MICHAEL

Waterman

CYBERSECURITY ARCHITECT
ACA IT-SOLUTIONS

Klikken op een dubieuze link in een e-mail vol spelfouten, dat doet geen mens meer. *Toch?* Onderzoek wijst uit dat cybercriminelen makkelijker, vaker en met grotere impact binnendringen in ons zakelijke en privéleven. De *emotionele schade* kan zelfs zo heftig zijn, dat Slachtofferhulp Nederland er nu een grote bewustwordings-campagne aan wijdt. *“Ik heb een succesvolle ondernemer door een cyberhack zien veranderen in een huilend wrak”.*

TEKST *Martijn van der Ven* | **FOTOGRAFIE** *Erik de Brouwer*

"Criminele organisaties opereren als *ondernemingen met een verdienmodel* en JIJ bent de 'klant"

Een radiocommercial van Slachtofferhulp Nederland schetst de pijnlijke dagelijkse praktijk. "Achter die ene e-mail schuilt een organisatie met geslepen cybercriminelen die met de nieuwste technologie jouw gegevens stelen of versleutelen. *Niet zo gek dat je die link vertrouwde." De boodschap van de campagne 'Online oplichting is een serieuze misdaad' is duidelijk: vroeg of laat kom je aan de beurt.* Die woorden klinken ook uit de mond van Michael Waterman, Cybersecurity Architect bij het Eindhovense ACA IT-Solutions. "De methodes die criminelen gebruiken om binnen te dringen in je computer of netwerk zijn bijzonder geraffineerd. Een virusscanner of firewall houdt kwaadwillenden echt niet tegen."

Kat- en muisspel

Waterman weet waarover hij praat. Zijn IT-bedrijf is een dochteronderneming van accountantskantoor Crowe. Afgelopen zomer werd dit kantoor zelf slachtoffer van een onvangrijke hack. *Hoe kon dat gebeuren? "Een toevalstreffer. Cybercriminelen gooien op grote schaal sleepnetten uit, op zoek naar zwakke plekken in IT-systemen van organisaties. Massa is kassa.* Zelf heb je daar geen invloed op, want het is een continu kat- en muisspel tussen hackers en ontwikkelaars van hard- en software. Voor ons was deze gebeurtenis een bevestiging dat onze voorzorgmaatregelen goed hebben gewerkt. Er zijn geen datalekken geweest, onze back-ups deden wat ze moesten doen en we waren snel weer up & running. *De best mogelijke uitkomst na een ongewenste testcase."*

Nieuwe dienstverlening

Wat als de cybercriminelen wél waren geslaagd? Wat was dan de schade geweest? Waterman onderscheidt economische en emotionele schade. "Wanneer je te maken krijgt met gijzelsoftware, wordt gemiddeld 2% van je jaaromzet opgeëist. Dat bedrag is niet toevallig gekozen en staat gelijk aan de opbrengsten van een normale werkweek. De criminelen hopen dus te bereiken dat je zo snel mogelijk betaalt en dreigen soms ook nog meer aanvallen. Alleen al in 2022 werd in Nederland meer dan twee miljoen euro aan losgeld overgemaakt naar malafide groepen zoals het Russische Lockbit en BlackCat. Voor zover wij weten dan, want lang niet alle gedupeerden doen aangifte. En je zult het misschien niet geloven, maar over de prijs van de sleutel waarmee je je gegevens weer ontcijfert kun je met de cybercriminelen onderhandelen!

Sterker nog, vaak is degene met wie je contact hebt uiterst behulpzaam en beleefd. Er zijn zelfs criminele organisaties die vinden dat ze jou en je bedrijf een dienst bewijzen met hun datagijzeling. We hebben het hier over een lucratieve mondiale business, de ethische aspecten daargelaten. Een business die razendsnel groeit. Deze criminele organisaties opereren als ondernemingen met een verdienmodel en jij bent de 'klant'. Of je nu wilt of niet. Aan te pakken zijn deze 'dienstverleners' nauwelijks. Ze wanen zich veilig en pronken op social media met hun criminele vermogen."

Privé-gegevens openbaar

Wat een inbreuk van je digitale privacy kan doen op emotioneel vlak, zag Waterman met eigen ogen. Hij werkte jarenlang namens Microsoft samen met justitie in zaken van afdreiging. *"Enkele werknemers bij een klant bewaarden allerlei privé-gegevens op hun zakelijke computer en kregen te maken met datagijzeling. Er werd gedreigd met het openbaren van gevoelige informatie die hen en het bedrijf, maar ook hele gezinnen kon raken.* Cybercriminelen deinzen nergens voor terug. Dan zie je een door de wol geverfde ondernemer ineens veranderen in een uitgeput wrak. De impact van zo'n incident is niet te bevatten. Mijn advies aan ondernemers: zorg ervoor dat medewerkers hun zakelijke laptop of mobile device alleen voor zakelijke doeleinden gebruiken."

Zero trust

Niemand vraagt erom door cyberbendes te grazen te worden genomen. Maar volgens Waterman zetten met name mkb-bedrijven de achterdeur soms wagenwijd open. "Veel bedrijven leven nog in 2003 als het gaat om cybersecurity. Dat komt omdat men in het mkb gewend is uit te gaat van vertrouwen. Bovendien leeft er het idee dat IT altijd alles en iedereen beschermt. Terwijl zero trust het uitgangspunt zou moeten zijn. Met andere woorden: beperkt de toegang tot vitale bedrijfsdata, laat gebruikers zich valideren en richt de IT-architectuur zo in dat er in geval van nood een plan B is. Het ontbreekt in veel gevallen aan goede procedures die nodig zijn na een cyberaanval. En wanneer je back-ups maakt, vergeet dan niet om deze periodiek te testen, want ervan uitgaan dat alles werkt kun je je niet permitteren."

Cyberweerbaarheidsonderzoek MKB Brabant

Om een betrouwbaar beeld te krijgen, deed ACA IT-Solutions in samenwerking met netwerkorganisatie MKB Eindhoven en Fontys ICT Hogeschool een grootschalig onderzoek naar de cyberweerbaarheid van mkb-bedrijven. Meer dan 200 Brabantse ondernemingen namen deel. De conclusies liegen er niet om. Bij niet meer dan 50,8% van de respondenten staat het thema cybersecurity periodiek op de agenda van de directie. Slechts een krappe meerderheid beschikt over procedures voor informatiebeveiliging en cyberincidenten. Waterman: *"We zien dat er nog te weinig betrokkenheid en prioriteit is bij de directie.* Daardoor is er een gebrek aan kennis op het gebied van cybersecurity en actueel inzicht in de methodieken van cybercriminelen. Ondanks de talrijke ransomware-incidenten die het nieuws haalden, zoals bij VDL en Jumbo, is men op directieniveau vaak nog in de veronderstelling dat cybercriminelen het alleen hebben gemunt op multinationals. Een bende als BlackCat maakt geen onderscheid in het type organisatie en heeft slachtoffers gemaakt in verschillende sectoren waaronder retail, transport en financiële dienstverlening."

De zwakste schakel

Waterman pleit ervoor dat mkb-bedrijven hun cybersecuritybeleid serieus gaan nemen. Anderhalf tot twee procent van de jaaromzet zou volgens de expert structureel geïnvesteerd moeten worden in cyberweerbaarheid. *"Het afsluiten van een cybersecurityverzekering is een goede start.* De voorwaarden die bij zo'n verzekering horen, kun je zien als een praktische checklist voor je informatiebeveiliging. Daarnaast zet multi-factor authenticatie, bijvoorbeeld het invoeren van een inlogcode via de smartphone, een extra slot op de

"Een virusscanner of firewall *houdt kwaadwillenden echt niet tegen."*

deur naar je bedrijfsdata. Want hoe je het ook wendt of keert, de mens is vaak de zwakste schakel. Tot slot leidt het niet adequaat uitvoeren van patches en updates tot een snoepwinkel voor cybercriminelen. *Het zijn quick wins, want voor een structurele verbeterslag blijft permanente aandacht op directieniveau en regie op IT noodzakelijk."* ■