12 — Avidea Südtirol:
Von Family zu Adults only

30 — Spezial Hotelgastro:
Roboter in der Küche

50 — Adinas Lab in Berlin:
Testhotel statt Testzimmer

Tophotel

PEOPLE | BUSINESS | TRENDS

„Probleme offen anzusprechen, dazu gehört sehr viel Vertrauen. Erst recht, wenn es um Führungsmüdigkeit geht.“

Katharina Darisse, Geschäftsführerin Fair Job Hotels, im #Monotalk

6–2024

tophotel.de

Wie Cyberpolicen schützen

Für Unternehmen gehören sie mit zu den größten Risiken: Hackerangriffe aus dem Internet. Um den Betrieb vor den Folgen einer Attacke zu schützen, lohnt es sich, eine Cyberversicherung abzuschließen. Diese übernimmt nicht nur Kosten, sondern kann kleine Betriebe auch bei der Vorsorge unterstützen.

Auf mehr als 220 Milliarden Euro jährlich beziffert der Verband Bitkom die Schäden für die deutsche Wirtschaft durch Diebstahl, Spionage und Sabotage aus dem Internet. Die Straftaten nehmen nicht nur Jahr für Jahr drastisch zu, sie werden auch „professioneller". Unternehmen werden genauso attackiert wie Krankenhäuser oder Verwaltungen. Dennoch haben kleine und mittlere Unternehmen nur ein geringes Bewusstsein für die Risiken durch Cyberangriffe. Das zeigen Untersuchungen der Forsa Gesellschaft für statistische Analysen und des Gesamtverbandes der Versicherer (GDV).

Demnach halten sich die meisten Unternehmer für deutlich besser gegen Cyberattacken geschützt, als sie es tatsächlich sind. Vier von fünf Unternehmen glauben, dass ihre Computersysteme umfassend geschützt seien. Laut GDV-Erhebungen ist aber in jedem zweiten Unternehmen niemand explizit für die IT-Sicherheit verantwortlich, und es gibt keine Notfallpläne für eine Cyberattacke. Weniger als ein Drittel der Betriebe bieten ihren Mitarbeitenden dazu Schulungen an. Viele halten ihre Firma für zu klein oder ihre Daten für „nicht interessant". Dabei werden Unternehmen mit weniger als 50 Mitarbeitenden tatsächlich häufiger angegriffen als größere Betriebe.

Sicherheitslücken erkennen

Weitere Sicherheitslücken bieten die Computersysteme selbst: Zwölf Prozent der Unternehmer spielen Sicherheitsupdates nicht automatisch ein, 24 Prozent verzichten auf wöchentliche Sicherheitskopien ihrer Daten, und 25 Prozent lassen auch einfachste Passwörter zu. Nur jedes fünfte Unternehmen erfüllt alle Basisanforderungen an die IT-Sicherheit. Gezielte Angriffe auf IT-Systeme sind eher die Ausnahme. Die Bedrohung kommt per E-Mail: Fast 60 Prozent der erfolgreichen Angriffe wird durch Mitarbeitende ausgelöst, die verseuchte Anhänge öffnen oder schädliche Links anklicken.

Mehrwert durch Versicherung

Doch wie kann man IT-Systeme schützen und dafür sorgen, dass die Beschäftigten Angriffe erkennen und schadhafte E-Mails löschen? Einen wirkungsvollen Weg zeigen Cyberversicherungen auf. Geringe Schadenszahlen liegen im Interesse der Gesellschaften. Deshalb bieten sie rund um den Versicherungsschutz noch weitere Serviceleistungen, die die Unternehmen resistenter gegen Hackerangriffe machen. Außer der Kostenübernahme im Schadenfall liegt ein großer Mehrwert einer Cyberpolice in der Sicherheitsberatung und der Krisenunterstützung. Wer einen Vertrag abgeschlossen hat, kann von einer 24/7-Schaden-Hotline sowie der Hilfe und Beratung durch Spezialisten profitieren. Meist müssen bei einem Angriff ganze Systeme neu aufgesetzt und es muss mit Kunden und Lieferanten kommuniziert werden. Bei Datenschutzverletzungen bedarf es häufig eines Rechtsbeistands. Am stärksten in den Fokus ist jedoch das Thema Prävention gerückt. Die Versicherer bieten Schulungen an, die Mitarbeitenden zeigen, wie Hacker vorgehen und schadhafte E-Mails erkannt werden. Attacken auf das Unternehmen werden simuliert, durch Vortäuschen falscher Identitäten und Spam- oder Phishing-E-Mails. Das lohnt sich, wie aktuelle Schadenzahlen zeigen: Weil mehr Angriffe erkannt werden, sind die durchschnittlichen Schadenkosten um 25 Prozent gesunken.

ZUSATZ-LEISTUNGEN

Achten Sie beim Abschluss einer Cyberversicherung nicht nur auf eine ausreichende Versicherungssumme, sondern auch auf die zusätzlichen Leistungen, die mit dem Vertrag verbunden sind. Wenn Ihre IT resistent gegen Angriffe ist, Ihre Mitarbeiterinnen und Mitarbeiter gut geschult und sensibel sind und Sie einen Notfallplan besitzen, muss die Cyberversicherung seltener greifen, weil Sie weniger Schäden zu beklagen haben. Und denken Sie an den Betriebsunterbrechungsschutz bei Cyberangriffen. Die Hälfte aller attackierten Betriebe braucht bis zu drei Tage, um wieder arbeitsfähig zu sein, jeder fünfte sogar noch länger. In dieser Zeit kann im schlechtesten Fall im Hotel niemand einchecken, die Zimmer benutzen oder mit seiner Kreditkarte bezahlen.

Zum Autor

Alexander Fritz (B. A. Versicherungswirtschaft) ist Geschäftsführer der Fritz & Fritz GmbH (Margetshöchheim). Als Sachverständiger ist er auf Risikomanagementkonzepte und Pakete zur Unternehmensabsicherung für die Hotellerie spezialisiert.

Kontakt

Fritz & Fritz GmbH
Tel.: +49 931 468650
a.fritz@fritzufritz.de
www.fritzufritz.de

Bild: Fritz & Fritz