expertenReport

Quelle: experten.de, KI-generiert

Cyber-Angriffe: Jedes dritte betroffene KMU sieht Existenz gefährdet

Nathalie Pappelbaum

Cyber-Angriffe können für kleine und mittlere Unternehmen schnell zur wirtschaftlichen Belastungsprobe werden. Eine aktuelle Untersuchung zeigt, welche Folgen erfolgreiche Attacken haben – und dass zwischen dem Bewusstsein für Cyber-Risiken und den verfügbaren Budgets weiterhin eine Lücke besteht.

Im internationalen Vergleich sind deutsche KMU vergleichsweise häufig versichert. 39 Prozent verfügen über eine vollumfängliche Standalone-Cyber-Versicherung, weltweit sind es 31 Prozent. Weitere 32 Prozent der deutschen Unternehmen haben Cyber-Gefahren über eine andere Versicherung abgedeckt.

Finanzbetrug und DDoS-Attacken besonders häufig

Bei den erfolgreichen Angriffen steht Finanzbetrug durch Payment Diversion mit 45 Prozent an erster Stelle. DDoS-Attacken folgen mit 42 Prozent. Bei 40 Prozent der erfolgreichen Angriffe wurden IT-Ressourcen missbraucht.

Weitere Angriffsergebnisse waren der Verlust unverschlüsselter Daten mit 35 Prozent und verschlüsselter Daten mit 28 Prozent. Ransomware- und Erpressungsfälle machten 27 Prozent aus.

Die Folgen können den laufenden Geschäftsbetrieb erheblich beeinträchtigen. Betroffene deutsche KMU standen nach einem erfolgreichen Angriff im Durchschnitt 41,7 Stunden still. Im weltweiten Vergleich waren es 31,6 Stunden.

Reputationsschäden werden stärker gefürchtet

Auffällig ist die Diskrepanz zwischen wahrgenommenen und tatsächlich eingetretenen Folgen. 48 Prozent der deutschen KMU nennen Reputationsschäden als ihre größte Befürchtung.

Unter den tatsächlich betroffenen Unternehmen berichten jedoch 25 Prozent von einer negativen Öffentlichkeitswirkung, 21 Prozent vom Verlust von Geschäftspartnern und 18 Prozent vom Verlust von Kunden.

Gleichzeitig gewinnen Cyber-Risiken auf Managementebene an Bedeutung. Nach einem Angriff koppeln 41 Prozent der deutschen Unternehmen die Vergütung der Führungsebene an Cyber-Security-Ziele. Global liegt dieser Anteil bei 32 Prozent.

„Viele deutsche KMU sind für Cyber-Risiken sensibilisiert und investieren in Absicherung. Ein erfolgreicher Angriff kann dennoch schnell existenziell werden. Im Ernstfall zählen vor allem Liquidität, Geschäftsbetrieb und schnelle Unterstützung“, sagt Klemens Lemke, Underwriting Manager Cyber bei Hiscox. Eine vollwertige Standalone-Cyber-Versicherung könne finanzielle Schäden abfedern und Unternehmen mit Expertenhilfe durch einen Vorfall begleiten.

Mehrheit investiert in Cyber-Resilienz

Die große Mehrheit der deutschen KMU reagiert auf die wachsenden Risiken. 97 Prozent ergreifen Maßnahmen zur Stärkung ihrer Cyber-Resilienz. Am häufigsten investieren die Unternehmen in aktualisierte Security-Trainings (65 Prozent), zusätzliches Personal (59 Prozent) und Software (55 Prozent).

Die finanziellen Mittel bleiben allerdings häufig begrenzt. 58 Prozent geben pro Jahr weniger als rund 8.700 Euro beziehungsweise 10.000 US-Dollar für entsprechende Maßnahmen aus. Zwölf Prozent investieren überhaupt nichts.

KI schafft zusätzliche Cyber-Risiken

Auch Künstliche Intelligenz verändert die Risikowahrnehmung. Als größte KI-bezogene Bedrohung für die kommenden fünf Jahre nennen 45 Prozent der deutschen KMU Data Poisoning.

Es folgen Schwachstellen durch KI-Tools von Drittanbietern wie ChatGPT mit 44 Prozent. 43 Prozent sehen eine zu starke Abhängigkeit von KI beziehungsweise eine nachlassende menschliche Kontrolle als Risiko. Ebenso viele befürchten, dass KI die Kontrolle über Unternehmensdaten übernehmen könnte.

Damit wächst für Unternehmen der Druck, Cyber-Risiken nicht nur technisch, sondern auch strategisch und organisatorisch zu berücksichtigen.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4951894/Cyber-Angriffe-Jedes-dritte-betroffene-KMU-sieht-Existenz-gefaehrdet/