HISCOX IDD-DAYS '25

Cyber-Alarm:

Trends, aktuelle Bedrohungen und Praxisfälle

10. April 2025

Ihre Referenten

Gisa Kimmerle

Product Head Cyber

Unser Gast: Frank Rustemeyer

COO HiSolutions

Die wichtigsten Erkenntnisse aus dem CRR 2024

Die Cyber-Risikolage hat sich abermals verschärft

HISCOX

60% der deutschen Unternehmen wurden 2024 **häufiger als im Vorjahr angegriffen**

Zum Vergleich: 2023 sagten **58%, dass sie häufiger als 2022 attackiert** wurden

Im Durchschnitt wurden deutsche Unternehmen binnen 12 Monaten **49-mal von Cyber-Kriminellen attackiert** (erfolgreiche und abgewehrte Angriffe zusammengerechnet)

Wie gingen die Cyber-Kriminellen vor?

Top 3 der häufigsten „first points of entry“ bei erfolgreichen Cyber-Angriffen (Mehrfachnennungen möglich):

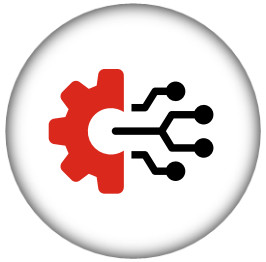
1	**55%**	Über den **Unternehmensserver in der Cloud** (z.B. durch Schwachstellen beim Webserver oder Kompromittierung von Zugangsdaten)
2	**47%**	Über **Mitarbeitende** (z.B. durch Phishing / Social Engineering / Spoofing)
3	**46%**	Über **Kompromittierung von Geschäfts-E-Mails** (z. B. durch Hacking von Zugangsdaten oder Servern)

Welche Arten von Cyber-Attacken sind auf dem Vormarsch?

55%

Zahlungsumleitungsbetrug (oft durch missbräuchliche Verwendung der Unternehmens- oder einer fremden E-Mail, um Gelder auf ein Konto der Angreifer umzuleiten)

47%



Distributed Denial of Service (DDoS)-Angriff (d. h. der Angreifer macht das Netzwerk durch Unterbrechung der Dienste für die vorgesehenen Nutzer unzugänglich)

46%

Missbrauch von IT-Ressourcen (d. h. Nutzung der Infrastruktur für die Erstellung eines Botnetzes oder den Beitritt zu einem Botnetz, das Hosten von Malware, das Mining von Kryptowährungen)

Wie schätzen deutsche Unternehmen das Cyber-Risko ein?

79% geben an, Cyber-Resilienz sei **ein wichtiges bzw. sehr wichtiges übergreifendes Unternehmensziel**

70% sagen, sie haben für **starke Cyber-Abwehr-mechanismen** im Unternehmen gesorgt, z.B.:

- 76% haben eine Person bzw. ein Team, die explizit für Cyber-Sicherheitsthemen zuständig sind
- 45% geben 6-10% ihres gesamten IT-Budgets für Cyber-Sicherheit aus, 44% sogar über 11%

Auswirkungen von Cyber-Attacken

Betriebsunterbrechungen

Wie lange dauerte es, bis die angegriffenen Unternehmen den Normalbetrieb wiederherstellen konnten (z. B. alle manuellen Umgehungslösungen entfernen und alle Dienste wiederhergestellt/neu aufgebaut)?

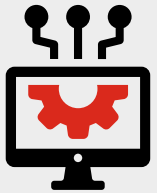
- 7%: bis zu einer Woche
- **27%: 1-2 Wochen**
- **26%: 2-4 Wochen**
- **30%: 1-3 Monate**
- 7%: mehr als 3 Monate

Was waren die häufigsten Auswirkungen von Cyber-Attacken auf die Unternehmen?

63%: Signifikante Kosten, die spürbare finanzielle Auswirkungen auf das Unternehmen hatten

50%: Schwierigkeiten bei der Gewinnung neuer Kunden

46%: Es gingen Kunden verloren



Auswirkungen von Cyber-Attacken

HISCOX

Was passierte nach der Zahlung von Lösegeld?

42%: Obwohl wir den Wiederherstellungsschlüssel erhalten haben, **mussten wir die IT-Systeme neu aufbauen**

34%: Wir konnten **nur einen Teil unserer Daten** wiederherstellen

27%: Unsere **Daten wurden trotzdem geleakt**

22%: Der **Wiederherstellungsschlüssel funktionierte nicht**

22%: Die Hacker **forderten mehr Geld**

16%: Wir konnten **alle unserer Daten wiederherstellen**

Cyber-Resilienz

Top 3 Gründe, warum Unternehmen in die Verbesserung ihrer Cyber-Resilienz investiert haben

1	Um Betriebsunterbrechungen zu vermeiden	**46%**
2	Um regulatorische Vorschriften zu erfüllen	**44%**
3	Weil wir unseren Business-Partnern zeigen wollen, dass wir Cyber-Sicherheit ernst nehmen	**36%**

Die 3 größten Hindernisse, die einer höheren Cyber-Resilienz entgegenstehen

1	Sich rapide ändernde Cyber-Bedrohungen	**43%**
2	Zu limitierte Budgets für Cyber-Sicherheit	**42%**
3	Zu wenig Verständnis/Aufmerksamkeit für Cyber-Risken bei Mitarbeitenden	**38%**

Stichwort Digital Trust: Man möchte nicht nur sicherstellen, dass das eigene Unternehmen geschützt ist, sondern dass man auch seinen Partnern gegenüber verlässlich in puncto Cyber ist!

Welche “Cyber Readiness” haben Unternehmen in Deutschland?

HISCOX

8%: Minimal – Grundlegendes Bewusstsein für Cyber-Resilienz, mit minimalen formalen Prozessen und Ad-hoc-Reaktionen auf Cyber-Vorfälle.

28%: Ad hoc – Einige formale Prozesse sind vorhanden, aber die Umsetzung ist uneinheitlich und oft reaktiv. Nur wenige Schulungs- und Sensibilisierungsprogramme

33%: Basis – Festgelegte und dokumentierte Prozesse mit regelmäßigen Überprüfungen und Aktualisierungen. Mittleres Niveau der Mitarbeiterschulung und -sensibilisierung. Reaktionspläne auf Vorfälle werden regelmäßig getestet.

26%: Fortgeschritten – Integrierte Prozesse in der gesamten Organisation, mit Metriken zur Nachverfolgung. Verfahren zur kontinuierlichen Verbesserung sind vorhanden. Hohes Maß an Mitarbeiterschulung und proaktiver Incident Response

4%: Vorbildlich – Best-in-Class-Praktiken, die vollständig in die Geschäftsstrategie integriert sind. Kontinuierliche Innovation und Verbesserung der Cyber-Resilienz. Starke Zusammenarbeit mit externen Partnern und Stakeholdern.

HISCOX

CYBER-Fälle
aus der PRAXIS

PRAXISFÄLLE
Fall 1: Zahlungsumleitungsbetrug

- Start-Up im Gesundheitsbereich, < 50 Mitarbeiter
- Unbefugter Zugriff aus dem Ausland auf die M365-Postfächer von Geschäftsführungsmitgliedern, vermutlich durch Nutzung der MFA-Lösung in unsicheren Umgebungen
- Heimliche Einrichtung von Weiterleitungsregeln
- Abfangen und Manipulieren mehrerer Rechnungsdokumente unter Nutzung von Tippfehler-Domains
- In der Folge Zahlung auf falsche Konten von über 300 Tsd. EUR

Schadenhandling

- Aufklärung des Angriffswegs und Schließen von Lücken
- Absicherung der MFA-Konfiguration
- Identifizierung potenziell betroffener Geschäftspartner

PRAXISFÄLLE
Fall 2: Angriff auf Cloud-Infrastruktur

- Anbieter eines Online-Angebots, das Kunden in ihre Webseiten einbinden
- Erfolgreicher Einbruch durch einen White-Hat-Hacker in eine Kunden-Webseite
- Darüber Rückgriff auf Systeme des Dienstleisters mit Datenbeständen mehrerer weiterer Kunden
- Umfang der Zugriffsmöglichkeiten und der Betroffenheit unklar
- In der Folge Gesamtkosten von rd. 28 Tsd. EUR

Schadenhandling

- Ermittlung des Angriffswegs
- Prüfen eines möglichen Datenabflusses
- Absichern der bestehenden Umgebungen

HISCOX

IHRE fragen

Hiscox Deutschland wird 30!

HISCOX

Zum Jubiläum verlosen wir tolle Preise!

3 Jahrzehnte – 3 Gewinne

QR-Code scannen, Newsletter abonnieren und im Lostopf landen:

Mit dem Hiscox Newsletter beraten Sie Ihre Kunden stets aktuell informiert.

Sichern Sie sich 1 von 3 eventim-Gutscheinen im Wert von je 150 Euro! Verlost wird unter allen Newsletter-Neuanmeldungen bis 01. Juni 2025.

HISCOX

Vielen Dank!