Doeltreffende aanpak van cyberincidenten

BEDRIJVEN HOEVEN GEEN DOELWIT TE ZIJN OM SLACHTOFFER TE WORDEN VAN CYBERCRIMINALITEIT, STELT CEO INGE BRYAN VAN FOX-IT, DE SPECIALIST IN IT-BEVEILIGING MET MEER DAN TWINTIG JAAR ERVARING. HOE SNELLER BEDRIJVEN REAGEREN OP SIGNALEN VAN MOGELIJKE INDRINGERS, DES TE BEPERKTER DE SCHADE. "IEDER UUR SCHEELT HANDENVOL GELD."

Geen enkel bedrijf is immuun voor de dreiging van hackers of malware, stelt Inge Bryan, CEO van Fox-IT, opgericht in 1999 en daarmee het oudste IT-beveiligingsbedrijf in Europa, vermaard om zijn snelle en doeltreffende reactie op cyberincidenten. "Elk bedrijf zou zichzelf moeten afvragen hoe verstoringen in de IT zijn kernwaarden kunnen bedreigen. Je hoeft geen doelwit te zijn om slachtoffer te worden. Ook bedrijven met prachtige maatschappelijke doelstellingen kunnen platgehackt worden. Aanvallers kijken alleen of er wat te halen valt: geld, persoonsgegevens, intellectueel eigendom. De technologie kan in grote mate bepalen of je slachtoffer wordt van een bepaalde aanvalsmethode."
Bryan leidt Fox-IT sinds januari 2021. Aandacht voor het feit dat ze dit als vrouw doet in een sector waar mannen in de overgrote meerderheid zijn, voelt ongemakkelijk.

‘We hebben met afstand de meeste ervaring en verzamelen onze eigen dreigingsinformatie’

“Het gaat om de inhoud”, aldus Bryan. Het laat onverlet dat diversiteit in de organisatie volgens haar heel belangrijk is, op alle fronten. “Voor meer leeftijdsdiversiteit hebben we het bestuur verjongd. Het maakt echt uit dat ik twintig jaar scheel met de jongste bestuurder.” Daarnaast hecht Bryan grote waarde aan neurodiversiteit, de diversiteit in denken die collega’s met bijvoorbeeld autisme, ADHD of hoogbegaafdheid meebrengen. “Dat verwelkomen we zeer.”

Preventieve veiligheid

Het is volstrekt onvoorspelbaar of en wanneer een bedrijf te maken krijgt met een cyberaanval, zoals het evenmin te voorkomen is dat ooit ergens brand uitbreekt. Er zijn meer parallellen: goede preventie kan de schade beperken, net als vooraf oefenen wat te doen bij een aanval of brand. Vertaald naar IT betekent het volgens Bryan onder meer dat bedrijven hier om te beginnen goed voor moeten zorgen. “Weten wat je in gebruik hebt, software up-to-date houden. Dat is de basis. Dan is er nog geen veiligheidsexpert aan te pas gekomen.” Een ander advies is om een draaiboek te maken voor een cyberaanval, naar analogie van dat voor een brand, waarin staat of je de lift nog mag gebruiken. “Moet iedereen uitloggen of juist niet?”

Verder wil Bryan organisaties op het hart drukken dat de vervangingscyclus in de IT vele malen korter is dan die in de operationele techniek. “Apparatuur of software die nog werkt is aan vervanging toe zodra de fabrikant die niet meer ondersteunt en geen nieuwe beveiligingsupdates meer uitbrengt.” Ze snapt het als overheidsinstellingen geld dan bij voorkeur anders besteden, maar vanuit beveiligingsperspectief is dat een slechte keuze.

Bryan pleit ook voor een gecoördineerde aanpak van cyberdreiging, bijvoorbeeld door oefeningen per veiligheidsregio te organiseren en informatie over aanvallen nog beter te delen tussen bedrijven. De benoeming van een staatssecretaris voor digitalisering in kabinet-Rutte IV is een andere positieve ontwikkeling. “Niet eerder heb ik een bewindspersoon zo expliciet horen zeggen dat cybersecurity een grondrecht is dat de overheid dient te beschermen.”

Beveiligingsexpertise

Fox-IT komt bij veel bedrijven binnen na een incident, variërend van een aanval met gijzelsoftware tot minder duidelijke verstoringen: het valt op dat er iets niet in de haak is, zonder dat precies aan te geven is wat. Om de vergelijking met brand nogmaals te maken: als ergens rook begint te kringelen, is er iets aan de hand. “Bedrijven hebben de neiging om eerst zelf te gaan zoeken naar de oorzaak, maar het beste is dat ze ons zo snel mogelijk bellen.” De groei van de organisatie, die inmiddels meer dan vijfhonderd experts telt, bewijst dat dit steeds vaker gebeurt. In Nederland en tegenwoordig ook meer en meer elders in Europa.

Waarom juist Fox-IT? “Omdat we de beste zijn”, zegt Bryan gedecideerd. “We hebben met afstand de meeste ervaring en verzamelen onze eigen dreigingsinformatie over wat zich op het net beweegt, met name wat criminele groepen daar doen. Zodoende kunnen we sneller dan wie ook reageren bij incidenten en effectiever optreden.”

Fox-IT richt zich bij het opsporen van incidenten vooral op datapakketjes met het grootste risico, met dank aan hiervoor speciaal ontwikkelde software. “Zo kunnen we onze analyse veel sneller maken.” Het belang van snelheid valt niet te onderschatten. “Ieder uur scheelt handenvol geld. Dat kan tot tonnen en bij grotere bedrijven tot miljoenen schelen. Getroffen bedrijven kunnen we helpen met een plan om de impact van cyberdreiging in de toekomst te beperken.” En, besluit Bryan: “We stellen het belang van onze klanten echt centraal. Onze experts zijn 24/7 beschikbaar én we zijn flexibel genoeg om op locatie te werken als klanten dat willen.”

DEEL ONLINE