

Cyberschutz für Hotellerie und Gastronomie

2016 ist die Zahl von Computerattacken explosionsartig um 1.270 Prozent angestiegen. Hackerangriffe und Datendiebstahl treffen dabei nicht nur große Unternehmen. Auch Hotel- und Gastronomiebetriebe sind immer häufiger unter den Opfern.

Die finanziellen Folgen von Cyberkriminalität können sehr schnell existenzbedrohende Ausmaße annehmen. Der Verlust oder die Verschlüsselung von Buchung- und Kundendaten, von Bank- und Kreditkartennummern oder die Sperrung von Zugangssystemen können den ganzen Betrieb innerhalb von Sekunden lahmlegen.

Beispiele:

- Verlust von Kunden- und Kreditkartendaten bei der Hilton-Kette: Missbrauch von Kreditkartendaten im großen Stil (09/2015: Quelle: heise.de)
- Internetkriminelle verschaffen sich zunächst Zugriff auf das Buchungssystem und die Kasse eines Hotels in Österreich und sperren schließlich das Schließsystem der Gästezimmer. Erst nach Zahlung eines Lösegeldes kann der Hotelbetrieb weiterlaufen (AHGZ 01/2017)
- Hacker initiieren massive Server-Anfragen, die das Hotelsystem aufgrund der hohen Last zusammenbrechen lassen.
- Ein ehemaliger leitender Hotellangestellter hat sich unerlaubten Zugriff zur Sicherheitsdatenbank des Hotels mit

Konto- und Kreditkarteninformationen verschafft (Quelle: chub.com)

Die Risiken sind vielfältig und folgenschwer

Je größer die zu verwaltenden Datenmengen und die Abhängigkeit von der Technik, desto größer sind die Cyber-Risiken für Ihr Unternehmen. Schwachstellen in den IT-Systemen und mangelndes Sicherheitsbewusstsein der Mitarbeiter machen es Kriminellen leicht.

Es drohen schwerwiegende finanzielle Folgen, wie Ertragsausfall durch eine Betriebsunterbrechung oder Schadenersatzansprüche Dritter nach einem Datenverlust.

Die Risiken der Vernetzung

Cyberkriminalität boomt

250 Mio. Schadprogramme gibt es heute weltweit und 300.000 Varianten kommen jeden Tag neu dazu

Es gibt schätzungsweise 60 global agierende Cybercrime-Organisationen

Circa 1 Million Computer sind in Deutschland von Kriminellen gekapert worden

1 Mio.

30 % der Unternehmen haben 2013 oder 2014 einen IT-Sicherheitsvorfall festgestellt,

2/3 der Fälle wurden – absichtlich oder unabsichtlich – durch Mitarbeiter verursacht

Deutschland hat 2013 den traurigen 1. Platz bei den Schäden belegt, die durch Cyberangriffe verursacht werden – insgesamt

46 Mrd. €

1.000 €

kostet durchschnittlich ein gestohlenes IT-Sicherheitszertifikat auf dem deutschen „Online-Schwarzmarkt“

Quellen: Cisco: Visual Networking Index 2014; GSMA: Understanding the Internet of Things (Juli 2014); GSMA: Connected Living: How China is set for Global M2M Leadership (Juni 2014); Raspberry Pi Stiftung; BSI: Die Lage der IT-Sicherheit in Deutschland 2014; BITKOM Research 2015; Kaspersky Lab 2015; CSIS: Net Losses, Estimating the Global Cost of Cybercrime (Juni 2014)
© Grafik: www.gdv.de | Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

Bedarfsorientierte Versicherungskonzepte

Der Fritz & Fritz Cyber-Schutz bietet Sicherheit und deckt finanzielle Risiken ab, die durch Cyberattacken und Datenrechtsverletzungen auf Sie zukommen können.

① Cyber- und Daten-Eigenschaden

Versicherungsschutz für die Beschädigung, Zerstörung, Veränderung, Blockierung oder den Missbrauch der IT-Systeme, Programme oder elektronischen Daten infolge eines Hacker-Einbruchs, einer Denial-of-Service (DoS) Attacke oder einer Infektion des IT-Systems durch Schadsoftware (Viren, Trojaner).

② Betriebsunterbrechung

Versicherungsschutz für die Unterbrechung des Geschäftsbetriebes durch Ausfall der IT-Systeme in Folge von Viren und Schadsoftware, Hacker-Angriffen und Eingriffen Dritter in die Systeme des Versicherungsnehmers.

③ Erpressung

Versicherungsschutz für die Erpressung im Zusammenhang mit angedrohter oder bereits erfolgter Beschädigung, Zerstörung, Veränderung, Blockierung oder den Missbrauch der IT-Systeme, der Programme oder der elektronischen Daten.

④ Kreditkartenschaden

Versicherungsschutz beim Verlust oder der Beschädigung von Kreditkartendaten und -programmen für Verstöße gegen Kreditkartenverarbeitungsvereinbarungen, Verletzungen der Payment Card Industry Data Security-Standards oder Verstöße gegen vertragliche Vereinbarungen im

Zusammenhang mit Bezahlssystemen wie Bankkarten oder Zahlungsprozessoren.

⑤ Vertrauensschaden

Versicherungsschutz bei Vermögenseigenschäden durch vorsätzliche Verwirklichung von Vermögensdelikten wie Betrug, Unterschlagung oder Diebstahl von Firmengeldern sowie Sachbeschädigung an den IT-Systemen.

⑥ Haftpflicht

Versicherungsschutz für die Folgen aufgrund von Verstößen gegen die Cyber-Sicherheit, den Datenschutz sowie gegen Geheimhaltungspflichten und Datenvertraulichkeitserklärungen.

Die Bausteine ① bis ⑥ sind für Ihren Cyberschutz frei wählbar. Wir erstellen Ihnen gerne ein individuelles Angebot. Sprechen Sie uns an!



Weitere Informationen unter:

Telefon +49 (0) 931 / 468 65- 0 oder

E-Mail: info@fritzufriz.de