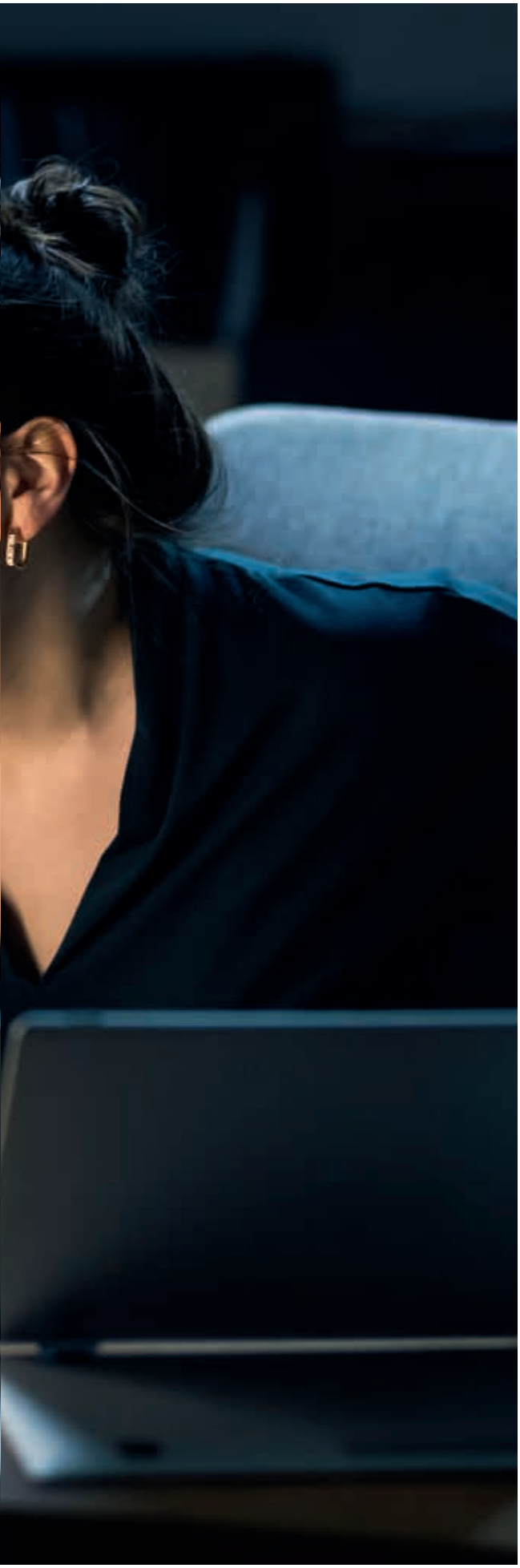
Gebukt onder cyberdreiging

Anno 2021 is er sprake van een volwassen cybercrimineel ecosysteem, meldt de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Hoe beïnvloedt deze loopgravenoorlog de accountant in business? En wie is het meest kwetsbaar? “Het is te ondoorzichtig geworden.”

TEKST **PETER STEEMAN** BEELD **ISTOCKPHOTO**



Trend Micro, wereldwijd marktleider op het gebied van cybersecurity-oplossingen, meldt een toename van 47 procent van cyberbedreigingen bij haar klanten over de eerste zes maanden van dit jaar. Zo'n 46 procent van de mkb-bedrijven in Nederland geeft aan dat ze ermee te maken hebben gehad. De schade van *ransomware* is groot. Schattingen lopen uiteen van miljoenen tot miljarden.
Moeten cyberdreigingen niet het domein vormen van IT-professionals die iets begrijpen van Trojaanse paarden, *malware* en geïnfecteerde servers? Nee, vindt Sander Zeijlemaker, directeur van Disem Institute. Hij geeft cursussen aan NBA-leden over de rol van financials bij cybersecurity. "Digitale veiligheid is onderdeel van de bedrijfsvoering, net als marketing en logistiek. Als je dat overlaat aan de IT-specialist, zet je het apart. Waarom wel praten over bedrijfspositionering maar niet over digitale veiligheid? Het is een holistisch vraagstuk dat raakt aan medewerkers, klantprocessen, werkplekken, intellectueel eigendom. Als financial heb je daarin een centrale rol, omdat je kan zien welke maatregelen elkaar versterken. Je kan over schuttingen kijken. Voorwaarde is dat je de dynamiek begrijpt en de instrumenten hebt om de juiste vragen te stellen."

De cybercrimineel is een tegenstander die voortdurend loert op een zwakke plek. Soms schiet hij met hagel, soms met een gerichte aanval. Daarom moet je wat je neerzet continu observeren en aanpassen. Zeijlemaker: "Traditioneel wordt er bij investeringen in *security* veel met lijstjes gewerkt. Vaak wordt uitgegaan van een *benchmark*. Voldoen we aan de beveiligingsstandaarden? Dat geeft niet zoveel zekerheid als je zou wensen. Standaarden geven houvast gebaseerd op het verleden. De aanvaller boeit het niet of je aan een standaard voldoet. Die zoekt continu naar een opening en als hij succesvol is schiet het aantal aanvallen omhoog. Na iedere aanval is er een reflex om te investeren, bijvoorbeeld in detectiesoftware. Dat betekent niet dat je daarmee klaar bent. Iedere keer als een proces wordt aangepast en nieuwe servers worden aangeschaft moet die detectiesoftware op die nieuwe servers worden geïnstalleerd. Dat lijkt een detail, maar de IT- en security-mensen hebben veel potjes op het vuur en werken onder hoge druk. Ze moeten naast het dagelijkse beheer de langetermijnstrategie invullen, juniormedewerkers opleiden en constant op incidenten reageren. Daarom moet de financial zich bij zo'n investering afvragen: hoe zorgen we dat die detectie op niveau blijft? De financial moet zich afvragen: Werkt het wat we doen?"

Tastbaar

"Mijn handen zouden jeuken om er mee aan de slag te gaan", antwoordt Pim Takkenberg, general manager Northwave, op de vraag of hij in de huidige tijd eindverantwoordelijk zou willen zijn voor de cybersecurity in een grote organisatie. "Je kan met eenvoudige maatregelen je beveiliging verhogen. Veel aanvallen zijn succesvol doordat systemen niet *up to date* zijn. Ze hebben bijvoorbeeld geen *backup* om op terug te vallen als data wordt versleuteld. Dat is gewoon een kwestie van eigenaarschap tonen in beleid en procedures. Verzamel de juiste mensen, agendeer het en bouw er een jaarlijkse cyclus overheen. De cfo heeft →

daarin misschien wel de belangrijkste rol omdat hij in veel gevallen security in zijn portefeuille heeft. Je moet er bovenop zitten. En reserveer tien procent van je IT-budget voor security. In de praktijk wordt geld makkelijker uitgegeven aan hardware. Dat is tastbaar.'
Iedere aanval fungeert als een *wakeupcall*, is de ervaring van Takkenberg. "De beste les is als het je overkomt. Dan wordt het concreet. Als bij een aanval de hele onderneming *out of business* is, zitten we dagelijks aan tafel met het management. We maken mee dat ze boos of verbijsterd zijn. Als er bewustwording is, komen er budgetten. Je ziet waar het mis is gegaan. Bij een gewone inbraak vind je moeilijk sporen, maar bij een digitale inbraak kun je vrijwel de hele route die cybercriminelen namen terugvinden. Soms moet je het management zelfs afremmen. We laten ze altijd beter beveiligd achter."
Het businessmodel van cybercriminelen lijkt vooralsnog gezonder dan dat van de verzekering tegen *ransomware* aanvallen. "Het totale bedrag wat bedrijven in Nederland aan premies betalen is 17 miljoen euro. Die premies zijn veel te laag", aldus Takkenberg. "Meestal wordt door ransomware-criminelen tussen de 0,4 en twee procent van de jaaromzet gevraagd. We zien dat in vier van de vijf gevallen wordt betaald."

Inleveren

Hoppenbrouwers Techniek werd op 2 juli getroffen door een cyberaanval. Geen gerichte aanval gelukkig, stelt businesscontroller Dirk Bakkers vast. "Op vrijdagavond merkte één van onze IT-medewerkers dat er niet meer op het systeem kon worden ingelogd. Al heel snel sloeg hij alarm en werden alle servers afgeschakeld. Omdat de hoofdaanval was gericht op Kasea, een leverancier wiens *tools* we gebruiken om op afstand software te beheren, bleef de schade beperkt. Op zaterdag zaten we met honderdvijftig man en ingehuurde experts op kantoor. Iedereen moest zijn laptop inleveren. Die werden net als de computers opnieuw geïnstalleerd. We hebben apparatuur die meerdere keren per dag een backup maakt. Dat bewees hier zijn dienst. Daardoor hadden we een heel goed en snel *recovery*-proces. Op zondagavond waren de meeste systemen weer operationeel. We hebben geen ransom betaald."
Wat heeft de aanval teweeggebracht? "Het maakt je nog meer bewust van de risico's, al moet ik zeggen dat die bewustwording er al was binnen de organisatie. Ik ben zelf in 2018 aangenomen als controller Projecten & risk, juist om aandacht te besteden aan een grotere alertheid van medewerkers ten aanzien van risicomanagement. De belangrijkste aanpassing die we naar aanleiding van de aanval deden was de inrichting van een *security operations center* dat onze servers monitort. En de premie van onze ransomware-verzekering steeg. Die verzekering verliep in augustus. De nieuwe premie is hoger, maar staat nog steeds in geen verhouding tot de mogelijke schade die een *ransomware*-aanval veroorzaakt. We zijn aan het onderzoeken of de verzekerde waarde van onze ransomware-verzekering in de toekomst niet verder omhoog moet."

'De aanvaller boeit het niet of je aan een standaard voldoet.'

Investeringslijstje

Het is jammer dat pas bij een aanval wordt onderkend hoe belangrijk je IT-infrastructuur is, vindt Andre van Wezel, director Finance & control bij cybersecurity-specialist Route443. "Eigenlijk moet cybersecurity aan bod komen tijdens je jaarlijkse strategische heisessie. Dan bespreek je waar je naar toe wilt en wat de belangrijkste risico's zijn waar je je tegen moeten wapenen. Dit is een bedrijfsrisico, net als de aanvoer van je grondstoffen. Wat doe je als er een

schip dwars ligt in het Suezkanaal? Over die risico's wordt wel gesproken. Hoelang kan je doorgaan zonder je netwerk? Met die vraag gebeurt niets. Ik heb de afgelopen jaren veel in de logistieke sector gewerkt als zelfstandig adviseur van het management bij operationele en strategische vraagstukken. In al die jaren zag ik nooit dat op het investeringslijstje stond dat er moest worden voorkomen dat criminelen via IT-systemen kunnen inbreken. Ondernemingen investeren liever in fysieke alarmsystemen om de loodsen vol waardevolle spullen te beschermen.
Ook aan de brandveiligheid wordt gedacht. Ondertussen wordt er ingebroken via een IT-netwerk waarvan niemand weet hoe kwetsbaar het is, terwijl de schade vele malen groter is."
De ongelijke strijd tussen bedrijven en cybercriminelen is volgens Van Wezel een direct gevolg van de grote veranderingen op IT-gebied. "De afgelopen vijf jaar is IT razendsnel getransformeerd naar de *cloud*. De traditionele IT-organisatie is daar nauwelijks op aangepast. Van een gesloten in eigenbeheeromgeving ga je over naar een omgeving die overal en nergens staat. Vijf jaar geleden kon je zien hoe een server was beveiligd. Ook als het een virtuele server was kon je onder de motorkap kijken. Nu werken we in de cloud. Dat is een kostenverhaal. De IT-afdeling haalt er een externe partij bij, maar kan niet langer doorgronden wat de zwaktes zijn. Als we bij *prospects* komen is de standaardreactie vrijwel altijd 'wij hebben het goed geregeld'. Hoe weet je dat? Dat vertelt mijn IT-afdeling mij. De werkelijkheid is dat ze het niet weten. Het is te ondoorzichtig geworden."

RANSOMWARE

Dat gebrekkige IT-beveiliging grote gevolgen kan hebben, werd in Nederland pijnlijk duidelijk toen grote Rotterdamse containerterminals van APM vanwege een *ransomware*-aanval in 2017 enkele dagen dicht moesten. Als gevolg daarvan moesten wereldwijd veel bedrijven langer wachten op hun goederen. De directe schade voor APM en de rest van de transportketen was naar schatting vele honderden miljoenen euro's.
De *hack* bij APM staat niet op zichzelf. In de afgelopen jaren waren *ransomware*-aanvallen schering en inslag, in allerlei sectoren. Systemen worden meestal geïnfecteerd doordat een medewerker op een link klikt in een mailtje. Wanneer systemen niet goed zijn beveiligd, kunnen *hackers* zichzelf vaak de toegang verschaffen tot alle IT-systemen van het bedrijf en data 'gijzelen'.
Meestal wordt niet prijsgegeven of, en hoeveel, er betaald is om data weer terug te krijgen, maar de schade loopt met regelmaat in de miljoenen. Eerder dit jaar werd vleesverwerker JBS gehackt, waardoor honderden vleesverwerkers in de Verenigde Staten en Australië de deuren moesten sluiten. Het bedrijf betaalde elf miljoen dollar om weer toegang te krijgen tot zijn systemen; de schade voor de hele vleesverwerkingsindustrie was aanzienlijk. Kortgeleden werd ook de Amerikaanse softwareleverancier Kaseya slachtoffer van een grote *ransomware*-aanval, waardoor alleen al in Nederland honderden bedrijven werden getroffen. Bedrijven lieten weten dat er vaak enkele miljoenen aan losgeld moest worden betaald.

Water

De redenering dat cloud-diensten cybercriminelen in de kaart spelen is te kort door de bocht, aldus Jos van Schaijk, cfo van Speakap, een SaaS-platform dat door bedrijven wordt gebruikt om hun interne communicatie te ondersteunen. "Professionele hackers zoeken de zwakke plekken. Zoals water stroomt naar de laagste plek, zo zijn aanvallen succesvol bij bedrijven die achterlopen. Ik heb mij de afgelopen acht jaar gespecialiseerd in SaaS- (*Software as a Service*) businessmodellen. Je praat over data en processen van klanten die op jouw platform draaien. Dat betekent dat je informatieveiligheid *top of the bill* moet zijn. Je moet dat kunnen aantonen met onder ander een ISO 27001-certificering en een SOC 2-verklaring. Dat geldt voor ons als aanbieder, maar ook voor onze leveranciers waaronder de hosting-partijen waar onze data draait."
Speakap heeft een *security officer*, een *dataprivacy officer*, een cto en een securityteam. Wat blijft er nog over voor de cfo? "Ik ben vooral gespitst op de *business continuity*. Als je door een aanval wordt geraakt, hoe snel zijn we dan weer *up and running*? Wat zijn de risico's? Is de klantdata optimaal beschermd? Daarvoor kijk ik naar rapportages en schuif aan bij vergaderingen van het securityteam. Ik wil weten welke software er draait. Waarom het nodig is en wat het kost. Je gebruikt de modernste technologieën, maar dat betekent niet dat je automatisch voor de duurste oplossing moet gaan."

Sloten

"De huidige golf van ransomware-aanvallen verrast mij absoluut niet", aldus Michel Zandbergen, manager bij FSV Risk advisory, adviesbureau in riskmanagement en internal audit. "Als criminelen een gat zien springen ze er in. In 2011 heb ik mij verdiept in *phishing*- en *malware*-aanvallen. Op dat moment hield ik mij bij ABN Amro bezig met security en intelligence management. De internetfraude steeg van tien miljoen euro in 2010 naar 35 miljoen het jaar daarop. Of bestuurders voldoende hun rol pakken hang af van de grootte van het bedrijf. Bij financiële instellingen zoals banken of verzekeraars en bedrijven die IT als hun corebusiness hebben wel. Multinationals hebben riskafdelingen en accountantskantoren die ze daarop kunnen *challengen*. Maar mkb-bedrijven, waar IT geen core competentie is, zijn kwetsbaar. Die hebben vaak ook een minder ontwikkelde riskafdeling. De bestuurders hebben er minder oog voor."
Zorg dat de juiste mensen nadenken over je IT-security, is het advies van Zandbergen. "In veel organisaties worden deskundigen te veel de operatie ingetrokken. Als je de hele dag druk bent met het controleren van de sloten, kom je te weinig toe aan een goede risicoanalyse. Dat ligt op het bord van de ciso, maar ook IT-auditors moeten daarin hun rol pakken. Ik geef les aan IT-auditors aan de VU in Amsterdam. In de jaarrekeningcontrole ligt de nadruk op de veiligheid en betrouwbaarheid van systemen en de daaruit voortkomende informatie. De risico's van cybersecurity vormen daar maar een bescheiden onderdeel van. Ik daag ze uit daar meer aandacht aan te besteden."←