Macam EXPERTISE

Ausgabe 3 vom 06.05.2021

Cyberrisk – Begriff und Hintergründe zur neuen Gastro-/Hotel-Pool-Lösung

Cyberrisk ist längst kein Phänomen mehr, sondern eine reale Bedrohung. Die Versicherungsbranche betrachtet Cyberrisk, zusammen mit Pandemie, als die zwei grossen Gefahren, welche Wirtschaft und Gesellschaft zukünftig gefährden. Unsere Abhängigkeit zu IT-Systemen, zum Internet, zu externen Servern etc. steigt von Jahr zu Jahr. Wir sind angreifbar, erpressbar und tatsächlich sind in jüngster Zeit vermehrt Hoteliers und auch Gastronomen Opfer von Cyberattacken geworden. Der Versicherungsschutz wird mehr und mehr nachgefragt. Die Integration von Cyberrisk in unsere Pool-Lösung ist daher die logische Konsequenz.

Der Begriff Cyberrisk bezieht sich auf eine Vielzahl potenzieller Risiken, die im Zusammenhang mit der Technologie oder mit Informationen eines Unternehmens stehen. Dazu gehören Identitätsdiebstahl, die Weitergabe von sensiblen Informationen, Betriebsunterbruch etwa nach einem Hackerangriff, Schäden an Datensätzen durch einen Hacker, Diebstahl von wertvollen Daten, die Einführung von Malware und anderen schädlichen Computercodes oder auch Fehler der eigenen Mitarbeiter, die zur Weitergabe vertraulicher Informationen oder der Schädigung der Reputation des Unternehmens führen.

Cyberrisk impliziert aber nicht nur Gefahren an der eigenen IT-Infrastruktur, sondern geht viel weiter und berührt dabei heikle rechtliche Themen aus den Bereichen Datenschutz-, Persönlichkeits- und Haftpflichtrecht. Ein Beispiel hierfür ist die Europäische Datenschutzgrundverordnung (EU-DSGVO), an welches sich auch das schweizerische Datenschutzgesetz (DSG) angleicht. Diese Verordnung besagt u.a., dass Betriebe, die Personendaten von Endnutzern bekommen, für diese Daten auch dann verantwortlich sind, wenn sie an Drittanbieter weitergegeben werden. Für die Hotellerie aber auch immer mehr für die Gastronomie, sind solche Bestimmungen von hoher Relevanz, da zahlreiche Buchungen, inklusive der benötigten Daten, über Onlineportale abgewickelt werden.

Klassische Cyber-Risiken sind:
Ransomware: Hierbei infiziert eine Schadsoftware die Rechner des Opfers und verschlüsselt dort Daten. Dies führt dazu, dass die betroffenen IT-Systeme lahmgelegt werden. Dies kann bspw. für ein Hotel bedeuten, dass von der Reservationssoftware bis hin zur Software für die Verwaltung der Zimmerschlüssel sämtliche Systeme nicht mehr funktionsfähig sind.

Phishing: Hier wird ein «Köder» (bspw. fingierte E-Mail) verwendet, um an das Passwort und/oder andere Informationen des Opfers zu gelangen. Dabei wird meist ein Link zu einer präparierten Webseite mitgesendet, die beim Öffnen entweder direkt Schadsoftware auf den Rechner des Opfers lädt, oder vom Opfer Daten wie beispielsweise Passwörter oder Kontoverbindungen verlangt.

Kreditkartenbetrug: Hier geht es meist um die Verwendung von gestohlenen Kreditkartennummern oder das Fälschen von Kreditkartendaten. Die Ausprägungen sind Vielfältig: Mit einer gefälschten E-Mail wird bspw. direkt nach den Daten gefragt oder die Daten werden über eine ungesicherte Webseite gestohlen. Dies kann den Betrieb, aber auch direkt die Gäste betreffen, wenn beispielsweise das System des Betriebs angegriffen wurde.

Insider: Eine oft unterschätzte Bedrohung sind Angriffe durch Mitarbeitende. Die Schadenerhebungen im Bereich Cyberrisk zeigen auf, dass ein hoher Prozentsatz von Angriffen und Datenabflüssen von internen Mitarbeitenden durchgeführt und/oder zumindest ermöglicht wird.

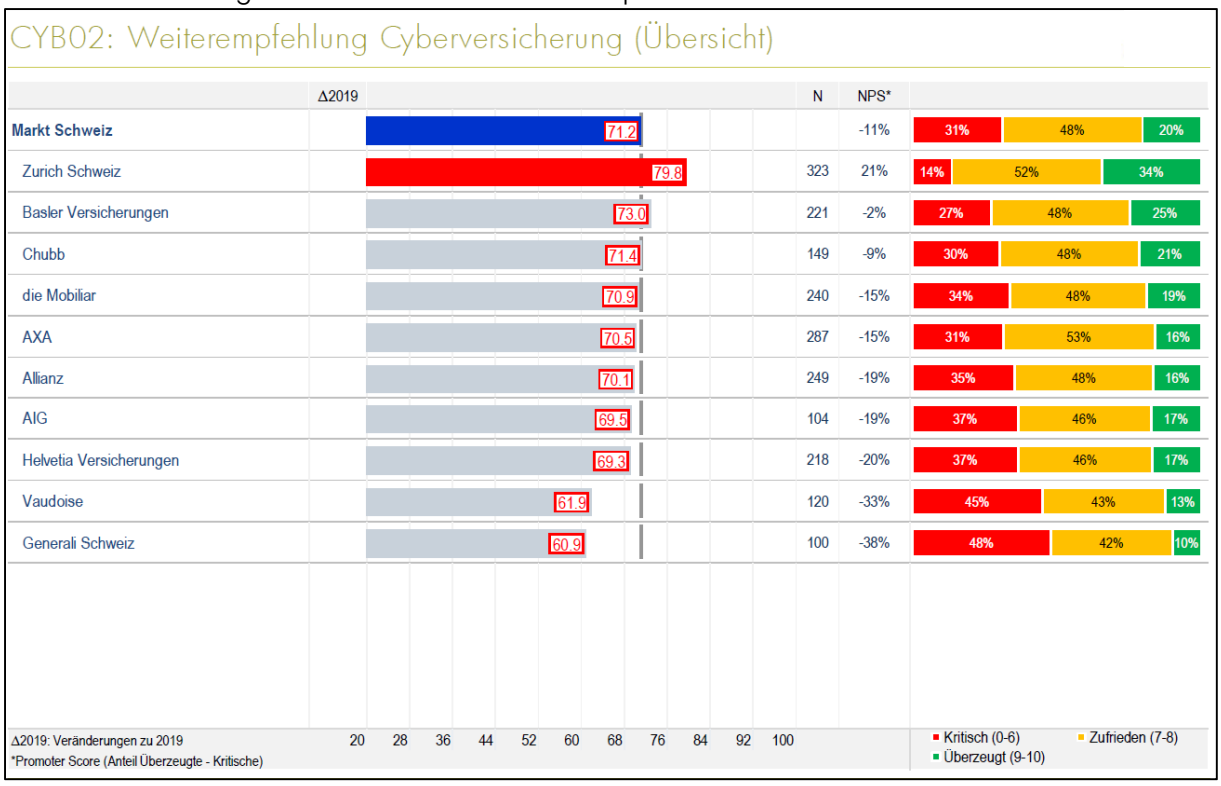
CEO-Fraud: Hier werden Buchhalter oder andere zahlungsberechtigte Mitarbeitende angewiesen, hohe Summen auf ein fremdes Konto zu überweisen. Dafür täuschen die Angreifer die Identität des CEO vor und verlangen oftmals Verschwiegenheit vom betroffenen Mitarbeitenden.

Versicherbarkeit von Cyber-Risiken

Cyberrisk ist unter den Versicherungsprodukten noch sehr jung. Längst nicht jeder Cyber-Vorfall findet Deckung in aktuellen Versicherungslösungen. Bspw. der oben erwähnte Kreditkartenmissbrauch – das Bezahlen mit gestohlener Kreditkarte – oder CEO Fraud ist typischerweise nicht über eine Cyberrisk Versicherung gedeckt. Ein grosses Problem der Versicherer ist, dass die Schäden aus Cyberrisk kaum verlässlich kalkuliert werden können, da neben direkt zurechenbaren Kosten auch erhebliche nicht direkt messbare Kosten, wie beispielsweise Reputationsverluste oder Erpressungsverhandlungen einfliessen. Mit steigender Schadenerfahrung, werden die Versicherer aber ihre Produkte laufend adaptieren und verbessern. Was dabei klar ist, ist das mit der steigenden Bedrohung von Cyber-Risiken auch die Prämientarife im Versicherungsmarkt fortlaufen einer Erhöhung unterworfen sind.

Macam-Pool-Lösung Cyberrisk

Dass wir die Deckung bei der Zurich Versicherung eingekauft haben, macht aufgrund unseres Pool-Konstruktes Sinn. Wir haben aber auch Marktvergleiche in unseren Entscheid einfliessen lassen, wo das Produkt der Zurich Versicherung als eines der besten abschneidet. Dies zeigt auch bspw. das Ergebnis einer aktuellen Erhebung vom Marktforschungsinstitut ValueQuest[1], wo die führenden schweizerischen Versicherungsbroker angegeben haben, dass sie das Produkt der Zurich Versicherung am ehesten ihren Kunden empfehlen würden:



[1] Broker-Panel Schweiz 2020, Teilmarkt Cyber-Versicherung, ValueQuest GmbH, 2020

Der Deckungsumfang im Pool entspricht dem PREMIUM Paket der Zurich Versicherung. Nachstehend ein Auszug aus dem Fact-Sheet der Zurich Versicherung, wo die versicherten Deckungsbausteine umschrieben sind:

Allgemeine Informationen

- 24/7 erreichbares Krisenmanagement
- Deckung des eigenen Computernetzwerks sowie Service- und Cloud-Anbietern
- Deckung von Computerkomponenten von industriellen Kontrollsystemen, Produktionsanlagen und Medizinalgeräten
- Weltweite Deckung
- Freie Dienstleisterwahl im Schadensfall
- Vorsätzliche Handlungen von Mitarbeitern eingeschlossen (ohne Bereicherungsabsicht)

Deckungsbaustein Cyber-System- und Datenwiederherstellung

- Wiederherstellung oder Wiederbeschaffung von Daten und Informationen
- Technische Abklärungen und IT-forensische Analysen: Was ist genau passiert?
- Wiederbeschaffung von beschädigter Hardware (Bricking)
- Identifikation von Software Schwachstellen und Massnahmen zur Sicherheitsverbesserung (Betterment)
- Cyber-Erpressungszahlungen und Kosten für die Abwehr von Cyber-Erpressungen

Deckungsbaustein Cyber-Haftpflicht

Schadenersatz und Abwehr von ungerechtfertigten Ansprüchen bei/im Zusammenhang mit:

- Verlust, Diebstahl oder Veröffentlichung von Daten – unabhängig von einem Cybervorfall
- Verletzung von Datenschutzrecht (inklusive GDPR)
- Verletzung von Namens-, Urheber- und Markenrechten
- Verfahrenskosten und Verteidigungskosten

Deckungsbaustein Cyber-Krisenmanagement

- Prüfung von Meldepflichten und Benachrichtigungspflichten
- Benachrichtigung von betroffenen Personen auf freiwilliger Basis
- behördliche Verfahren sowie (versicherbare) Strafen und Bussen
- Vertragsstrafen bei einem Verstoss gegen PCI DSS-Standards
- Call Center, Kreditkarten-Monitoring und Identity-Monitoring für betroffene Personen
- Goodwill Aktionen wie beispielsweise Rabattaktionen und Preisnachlässe für betroffene Personen
- Planung und Umsetzung von Public Relations-Kampagnen bei negativer Medienberichterstattung

Deckungsbaustein Cyber-Rechtsschutz

- Beratung betreffend juristischer Sofortmassnahmen
- Geltendmachung von Schadenersatzansprüchen
- Strafverteidigung bei fahrlässiger Verletzung von Datenschutzbestimmungen

Deckungsbaustein Cyber-Betriebsunterbruch und Mehrkosten

- Aufgrund eines Cybervorfalls oder einer Fehlbedienung (Systemfehlers)
- Aufgrund einer behördlichen Anordnung in Folge einer Datenschutzverletzung
- Deckung von Nettogewinnausfall sowie Mehrkosten zur Aufrechterhaltung des Betriebs

Deckungsbaustein Cyber-Crime

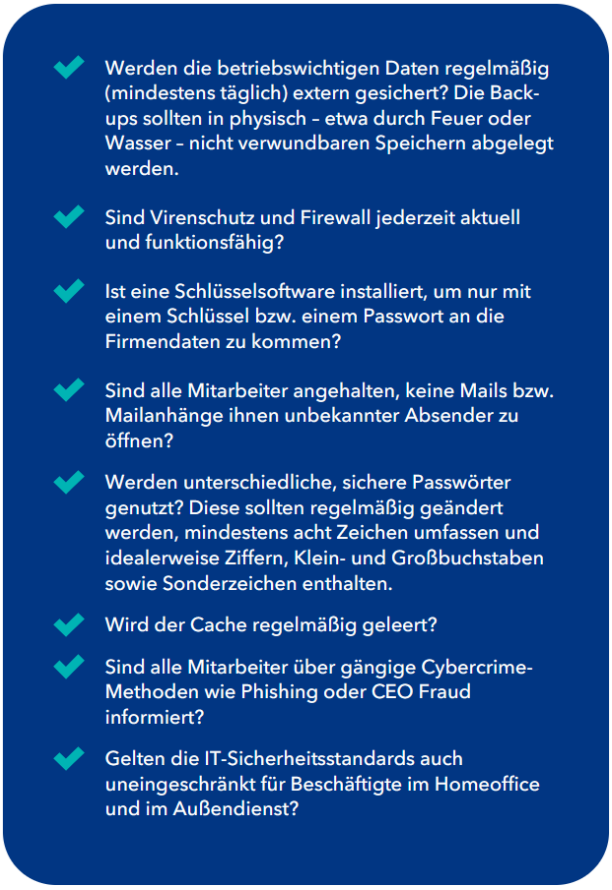
- Cyber-Betrug aufgrund von aktiven Täuschungshandlungen durch Dritte (Social Engineering)
- Cyber-Diebstahl durch Manipulation der Computersysteme durch Dritte (E-Banking Hacking)

Zu den Obliegenheiten des Versicherungsnehmers
Damit der Versicherungsschutz vollumfänglich greift, ist der Versicherungsnehmer gehalten einen Mindestschutz seines IT-Systems zu gewährleisten. Werden die Obliegenheiten nicht eingehalten, so kann die Versicherung im Schadenfall seine Leistungen kürzen oder gar ablehnen. In Art. 6 der AVB's sind die Obliegenheiten geregelt. Nachstehend ein Auszug aus diesem Artikel:

Die versicherten Unternehmen sind unter anderem verpflichtet:

- *Computer sowie Computerprogramme und -netzwerke auf einem angemessenen Stand der Technik zu halten und vor unberechtigtem Eindringen Dritter zu schützen (beispielsweise mittels Firewall und Antivirusprogrammen)*
- *die Sicherung von digitalen Daten (Backups) in angemessenen Zeitabständen vorzunehmen, mindestens jedoch alle 30 Tage*
- *nach Bekanntwerden von neuen Sicherheitslücken die durch den Softwarehersteller zur Verfügung gestellten Sicherheitsaktualisierungen (Patches) in einem angemessenen Zeitabstand vorzunehmen, spätestens jedoch 30 Tage nach dem Erscheinungsdatum*

Um die IT Sicherheit im eigenen Betrieb sicherzustellen, gibt es diverse Handlungsempfehlungen. Hier eine Check-Liste von „cybercheck.de"[2]:



[2] https://cybercheck.de/cyber-blog/cybersicherheit-schnell-checkliste-fur-kmu#

Zur Abrundung der Thematik sind nachstehend noch drei aktuellere Artikel beigelegt, die sich allesamt mit Cyberrisk Vorfällen in der Gastronomie und v.a. der Hotellerie befassen:

1. Die unterschätzte Gefahr
2. Hacker erpressen Hotels!
3. Hyatt als Opfer von Cyber-Kriminellen

Freundliche Grüsse

Malick Gueye

Die unterschätzte Gefahr[3]

Hotellerie 24. Jun. 2018
Datenklau, Hackerangriffe und Online-Erpressung: Cyber-Kriminalität ist ein Risiko, mit dem sich die Hotellerie und Gastronomie künftig noch intensiver auseinandersetzen müssen.

Die Meldungen über digitale Attacken auf Hotels häufen sich. Hier eine kleine Auswahl an Schlagzeilen: «Hacker erpressen Hoteliers», «Cyber-Angriff legt Luxushotel lahm», «Kreditkartendaten von Gästen aus 41 Hyatt-Hotels gestohlen», «Hacker attackieren 1200 Hotels der Intercontinental Group».
Wer nun meint, bloss internationale Kettenbetriebe oder Luxushotels seien für Hacker interessant, irrt sich. Ein Cyber-Angriff kann jeden Betrieb treffen. Und er kann aus ganz verschiedenen, teilweise völlig unerwarteten Richtungen kommen.

Angriff aus den eigenen Reihen

«Experten schätzen, dass zwei bis vier Prozent der Mitarbeitenden eine erhöhte Bedrohung für die Cyber-Sicherheit eines Betriebes darstellen», sagt Raphael Schmid, Broker Financial Lines & Cyber bei der Aon Schweiz AG. Aon ist ein Dienstleistungsunternehmen in den Bereichen Versicherungs- und Rückversicherungsvermittlung, beruflicher Vorsorge und Anlagelösungen. Mit diesen Prozentzahlen sind nicht Mitarbeitenden gemeint, die aus Unwissenheit oder Unachtsamkeit Viren und Trojaner herunterladen. Gemeint sind Angestellte, die einen dehnbaren Ethikbegriff haben oder sogar böswillig gegen die Interessen des Arbeitgebers handeln. Ein Beispiel dafür ist der Fall eines Restaurants, bei dem ein paar Angestellte zusammen das Kassenprogramm austricksten. Und zwar so, dass sie über Monate hinweg täglich kleine Beträge für sich abzweigen konnten. Mit der Zeit läpperte sich einiges zusammen. Diese «Kleinvieh macht auch Mist»-Taktik ist bei Cyber-Kriminellen weit verbreitet und wird erfolgreich angewandt.

Monatelang freie Hand

Dadurch, dass sie jeweils pro Tag nur kleine Geld- oder Datenmengen bewegen, fällt ihre Anwesenheit im IT-System einer Firma oft kaum auf. Die Cyber-Kriminellen fliegen quasi unter dem Radar und können ungehindert Daten klauen oder die IT eines Unternehmens anderweitig missbrauchen. Zum Beispiel, um gefälschte Identitäten zu erstellen. Sowohl für Personen wie auch für Firmen.
So bezog in einem Fall in Basel ein Angestellter, den es gar nicht gibt, monatelang Lohn. Ein Betrüger hatte sich Zutritt in die Datenbank der Personalabteilung einer grossen Firma verschafft. Er erstellte dort für sich ein Fake-Profil, gab sich selbst eine entsprechende Zugangsbewilligung für die IT und überwies sich ein grosszügiges Salär. Erst nach Monaten flog er auf.
In den letzten Jahren waren Hacker im Schnitt 229 Tage, also fast acht Monate, im IT-System eines Unternehmens aktiv, bevor sie entdeckt wurden. «Die Sicherheitsmassnahmen werden laufend besser, so dass Attacken schneller erkannt werden», sagt Raphael Schmid.
Sofort zu erkennen geben sich hingegen Cyber-Erpresser. Sie blockieren Daten, Passwörter, Schlüssel-, Kassen- oder Haustechniksysteme und geben sie nur gegen Bezahlung eines Lösegeldes wieder frei. Eine Massnahme, um es Cyber-Kriminellen möglichst schwer zu machen, ist die Sensibilisierung der Mitarbeitenden in Bezug auf Phishing, Social Engineering, trojanisierte Software und Watering Holes. Europäische Datenschutzregeln gelten auch für Schweizer Hotels
Raphael Schmid rät, interne Cyber-Sicherheitsrichtlinien und -Prozessabläufe festzulegen. Was ist bei einem Cyber-Angriff zu tun? Wie überbrückt man die Zeit, bis wieder wie gewohnt gearbeitet werden kann? Das sollte wie das Verhalten bei einem Brand immer wieder geübt werden.
«Der Umgang mit Cyber-Risiken bedingt ein Konzept», sagt Schmid weiter. Ins Konzept gehören Risikoanalysen, Quantifizierungsprojekte, realistische Hacker-Attacken-Tests und eine Cyber-Versicherung. Die kann den Betrieb nicht vor Angriffen schützen, aber vor den Kosten für Schadensbegrenzung und -behebung sowie vor finanziellen Folgeschäden und ermöglicht den Zugang zu professioneller Unterstützung im Krisenfall. Zum Beispiel bei Datenklau.

[3] https://www.hotellerie-gastronomie.ch/de/artikel/die-unterschaetzte-gefahr

Seit Mai gilt die neue europäische Datenschutzgrundverordnung (DSGVO). Sie sieht Bussen bis zu 20 Millionen Euro vor, wenn der Datenschutz nicht eingehalten wird. Obschon es sich um eine europäische Verordnung handelt, gilt sie auch für Schweizer Hotels, die Gäste aus dem EU-Raum beherbergen. Auf Gästedaten, vor allem Kreditkarteninfos, haben es Cyber Kriminelle besonders abgesehen. Deshalb sollte man am besten nur jene Gästedaten sammeln und den Mitarbeitenden zugänglich machen, die sie für ihre Arbeit wirklich brauchen.

Vernetzen, aber sicher!

WLAN für Hotelgäste, Mitarbeitende, die geschäftliche Mails auf ihren privaten Tablets beantworten, Kopierer und Kaffeemaschinen, die selbständig mit dem Servicetechniker kommunizieren – jedes Gerät, das einen Onlinezugang hat, ist ein mögliches Einfallstor für Cyber-Kriminelle und somit ein ernst zu nehmendes Sicherheitsrisiko.

«Es wird oft ausgeblendet, dass ein Hotel mit anderen Unternehmen und Zulieferern verbunden ist, über deren Sicherheitsmassnahmen man in der Regel nichts oder nur wenig weiss», warnt Raphael Schmid. So wie eine Billardkugel über ein mehrfaches Bandenspiel ins Loch versenkt werden kann, gelangen auch Cyber-Kriminelle über verschlungene Umwege ins IT-System eines Hotels. Das lässt sich beim heutigen Stand der Digitalisierung und Vernetzung kaum vermeiden. Aber eindämmen. Zum Beispiel durch getrennte Internetzugänge für den Gästebereich und den eigentlichen Hotelbetrieb.
(Riccarda Frei)

Hacker erpressen Hotels![4]

Cyber-Kriminalität in Schweizer Hotels: Kriminelle verschlüsseln Daten und fordern Lösegeld. Wie können sich Hoteliers schützen?

November 28, 2017

Jedes Hotel besitzt sensible Daten und Informationen von Kunden, doch die meisten Hotels sind nicht ausreichend gegen Cyberkriminalität geschützt – Kriminelle verschlüsseln ihre Dateien und fordern Lösegeld. Ein brisantes Thema, welches die Branche in Zukunft stark beschäftigen wird.

Die Anfrage für eine Reservierung kam auf Englisch, ein Mitarbeiter an der Rezeption klickte unbedacht auf einen Link am Ende der E-Mail. Kurz darauf klingelte bei Hotelmanager Thomas Müller*, der auf der Rückreise aus den Ferien war, das Telefon Sturm. Fast alle Programme der Hotelrechner seien lahmgelegt, Mail-Verkehr nicht möglich, wichtige Dateien verschlüsselt, berichteten die Mitarbeiter des Viersternehauses im Raum Zürich. Mehr noch: Auf dem Bildschirm sei eine Lösegeldforderung erschienen. 1500 Dollar müsse er zahlen, um wieder an seine Dateien zu kommen.

Die Ursache: eine Schadsoftware, die Daten verschlüsselt und Lösegeld fordert, im Fachjargon „Ransomware“ genannt. Müller hatte Glück im Unglück. Das Reservationsprogramm war nicht betroffen, er konnte noch Rechnungen ausstellen und Gäste einchecken.

Anders lief es vor einigen Jahren bei Thierry Geiger: In seinem Bündner Viersternehotel Saratz legte Ransomware mehrere Tage lang das System komplett lahm. «Wir mussten alle Rechnungen von Hand schreiben, auf Papierlisten eintragen, wo welche Gäste untergebracht sind. Wären wir ausgebucht gewesen, wären wir abgesoffen.»

Beide Hoteliers zahlten kein Lösegeld und konsultierten Experten für Informationstechnik. Die Sicherheitslücke kam teuer zu stehen: 10 000 Franken musste Müller berappen. Geiger zahlte gar 50 000 Franken, unter anderem für neue Server. Ein österreichisches Hotel traf es noch härter. Nach einem Ransomware-Angriff funktionierte nicht einmal mehr das System für die elektronischen Zimmerschlüssel. Die Beispiele sind keine Einzelfälle.

«Es gibt vermehrt Ransomware-Angriffe, und vielen Hoteliers ist die Gefahr nicht ausreichend bewusst», sagt Hotelleriesuisse-Präsident Andreas Züllig. Einzelne handelten gar fahrlässig, indem sie ihre Systeme nicht ausreichend schützten.

Zahlen zur Cyberkriminalität in der Hotellerie gibt es nicht. Das Bundesamt für Polizei erhielt 2015 insgesamt über 300 Meldungen zu Ransomware, die Attacken nähmen weiter zu, sagt eine Sprecherin. Wie stark, lassen Daten des auf Sicherheitssoftware spezialisierten Unternehmens Kaspersky erahnen. Waren 2014 nur 128 Firmenkunden in der Schweiz betroffen, so waren es im letzten Jahr schon 2324. Zunächst seien die Angriffe vorwiegend gegen Privatpersonen gerichtet gewesen, mittlerweile häuften sich die Fälle bei Unternehmen, sagt ein Sprecher. Es kann jeden treffen, ob Handwerksbetrieb oder Arztpraxis, Spital oder Treuhänder.

Die Hoteliers sprechen nicht gern über das Thema, sie fürchten um ihren Ruf. Von Anzeigen verspricht man sich wenig Erfolg. Geiger meldete sich bei der Polizei: Sie konnte ermitteln, dass der Angriff von der Ukraine aus erfolgte. Die Strafverfolgung war unmöglich.

Vielfach sind die Behörden überfordert, einzig der Kanton Zürich unterhält ein Kompetenzzentrum für Cyberkriminalität. Und das, obwohl dem Bundesamt für Polizei 2015 über 11 000 Cybercrime-Fälle gemeldet wurden. Es rät von Lösegeldzahlungen ab, weil nicht gewährleistet sei, dass die

[4] https://www.hotelinsider.ch/aufgepasst-hacker-erpressen-hotels/

Daten tatsächlich entschlüsselt werden. Kommt hinzu, dass die Schadsoftware immer raffinierter wird.

«Es gibt neuerdings Trojaner, die nach einer Lösegeldzahlung erneut zuschlagen», sagt Pascal Mittner von der IT-Sicherheitsanalysefirma First Security Technology. «Oder solche, die so programmiert sind, dass sie erst mit der Verschlüsselung beginnen, wenn sie herausgefunden haben, wo eine Sicherheitskopie der Daten abgespeichert ist.»

Ein Back-up gilt als einziger Ausweg nach einer Verschlüsselung. Mit seiner Hilfe können Server und Endgeräte neu aufgesetzt, die Daten gerettet werden. Wenn dieses Back-up aber auch verschlüsselt sei, zahle der eine oder andere dann doch lieber Lösegeld, sagt Mittner.

Wie können Hoteliers derartige Angriffe vermeiden? IT-Experte Herbert Stieger von der Firma Informatica hält eine wirksame Firewall und einen gut eingestellten Spamfilter, der verdächtige E-Mails gar nicht erst ins Postfach lässt, für am wichtigsten. Seine Firma betreut IT-Systeme von über 120 Kunden aus verschiedensten Branchen. Stieger sieht im Schnitt einen Ransomware-Fall im Monat.

Immer wieder erlaubten Hotels ihren Mitarbeitern aber auch, private Mails im Browser zu öffnen, sagt Hans Hänny von der IT-Firma Client Systems, der rund 120 Hotels betreut. Dann helfe selbst der beste Spamfilter für die Geschäftsadresse nichts. Der Virenscanner ist umstritten, meist wird er empfohlen, aber er muss laufend aktualisiert werden. Entscheidend ist die Schulung der Mitarbeiter. Die Hotellerie birgt spezielle Risiken. Die Belegschaft ist gross und wechselt häufig. Zudem geht es um umfangreiche Kundendateien. Auch Datenklau gilt als gängiges Motiv von Cyberattacken. «Seien wir ehrlich, ich weiss alles über Sie, ich habe Ihre Adresse, Telefonnummer, Ihre Passnummer», sagt ein Hotelier.

Ernst Wyrsch, Präsident von Hotelleriesuisse Graubünden, schätzt, dass gerade Vier- und Fünfsternehäuser in prominenten Orten wie St. Moritz, Gstaad, Zermatt oder Davos für Hacker interessant sind. Informationen darüber, wer während des Weltwirtschaftsforums wo logiert, dürften einen hohen Wert besitzen.

Manche Hotels richten mit dem Gratis-WLAN für die Gäste auch gleich die Sicherheitslücke ein. Das Gäste-WLAN muss von jenem für die Mitarbeiter abgekoppelt sein, um unerwünschte Zugriffe zu verhindern. Das sei nicht immer der Fall, sagt Hotelleriesuisse-Präsident Züllig. Denn IT-Sicherheit erfordert hohe Investitionen. Rund 30 000 Franken investierte Züllig im eigenen Haus, dem Schweizerhof auf der Lenzerheide, in eine neue, sichere Infrastruktur. Jeden Monat werden Dutzende Seiten gesperrt, auf denen Gäste oder Mitarbeiter unterwegs waren und die vom Sicherheitssystem als riskant eingestuft wurden.

Auch Kreditkarteninformationen sind ein beliebtes Ziel von Hackern. Während Buchungsplattformen wie Booking.com Kreditkartennummern selbst verwalten, verzichten Hoteliers vermehrt darauf – aus Angst, bei einem Datendiebstahl zur Verantwortung gezogen zu werden. Derartige Informationen würden nicht abgespeichert, sagen mehrere Hoteliers. Im digitalen Zeitalter erfassen viele die Kreditkartendaten wenn überhaupt handschriftlich. «Und dann ab damit in den Safe», sagt der Direktor eines Kongresshotels.

*Name der Redaktion bekannt

Hyatt als Opfer von Cyber-Kriminellen[5]

Mitte Oktober sorgte der Datendiebstahl von Kreditkarteninformationen bei Hyatt für Aufsehen. Die Hotelgruppe wurde bereits zum zweiten Mal in diesem Jahr gehackt – und zwar im großen Stil. Die Täter installierten eine sogenannte Malware auf den Hyatt-Systemen, diese übermittelte dann sämtliche Gästedaten an die Hacker.

IT-Experten sehen in der zunehmenden Digitalisierung und Vernetzung der Hotels ein großes Risiko für Angriffe. Offizielle Zahlen oder Beispiele von betroffenen Hotels liegen jedoch nicht vor. Doch obwohl Hotelverbände ihre Mitglieder laufend mithilfe von Vorträgen oder Seminaren sensibilisieren und zahlreiche Ketten sich den Datenschutz auf die Fahnen schreiben – nicht jedes Hotelmanagement ist aufgeklärt und schützt sich ausreichend. Da ist sich auch Ivan Bütler sicher. Er ist selber Hacker – allerdings kein krimineller. Der Schweizer nutzt sein Wissen, um Firmen vor Angriffen aus dem Internet zu schützen und gründete das Ethical-Hacking-Unternehmen Compass Security. „Die Aufklärung der Hotels über aktuelle Bedrohungen ist ein laufender Prozess – das Internet entwickelt sich ständig weiter." Zahlreiche neue Chancen wie etwa Bitcoin oder Internet of Things seien Trends, denen auch Hotels folgen möchten – der Spagat zwischen der Nutzung dieser neuen Geschäftschancen und der entsprechenden Absicherung der Bedrohung gelingt laut Bütler allerdings nicht immer. „Sicherheit ist ein mühsamer Aspekt, der mit Kosten und weniger Usability gekoppelt ist. Darum gewinnt meist der Kundennutzen und die Security erhält keine oder die zweite Priorität."

Die Schwachstellen wurden auch kürzlich in einer Diskussionsrunde auf der Plattform der Zürcher Hoteliers deutlich. Nicht nur Bütler warnte davor, sondern unter anderem auch der Staatsanwalt des Kantons Zürich, Stephan Walder. Sehr oft ginge es bei der Cyberkriminalität nämlich um Erpressung. Hacker installieren Malware auf den Sytemen des Hotels – ähnlich wie bei Hyatt. Allerdings verschlüsseln diese Programme zahlreiche Daten und fordern zur Freischaltung Lösegeld. So geschehen Anfang des Jahres im Hotel von Elio Frapolli in Dietikon. Er ist den Forderungen nachgekommen – und musste dennoch im Nachhinein die gesamte Hard- und Software im Hotel austauschen, was den Hotelier insgesamt rund 100 000 Franken kostete.

In Ivan Bütlers Augen sind gerade Hotels so verwundbar, weil Fremde die Gäste leichter ausspionieren können als in deren Zuhause. Worauf es ein Hacker abgesehen hat, sei ganz unterschiedlich – Kreditkartendaten, persönliche Informationen, oder vertrauliche und geheime Infos von Laptops und Handys. Das Hotel sei auch ein idealer Ort, um Personen zu orten, deren Bewegungen und Kommunikationsverhalten zu analysieren oder auch Trojaner und andere Malware auf die persönlichen Geräte der Hotelgäste zu pflanzen. Wirklich schwierig sei es für einen Profi dabei nicht, ein Hotel oder dessen Gäste zu hacken. „Es kommt einfach darauf an, wie gut der Angreifer ausgerüstet ist", so Bütler.

Neue Technologien wie Smart-TVs oder digitale Zimmerschlüssel spielen den Hackern dabei in die Karten – denn Hoteliers sehen zunächst den Mehrwert für den Gast und lassen, so Bütler, Sicherheitsaspekte außen vor. „Erst wenn etwas passieren sollte – wenn beispielsweise via eingebaute Kamera des Smart-TV irgendwelche unpässlichen Inhalte an die Öffentlichkeit gelangen – wird diese Technik auch als Gefahr und Bedrohung wahrgenommen", warnt der IT-Experte.

Jedes Hotel sollte sich – und damit auch die Gäste – vor Angriffen aus dem Internet im Vorhinein schützen. So ist es zum Beispiel ratsam, ein effektives Risikomanagement einzuführen, so Alexander Fritz, Geschäftsführer der Fritz & Fritz Risikoberatung. Es gibt für Hotels und Unternehmen einen speziellen Versicherungsschutz. Zum einen ist das eine Eigenschadenversicherung (Cyber-Versicherung), die Ansprüche Dritter und deren Abwehr bei

[5] https://www.hotelinsider.ch/aufgepasst-hacker-erpressen-hotels/

Verletzung des Datenschutzes, der Vertraulichkeit und des Persönlichkeitsrechts umfasst. Zum anderen deckt eine sogenannte Cyber-Haftpflicht Schäden durch eigenes Verschulden ab.
Ivan Bütlers Vorschlag: „Ein IT-Sicherheitsbeauftragter sollte sich über die neuen Cyber-Bedrohungen im Klaren sein und ein Abwehr-Sicherheitsdispositiv aufbauen." Zudem sollte es einen Notfallplan geben, falls ein Cyber-Ereignis eintritt. Dennoch betont er: „Niemand ist vor einer Hackerattacke 100-prozentig sicher." Sollte ein Hotel Opfer der Cyberkriminalität werden, müsse es seine Sicherheitsmaßnahmen überarbeiten und Anpassungen vornehmen. Die Experten raten außerdem dazu, so schnell wie möglich Kontakt mit der Polizei aufzunehmen.

QuelleTages Anzeiger (Sonntagszeitung) Cornelia Krause, Zürcher Hotelierverein, Top Hotel Deutschland