De gemiddelde kost van cyberincidenten voor kleine bedrijven is ongeveer 145.000 euro, voor middelgrote bedrijven 500.000 euro en voor grote bedrijven kan dit oplopen tot meer dan 1,5 miljoen euro. Dit bedrag omvat niet alleen directe kosten zoals productieverlies en crisismanagement, maar ook verborgen kosten zoals reputatieschade en juridische boetes. Desondanks blijkt uit recent onderzoek van CyberContract dat de overgrote meerderheid van de kmo's onvoldoende maatregelen neemt om hun digitale veiligheid te waarborgen.

Bedrijfsadvies

Kmo's onderschatten de gevolgen van ontoereikende cyberbeveiliging

Veel bedrijven realiseren zich niet hoe kwetsbaar ze zijn voor cyberaanvallen. "Het gaat niet alleen om grote ransomware-aanvallen, maar ook om datadiefstal, factuurfraude, identiteitsfraude … Die worden veelal mogelijk gemaakt door simpele menselijke fouten of technische tekortkomingen zoals onveilige wachtwoorden, verouderde software of het niet gebruiken van multi-factor authenticatie (MFA)," legt Stef Vermeulen General Manager van CyberContract uit.

"Door de toename van digitale kwetsbaarheden kunnen hackers eenvoudig toegang krijgen tot bedrijfssystemen via onveilige applicaties, verkeerd geconfigureerde e-mailinstellingen of open poorten in bedrijfsnetwerken."

CyberContract heeft recent 309 Belgische kmo's gescand om hun digitale beveiliging in kaart te brengen. De resultaten zijn zorgwekkend: op een schaal van A (zeer goed) tot F (zeer slecht) behaalde geen enkel bedrijf de hoogste beveiligingsscore 'A' en maar 15% van de bedrijven scoorde een 'B'. 41% van de bedrijven behaalde een gemiddelde 'C'-score, wat betekent dat er dringend actie nodig is om de digitale kwetsbaarheden aan te pakken. Bovendien bevindt meer dan 43% van de bedrijven zich in de 'rode zone' met een score 'D' of 'F', wat hen bijzonder vatbaar maakt voor cyberaanvallen.

"Het is essentieel dat bedrijven hun 'openstaande digitale ramen en deuren' sluiten," stelt Stef Vermeulen. "Veel bedrijven onderschatten de impact van datalekken en slecht geconfigureerde e-mailbeveiliging, die cybercriminelen in staat stellen identiteitsdiefstal en gerichte phishingaanvallen uit te voeren. Deze twee veelvoorkomende digitale 'open ramen en deuren' bieden hackers een gemakkelijke toegangspoort om zonder enige vorm van inbraak de identiteit van het bedrijf én haar medewerkers over te

nemen.. Wij adviseren bedrijven daarom om e-mailbeveiliging zoals SPF (Sender Policy Framework) en DMARC (Domain-based Message Authentication, Reporting & Conformance) correct in te stellen en DNSSEC (Domain Name System Security Extensions) te implementeren om identiteitsfraude te voorkomen."

Uit het onderzoek blijkt dat maar liefst 53% van de bedrijven e-mailadressen heeft die betrokken zijn geweest bij datalekken, wat de kans op misbruik van vertrouwelijke gegevens vergroot. Daarnaast heeft 51% van de bedrijven de SSL/TLS-beveiliging niet correct ingesteld, waardoor ze kwetsbaar zijn voor cyberaanvallen via nepwebsites die op legitieme platforms lijken.

Stef Vermeulen, General Manager van CyberContract

Naast technologische maatregelen is de bedrijfscultuur van cruciaal belang. Medewerkers moeten bewust worden gemaakt van de risico's van cybercriminaliteit en de noodzakelijke veiligheidsmaatregelen die ze moeten nemen om het bedrijf te beschermen. "De beste technologie is nutteloos als de mensen binnen het bedrijf niet voortdurend bezig zijn met de cyberveiligheid van hun bedrijf," voegt Stef Vermeulen toe. Het is net als autorijden: je kan dit niet veilig doen als je maar af en toe oplet. Bedrijven hebben buiten de almaar strenger wordende wetgeving (NIS2, DORA…) de morele plicht te investeren in digitale veiligheid en moeten zich voorbereiden op het geval er toch iets misgaat. Vermits de gemiddelde kmo geen incident response team heeft, kan een kwalitatieve cyberverzekering hulp bieden om snel en effectief te reageren bij een incident.

CyberContract biedt zo'n verzekeringsoplossing aan die gericht is op risico's zoals datalekken, ransomware-aanvallen en bedrijfsstilstand door IT-verstoringen. Daar hoort ook gespecialiseerde hulp bij (24/7 Hotline, IT-Forensic- en juridische experten). Het product is speciaal ontworpen voor kmo's en middelgrote organisaties en biedt ook preventieve diensten aan, zoals het in kaart brengen van de openstaande digitale ramen en deuren, cybersecurity coaching, assessments (technische scanning & auditing) en training voor medewerkers. CyberContract wordt ondersteund door AG Insurance en Euromex.

> **"Verzekeringsadviseurs moeten hun klanten meer op de gevaren wijzen"**

DIGITALE RAMEN EN DEUREN

Ramen en deuren sluiten als je vertrekt, dat doet iedereen zonder erbij na te denken. Maar verrassend genoeg vergeten veel bedrijfsleiders dat ook hun digitale ramen en deuren dicht moeten blijven om cybercriminelen buiten te houden. De kans op een bedrijfsinbraak is 1:250, de kans op een cyberaanval is 1:5 volgens een studie van VLAIO (het Vlaams Agentschap voor innoveren en ondernemen, www.vlaio.be).