MS Amlin: Data zijn de kroonjuwelen van jouw bedrijf

Wanneer je als bedrijf niet bij je data kunt, dan kunnen de gevolgen enorm zijn. “De data van een bedrijf zijn echt je kroonjuwelen”, stelt Patricia Langermans, Specialist Underwriter Cyber bij MS Amlin. “Hackers zijn vaak niet eens geïnteresseerd in jouw data, ze weten wel dat jij ervoor wilt betalen.”

Dat cybersecurity inmiddels een belangrijk item is, moge duidelijk zijn. In Nederland alleen al bedraagt de jaarlijkse economische schade € 10 miljard. 60% van de Nederlandse bedrijven heeft met een of andere vorm van cybercrime te maken. “Ik durf zelfs te stellen dat dit bijna 100% is”, zegt Patricia Langermans. Cybercriminelen zitten gemiddeld 11 maanden in je systeem voordat je dit ontdekt. “Dat betekent dat iemand dus al geruime tijd in je systemen heeft kunnen rondsnuffelen en al ik weet niet wat aangericht kan hebben.” 63% van de gemelde datalekken bij de Autoriteit Persoonsgegevens heeft als oorzaak het verkeerd versturen van persoonsgegevens. “Dat laat dus zien dat het heel vaak om menselijke fouten gaat”, stelt Langermans.

Steeds professioneler

Cybercriminelen worden steeds professioneler. Kon je vroeger een phishingmail herkennen aan de talloze spelfouten, inmiddels is het nauwelijks nog van het origineel te onderscheiden. “Nog steeds hebben cybercriminelen financiële instellingen en ziekhuizen in het vizier, maar het beperkt zich allang niet meer tot alleen de grote bedrijven. Ook particulieren en het midden- en kleinbedrijf zijn steeds vaker slachtoffer van hackers. Vaak gaat het daarbij om zogeheten ransomware. Je krijgt pas weer toegang tot je data als je het losgeld hebt betaald. Bovendien plaatsen we op sociale media veel berichten zoals waar we naar toe op vakantie zijn of waar we wonen. Een hacker die uit is op je geld of je identiteit wil stelen, hoeft alleen maar (bijna) alles wat je zelf bekend maakt te combineren. Recent hoorde ik een verhaal van een bedrijf dat op verzoek van de directeur, die naar een exotische bestemming op vakantie was, een bedrag met spoed had overgeboekt in verband met een calamiteit. Pas bij het tweede verzoek om geld over te maken, kregen ze argwaan. De hacker wist precies wie de directeur was, waar hij werkte en dat hij op vakantie was. Het personeel had dus in eerste instantie ook geen argwaan, want het klopte allemaal. Zo makkelijk is het dus”, zegt Langermans.

MS Amlin is een toonaangevende verzekeraar, onderdeel van de wereldwijde top-10 verzekeringsgroep MS&AD. Als expert begrijpen wij het belang van een goede CyberHealth. Onze Cyberverzekering biedt een zeer uitgebreide dekking en ook directe ondersteuning om schade te beperken.

Creëer vooral bewustwording

Geen angst creëren

Ondanks dat bovenstaande voorbeelden angstig zijn, wil Langermans wegblijven van angst creëren. “Internet is niet meer weg te denken uit ons leven. Wat bedrijven wel moeten doen is meer bewustwording creëren zodanig dat zij attent zijn op alle mogelijke vormen waarin cyberincidenten zich kunnen aandienen. Bovendien kunnen bedrijven zelf ook al veel doen ter voorkoming van cyberincidenten. Kijkend naar de werkvloer en wetende dat de mens vaak de zwakste schakel is, begint daar de bewustwording. Zorg voor een goed plan, verzorg trainingen voor je personeel, hanteer een goed wachtwoordenbeleid, laat geen usb-sticks rondslingeren. Een tas vol met dossiers mee naar huis, kan ook al een datalek veroorzaken. Het heeft zeker niet altijd alleen maar met IT te maken”, betoogt Langermans.

Informatiebeveiliging

Volgens Langermans is door de digitalisering en de AVG het beveiligen van informatie ‘key’. “Dat is voor ons het uitgangspunt geweest bij de ontwikkeling van onze Cyberverzekering. Het beveiligen van informatie voorkomt dat kritische bedrijfsinformatie in de verkeerde handen valt. Het is een doorlo-

Patricia Langermans: "Effectieve risicoanalyse en crisisbeheersing zijn essentieel geworden om de naam en reputatie van je bedrijf te beschermen".

pend proces, met twee doelen: de bedrijfscontinuïteit veiligstellen en schade voorkomen. Wij hanteren een unieke benadering door aan te sluiten op de meest cruciale componenten van informatiebeveiliging: Beschikbaarheid, Integriteit en Vertrouwelijkheid. Bij **beschikbaarheid** gaat het om het waarborgen dat geautoriseerde gebruikers tijdig toegang hebben tot informatie. **Integriteit** gaat om het waarborgen van de juistheid en volledigheid van informatie. Bij **vertrouwelijkheid** gaat het om het waarborgen dat informatie alleen toegankelijk is voor geautoriseerde personen. Uiteindelijk gaat het om de keten Mens – Proces – Techniek", zegt Langermans.

First Response Team

Met de op 7 mei gelanceerde Cyberverzekering speelt MS Amlin hierop in. "Ik ben mega-trots op deze verzekering. Naast de financiële compensatie, hebben we een daadkrachtig hulpteam 24/7 klaarstaan. De verzekering is geschikt voor alle soorten bedrijven. Van start-ups tot grote internationale ondernemingen. Bij ons geen losse modules, gewoon een zeer uitgebreide dekking, die rust en gemak biedt. Wij hebben er ook voor gekozen om een inloopdekking van 2 jaar in te bouwen, voor de eerste 72 uur geldt geen eigen risico voor het inschakelen van ons First Response Team. Wij adviseren ook altijd meteen te bellen als men denkt dat er sprake is van een cyberincident. Liever een keer te veel gebeld, dan dat wij te laat worden ingeschakeld", aldus Langermans.
Voor het First Response Team werken wij samen met een aantal gerenommeerde partners. Dat is International Security Partners voor het directe crisismanagement. Kennedy Van Der Laan voor alle juridische vraagstukken, Grant Thornton voor forensisch onderzoek en IT-ondersteuning en Bex*communicatie voor de in- en externe communicatie in het kader van imago- en reputatieschade. Bovendien kunnen onze verzekerden tegen een gereduceerd tarief een Online Cyber Risicoanalyse laten uitvoeren. De resultaten hiervan zijn niet van invloed op de hoogte van de premie. Het helpt wel om inzicht te krijgen waar je nu staat en welke stappen je nog kunt zetten om je onderneming veiliger te maken. Daarnaast bieden wij ook een e-learning Cyber Awareness aan.

Ondersteuning makelaars

Onze aangesloten makelaars kunnen rekenen op adequate ondersteuning zodat zij hun klanten goed te woord kunnen staan. Wij verzorgen trainingen en tijdens ons event begin juni hebben wij een cybergame gespeeld. Dat gaf de aanwezige makelaars al zoveel inzicht in de risico's en maatregelen die jezelf kunt treffen en ook hoe zij hun eigen klanten daarin kunnen adviseren. Langermans: "Bovendien ben ik zelf beschikbaar om de makelaars te ondersteunen. Ik heb zelf bij een makelaar gewerkt en de laatste vijf jaar klanten geadviseerd in het managen van cyberrisico's."

Lees meer over de Cyberverzekering op msamlin.com/cyberverzekering.