So tun, als wären die Hacker drin

Der Hacker-Angriff auf Marriott zeigt nach Meinung von Experten vor allem eines: Es kann jeden treffen. Umso wichtiger ist die Vorbereitung auf den Ernstfall.

PATRICK TIMMANN

Es ist einer der grössten bekannten Cyber-Angriffe überhaupt: Hacker haben Daten von bis zu 500 Millionen Personen aus der Gästedatenbank der weltgrössten Hotelgruppe Marriott abgeschöpft. Betroffen sind neben Personendaten wie Namen und E-Mail-Adressen zum Teil auch besonders sensible Informationen wie Kreditkartenangaben und Reisepassnummern. Wer die Täter sind, auf welche und wie viele Kundendaten genau sie Zugriff hatten und wie die entwendeten Informationen missbraucht wurden – all dies liegt aktuell noch im Dunkeln. Fest steht, dass der eigentliche Angriff bereits 2014 erfolgte und damals das Hotel- und Freizeitunternehmen Starwood betraf. Mit der Übernahme der Gruppe im Jahr 2016 kaufte Marriott unwissentlich auch das Hacker-Problem mit ein. Auf die Schliche kam der Konzern den Tätern erst im September dieses Jahres. Publik wurde der Vorfall dann Ende November.

Vier Jahre nach dem Angriff und eine Megafusion später fragt man sich: Haben Starwood und Marriott die Cyber-Sicherheit vernachlässigt? Die Experten wollen von solch pauschalen Schuldzuweisungen nichts wissen. «Im Nachhinein ist es immer leicht, jemanden an den Pranger zu stellen. Ich wäre mit Statements sehr zurückhaltend. Es gibt vermutlich viele Firmen, die infiziert sind, es aber noch nicht wissen», meint Thomas Koller, Chief Innovation and Product Officer bei der Schweizer Versicherungs- und Beratungsfirma IBC. Auch Sandro Müller, CEO der Zürcher IT-Sicherheitsfirma goSecurity, will nicht leichtfertig vorverurteilen: «Ich masse mir nicht an, dies zu beurteilen. Nur weil die Hacker schon lange im System sind, heisst das nicht, dass fahrlässig gehandelt wurde.» Ähnlich ist die Einschätzung von Stephan Walder, Stv. Leitender Staatsanwalt des Kantons Zürich. Dass ein Hacker-Angriff erst nach längerer Zeit erkannt wird, sei nichts Aussergewöhnliches. Zudem würden viele Schadprogramme erst nach einiger Zeit aktiv. Walder ist Leiter des Kompetenzzentrums Cybercrime. «Die Malware ist zum Teil hochkomplex. Sie sind bei der Bekämpfung auf Spezialisten angewiesen», mahnt der Jurist. Grundsätzlich hält er einen Cyber-Angriff für jederzeit möglich. «Eine grosse Hotelgruppe wie Marriott ist ein beliebtes Angriffsobjekt von Hackern», so Walder. Beim Thema Cyber-Sicherheit gebe es immer zwei Faktoren: die Technik und den Menschen. Selbstverständlich müsse man sich auf technischer Ebene gegen Angriffe rüsten und auch die Mitarbeitenden für das Thema Cyber-Sicherheit sensibilisieren. Aber: «Das Risiko lässt sich nie ganz ausschliessen, sondern immer nur minimieren. Absolute Sicherheit gibt es nicht.»

> «Eine grosse Hotelgruppe wie Marriott ist ein beliebtes Angriffsobjekt.»
>
> **Stephan Walder**
> Stv. Leitender Staatsanwalt ZH

Vorbereitet auf den Brandfall, konfus beim Cyber-Angriff

«Keiner hört das gerne, aber es kann jeden treffen», resümiert Sandro Müller den Konsens unter den Experten. Umso wichtiger sei es, dass sich Hotels nicht nur mit der Abwehr von Angreifern, sondern auch mit den Folgen eines bereits erfolgten Cyber-Angriffs auseinandersetzen. «Ich würde jedem Hotel ans Herz legen, verschiedene Krisenszenarien durchzudenken und sich zu überlegen, wie man im Ernstfall am besten reagiert», sagt Thomas Koller. «Proben Sie die Krisenkommunikation, schulen Sie die Reaktionen Ihrer Mitarbeitenden, erstellen Sie einen Plan und trainieren Sie ihn», lautet sein Rat. Der Bereich Cyber-Sicherheit werde vielerorts noch nicht ernst genug genommen. «Alle reden immer vom grossen Feuer und proben den Brandfall, die Evakuation. Aber niemand übt den Cyber-Ernstfall am Computer.»

«Die Kultur im Unternehmen bezüglich des Themas Sicherheit ist wichtig, aber ein Restrisiko bleibt», wiederholt Sandro Müller noch einmal. Deshalb empfehle er Unternehmungen eine grundsätzlich andere Herangehensweise an das Cyber-Problem: «Gehen Sie davon aus, dass die Hacker bereits bei Ihnen im System drin sind. Bauen Sie nicht einfach eine grosse Mauer um sich herum, sondern schaffen Sie auch interne Strukturen und Hürden, die Hackern das Leben schwer machen.» Eine Denkweise, die von der Geschäftsführung durchaus Mut erfordert, wie Müller zugibt.

Bis ein Unternehmen von einem Hacker-Angriff erfährt, vergehen oft viele Monate.
Pixabay/Montage htr

Hilfe beim PR, aber keine Kompensation entgangener Umsätze

Ist ein Angriff einmal erkannt, beginnt die Krisenbewältigung. Abgesehen von der Schadensbegrenzung und -bewältigung an der Infrastruktur (Eigenschaden) sowie an Dritten (Haftpflichtschaden), wird gerade im Social-Media-Zeitalter ein weiterer Bereich zunehmend wichtiger: der Schutz vor Reputationsschäden. Ob und wie sich Marriott gegen den Verlust des guten Rufs und damit einhergehenden Buchungsrückgängen versichert hat, wollte die Gruppe auf Anfrage nicht beantworten. Auch darüber, ob bereits Rückstellungen für Schadensersatzforderungen seitens Dritter vorgenommen wurden, schweigt sich der Konzern aus.

In der Schweiz ist eine Versicherung von Umsatzausfällen durch Rufschäden noch unüblich. «Grundsätzlich kann man den Verlust der Reputation eigentlich nicht messen, weswegen auch eine Wiederherstellung ebendieser nicht gemessen werden kann», teilt Leilah Ruppen von der Mobiliar mit. Ihre Versicherung übernehme im Rahmen der Cyber-Schutz-Versicherung für Unternehmen je nach Deckungsgrad Kosten für das Public-Relations-Management. Die Entschädigung umfasse auch «Kosten für die Begrenzung eines bei einem Kunden des Versicherungsnehmers entstandenen negativen Eindrucks durch die Medienberichterstattung.

> «Die Sicherheitskultur im Unternehmen ist wichtig, aber ein Restrisiko bleibt.»
>
> **Sandro Müller**
> CEO goSecurity

Ähnliche Leistungen umfasst auch die Axa-Arag Rechtsschutzversicherung, wie Mediensprecherin Anna Ehrensperger auf Anfrage mitteilte. Im Rahmen der Sachversicherung und Haftpflichtversicherung übernehme die Axa für Firmenkunden auch die Kosten für die Krisenkommunikation (bis 50 000 Franken) «für die unmittelbare Abwendung oder Minderung eines möglichen Reputationsschadens nach einem versicherten Ereignis». Dafür werde dem Kunden eine PR-Agentur «zur Seite gestellt», welche ihn unterstützt und berät.

Der Teufel liegt freilich im Detail. Auch die SwissRe bietet eine Cyber-Police an, diese decke jedoch in erster Linie Eigen- und Drittschäden ab, erklärt Christian Wertli, Head of Innovative Risk Solutions des Bereichs Corporate Solutions des Rückversicherers. «Für Buchungsausfälle bräuchte man tatsächlich eine Shitstorm-Versicherung», so der Fachmann in Anspielung auf seine Aussagen gegenüber Medien der Tamedia-Gruppe Anfang November. Damals lag der Fokus jedoch auf möglichen Reputationsschäden aufgrund negativer Gästekommentare auf Bewertungs- und Buchungsplattformen. Wie man eine Rufschädigung durch einen Hacker-Angriff versicherungstechnisch abdecken könnte, müsste man im Einzelfall genau abklären. «Da braucht es eine massgeschneiderte Lösung.»

Leitfaden Cyber-Sicherheit unter
hotelleriesuisse.ch → Services → Ganzheitliche Sicherheit