SOPHOS

RANSOMWARE-REPORT 2025: DEUTSCHLAND

Ergebnisse einer unabhängigen Befragung von 300 deutschen Unternehmen*, die im vergangenen Jahr von Ransomware betroffen waren.

* Zur besseren Lesbarkeit wird im Report einheitlich von „Unternehmen" gesprochen. Gemeint sind damit alle Arten von Organisationen, einschließlich öffentlicher Einrichtungen, Non-Profit-Organisationen und anderer nicht unternehmerischer Strukturen.

SOPHOS-WHITEPAPER – JUNI 2025

Über den Report

Der Report basiert auf den Ergebnissen einer unabhängigen Befragung von 3.400 IT-/Cybersecurity-Entscheidern, deren Unternehmen im letzten Jahr von Ransomware betroffen waren, darunter 300 aus Deutschland.

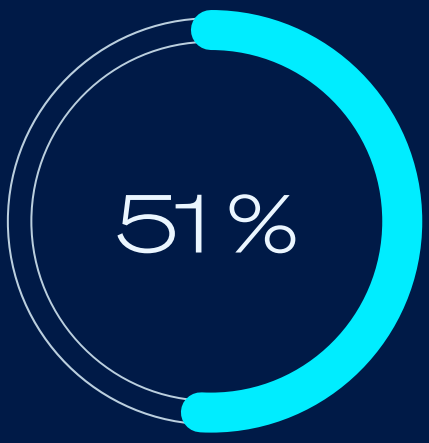
Die Befragung wurden von Sophos in Auftrag gegeben und von einem spezialisierten Drittanbieter von Januar bis März 2025 durchgeführt.

Die Befragten arbeiten alle in Unternehmen mit 100 bis 5.000 Mitarbeitenden und wurden gebeten, die Fragen basierend auf ihren Erfahrungen der letzten 12 Monate zu beantworten.

Der Report beinhaltet Vergleiche mit Ergebnissen aus unserer Befragung von 2024. Alle Finanzdaten sind in US-Dollar angegeben.

Erfahrungen von 300

IT-/Cybersecurity-Entscheidern aus Deutschland, deren Unternehmen im vergangenen Jahr von Ransomware betroffen waren



Prozentsatz der Angriffe, die zu einer Verschlüsselung von Daten führten

Durchschnittliche Lösegeldzahlung in Deutschland im vergangenen Jahr

Durchschnittliche Wiederherstellungskosten nach einem Ransomware-Angriff

Gründe, warum deutsche Unternehmen Opfer von Ransomware werden

- **Ausgenutzte Schwachstellen waren die häufigste technische Ursache von Angriffen**. Sie wurden in 42 % der Fälle zum Einfallstor. Danach folgten kompromittierte Zugangsdaten. Sie wurden in 20 % der Fälle als Auslöser identifiziert. Schädliche E-Mails kamen in 19 % der Angriffe zum Einsatz.
- **Zu wenig Personal/Kapazitäten waren die häufigste betriebliche Ursache** und wurden von 47 % der deutschen Befragten genannt. 45 % nannten sowohl bekannte als auch unbekannte Sicherheitslücken als mit verantwortlich dafür, dass ihr Unternehmen Opfer von Ransomware wurde.

Auswirkungen auf Daten

- **51 % der Angriffe führten zu einer Verschlüsselung von Daten.** Dieser Wert entspricht dem weltweiten Durchschnitt von 50 %, ist jedoch ein deutlicher Rückgang gegenüber den von deutschen Befragten gemeldeten 79 % im Report 2024.
- **In 24 % der Angriffe mit einer Datenverschlüsselung** wurden auch Daten gestohlen – ein Rückgang gegenüber den im letzten Jahr gemeldeten 30 %.
- **95 % der deutschen Unternehmen, deren Daten verschlüsselt wurden, konnten sie wiederherstellen**. Dieser Wert liegt knapp unter dem weltweiten Durchschnitt.
- **63 % der deutschen Unternehmen zahlten Lösegeld und erhielten Daten zurück** – ein deutlicher Anstieg gegenüber dem Vorjahr, als der Anteil noch bei 42 % lag.
- **59 % der deutschen Unternehmen stellten verschlüsselte Daten mithilfe von Backups wieder her** – ein deutlicher Rückgang gegenüber den im Vorjahr gemeldeten 75 %.

Lösegeldforderungen und -zahlungen

- Die **durchschnittliche Lösegeldforderung in Deutschland betrug im letzten Jahr 600.000 US$**, ein Rückgang von 86 % gegenüber den 2024 gemeldeten 4,4 Mio. US$.

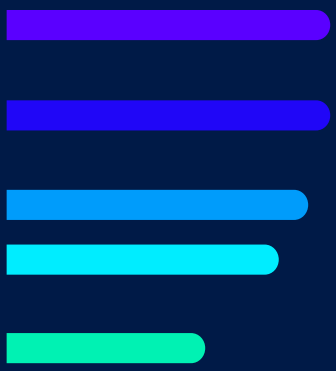
Durchschnittliche Lösegeldforderung in Deutschland im vergangenen Jahr

- 49 % der **Lösegeldforderungen beliefen sich auf mindestens 1 Mio. US$**, ein Rückgang gegenüber den 62% von 2024.
- Deutsche Unternehmen zahlten im letzten Jahr **durchschnittlich 411.600 US$ Lösegeld** – 93 % weniger als die im Vorjahr gemeldeten 5,5 Mio. US$.
- **Deutsche Unternehmen zahlten in der Regel** 86 % des geforderten Lösegelds, was dem weltweiten Durchschnitt von 85 % entspricht.
  - 47 % **zahlten WENIGER als ursprünglich gefordert** (weltweiter Durchschnitt: 53 %)
  - 32 % **zahlten GENAU die ursprüngliche Forderung** (weltweiter Durchschnitt: 29 %)
  - 20 % **zahlten MEHR als ursprünglich gefordert** (weltweiter Durchschnitt: 18 %)

Geschäftliche Folgen von Ransomware

- Ohne Berücksichtigung von Lösegeldzahlungen **meldeten deutsche Unternehmen nach einem Ransomware-Angriff durchschnittliche Wiederherstellungskosten von 1,56 Mio. US$** – ein deutlicher Rückgang gegenüber den von deutschen Befragten 2024 gemeldeten 2,2 Mio. US$. Dazu zählen Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangene Geschäftschancen etc.
- **Deutsche Unternehmen sind schneller geworden bei der Wiederherstellung nach einem Ransomware-Angriff**. 64 % gelang es, die Angriffsfolgen in bis zu einer Woche zu beseitigen, im Vergleich zu nur 24 % im Vorjahr. Nur 9 % benötigten zwischen einem und sechs Monaten für die Wiederherstellung, was ein deutlicher Rückgang gegenüber den 34 % vom Vorjahr ist.

Auswirkungen von Ransomware auf Mitarbeitende in IT-/Cybersicherheits-Teams von Unternehmen, in denen Daten verschlüsselt wurden



44 % berichten von **mehr Stress oder Angst** vor künftigen Angriffen.

44 % berichten von **Fehlzeiten bei Mitarbeitenden** wegen Stress/psyschischen Problemen.

41 % berichten von **mehr Druck** aus der Führungsetage.

37 % berichten von **Schuldgefühlen**, weil der Angriff nicht gestoppt wurde.

27 % berichten, dass **die Teamführung ausgetauscht wurde**.

Empfehlungen

Ransomware bleibt eine der größten Bedrohungen für deutsche Unternehmen. Da Angreifer ihre Angriffsmethoden ständig weiterentwickeln, muss die Cyberabwehr der Unternehmen damit Schritt halten. Die Erkenntnisse aus diesem Report zeigen, auf welche Bereiche sich Unternehmen beim Schutz vor Ransomware künftig konzentrieren sollten.

- **Prävention.** Die beste Abwehr eines Ransomware-Angriffs ist es, wenn die Angreifer sich keinen Zugang zu Ihrem Unternehmen verschaffen konnten. Ihr Ziel sollte es sein, sowohl die technischen als auch die betrieblichen Ursachen von Angriffen zu reduzieren, auf die in diesem Report eingegangen wurde.
- **Schutz.** Ein starkes Sicherheits-Fundament ist ein Muss. Endpoints (einschließlich Server) sind das Hauptziel von Ransomware-Akteuren. Stellen Sie daher sicher, dass diese ausreichend geschützt sind, u. a. mit speziellem Anti-Ransomware-Schutz, um bösartige Verschlüsselungen zu stoppen und rückgängig zu machen.
- **Erkennung und Reaktion.** Je schneller Sie einen Angriff stoppen, desto besser. Ein wesentlicher Teil Ihrer Verteidigung ist das Erkennen von Angriffen und eine schnelle Reaktion – und zwar rund um die Uhr. Wenn Ihnen intern Ressourcen oder Expertise fehlen, können Sie mit einem zuverlässigen Anbieter für Managed Detection and Response (MDR) zusammenarbeiten.
- **Planung und Vorbereitung.** Mit einem gut durchdachten Incident-Response-Plan, d. h. einem Plan für die Reaktion auf Vorfälle, reduzieren Sie erheblich die Auswirkungen eines schwerwiegenden Vorfalls. Erstellen Sie hochwertige Backups und üben Sie deren Wiederherstellung regelmäßig.

SOPHOS

Sie möchten mehr darüber erfahren, wie Sophos Sie bei der Optimierung Ihrer Ransomware-Abwehr unterstützen kann? Sprechen Sie mit einem unserer Ansprechpartner oder besuchen Sie **www.sophos.de**

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen und Organisationen aller Größen und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Unsere Lösungen nutzen modernste Next-Gen-Funktionen mit Machine Learning und künstlicher Intelligenz und sorgen für einen effektiven Schutz von Unternehmensdaten.

2025-07-10 DE-WP (DD)