



COLUMN VAARTWEG 81

Cybercriminaliteit

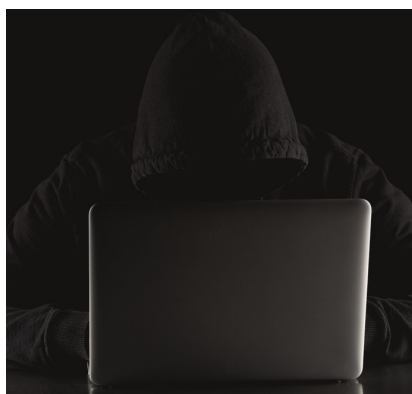
Cybercriminaliteit is overal om ons heen. Er gaat geen dag voorbij of je leest in de krant over websites die gehackt zijn, onveilige wiferverbindingen en ransomware die computers gijzelt en pas na betaling van losgeld weer vrijgeeft.

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. Ter vergelijking: de schade door 'gewone' diefstal bedraagt jaarlijks ongeveer 1 miljard euro.

Zeker in de medische wereld 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. Ook de tandtechnicus beschikt over veel persoonlijke en vertrouwelijke, al dan niet medische persoonsgegevens van patiënten en het belang van een veilige cyberomgeving is zonneklaar. De route naar een optimale bescherming tegen cybercriminaliteit telt vier eerste 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.



Maak iemand verantwoordelijk

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 verdient aanbeveling. Uiteraard is het ook belangrijk dat de instellingen regelmatig worden gecheckt en dat software updates krijgt.

Geef periodiek voorlichting

Zorg dat medewerkers steeds goed voorgelicht worden over de aanpak om cyberrisico's te minimaliseren. Maak ook duidelijk welke rol medewerkers hierin spelen en wat van ze

verwacht wordt. Denk daarbij aan het nut van sterke, regelmatig wijzigende wachtwoorden.

Maak een calamiteitenplan

Ondanks alle maatregelen kan het toch voorkomen dat cybercriminelen een voet tussen de deur krijgen. Het spreekt dan ook voor zich dat er back ups zijn van bestanden. Zorg ook voor een draaiboek waarin staat wat te doen als de onderneming toch getroffen wordt door cybercriminaliteit. Ook zulke herstelprocedures zijn in feite preventieve maatregelen. Ze voorkomen dat de bedrijfscontinuïteit in gevaar komt. Ook al zijn alle preventieve maatregelen genomen, dan nog zou het kunnen dat een cybercrimineel toegang tot uw ICT systeem krijgt en mogelijk privacygevoelige gegevens kan verwerken. De kosten die met het herstel daarvan te maken hebben, zouden verzekerd kunnen worden op een cyberverzekering. Dan gaat het niet alleen over uw aansprakelijkheid jegens derden, maar ook over uw eigen kosten als forensisch onderzoek en bedrijfsschade.

Wilt u meer informatie over relevante verzekeringen voor onze branche, neem dan contact op met Theo Vijfhuizen van Steijnborg Assurantiën op 035-6238940.

