel IT-kennis hebben, scoren hoger op cyberweerbaarheid

Investeringen in IT-opleidingen voor personeel en een sanctiebeleid voor medewerkers die zich cyberonveilig gedragen, beperken het risico op slachtofferschap. Een uitdaging blijkt echter: hoe zorgen we ervoor dat het mkb ook daadwerkelijk maatregelen gaat nemen om zich beter te beschermen? Een belangrijke conclusie is dat we op dit moment nog onvoldoende weten over manieren om mkb'ers bewuster te maken van de risico's die digitalisering met zich meebrengt.

#### WAT IS CYBERWEERBAARHEID?

Cyberweerbaarheid is hier gedefinieerd als 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 deze ook moet kunnen detecteren als zij 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. Het gedrag van het management en medewerkers speelt in onze ogen een belangrijke rol hierin. Hun cyberveilig gedrag is immers een cruciale voorwaarde om een organisatie te beschermen tegen cybercriminaliteit.

#### HOE CYBERWEERBAAR ZIJN MKB-RETAILERS?

Bijna de helft van de 56 bedrijven uit de regio Den Haag die meededen aan ons onderzoek geeft aan slachtoffer te zijn geweest van cybercriminaliteit in de laatste 12 maanden. Dit is in lijn met cijfers uit landelijk onderzoek van De Haagse Hogeschool. 12 procent heeft hiervan schade ondervonden. Dit cijfer is lager dan het cijfer uit het landelijke onderzoek (20 procent). Toch bestaat de vrees dat het aantal incidenten, door het toegenomen belang van ICT voor het mkb, alleen maar zal toenemen de komende jaren . Waarschijnlijk zal ook de schade die retailers hiervan ondervinden toenemen. Het is dus belangrijk dat mkb'ers cyberweerbaar zijn.

Veel bedrijven hebben al voorschriften over cyberveilig gedrag

Als we kijken naar de cyberweerbaarheid van mkb-retailers dan valt op dat zij maar in beperkte mate weerbaar zijn. Ons onderzoek toont aan dat hier ruimte is voor verbetering. Deelnemende retailers zijn relatief gezien het best in staat om te 'reageren' en het minst goed in staat om te 'leren', maar de verschillen zijn niet groot. Een mogelijke voorspeller van de cyberweerbaarheid blijkt de IT-kennis van het personeel te zijn. Bedrijven met medewerkers die relatief veel IT-kennis hebben, scoren hoger op cyberweerbaarheid. Ook blijkt dat bedrijven die een sanctiebeleid voor medewerkers hebben die zich cyberonveilig gedragen, doorgaans meer cyberweerbaar zijn. Veel bedrijven hebben al voorschriften over cyberveilig gedrag. Ons onderzoek wijst op het belang van een sanctiebeleid op het niet naleven van deze voorschriften.

#### RISICOCOMMUNICATIE OVER CYBERCRIME

Ondanks alle moeite die we hebben genomen om retailers in de regio Den Haag te betrekken bij dit onderzoek was de belangstelling voor deelname beperkt. Cybercriminaliteit lijkt onder retailers nauwelijks te leven. Mkb'ers achten zichzelf veelal niet interessant voor cyberaanvallen en zien cybercriminaliteit

niet als een prominent risico. Het zijn vooral de sociaaleconomische ontwikkelingen en fysieke veiligheid waar de mkb'ers van wakker liggen. Dit brengt de uitdaging met zich mee: hoe dan toch deze groep te overtuigen van het belang van cyberweerbaarheid? Onderzoek naar de effectiviteit van risicocommunicatie in een dergelijke setting kan uitsluitsel geven.

Te denken valt aan onderzoek naar cyberweerbaarheid bij bedrijven in een andere sector

Risicocommunicatie omvat voorlichting en communicatie over risico's waaraan mensen kunnen blootstaan voordat zich een ramp voordoet. Op dit moment weten we nog onvoldoende over effectieve manieren om mkb'ers bewuster te maken van de risico's die digitalisering met zich meebrengt. Deels heeft ons onderzoek geleid tot een zekere mate van reactiviteit van mkb-retailers: het meedoen aan het onderzoek lijkt de mening over het belang van cyberweerbaarheid en mogelijk ook het gedrag van de respondenten in positieve zin te hebben beïnvloed, zo hebben wij ervaren. Daarmee kan ons onderzoek als een vorm van risicocommunicatie worden gezien. Maar veel weten we nog niet. Vervolgonderzoek naar cyberweerbaarheid, vooral naar risicocommunicatie omtrent cybercrime – en daarmee inzicht in hoe deze moeilijke doelgroep kan worden bereikt – kan hier uitsluitsel over geven.

**BEDRIJVEN IN EEN ANDERE SECTOR**

Met het oog op vervolgonderzoek valt bovendien te denken aan onderzoek naar cyberweerbaarheid bij bedrijven in een andere sector. Dan kunnen uitspraken worden gedaan over hoe de weerbaarheid zich verhoudt tussen sectoren. Bedrijven in andere sectoren, zoals de industrie, hebben mogelijk een grotere afhankelijkheid van ICT voor de bedrijfsvoering dan retailers. Cybercriminaliteit vormt voor deze bedrijven dan ook mogelijk een nog grotere bedreiging dan voor retailers. De vraag is echter of deze sector dan ook meer cyberweerbaar is. En zo ja, leidt dit dan tot minder incidenten en lagere schade? <<

**Onderzoek naar cyberweerbaarheid**

Cyberweerbaarheid is onderzocht met behulp van een vragenlijst met stellingen. Deze stellingen meten het vermogen om te kunnen 'anticiperen', 'detecteren', 'reageren' en 'leren' van cyberincidenten. 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 de stellingen, hoe meer cyberweerbaar het is. De score loopt van 1 tot en met 6 punten per stelling. Een gemiddelde score van 3,5 punten of hoger zien wij als een voldoende. De gemiddelde score voor cyberweerbaarheid van mkb-retailers in de regio Den Haag is 3,46. Dit is net geen voldoende. In totaal zijn 375 retailers benaderd in 6 winkelgebieden. Hiervan hebben 57 mkb'ers uit 56 verschillende bedrijven de enquête ingevuld. Het betreft vooral bedrijven met 10 of minder medewerkers (82 procent).

*Rick van der Kleij, Susanne van 't Hoff-de Goede, Michelle Ancher en Rutger Leukfeldt zijn werkzaam bij de Haagse Hogeschool, Lectoraat Cybersecurity in het mkb. Iris de Bruin studeerde ten tijde van het schrijven van het artikel aan de Haagse Hogeschool, Rick van der Kleij en Rutger Leukfeldt werken respectievelijk ook bij TNO en het NSCR.*
*Rick van der Kleij is bereikbaar voor vragen en discussies via e-mail: r.vanderkleij(at)hhs.nl.*