# Eine offene Beziehung

**Wenn die Achtsamkeit auf der Strecke bleibt: Im Hotel und auf Reisen kümmert viele Menschen der Datenschutz, den sie sonst einfordern, wenig.**

Die neuen Herren haben keine Kosten und Mühen gescheut. Mehr als fünf Jahre und eine dreistellige Millionensumme waren nötig, um eine verlassene Rostlaube zum Viersternehotel zu verwandeln. Der Tour Pleyel, in den 1970er-Jahren in der Pariser Banlieue Saint-Denis als mit Cortenstahl verkleideter Büroturm errichtet, beherbergt nun beinahe 700 Zimmer, Skybar, Fitness-Center und Frankreichs höchsten Swimmingpool in fast 140 Meter Höhe. Mit Blick über Paris.

Letzteres zu betonen, ist den Betreibern wichtig. Bei allen Hoffnungen, welche die H-Hotels-Gruppe aus Hessen und ihr US-Partner Wyndham auf Geschäftsreisende mit dichten Terminkalendern setzen – sie müssen auch an die Social-Media-affine Klientel denken. Aber tun sie das ernsthaft? Aus Sicherheitsgründen lässt sich keines der Hotelfenster auch nur einen Spalt breit öffnen. Das WLAN im Haus dagegen: offen. Für wen und was auch immer.

Man könnte sich darüber amüsieren, wenn Reisende nicht ständig auf ähnliche Bedingungen träfen: Das Internetangebot in Hotels, Cafés, Museen oder Verkehrsmitteln ist gratis, aber unverschlüsselt, egal wie oft Experten vor Cyberattacken warnen. Selbst deutsche Offiziere konnten im vergangenen Jahr bei ihren Gesprächen über eine mögliche Lieferung von Marschflugkörpern in die Ukraine abgehört werden. Einer der Beteiligten hatte sich über eine offene Leitung seines Hotels in Singapur in die Konferenz eingewählt. Da liegt das Problem: „Daheim wird gewissenhaft bei der Einrichtung des Routers auf die Verschlüsselung geachtet. Im Hotel und auf Reisen bleibt scheinbar die Achtsamkeit zu oft auf der Strecke“, sagt Achim Möhrlein. „Komisch, aber das ist der Effekt: Wenn es kostenlos und einfach ist, dann wird es akzeptiert.“

Möhrlein ist Geschäftsführer von The Cloud Networks. Das Münchner Unternehmen gehört zu den führenden Anbietern in Europa für professionelle WLAN-Netzwerke. Kunden sind Flughafen-Betreiber, Städte und die Deutsche Bahn, aber auch Supermärkte und Hotels. Bei Letzteren stehe häufig der Service-Gedanke im Vordergrund, beobachtet Möhrlein.

Ein unverschlüsseltes WLAN ohne Zugangscodes erscheine gerne als die einfachere und bequemere Lösung, bestätigt Christian Reinfurt, Geschäftsführer des zur Deutschen Telekom gehörenden IT-Spezialisten Goingsoft. „Oft herrscht auch die Meinung vor, dass das vermeintlich umständliche Eingeben von WLAN-Schlüsseln und Passwörtern den Gästen nicht zugemutet werden könne.“

Das von 21 europäischen Ländern praktizierte Klassifizierungssystem Hotelstars Union belohnt einen Regenschirm auf dem Zimmer oder an der Rezeption mit drei Punkten bei der Sterne-Vergabe. Ab drei Sternen gehört er sogar zum Mindeststandard. Ein Türspion bringt ebenfalls drei Punkte und eine zusätzliche Schließvorrichtung an der Zimmertür sogar fünf. Verschlüsseltes WLAN dagegen findet im aktuellen, von 2025 bis 2030 geltenden Katalog mit 239 Qualitätskriterien keine Erwähnung.

Die Frage nach den praktizierten Sicherheitsvorkehrungen beantworten Verbände und Betreiber ausweichend. Selbst dort, wo – wie bei Motel One – nach einem Hacker-Angriff 2023 die Standards überarbeitet wurden. „Wir setzen umfassende und fortlaufende Maßnahmen ein, um sicherzustellen, dass persönliche Informationen vertraulich behandelt und vor unbefugtem Zugriff geschützt werden“, teilt eine Sprecherin mit. „Mit unseren langjährigen Partnern arbeiten wir stets an Optimierungsprozessen und führen regelmäßige Sicherheitsüberprüfungen unserer Systeme durch.“ Auf Nachfrage, was darunter zu verstehen sei, schreibt sie zurück: „Ich kann Ihr Interesse an dem Thema verstehen, aber ich bitte um Ihr Verständnis dass wir hierzu keine weiteren Auskünfte geben.“

Dabei könnte die Kette, deren Gäste um Adress- und Rechnungsdaten beraubt wurden und zum Teil sogar ihre Kreditkarten-Informationen im Darknet wiederfanden, doch mit ein paar Details für sich werben, findet auch Constantin Cremerius, Verkaufsmanager bei m3connect. Der Provider für drahtlose Internetdienste ist „Preferred Partner“ des Hotelverbands Deutschland und hat auch bei Motel One Hand angelegt. Neben einem WLAN-Zugang ohne Authentifizierung gibt es dort die Möglichkeit, eine verschlüsselte Verbindung anzulegen. Dazu sind die Eingabe einer E-Mail-Adresse und eines Passworts nötig. „Ein modernes WLAN mit hohem Sicherheitsstandard trägt nicht nur zur Zufriedenheit der Gäste bei, sondern stärkt auch das Vertrauen in das Haus und dessen Marke“, betont Cremerius. „Die Qualität eines Hauses wird definitiv auch durch die digitale Infrastruktur mitbestimmt.“ Weit herumgesprochen hat sich das anscheinend noch nicht. In der Regel wird hervorgehoben, dass der Internetzugang kostenfrei ist. Im Münchner Fünfsternehaus Sofitel Bayerpost wird im Room directory um die Eingabe der E-Mail-Adresse „zur Sicherheit“ gebeten. Ohne weitere Erklärung. „Tatsächlich ist es so, dass bei Gästebewertungen das Thema sicheres/verschlüsseltes Internet so gut wie nicht von unseren Gästen thematisiert wird“, teilt eine Sprecherin der Accor-Gruppe mit, zu der Sofitel gehört.

„Das ist verständlich, denn die meisten Menschen erwarten, dass die angebotenen Netzwerke sicher sind“, meint Cremerius. „Aus diesem Grund ist es wichtig, sowohl Gäste als auch Hoteliers für das Thema zu sensibilisieren. Es geht nicht darum, Ängste zu schüren, sondern um ein Bewusstsein dafür, wie die Sicherheit verbessert werden kann.“

Die aber hat einen Preis, den Hoteliers scheuen. „Investitionen in eine moderne und sichere WLAN-Infrastruktur werden oft aufgeschoben“, erlebt Christian Reinfurt immer wieder. Im Vergleich zu anderen Investitionen werde der „Mehrwert hier nicht direkt sichtbar und ist deswegen auch schwerer greifbar oder bezifferbar“.

Selbst eine Client Isolation, wie sie die Deutsche Bahn in Zügen und auf Bahnhöfen nutzt, damit die Geräte verschiedener Nutzer nicht untereinander kommunizieren können, ist in Hotels schwierig umzusetzen. „Die Komplexität ist, Client Isolation zwischen den Nutzern herzustellen, aber nicht beispielsweise zum SmartTV“, erklärt Achim Möhrlein. Der Gast wolle ja womöglich sein Laptop mit dem Fernseher verbinden. „Damit stellt sich wieder die Frage nach den Kosten: Man muss auswählen, was ist erlaubt, was nicht, dazu muss man viel Technologie, Know-how und Konfiguration in das WLAN-Netz investieren.“

Ein Gast kann nicht überprüfen, ob ein Hotel über Client Isolation verfügt. Und das Personal an der Rezeption ist auf Fragen danach nicht vorbereitet und entsprechend überfordert, wie Stichproben zeigten. Nach einigem Zögern teilt eine Sprecherin der H-Hotels mit, „dass in nahezu allen unserer über 60 H-Hotels Client Isolation als Sicherheitsfeature vorhanden ist“. Nahezu? „Die Verbindung ist unverschlüsselt und der Traffic ins Internet offen. Wir arbeiten jedoch mit Client Isolation, damit die Gäste sich untereinander nicht sehen oder sich verbinden könnten“, klärt eine Sprecherin von 25hours nach schriftlicher Anfrage auf. Ihre Kollegin von Ruby Hotels bestätigt „Maßnahmen wie Client Isolation sowie zusätzliche Sicherheitsvorkehrungen auf Switch- und Firewall-Ebene“.

Gerald Scheurmann-Kettner geht das Thema entschieden an. „Es gibt Dinge, über die kann man diskutieren. Nicht über Sicherheit“, sagt der für die IT verantwortliche Chief Information Officer von Event Hotels. Die Hotel-Management-Plattform betreibt in Europa fast 60 Häuser überwiegend unter den Marken Mercure, Ibis und Pullman – und investiert laut Scheurmann-Kettner viel Geld in verschlüsseltes Internet. Schon aus eigenem Interesse. „Sollten einzelne Gäste über das Hotel-WLAN etwas Unbefugtes tun, hat das Haus eine Auskunftspflicht.“ Dass alle anderen von der Wachsamkeit profitieren, koste sie keinen Cent extra. „Ich kann nicht verkaufen, dass meine Hotels sicherer sind als andere. Die Leute beanspruchen, sicher über die Straße zu laufen, aber nicht, sicher im Netz unterwegs zu sein.“ Als „typisch deutsches Paradoxon“ bezeichnet Scheurmann-Kettner, dass dort jeder und jede inzwischen Privates und Geschäftliches teile, „aber allergisch reagiert, wenn der Staat Daten abgreifen will, was der Sicherheit dienen würde“.

Dass selbst Geschäftsreisende, die es besser wissen sollten, oft ein leichtes Angriffsziel sind, illustriert eine aktuelle Umfrage im Auftrag des Deutschen Reiseverbandes. Lediglich 38 Prozent der befragten Unternehmen verbieten ihren Mitarbeitenden demnach die Nutzung privater Geräte für dienstliche Zwecke. Nur 41 Prozent schreiben ihnen vor, ein sogenanntes Virtual Private Network (VPN) zu nutzen.

Der über ein ungeschütztes öffentliches Internet laufende Netzwerkverkehr wird dabei innerhalb eines eigenen VPN-Servers verschlüsselt. Zudem verschleiern VPN-Server den tatsächlichen Standort sowie die Onlineidentität gegenüber Dritten. „Da brauchen wir uns aber nichts vormachen“, sagt Möhrlein. „Wer keinen VPN-Client von seinem Arbeitgeber zur Verfügung gestellt bekommt, der hat ihn privat eher selten installiert.“ Das gilt auch für die Instagramer vor der Pariser Skyline.

KARIN FINKENZELLER