Gefahr aus dem Cyberraum

Attacken auf die IT-Infrastruktur können den ganzen Hotelbetrieb lahmlegen. Darum braucht es durchdachte technische Schutzvorrichtungen. Auch der Faktor Mensch ist mitzubedenken.

Andreas Lorenz-Meyer

iStockphoto

Im Dezember 2022 horchte die Branche auf: Die IT-Netzwerke der H-Hotels waren attackiert worden. Wie ist der Vorfall einzuordnen? Tatsächlich wachse die Gefahr von Cyberangriffen, sagt Thomas Hildebrand, Director of Finance, IT & Purchasing und Mitglied der Geschäftsleitung von The Living Circle. Er beobachtet, dass die Angreifer immer cleverer und dreister werden. Die Hotellerie wiederum schenke dem Thema IT-Sicherheit zu wenig Aufmerksamkeit. «Darum sind viele Häuser ein recht leichtes Ziel für Ransomware-Angriffe.» Dies sind Cyberangriffe, bei denen eingeschleuste Schadsoftware Daten verschlüsselt. Für die Entschlüsselung verlangen die Angreifer ein Lösegeld (ransom).

Es gilt, die IT-Infrastruktur rechtzeitig fit zu bekommen . Denn jeden kann es jederzeit erwischen. Wobei Hotels nicht den Sicherheitsstandard von Banken anstreben müssten, so Hildebrand. Dieser wäre in der Branche auch gar nicht finanzierbar. «Jedoch sollten sie dem Thema genug Gewicht geben – und dann notwendige Massnahmen treffen.»

Mehrmals täglich Daten sichern

Für eine solide IT-Sicherheitsstruktur sind ein sorgsam entwickeltes Konzept und ein segmentiertes lokales Netzwerk notwendig. Ein Netzwerk, das wiederum in verschiedene virtuelle, voneinander getrennte Netzwerke unterteilt ist. Hildebrand erläutert dessen Nutzen: «Konnten Angreifer in ein Netzwerk eindringen, haben sie damit noch lange nicht die komplette Infrastruktur gekapert. Es gibt für sie kaum eine Möglichkeit, in ein anderes Netzwerk zu gelangen.» Beispiel: Ist die Buchungsmaschine betroffen, bleibt die Enterprise-Resource-Planning-Software unbeschadet. «Ein wirksamer Schutz ist nur durch die Segmentierung überhaupt realisierbar», meint Hildebrand. Auch gute Back-up-Lösungen seien zentral. Wobei die Datensicherung mehrstufig ablaufen sollte, intern und extern über eine verschlüsselte Cloud-Lösung. Schon gesicherte Datensätze sollten nicht überschreibbar (read only) sein. Hildebrand rät auch zu kurzen Back-up-Intervallen. «Die Datensicherung muss mehrmals täglich stattfinden. So lässt sich der Datenverlust bei einem Angriff auf wenige Stunden begrenzen, der Schaden wird minimiert.» Hotels könnten so kaum mehr erpressbar werden.

Was Cyberattacken anrichten, erlebte das «Waldhaus Flims» im Herbst 2021. Hackern gelang es, in die IT-Struktur einzudringen. Der Betrieb war während zweier Wochen stark eingeschränkt. Auf personenbezogene Daten konnten die Angreifer nicht zugreifen, da diese verschlüsselt waren. «Zudem hatten wir die Back-ups inhouse auf getrennten Netzwerken», so Direktor Bosko Grozdanic. Nach der Attacke wurden zur Sicherheit nur die Datenbanken aus dem Back-up wiederhergestellt. Das Hotel analysierte die IT-Schwachstellen und behob sie durch Implementation neuer Tools. Diese werden nun regelmässig einem Härtetest unterzogen: Eine Drittfirma ist beauftragt, das System immer wieder anzugreifen. «So erkennen wir Sicherheitslücken – sofern es sie gibt – und können diese sofort schliessen.»

459

Hacking-Angriffe wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) im Jahr 2022 gemeldet. «Hacking-Angriff» ist definiert als «Eindringen in ein System oder Konto».

159

Meldungen bezogen sich 2022 auf Ransomware-Angriffe. Diese sind der Kategorie Schadsoftware-Angriffe zugeordnet.

Im Zweifelsfall Mail löschen, im Ernstfall Verbindung kappen

Grozdanic achtet auch auf den Faktor Mensch – eine von Hackern bevorzugt anvisierte Schwachstelle. Sie verschicken Mails, die mit Malware-Links versehen sind und einen auffordern, draufzuklicken. Wer dies tut, lässt die Angreifer ins System. Grozdanic sieht darin «einen der empfindlichsten Angriffspunkte». Umso wichtiger sei es, das Personal zu schulen. Mitarbeitende müssten jede Mail aufmerksam lesen und sich zweimal überlegen, ob sie einen Link öffneten. Im Zweifel: lieber löschen. Um zu testen, ob die Regel beherzigt wird, lässt sich das Hotel regelmässig Fake-Mails zuschicken. Wenn ein Angriff gelingt, kommt es auf Schnelligkeit an. Das Hotel muss sofort alle Internetverbindungen kappen und die Server mit einem Back-up überspielen, das nicht vom Hackerangriff befallen wurde. Auf Erpressungsversuche dürften Hotels auf keinen Fall eingehen, sagt Grozdanic.

Nachgefragt

zvg

Thomas Orlamünder
Unabhängiger IT-Berater und Inhaber der Firma Evoloque Consulting

Hundertprozentige Sicherheit vor Cyberangriffen sei eine Illusion, sagt der Thuner IT-Berater Thomas Orlamünder. Was Hotels beachten sollten, um die Gefahr zumindest zu minimieren.

Herr Orlamünder, Hacker verschicken häufig Mails mit Malware-Links. Welche Angriffspunkte gibt es im Hotel noch?
Jede Menge. Unsichere, unzureichend komplexe oder abgespeicherte Passwörter sind eine Schwachstelle. Genau wie eine grosszügige Vergabe von Benutzerberechtigungen. Auch ein falsch konfiguriertes Gäste-Wi-Fi kann gefährlich sein – fürs Hotel und, noch schlimmer, für die Gäste selbst. Hinzu kommen weniger offensichtliche Gefahren: Snack-Automaten oder Küchenmaschinen, die selbsttätig über das Internet kommunizieren.

Schauen wir auf die Hardware. Wie lässt sich IT-Infrastruktur sicher machen?
Eine Firewall mit Web-Filter wehrt Angriffe aus dem Internet ab und blockiert den Zugriff auf Webseiten, die als bedrohlich eingestuft sind. Für grössere Infrastrukturen mit eigenen Servern oder Speichersystemen empfiehlt sich ein Angriffserkennungs- oder Angriffsverhinderungssystem. Selbstverständlich müssen alle Komponenten der IT-Infrastruktur professionell konfiguriert und mit einem Virenschutz ausgestattet sein. Und sie müssen regelmässig aktualisiert werden – hier lohnt sich eine zentrale Überwachung.

Wozu raten Sie: Daten in der Cloud speichern oder auf dem hoteleigenen Server?
Cloudbasierte Hotelinformationssysteme sind in vielerlei Hinsicht die bessere Wahl. Sofern das Rechenzentrum professionell betrieben wird, gibt es dort mehr Möglichkeiten, Angriffe zu erkennen und abzuwehren. Ausserdem sind die Daten

«Ein falsch konfiguriertes Gäste-Wi-Fi kann gefährlich sein.»

ausserhalb des Hotels gespeichert – und so im Ernstfall auch ohne Zugriff auf die Hotelinfrastruktur via Tablet erreichbar. Daher ist das Kerngeschäft im Ernstfall nicht gefährdet.

Was ist bei der Wahl des Anbieters wichtig?
Hotels sollten sich regelmässige Back-ups, deren Aufbewahrungsfristen und die Absicherung der Infrastruktur vertraglich zusichern lassen. Zudem sollten sie klären, ob der Support auch an Wochenenden oder Feiertagen erreichbar ist und Probleme auch dann gelöst werden können. Idealerweise stellt der Anbieter gesicherte direkte Schnittstellen zu Buchungsplattformen zur Verfügung, wodurch zusätzlicher Aufwand vermieden und die Datensicherheit erhöht wird.

Sollte ein Angriff erfolgreich sein: Was ist bei der Datenwiederherstellung zu beachten?
Die Freude darüber, dass verloren gegangene Daten wieder da sind, währt manchmal nur kurz. Nämlich dann, wenn die Schadsoftware noch immer aktiv ist – und die Daten ein zweites Mal verschlüsselt. Daher müssen Hotels ihre IT-Infrastruktur nach einem Angriff unbedingt prüfen, Schwachstellen beseitigen und Schäden bereinigen. Bei lokal gespeicherten Daten kommt es dann zu einer längeren Unterbrechung.

Ransomware-Angriff

Hackerangriff auf H-Hotels

Am 11. Dezember 2022 attackierten kriminelle Hacker die IT-Netzwerke der deutschen Gruppe H-Hotels, die auch Häuser in der Schweiz hat. Die Angreifer konnten die mehrstufigen Schutzvorrichtungen durchbrechen und Teile der IT-Systeme verschlüsseln. Die Hotelgruppe informierte sofort die Behörden und untersuchte den Vorfall mithilfe externer Spezialisten und IT-Forensiker. Das Ergebnis: Die Cyberkriminellen hatten Daten gestohlen, darunter Namen und Mailadressen, aber keine nutzbaren Zahlungs- oder Bankinformationen. Öffentlichkeit, Partnerfirmen und Mitarbeitende wurden entsprechend informiert.

Schnelle und offene Kommunikation
Die Angreifer verlangten ein Lösegeld für die Entschlüsselung der Daten und drohten, diese sonst im Darknet feilzubieten. H-Hotels ging auf die Forderung nicht ein, woraufhin die Daten im Darknet auftauchten. Die Gruppe informierte darüber sofort. Besonders in solchen «herausfordernden Situationen» komme es auf «offene, transparente und schnelle Kommunikation» an, sagt die Hotelgruppe. Diese Strategie habe sich bewährt. Sie stärke das Vertrauen und schaffe Verständnis. Der Schaden hielt sich in Grenzen, da sofort alle Systeme heruntergefahren und vom Internet getrennt wurden. **alm**