SOPHOS

RANSOMWARE-REPORT DEUTSCHLAND 2026

Ergebnisse einer unabhängigen Befragung von 139 deutschen Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren.

SOPHOS-WHITEPAPER – JULI 2026

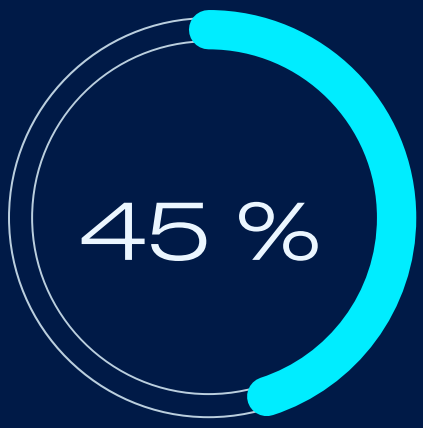
Über den Report

Der State of Ransomware Report, der nun im siebten Jahr erscheint, basiert auf den Ergebnissen einer unabhängigen Studie, die von Sophos in Auftrag gegeben wurde. Der diesjährige globale Report beruht auf den Erfahrungen von 2.158 IT- und Cybersecurity-Führungskräften, deren Unternehmen im vergangenen Jahr von Ransomware betroffen waren, darunter 139 aus Deutschland.

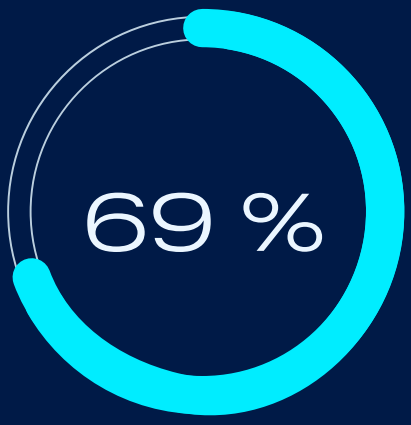
Die Umfrage wurde zwischen Januar und März 2026 durchgeführt. Die Befragten arbeiten alle in Unternehmen mit 100 bis 5.000 Mitarbeitenden und wurden gebeten, die Fragen basierend auf ihren Erfahrungen der letzten 12 Monate zu beantworten. Alle Finanzdaten sind in US-Dollar angegeben. Ausreißerwerte bei den Lösegeldforderungen ab 40 Mio. US$ wurden aus diesen Daten entfernt.

Erfahrungen von 139

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



Prozentsatz der Angriffe, die zur Verschlüsselung von Daten führten.



Bestätigten, dass der Ransomware-Vorfall des vergangenen Jahres ihr bedeutendster Identitätsangriff war.

Durchschnittliche Wiederherstellungskosten nach einem Ransomware-Angriff

Gründe, warum deutsche Unternehmen Opfer von Ransomware werden

- **Phishing war die häufigste technische Angriffsursache** und wurde bei 30 % der Angriffe eingesetzt, gefolgt von kompromittierten Anmeldedaten (24 %) und Schad-E-Mails (20 %). Die ausgenutzten Schwachstellen gingen deutlich zurück und sanken im Report von 2025 von 42 % auf 17 %.
- **(NEU) 69 % bestätigten, dass der Ransomware-Vorfall des vergangenen Jahres der bedeutendste Identitätsangriff auf ihr Unternehmen war.**
- **(NEU) Offengelegte Anwendungen und Systeme waren der häufigste Einstiegspunkt für Angriffe (32 %)** bei Ursachen, die nicht mit E-Mails oder Phishing zusammenhängen, gefolgt von Benutzergeräten (31 %) und Firewalls (25 %).
- **Schlechter Schutz (40 %) war die häufigste operative Angriffsursache,** gefolgt von unbekannten Schwachstellen und fehlendem Fachwissen, die mit jeweils 39 % gemeinsam den zweiten Platz belegten.

Auswirkungen auf Daten

- **45 % der Angriffe führten zu einer Verschlüsselung von Daten.** Dies liegt unter dem weltweiten Durchschnitt von 56 % und stellt einen Rückgang gegenüber den 51 % dar, die von deutschen Befragten im Report 2025 gemeldet wurden.
- **Bei 24 % der Angriffe mit Datenverschlüsselung wurden auch Daten gestohlen –** dies entspricht dem im Jahr 2025 gemeldeten Wert von 24 %.
- **97 % der deutschen Unternehmen, deren Daten verschlüsselt wurden, konnten sie wiederherstellen,** was dem weltweiten Durchschnitt entspricht.
- **45 % der deutschen Unternehmen zahlten Lösegeld und erhielten Daten zurück** – ein deutlicher Rückgang gegenüber dem Vorjahr, als der Anteil bei 63 % lag.
- **61 % der deutschen Unternehmen stellten verschlüsselte Daten mithilfe von Backups wieder her** – ein leichter Anstieg gegenüber den 59 % aus dem Report 2025.

Lösegeldforderungen

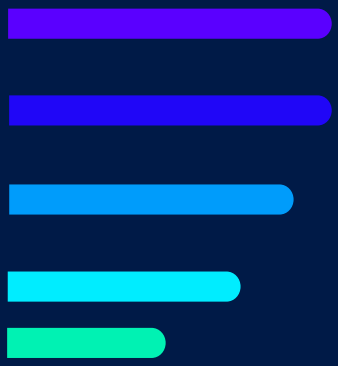
- **Die durchschnittliche Lösegeldforderung in Deutschland lag bei 400.000 USD,** ein Rückgang um 33 % gegenüber den 600.000 USD, die im Report 2025 gemeldet wurden.
- **45 % der Lösegeldforderungen beliefen sich auf 1 Million USD oder mehr,** ein Rückgang gegenüber den 49 %, die im Report 2025 gemeldet wurden.

Durchschnittliche Lösegeldforderung in Deutschland.

Geschäftliche Folgen von Ransomware

- **Ohne Berücksichtigung von Lösegeldzahlungen beliefen sich die durchschnittlichen Wiederherstellungskosten für deutsche Unternehmen nach einem Ransomware-Angriff laut dem diesjährigen Report auf 1,42 Mio. USD,** was ein leichter Rückgang gegenüber dem Durchschnitt von 1,56 Mio. USD ist, der im Report 2025 gemeldet wurde. Dazu zählen Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangene Geschäftschancen etc.
- **60 % der deutschen Unternehmen konnten ihr System innerhalb von bis zu einer Woche nach einem Ransomware-Angriff wiederherstellen,** was ein leichter Rückgang gegenüber den im Report 2025 gemeldeten 64 % ist. 12 % benötigten zwischen einem und sechs Monaten für die Wiederherstellung, ein geringfügiger Anstieg gegenüber den 9 % im Report 2025.

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



45 % berichten von mehr Stress oder Angst vor künftigen Angriffen.

45 % berichten von mehr Schuldgefühlen, weil der Angriff nicht gestoppt wurde.

44 % berichteten von Veränderungen der Prioritäten/ Fokusbereiche im Team.

40 % berichten von mehr Druck aus der Führungsetage.

27 % berichten, dass die Teamführung ausgetauscht wurde.

Empfehlungen

Stärken Sie die Identitätssicherheit zum Schutz vor Ransomware. Fast zwei Drittel der von Ransomware betroffenen Unternehmen in Deutschland bestätigten, dass der Ransomware-Vorfall auch ihr bedeutendster Identitätsangriff war. Unternehmen und Organisationen sollten Identity Threat Detection and Response (ITDR) priorisieren, Multi-Faktor-Authentifizierung über alle Zugangspunkte hinweg durchsetzen und regelmäßig sowohl menschliche als auch nicht-menschliche Zugangsdaten prüfen.

Verstärken Sie den Endpoint-Schutz für innovative KI-Modelle. Frontier AI beschleunigt die Erkennung und Ausnutzung von Schwachstellen. Eine starke Endpoint-Abwehr, die Exploit-basierte Angriffe automatisch stoppt, ist unerlässlich.

Priorisieren Sie E-Mail-Sicherheit. Da Phishing und Schad-E-Mails beinahe die Hälfte der Ursachen für Ransomware in Deutschland ausmachen, sollten Unternehmen und Organisationen moderne E-Mail-Filter einsetzen, DMARC-/DKIM-/SPF-Protokolle implementieren und in regelmäßige Phishing-Awareness-Trainings investieren.

Investieren Sie in Backup- und Wiederherstellungsinfrastrukturen. Unternehmen und Organisationen, die robuste Backup-Systeme unterhalten, konnten verschlüsselte Daten im vergangenen Jahr mit nahezu Rekordraten wiederherstellen. Backups sollten regelmäßig getestet, offline oder in unveränderlichen Formaten gespeichert und in einen dokumentierten Incident-Response-Plan integriert werden, der unter Druck ausgeführt werden kann.

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 **sophos.com/ransomware2026**.

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2026-08-03 DE-WP (TA) CRE-6007