expertenReport

Quelle: DALL-E

Angriffswelle auf den Mittelstand

Michael Fiedler

Mehr als zwei Drittel der deutschen Unternehmen waren im vergangenen Jahr Ziel von Cyber-Attacken. Besonders häufig betroffen: Zahlungsumleitungsbetrug, DDoS-Angriffe und Datenverluste. Der Hiscox Cyber Readiness Report 2025 zeigt, wie vielfältig die Angriffsmuster geworden sind – und welche wirtschaftlichen Folgen sie nach sich ziehen.

Die Angriffspunkte sind breit gestreut. 81 Prozent der Unternehmen sehen ihre eigene IT-Infrastruktur als häufigstes Einfallstor – von internen Servern über Cloud-Dienste bis hin zu mobilen Geräten und IoT-Systemen. Auch Angriffe über Lieferketten oder kompromittierte E-Mails gehören inzwischen zum Alltag. Besonders verbreitet ist der sogenannte Zahlungsumleitungsbetrug (Payment Diversion Fraud): 43 Prozent der betroffenen Betriebe gaben an, Opfer dieser Masche geworden zu sein.

Ebenfalls stark zugenommen haben DDoS-Attacken, die Webseiten oder Geschäftsprozesse gezielt lahmlegen, sowie der Missbrauch von IT-Ressourcen, etwa zum Schürfen von Kryptowährungen oder Hosten von Malware. Knapp ein Drittel der Befragten verlor den Zugriff auf verschlüsselte oder unverschlüsselte Daten. In rund jedem fünften Fall kam es zu einer Ransomware-Erpressung – mit teils gravierenden finanziellen und operativen Folgen.

Doch die wirtschaftlichen Schäden sind nur ein Teil des Problems. Der Report dokumentiert auch die sozialen und psychischen Auswirkungen innerhalb der Unternehmen. Rund 36 Prozent berichteten von erhöhtem Stress in der Belegschaft, 31 Prozent sogar von Burnout-Fällen nach einem Cyber-Vorfall. Zudem stiegen in jedem vierten Unternehmen die Krankenstände spürbar an. Neben direkter finanzieller Belastung und Reputationsschäden geraten damit zunehmend auch Personalabteilungen und Führungskräfte unter Druck.

29 Prozent der Befragten verursachten infolge eigener Sicherheitslücken Schäden bei Dritten – etwa durch Datenabfluss oder Lieferverzögerungen. Ein Viertel musste Kunden über den Verlust personenbezogener Daten informieren, was zusätzliche Kosten und Vertrauensverluste mit sich brachte. Ebenso viele Unternehmen gaben an, dass die Akquise neuer Kunden nach einem Vorfall deutlich schwieriger wurde.

Die Studie verdeutlicht, dass Cyber-Angriffe längst nicht mehr nur IT-Probleme sind, sondern ganzheitliche Krisen auslösen können. Neben technischen Schutzmaßnahmen wird daher der Ausbau eines integrierten Krisenmanagements immer wichtiger – einschließlich Kommunikations-, Rechts- und Compliance-Strategien.

Mit der steigenden Komplexität digitaler Lieferketten wächst der Druck, Sicherheitsprozesse regelmäßig zu testen und externe Partner zu überprüfen. 74 Prozent der Unternehmen führen laut Hiscox mindestens monatlich Schwachstellen-Checks durch, 72 Prozent prüfen die Cyber-Sicherheit ihrer Geschäftspartner. Diese Entwicklung zeigt, dass der Mittelstand zunehmend Verantwortung für die gesamte Wertschöpfungskette übernimmt – aber auch, wie viel noch zu tun bleibt, um Angriffen wirksam zu begegnen.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4946570/Angriffswelle-auf-den-Mittelstand/