NIS2 MAAKT ONDERNEMERS WEERBAAR

HET ROMANTISCHE BEELD VAN DE

CYBERHACKER

IS WEG

Het zal rond 2019 zijn geweest. Toen transformeerde het bekende computerhacken, dat voor velen nog een romantische lading had, naar het *'big business'* cybercrime-model waarvoor je moet waken. Van cybercrime kan iedere ondernemer de dupe worden, weten *'cybercops' Michael Waterman en Kevin Venrooij* van ACA IT-Solutions, dochterbedrijf van accountants- en adviesorganisatie Crowe Foederer. Te vaak bespeuren zij nog de *'het zal allemaal wel loslopen'-houding* bij ondernemers. Ook voor hen is er goed nieuws. Met de komst van de cybersecuritywet NIS2 ligt er een gouden kans voor ondernemers om hun bedrijf echt weerbaar te maken.

TEKST *Ronald Frencken* | **FOTOGRAFIE** *Erik de Brouwer*

‘De hacker van vroeger is nu een DOORGEWINTERDE CRIMINEEL die alleen aan zichzelf denkt. *Hij opereert in bendes die in staat zijn een bedrijf in gijzeling te nemen*. Klaar ben je’

Michael en Kevin hebben een warm securityhart. In de 25 jaar dat Michael in het vak zit, waarvan een groot aantal bij Microsoft, reisde hij de hele wereld over om deze cyberveiliger te maken. Tot hij op zoek ging naar kalmer vaarwater. Kevin zit al achttien jaar in het cybervak, en had voorheen een eigen bedrijf in netwerken en netwerkbeveiliging. Beiden streken neer bij ACA IT-Solutions in Eindhoven. Hier helpen ze mkb-ondernemers om bewust te worden van de kwetsbaarheid van het bedrijfsnetwerk, en om stappen te zetten om zo veilig mogelijk te werken.

Romantisch beeld

De term cybersecurity doet voor velen nog romantisch aan. Maar hij detoneert met de realiteit, weet Michael. **“We kennen het beeld van Hollywoodfilms:** powerdialogen vol IT-termen, razendsnelle vingers over een toetsenbord, programmeercode die over het scherm rolt, een auto die met een paar muisklikken wordt gehackt, en op het einde een uitgeschakelde cybercrimineel. **Is dat realiteit? Nee. Realistisch is wél dat cybercrime in onze samenleving verhard is**. De hacker van vroeger is nu een doorgewinterde crimineel die alleen aan zichzelf denkt. Hij opereert vaak in bendes die in staat zijn een bedrijf in gijzeling te nemen door bestanden pas tegen de betaling van fors losgeld weer toegankelijk te maken. Klaar ben je.” **Het romantische is er wel vanaf**, wil Michael maar zeggen.

NIS2

Michael en Kevin zetten met hun team van cyberspecialisten dagelijks stappen om de beveiliging van netwerksystemen van opdrachtgevers op peil te brengen. Hun doel is om de beveiliging minimaal naar **NIS2-niveau** te brengen, het recent opgestelde, **door de EU vastgestelde beveiligingsniveau**. “De Network and Information Sercurity-wet is gericht op het weerbaarder maken van Europa, ook tegenover internationale grootmachten die landen in Europa willen ontwrichten”, zegt Kevin. “Waar de NIS1 er vooral is voor vitale organisaties die belangrijk zijn voor de samenleving, zoals waterschappen en energiebedrijven, is de NIS2 verplichte kost voor organisaties in achttien bedrijfssectoren die indirect van belang zijn voor de vitaliteit van onze samenleving, variërend van het transportwezen tot de gezondheidszorg, en van de levensmiddelenbranche tot de financiële sector, telefonie- en internetproviders. Heel veel bedrijven moeten dus verplicht cyberveilig worden om de continuïteit van onze samenleving te kunnen waarborgen.”

Nog maar weinig tijd

De NIS2-wet van de EU is inmiddels in de lucht. Over één jaar, in oktober 2024, moet de wet afgestemd zijn op de regels van de afzonderlijke EU-landen. **Dan gaat hij echt los**. “Dat betekent dat bedrijven nog een jaar de tijd hebben om hun zaken te regelen” zegt Michael, ”en **wij weten: die tijd heb je hard nodig**.”

Michael waarschuwt niet voor niets. Deed dat al talloze keren. Nu wéér. **Waarom zo aandringen?** “Dat heeft te maken met de bijzondere doelgroep waar wij voor werken: mkb-ondernemers”, legt hij uit. “Typisch is dat secundaire ondernemerstaken bij hen pas op het netvlies komen als het echt niet meer anders kan. Denk bijvoorbeeld aan de bhv, of brandbeveiliging of de verzekeringen. Ook zaken die je liever niet doet, maar je wel moet. Maar zet je er nu geen vaart achter, dan ben je te laat. Je kunt zelfs een boete krijgen als je het niet op tijd regelt, of aansprakelijk worden gehouden als je een cyberincident had kunnen voorkomen.”

Zaken goed op orde

Ondernemers die voorbij hun primaire ondernemerstaken kijken, zien de voordelen van de NIS2. “Als je voldoet aan de NIS2-richtlijn, dan zijn de zwakke plekken in de beveiliging gedicht”, weet Kevin. “Met de NIS2 houd je je cybersecurity goed op orde. Cyberaanvallen hebben dan nog maar beperkt impact, en ook de financiële gevolgen bij een incident zijn beperkt. Doordat de organisatie veerkrachtiger is, is ook de bedrijfscontinuïteit gewaarborgd. Ook naar buiten toe doen ondernemers met de NIS2 hun voordeel. De richtlijn draagt bij aan de reputatie van het bedrijf. Je toont als ondernemer aan dat je op cybergebied je zaakjes op orde hebt, en dat levert indirect concurrentievoordeel op. De kans is bovendien zeer groot dat overheden en bedrijven in vitale sectoren NIS2 als voorwaarde zullen gaan stellen aan hun leveranciers in het mkb.”

Essentiële diensten
Energie | Transport | Bankwezen | Infrastructuur financiële markt | Gezondheidszorg | Drinkwater
Digitale infrastructuur | Afvalwater | Overheidsdiensten | Ruimtevaart | Beheer van ICT-diensten

Belangrijke diensten
Digitale aanbieders | Post- en koeriersdiensten | Afvalstoffenbeheer | Levensmiddelen
Chemische stoffen | Onderzoek | Vervaardiging / manufacturing

Lekker niets doen

Michael en Kevin maakten het de laatste tijd al meermaals mee: ondernemers die maar wat blij zijn als ze horen dat ze niet onder de NIS2-richtlijn vallen, en 'lekker niets hoeven te doen'. Niet de juiste instelling, als je het hen vraagt. "Gekeken naar de letter van de wet ben je met minder dan vijftig werknemers inderdaad niet verplicht tot de NIS2", legt Michael uit. "Maar het is niet slim als je nu geen stappen zet. De overheid reikt nu gratis handvatten aan om de cyberweerbaarheid op peil te krijgen. **Doe daar je je voordeel mee**."

Kippenmest

"Wij kwamen laatst in contact met een organisatie waarvan het hoofdkantoor was gehackt", zegt Michael. "Ze moesten losgeld betalen om bestanden weer ter beschikking te krijgen. Er heerste paniek, niemand wist wat te doen. Totdat bleek dat de nevenvestigingen ondanks de hack gewoon doordraaiden, en er niet veel aan de hand was. Echter, had het bedrijf vooraf werk gemaakt van zijn weerbaarheid, dan hadden ze geweten dat het zwaartepunt niet bij het hoofdkantoor maar bij de vestigingen zelf lag. **Het is goed om vooraf te weten wat je assets zijn, zodat je daar werk van kunt maken**. Dat scheelt onrust." Veel ondernemers denken nog steeds dat het niet zo'n vaart zal lopen met hun bedrijf. Dat kan een kostbare misrekening zijn, weet Kevin. Hij vertelt over een bedrijf in de bio-energie dat handelde in kippenmest. "Vijf man in de kippenstront", vat hij het beeld samen, "en ze kwamen toch op de radar bij cybercriminelen. Hun netwerk bleek een makkelijk doelwit. Iedereen kan de dupe worden. **Ons devies: maak het de crimineel zo lastig mogelijk**. Dan gaat hij een deur verder. Daarvoor is de NIS2."

Online sleutels

Michael en Kevin, en met hen alle andere cybersecurityspecialisten, weten het zeker: het is een utopie om te denken dat je cybercriminelen voor kunt blijven, of dat het einde van cybercriminaliteit in zicht is. "Op internet verschijnen dagelijks digitale sleutels die criminelen helpen om overal binnen te komen. **En er ontstaan constant nieuwe zwakke plekken in een bedrijfsnetwerk**. Kwetsbare bedrijven komen zo vanzelf in beeld bij cybercriminelen. Het is zaak om daar snel op te anticiperen, bijvoorbeeld door werk te maken van goed isoleren. Of door het realiseren van een zorgvuldig zero trust-beleid, waarbij je als medewerker bij het inloggen eerst moet aantonen dat je bent wie je zegt te zijn."

Schaarsverlichte ramen

In de harde wereld van de cybersecurity is geen plaats voor romantiek. Zeker niet in Nederland. Maar de specialisten van ACA IT-Solutions prijzen zich gelukkig dat zij werken in Nederland. "**Ons land heeft het beste netwerk ter wereld, en huisvest hostingproviders met de allerbeste voorzieningen**", zegt Kevin. "Dat biedt cybercriminelen, die soms met een legertje mensen vanuit een locatie aan de andere kant van de wereld toeslaan, allerlei mogelijkheden." Het beeld van een somber flatgebouw met schaarsverlichte ramen, van waaruit honderden mensen op onverstaanbaar commando gelijktijdig een gecoördineerde online aanval uitoefenen op een onwetend bedrijfje in de Nederlandse polder, roept onwillekeurig een romantisch beeld op. **Dat beeld heeft met de realiteit niets van doen**. Actie en verantwoordelijkheid nemen, met NIS2 in als leidraad, geeft de ondernemer de gewenste bescherming en rust. ■

‘De NIS2 is verplichte, essentiële kost voor ORGANISATIES in achttien bedrijfssectoren. *Heel veel bedrijven moeten dus verplicht cyberveilig worden*’

KEVIN VENROOIJ & MICHAEL WATERMAN