Break-Out-Session | 16:00 Uhr

Cyberangriffe auf Finanzabteilungen – Erfahrungen aus der Praxis

Litreca® Aktiengesellschaft | A member of enventa GROUP

- In den letzten Jahren haben sich Cyberangriffe zu einer der größten Bedrohungen für Unternehmen entwickelt.

- Rund die Hälfte aller deutschen Unternehmen wurde letztes Jahr Ziel von Cyberattacken, wie eine Umfrage von Statista ergab.

- Gerade im Treasury Management, wo Unternehmen ihre Finanzströme und Liquidität managen, können Cyberangriffe schwerwiegende Folgen haben.

- Ein erfolgreicher Angriff kann zum Beispiel dazu führen, dass Gelder abgezweigt oder Zahlungen manipuliert werden.

Was ist Ransomware?

Das englische Wort Ransom steht für Lösegeld und beschreibt die Absicht dieser Malware treffend: Ransomware sind verschiedene **Computerviren, die einzelne Dateien auf Ihrem Rechner verschlüsseln oder sogleich das gesamte Gerät sperren**.

Um wieder Zugriff auf Ihre Dateien zu erhalten, werden Sie zu einer **Lösegeldzahlung** aufgefordert. Betroffen von solchen Angriffen sind nicht nur Unternehmen, sondern auch Privatpersonen.

Zahlen & Fakten

21.818 €

kostet deutschen Unternehmen ein Cyberangriff im Durchschnitt.

(Quelle: Statista Research Department, 2022)

45 %

aller Vorstände sehen Cyberangriffe als das Top-Risiko für Ihren Konzern an.

(Quelle: KPMG AG 2019, „Cybersecurity ist Chefsache“)

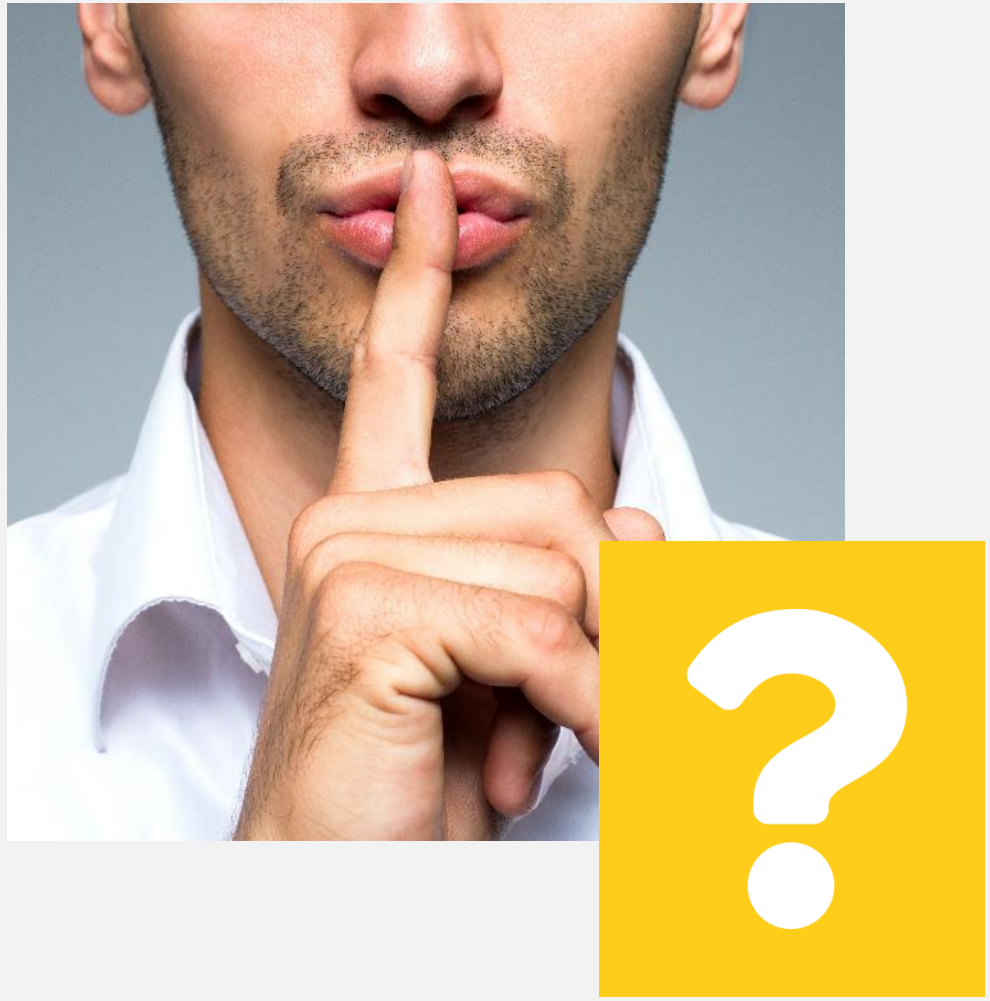
9 von 10

Unternehmen waren im Jahr 2021 von Cyberangriffen betroffen. In den Jahren davor waren es 75 %.

(Quelle: Bitkom Research, 2021)

- **34.000 Mails** mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen
- **15 Millionen** Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber
- **20.174 Schwachstellen** in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem Zuwachs von 10% gegenüber dem Vorjahr
- **69%** aller Spam Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.
- **90%** war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken der Sparkassen geschickt worden zu sein
- **78.000** neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

* Zahlen des BSI (Bundesamt für Sicherheit in der Informationstechnik)



Schweigen ist Gold?

Vor zwei oder drei Jahren haben Unternehmen einen erfolgreichen Cyberangriff nach Möglichkeit in der Öffentlichkeit noch schamhaft verschwiegen.

Inzwischen haben die Bedrohung und die Zahl der Angriffe massiv zugenommen.

Eines ist heute sicher, kein Unternehmen ist zu klein oder zu unbedeutend, um nicht von Cyberkriminellen angegriffen zu werden.

Jan Heimbeck

Director of Finance

H-Hotels GmbH

WILLKOMMEN BEI H-HOTELS.COM!

Welcome to H-Hotels.com!

Die H-Hotels GmbH blickt auf mehr als 50 Jahre Erfahrung als Gastgeber zurück und zählt mittlerweile zu den größten privat geführten Hotelgesellschaften in Deutschland. Seither setzt das Unternehmen auf frische Impulse und neue Akzente – und das immer unter Berücksichtigung der aktuellen Entwicklungen des Hotelmarktes. Um den individuellen und vielseitigen Ansprüchen ihrer Gäste gerecht zu werden, baut die H-Hotels Gruppe ihr eigens entwickeltes Markenportfolio kontinuierlich aus und steht mit innovativen, flexiblen Betriebskonzepten für nachhaltiges Wachstum.

The H-Hotels Group has a proud history as a host dating back more than 50 years and is one of the biggest privately managed hotel companies in Germany. As a hotel operator and a company also involved in redevelopment, it is consistently bringing fresh ideas to the German-speaking hotel market. With its own brand portfolio, the H-Hotels Group offers its guests the entire range of hotel experiences and is committed to sustainable growth with innovative and flexible operating concepts.

H-Hotels.com

PORTFOLIO

- HYPERION
- H4Hotels
- H2Hotels
- H+Hotels
- H.omes
- H.ostels

Maßnahmen von Litreca

- Neues Konzept mit einer cloudbasierten Lösung nach 3 Tagen beauftragt – alles aus einer Hand deshalb keine Abhängigkeit
- Es musste kein sonstiges Multibank System angebunden werden, sondern durch die direkte Anbindung des Zahlungsverkehrs schnell wieder handlungsfähig.
- System ist runtergefahren und Banken informiert, EBICS Zugänge sicherheitshalber gesperrt.
- Litreca begann mit der Umsetzung innerhalb von weiteren 3 Tagen. 10 Tage nach dem Angriff wurden bereits die ersten Banken und Cashpools wieder initialisiert und das Unternehmen war im Rahmen der „normalen Organisation“ handlungsfähig.
- Das Treasury wurde mit äußerster Priorität behandelt. Das ganze Team innerhalb von Tagen mit Macs ausgestattet damit schnell wieder online
- Rechenzentrum ist in Deutschland und voll zertifiziert. Jeder Kunde hat eine dedizierte Umgebung. Datenbank ist state of the art und wird vom Hersteller gewartet und betrieben.

Empfohlene Präventionen

- Ermitteln Sie den Status Quo und erfüllen Sie gleichzeitig Ihre Dokumentationspflichten nach dem IT-Grundschutz.
- Legen Sie klare Regeln für Ihre Kollegen fest, wie mit Downloads und geschäftlichen Informationen umzugehen ist
- Ermitteln Sie den Risikostatus Ihres Betriebs – und identifizieren Sie sofort, mit welchen Maßnahmen Sie Gefährdungen minimieren können.
- Ihre Kollegen sind Ihre „Human Firewall“ – Holen Sie sie mit ansprechenden Präsentationen
- Datensicherung sollte nach dem Angriff zur Verfügung stehen, am besten außer Haus – einmal die Woche wegspeichern, dann entsteht kein Verlust der Historie

HABEN SIE FRAGEN?

Vielen Dank für Ihre Aufmerksamkeit

Bleiben Sie bestens informiert und folgen Sie uns auf LinkedIn.