MANAGEMENT & STRATEGIEN

Versicherung als Instrument des Cyber-Risikomanagements

Motivbild: www.pixabay.com

In Deutschland ist mittlerweile jedes zweite Unternehmen von Cyber-Angriffen betroffen, immer wieder auch das Gastgewerbe. Eine aktuelle Studie des Munich Risk and Insurance Centers (MRIC) und der Cyber Risk Agency zeigt den Handlungsbedarf von Unternehmen auf und liefert konkrete Empfehlungen, wie sich diese sich durch effektives Cyber-Risikomanagement vor Kriminellen im Netz schützen können.
Cyber-Kriminelle verursachen in Deutschland jährlich Schäden in Höhe von zirka 55 Milliarden Euro. Davon entfallen etwa 16 Milliarden Euro auf Ermittlungsaufwände, Wiederherstellung der IT und Betriebsstillstand. Fälle wie das bereits vier Mal gehackte Seehotel Jägerwirt zeigen, dass trotz geeigneter Maßnahmen keine 100-prozentige Sicherheit erreicht werden kann. Pünktlich zum Start in die Wintersaison verschafften sich Cyber-Kriminelle vermutlich mit Hilfe eines Trojaners im Anhang einer fingierten E-Mail Zugang zum Zentralrechner des Hotels. Sie verschlüsselten alle Daten und forderten 1.500 Euro zur Freigabe der Daten per Entschlüsselungscode. ?Wir mussten in den sauren Apfel beißen und bezahlen. Wir waren mit 180 Gästen völlig ausgebucht, und die Urlauber kamen nicht mehr in ihre abgesperrten Zimmer?, berichtete der Hotelier Christoph Brandstätter. Sowohl Buchungssysteme, Webseiten und Kassensysteme als auch IoT-Geräte wie Fernseher mit Internetzugang haben technische Schwachstellen und genau diese finden Hacker regelmäßig. Nur wenige Fälle werden bekannt ? die Dunkelziffer betroffener Gastronomiebetriebe ist vermutlich sehr viel höher. Erst im August dieses Jahres hatten es Cyber-Kriminelle auf die Login-In-Informationen von Hotelgästen abgesehen. In mehreren

Hotels, vornehmlich in Europa und dem Mittleren Osten, wurden Hotelsysteme per E-Mail mit Malware verseucht. Nach Infizierung übernahmen die Cyber-Kriminellen die Kontrolle über die Gäste-WLANs und sammelten private sowie geschäftliche Passwortinformationen der Nutzer ein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im vergangenen Jahr 1.000 kritische Schwachstellen in gängiger Standardsoftware identifiziert. Hinzu kommt eine Zunahme an Schwachstellen in mobilen Endgeräten. Für Cyber-Kriminelle stellt jede dieser Lücken ein potentielles Einfallstor dar. Eine absolute IT-Sicherheit kann daher in keinem Unternehmen erreicht werden. Analysen der Cyber Risk Agency zeigen, dass insbesondere kleinere Unternehmen meist nur über geringe Sicherheitsstandards verfügen. So ist bei 48 Prozent der Unternehmen mit weniger als 100 Mitarbeitern der Reifegrad der Informationssicherheit als ?Gering? zu bewerten, bei größeren Unternehmen immerhin noch 32 Prozent.

Maßnahme: ?Cyber-Risikomanagement?

Für eine bestmögliche Abwehrstrategie zeigt die Studie Möglichkeiten der Kombination verschiedener Instrumente des Cyber-Risikomanagements auf. Auf Basis der Ergebnisse des Online-Tools CyberRiskRadar (www.CyberRiskAgency.de) wird der aktuelle Reifegrad des Cyber-Risikomanagements in kleinen und mittleren Unternehmen dargestellt und aufgezeigt, wie dieser durch konkrete weiterführende Schritte verbessert werden kann. Neben technischen Abwehrmaßnahmen und professioneller Datensicherung besteht demnach Handlungsbedarf vor allem bei personellen Sicherheitsmaßnahmen als auch beim Notfallmanagement der Unternehmen. Ein wesentliches Defizit besteht darin, dass die Unternehmen trotz der eheblichen Anzahl erfolgreicher Angriffe den Ernstfall noch nicht ausreichend vorbereiten, um Angreifern wirksam Paroli bieten zu können.

Trotz des wachsenden Angebots an Cyber-Versicherungslösungen nutzen nur sehr wenige deutsche Unternehmen dieses Instrument. Fast 70 Prozent haben keinen Versicherungsschutz für durch Cyber-Angriffe verursachte Eigenschäden und nur elf Prozent haben eine Cyber-Versicherung mit entsprechender Cyber-Assistance zur schnellen Unterstützung im Ernstfall. Ein Grund hierfür ist vermutlich die mangelnde Kenntnis vieler Entscheidungsträger über Cyber-Versicherungsprodukte und deren Möglichkeiten.

In den letzten sechs Jahren wurden in Deutschland Cyber-Versicherungen mit einem geschätzten Gesamtprämienvolumen von etwa 100 Millionen Euro (Quelle: KMPG) gezeichnet. Zum Vergleich ? die geschätzten weltweiten Prämien liegen bei zirka 4,1 Milliarden US-Dollar und sind zu beinahe 70 Prozent dem US-Markt zuzuordnen. Eine Cyber-Versicherung bietet neben der Deckung finanzieller Schäden auch Assistance-Leistungen und stellt damit auch eine Alternative zum Zukauf der erforderlichen Notfall-Expertise dar. Sie bietet damit die Chance auf einen schnellen Wiederanlauf der IT und deckt die Kosten für die Wiederherstellung und sonstige durch einen Cyber-Angriff entstandenen Aufwände sowie Ertragsausfälle während einer Betriebsunterbrechung.

Die Autoren kommen zu dem Schluss, dass die Mehrheit der angebotenen Cyber-Policen die wesentlichen finanziellen Risiken des Versicherungsnehmers abdeckt. Bei den Standarddeckungskomponenten, wie Betriebsunterbrechungsschäden, Ertragsausfällen und Kosten der System- und Datenwiederherstellung sowie bei Schäden aus Haftpflichtansprüchen von Kunden und Geschäftspartnern und diversen sonstigen

Krisenkosten, zum Beispiel für IT-Forensik, Krisenkommunikation und Rechtsberatung, unterscheidet sich das Angebot kaum. Bei neun Policen wurden jedoch zum Teil sehr umfassende und insbesondere für kleine und mittlere Unternehmen nur schwer erfüllbare Obliegenheiten (= Auflagen der Versicherung) identifiziert. Bei der Komponente der Assistance-Leistungen wurden insbesondere Unterschiede bezüglich der Handlungsfähigkeit der 24/7-Hotline, der verfügbaren Notfallkapazitäten und der Professionalität des Notfallteams (sog. CERT-Service = Computer Emergency Response Team) identifiziert.
Oliver Lehmeyer, Geschäftsführer und Gründer der Cyber Risk Agency, rät: ?Wer die Chancen der Digitalisierung nutzen möchte, der muss auch die damit einhergehenden Risiken managen. Gehen Sie als Unternehmen davon aus, dass Sie gehackt werden und bereiten Sie Ihr Unternehmen auf den Ernstfall vor.? Für Entscheidungsträger in Unternehmen bedeutet dies konkret, dass verstärkt digitale Kompetenz im Unternehmen aufgebaut werden muss, um den mit der Digitalisierung einhergehenden Risiken begegnen zu können. Daneben kann der Abschluss einer Cyber-Versicherung sinnvoll sein, um einerseits den finanziellen Risiken eines Cyber-Angriffs Rechnung zu tragen und mit der in den Policen integrierten Cyber-Assistance ein professionelles Notfallmanagement für das Unternehmen zu etablieren. Insbesondere kleine und mittlere Unternehmen haben hier Nachholbedarf, da diese im Vergleich zu großen Unternehmen in der Regel über geringere IT-Sicherheitsstandards verfügen.
Eine Kurzfassung der Studie ist auf der Webseite der Cyber Risk Agency downloadbar: