‘Organiseer onafhankelijke security’

2021 liet veelvoudig zien dat cybercrime een van de top drie ondernemingsrisico’s is. We gaan in gesprek met drie MT-leden van informatiebeveiliger Northwave. Ze staan dagelijks bedrijven bij die slachtoffer zijn van een cyberaanval. Die harde realiteit levert waardevolle inzichten om uw digitale veiligheid te vergroten.

“Eén ding staat vast: voor digitaliserende bedrijven is informatieveiligheid een sleutelactiviteit, want je continuïteit is in het geding. Helaas is die sleutelactiviteit vaak geen kerncompetentie. Dat zien wij elke dag in de praktijk van ons Computer Emergency Response Team (CERT). Aanvallers leggen bedrijven plat met forse financiële schade, een gedeukte reputatie en verstrekkende ontregeling van supply chains tot gevolg.” Dat zegt Talitha Papelard, Director Security Office.

Inge van der Beijl, Director Behaviour en Training, vult aan: “Het is een heftige ervaring om als bestuurder met je rug tegen de muur te staan en voor miljoenen te worden afgeperst door meedogenloze criminelen. Daarbij: lijkt de ‘root cause’ van zo’n hack aanvankelijk nog een klik op een foute link of een uitgebuite kwetsbaarheid; achteraf blijkt de diepere oorzaak vaak een gebrek aan doortastend securitymanagement. Dat maakt het extra pijnlijk.”

Losgeld cybercriminelen

“Het klinkt vast gek om te horen van een techneut, maar veel organisaties kiezen een te technische benadering.” Dat zegt Christiaan Ottow, CTO en Director Cyber Security. “Zeker zijn er goede IT-securitytools. Maar dat betekent niet dat je alleen op technische maatregelen kunt vertrouwen. Of dat het IT-team de verantwoordelijkheid kan dragen voor de hele aanpak. De gevolgen daarvan zien wij terug in incidenten. Dan is de back-up er opeens toch niet, want er bleek geen check te zijn op de werking of op de back-up van de back-up. De restoptie is dan om het losgeld te betalen.”

Integraal uitbesteden

In de visie van Northwave gaat het om onafhankelijk adequaat beschermen. Niet te veel en niet te weinig doen en altijd verantwoordbaar de regie voeren. Steeds meer bedrijven besteden dat integraal aan Northwave uit. Van der Beijl: “Mensen werken dagelijks met digitale informatie. Innovatie en groei zorgen steeds voor nieuwe processen. Cybercriminelen verzinnen nieuwe werkwijzen. Mens en technologie moeten zich in de context van de bedrijfsvoering snel aanpassen. Dat lukt als je in samenhang stuurt op drie aspecten: Business, Bytes en Behaviour. Zo borg je de balans tussen actuele risico’s en adequate maatregelen.”

Christiaan Ottow en Inge van der Beijl:
‘De CFO wil in control zijn. Wij garanderen dat.’

Ottow vervolgt: “Als een cliënt ons vraagt: wat doen we om een nieuwe hack te voorkomen, is ons antwoord: regel een onafhankelijk security office in. Borg de kwaliteit met een *information security management system*. Dan werk je gericht aan volwassenheid en veerkracht. Certificeer eventueel, bijvoorbeeld tegen de ISO27001-norm. En als je al zo’n certificering hebt, wees dan zelfkritisch: is de security officer een spil in de organisatie of nog de compliancegedreven outsider waar iedereen omheen mag werken?”

Interdisciplinaire aanpak

Informatieveiligheid vraagt om een grote diversiteit aan expertise. Bij Northwave werken daarom bedrijfskundigen, techneuten, juristen, analisten, ethical hackers, crisismanagers, forensische onderzoekers, psychologen en gedragsexperts interdisciplinair samen aan security. Van der Beijl geeft een voorbeeld: “U weet dat hackers vaak binnenkomen door phishing. Dus zet u e-learning in. Minder bekend: uit onderzoek blijkt dat meer kennis ook leidt tot meer overmoed. De gebruiker denkt: ik weet het, dus het gebeurt me niet. Is gedragsverandering al een vak apart, dit thema is ook nog eens erg beweeglijk. Daarom stoppen onze intelligence-experts de meest actuele dreigingsinformatie in de impulsen van onze gedragswetenschappers. Dat heeft behalve awareness dan ook alert, actief en adequaat handelen als uitkomst.”

Papelard besluit: “Onafhankelijk securitymanagement is vaak nog geen praktijk. De ICT-serviceprovider beheert bijvoorbeeld de ICT, maar doet ook de securitymonitoring. Een gedetecteerde kwetsbaarheid wijst echter niet alleen op een zwakke plek, maar legt ook problemen bloot wat betreft het beheer – van diezelfde provider. Wellicht met de beste intenties: de slager keurt zijn eigen vlees. Met ons tweede paar ogen voorkom je blinde vlekken. Onze opdrachtgevers willen ‘in control’ zijn. Ze kiezen voor professionele aandacht voor hun digitale veiligheid. Dat is wat wij hen garanderen.”

Northwave bestaat sinds 2006 en is volgens Financial Times een van de duizend snelst groeiende bedrijven in Europa. Er werken bijna tweehonderd experts op de kantoren in Utrecht, Brussel en Leipzig aan de digitale veiligheid van middelgrote en grootzakelijke cliënten in alle sectoren. <