CYBERCRIMINALITEIT IS ALOMTEGENWOORDIG. ER GAAT GEEN DAG VOORBIJ OF JE LEEST IN DE KRANT OVER WEBSITES DIE GEHACKT ZIJN, ONVEILIGE WIFI-VERBINDINGEN EN RANSOMWARE DIE COMPUTERS GIJZELT EN PAS NA BETALING VAN LOSGELD VRIJGEEFT. ALS KLAP OP DE VUURPIJL WAS ER LAATST HET NIEUWS DAT DE ANTIVIRUSSOFTWARE VAN KASPERSKY MOGELIJK ZELF GEHACKT IS, ZONDER DAT ZE HET DOOR HADDEN.

Wapen jezelf tegen cyberaanvallen

Het moge duidelijk zijn: het negeren van cyberrisico's is de slechtst denkbare verdediging. Ruim zestig procent van de ondernemers in Nederland geeft aan wel eens te maken te hebben gehad met cybercrime. De schade voor bedrijfsleven en overheid bedraagt zo'n 10 miljard euro, berekende Deloitte in 2016. Ter vergelijking: de schade door 'gewone' diefstal bedraagt jaarlijks ongeveer 1 miljard euro.

Zeker in onze branche is het voor de continuïteit van ondernemingen van groot belang dat ze zich bewust zijn van de cyberrisico's die ze lopen en zich wapenen tegen cybercrime. Meer dan 95 procent van de financieel dienstverleners geeft namelijk aan dat hun bedrijfsvoering in (zeer) grote mate afhankelijk is van computers en internet.

'Maak iemand verantwoordelijk voor ICT-zaken'

Tel daarbij op dat we werken met persoonlijke en vertrouwelijke persoons- en bedrijfsgegevens van onze klanten en het belang van een veilige cyberomgeving is zonneklaar. Zowel voor de financieel dienstverlener zelf als voor zijn klanten.

Gezien het belang van een goede verdediging tegen cybercrime, nam Adfiz in 2016 met vier andere brancheorganisaties deel aan de pilot 'veilig zakelijk internetten' van MKB-Nederland en VNO-NCW. Dit leverde een praktisch stappenplan op. De route naar optimale bescherming tegen cybercriminaliteit telt vijf stappen. Deze zijn niet alleen van technische aard, maar vooral ook organisatorisch gericht.

CREËER BEWUSTZIJN

Zorg dat iedereen binnen de onderneming de gevaren van online zijn kent. Dat betekent dat niet alleen de verantwoordelijke voor de ICT-omgeving dit tussen de oren moet hebben, maar werkelijk iedereen: van werkvloer tot management. Zo wordt draagvlak gecreëerd voor maatregelen en beleid.

NEEM TECHNISCHE MAATREGELEN

Maak iemand (intern of extern) verantwoordelijk voor ICT-zaken en laat deze collega onderzoeken of de beveiligingsinstellingen goed staan ingesteld en de juiste toegangsprocedures worden gebruikt voor zowel hard-

als software. In deze stap hoort tevens het gebruik van goede antivirussoftware of firewalls thuis. Het gebruik van veilige verbindingen voor je eigen website, zoals met een Secure Socket Layer (SSL) certificaat (herkenbaar aan het hangslotje in de browserbalk), verdient aanbeveling. Uiteraard is het ook belangrijk dat de instellingen regelmatig worden gecheckt en dat software updates krijgt.

REGEL EEN AANSPREEKPUNT

Wijs een medewerker aan die alle meldingen verzamelt en vragen over digitale veiligheid kan beantwoorden.

PAK MISBRUIK AAN

Zorg dat je medewerkers steeds goed voorlicht over je aanpak om cyberrisico's te minimaliseren. Maak ook duidelijk welke rol medewerkers hierin spelen en wat je van ze verwacht. Denk dan aan het nut van sterke, regelmatig wijzigende wachtwoorden. Wat ook goed werkt bij het creëren van bewustzijn is, aan de hand van cases laten zien hoe cybercriminelen te werk gaan. Phishing mails en nepwebsites ogen vaak bedrieglijk echt. Tot slot, wie zijn onderneming wil beschermen tegen cybercriminaliteit ontkomt er niet aan om streng op te treden tegen nalatige gebruikers. Wees daar open en duidelijk over.

ZORG VOOR HERSTELMAATREGELEN

Ondanks alle maatregelen die je treft, kan het toch voorkomen dat cybercriminelen een voet tussen de deur krijgen. Het spreekt dan ook voor zich dat je backups hebt van bestanden. Zorg er ook voor dat er een draaiboek is waarin staat wat te doen als de onderneming toch getroffen is door cybercriminaliteit. Ook zulke herstelprocedures zijn in feite preventieve maatregelen. Ze voorkomen dat de bedrijfscontinuïteit in gevaar komt. ■

Dit artikel wordt u aangeboden door Adfiz

Aan de slag met cybersecurity

VNO-NCW, MKB Nederland en enkele brancheorganisaties, waaronder Adfiz, hebben een uitgebreid ondersteuningspakket ontwikkeld waarmee je direct aan de slag kunt. Deze Cyber Academy helpt te bepalen aan welke zaken je aandacht moet besteden om goed voorbereid te zijn op een cyberaanval. Daarnaast worden er drie minicursussen aangeboden. Deze bieden meer inzicht en helpen bij het ontwikkelen van vaardigheden. Als je denkt dat je onderneming goed opgewassen is tegen cybercriminaliteit, dan volgt de ultieme test: de Cyber Risico Scan. Deze gratis applicatie geeft inzicht in het beveiligingsniveau van je website en bedrijfsnetwerk. Cyberrisico's vormen uiteraard ook een gevaar voor klanten. Het stappenplan om voorbereid te zijn tegen cybercriminaliteit heeft dan ook betrekking op je klantenkring, zowel zakelijk als particulier. Daarnaast ontwikkelen steeds meer verzekeraars speciale cyberpolissen. Zelf aan de slag met cybersecurity? Kijk op *adfiz.nl/cyber*