Hotel Hijackers

Großangelegter Datendiebstahl in der Hotelbranche

Wenn ein Cyberkrimineller darüber nachdenkt, ein Hotel anzugreifen, dann interessiert ihn vor allem sein möglicher Gewinn.

Hotels haben Millionen von Zimmern, die von Millionen von Kunden genutzt werden, was Millionen von Euro, Dollar etc. einbringt.

Ein weiterer Bonus, der für die Cyberkriminellen noch hinzukommt: Ein Großteil der Geschäfte läuft über

Kreditkarten

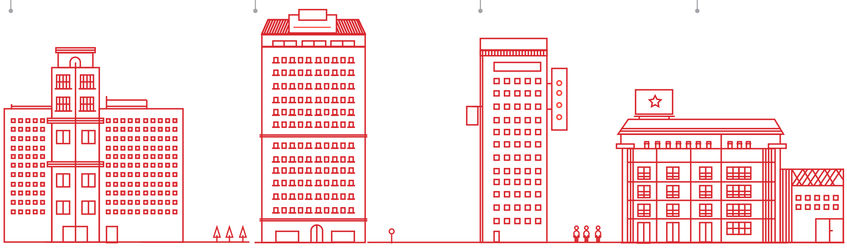
Die Fakten sprechen für sich

24 Hotels betroffen

Tausende von Kreditkarten gefährdet

Dutzende infizierter Computer und POS-Terminals

105 Hotels betroffen



White Lodging

Mindestens 24 Hotels waren in den Jahren 2013 und 2015 Opfer von Cyberattacken. Bei diesen Angriffen wurden die Kredit- und Kundenkarten der Gäste gestolen.

Mandarin Oriental

Im März 2015 infizierte Malware POS-Terminals und stahl gezielt Kreditkarteninformationen der Hotelkunden.

Trump Hotels

Von Mai 2014 bis Juni 2015 waren Computer und POS-Terminals in den Restaurants und Geschenkeläden der Hotels infiziert.

Starwood

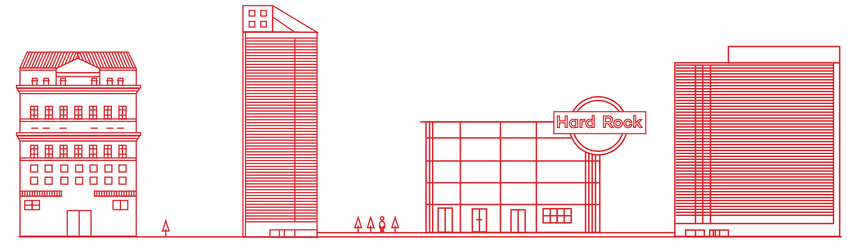
Im November 2015 wurden 105 Starwood-Hotels Opfer von Malware, die ihre POS-Terminals infizierte.

250 Hotels betroffen

Zugriff auf vertrauliche Informationen

Daten von 173.000 Kreditkarten gestohlen

1,5 Jahre infiziert, ohne es zu bemerken



Hyatt Hotels

Zwischen August und Dezember 2015 infizierte Malware POS-Terminals in 250 Hyatt-Hotels weltweit. Dies ist die bisher größte Cyberattacke in der Hotelgeschichte.

Hilton Worldwide

Im November 2015 bestätigte das Unternehmen, Opfer von Cyberattacken geworden zu sein. Kreditkarteninformationen wurden gestohlen, PIN-Codes blieben dem Vernehmen nach verschont.

Hard Rock Las Vegas

Vom 13. September 2014 bis zum 2. April 2015 griffen Hacker auf insgesamt 173.000 Kreditkartendaten zu, die in den Restaurants, Bars und Shops des Hard Rock Las Vegas genutzt wurden.

Rosen Hotels & Resorts

Das jüngste Opfer sind die Rosen Hotels & Resorts. Ihre POS-Terminals waren von September 2014 bis Februar 2016 mit Malware infiziert, ohne dass dies bemerkt wurde.

Die Hotelbranche ist zu einem der **Hauptziele für Cyberkriminelle** geworden.

Lassen Sie sich von uns schützen

Adaptive Defense 360 ist ein neu entwickeltes IT-Schutzsystem auf höchstem technischem Niveau, das erstmals Endpoint Protection (EPP) und Endpoint Detection and Response (EDR)-Fähigkeiten kombiniert.

Adaptive Defense 360 klassifiziert alle laufenden Prozesse auf den Endpoints und schützt so sowohl vor bekannter Malware als auch vor unbekannten Bedrohungen, wie Zero-Day-Attacken, APTs (Advanced Persistent Threats) und direkten Angriffen.

Adaptive Defense 360