Tophotel

PEOPLE | BUSINESS | TRENDS

„Wenn's keiner macht, selber machen – so gelangt man von der Herausforderung zum innovativen Geschäftsmodell."

Diana-Nadine Brammann,
Geschäftsführerin Nordsee Kollektiv

10–2021

tophotel.de

Cyber-Crime: Hoteliers sollten sich absichern

Ohne Internetauftritt und Buchungsportale keine Gäste. Der Siegeszug der Onlinebuchung hat dem Gastgewerbe in den vergangenen Jahren ein starkes Wachstum beschert. Aber es gibt nicht nur Vorteile im Netz, sondern auch drohende Gefahren, die besondere Vorsichtsmaßnahmen erfordern.

Jede neue IT-Lösung bringt den Gästen mehr Komfort, den Mitarbeitern eine Arbeitserleichterung oder verschlankt die Prozesse im Unternehmen. Je mehr Dienste des Hotels jedoch online gehen, desto mehr steigt auch das Risiko für den Betrieb. Eigene Buchungsmaschinen, Online-Bezahlsysteme, sogar die Haustechnik ist heute vernetzt und per App steuerbar – und kann ein Einfallstor für Hacker darstellen.

Fast täglich werden Kunden- und Zahlungsdaten gestohlen, Unternehmensdaten verschlüsselt oder ganze Sicherheits- und Hausschließsysteme lahmgelegt. Hoteliers melden Virus- und Trojanerangriffe oder Mail-Accounts, die plötzlich massenweise Spam verschicken.

Fingierte Mails und Fake-Identitäten

Besonders dreist: Das sogenannte Social Engineering. Hier nutzen Täter menschliche Eigenschaften und Verhaltensweisen als Angriffsfläche. Es wird mit fingierten Mails – der Täter gibt sich etwa als Geschäftsführer aus – eine Stress-Situation („ganz eilig“) ausgelöst. Der Mitarbeiter soll hohe Beträge überweisen – und tut dies dann vielleicht auch. Vorher werden Unternehmen und einzelne Mitarbeiter gezielt ausgespäht und deren Verhalten studiert.

Drucker als Sicherheitslücke

Auch Drucker und Scanner sind vernetzt und bieten ohne Sicherung ein Einfallstor für Betrugsfälle. So wird beispielsweise ein eingescannter Zahlungsbeleg an einen Dritten umgeleitet und so verändert, dass Zahlungen nicht mehr dort ankommen, wo sie ursprünglich ankommen sollten.

Gefahr kommt auch von innen

Nicht selten entstehen IT-Schäden nicht von außen, sondern durch die eigenen Mitarbeiter. Stress und Unzufriedenheit können zu fahrlässigem oder gar böswilligem Verhalten führen. So könnten Angestellte versuchen, sich auf Kosten des Unternehmens zu bereichern oder den Auftraggebern zu schaden.

Richtlinien einhalten

Fahrlässig handeln Mitarbeiter, die einer Organisation nicht absichtlich Schaden zufügen wollen, aber im Zweifelsfall fehlerhaft oder sorglos agieren. So könnte es etwa sein, dass Richtlinien zu Hard- und Software nicht eingehalten oder Login-Daten nicht sicher verwahrt werden. Es kann auch passieren, dass Bedrohungen nicht

Bild: Fritz & Fritz GmbH

Zum Autor

Alexander Fritz (B.A. Versicherungswirtschaft) ist Geschäftsführer der Fritz & Fritz Risikoberatung UG mit Sitz in Margetshöchheim. Als Sachverständiger ist er auf Risikomanagement-Konzepte und Pakete zur Unternehmensabsicherung für die Hotellerie spezialisiert.

Kontakt

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

erkannt werden. Mittlerweile gehen Experten davon aus, das im IT-Bereich 60 bis 80 Prozent aller Cybervorfälle auf menschliches Versagen zurückzuführen sind.

Was ist eine „Cyber-Versicherung“?

Einer der wichtigsten Bausteine eines Internetschutzes ist daher eine Eigenschadenversicherung, oder auch „Cyber-Versicherung“ genannt: Der Versicherungsschutz der Cyberpolice umfasst Ansprüche Dritter und deren Abwehr bei Verletzung des Datenschutzes, der Vertraulichkeit und des Persönlichkeitsrechts. Er beinhaltet ferner Eigenschäden infolge von Datenwiederherstellung und Ertragsausfall sowie Kosten für Forensik, für die Sicherung der Reputation und der Krisenkommunikation.

Weitere Bausteine

Ein weiterer Baustein ist die Cyber-Haftpflicht: Dieser Baustein deckt Schäden durch eigenes Verschulden ab. Dazu gehören sowohl die Kosten für eine Verletzung von Datenschutzrechten als auch die des Krisenmanagements. Dazu kommt der Rechtsschutz: Dieser schützt passiv, wenn dem Unternehmen Abmahnungen ins Haus flattern, oder bei der aktiven Durchsetzung eigener Forderungen. Wichtig bei Cyberpolicen ist, dass nicht nur Zahlungen geleistet werden. Im Gegensatz zu anderen Sachversicherungen müssen Daten, um sie wieder nutzbar zu machen, wiederhergestellt, entschlüsselt und gesichert werden. Solche „Assistance-Leistungen“ stellen in der Cyberpolice einen wichtigen Bestandteil dar.

TIPP: WAS TUN BEI EINEM CYBER-NOTFALL?

Deutet sich ein Cyberproblem an, so sind schnell eingeleitete Schritte – in der richtigen Reihenfolge – der Schlüssel zur Datenrettung!

Der erste Anruf gilt dem IT-Dienstleister des Cyberversicherers. Dieser hilft bei kleinen Problemen, aber auch bei Forensik im größeren Schadenfall. Zusätzlich kann kurzfristig ein Krisenteam zusammengestellt werden, bis hin zum Anwalt, der bei Problemen in Sachen Datenschutz unterstützt.

Ein guter Cyber-Versicherer hat eine 24/7-Krisenhotline, die schon bei Verdachtsfällen unterstützt. Die Hotline vermittelt IT-Spezialisten, die mit dem Kunden sprechen und sich beim Kunden im System aufschalten. So kann aus dem Verdachtsfall ein Leistungsfall werden. Der IT-Spezialist gibt dann verschiedene Schritte vor, zum Beispiel: Systeme abschalten, prüfen oder wiederherstellen.

Gut zu wissen ist zudem: Die Serviceleistungen der Cyber-Versicherung über deren IT-Hotline werden auch dann vom Versicherer übernommen, wenn ein Selbstbehalt vereinbart ist.