REPORT

Ransomware-Report 2026

Das sagen 2.158 IT- und Cybersicherheitsexperten aus 17 Ländern

SOPHOS

Einleitung

Die Ransomware-Landschaft verändert sich im Zuge der KI rasant. Unternehmen und Organisationen, die kontinuierlich in ihre Cybersecurity-Maßnahmen investieren, erzielen nachweislich bessere Ergebnisse, doch Ransomware-Angriffe verursachen nach wie vor Kosten in Millionenhöhe.

Dies ist die siebte Ausgabe des jährlichen Sophos Ransomware-Reports, der neue Daten zu Ransomware-Angriffen aus dem vergangenen Jahr bietet. Die Ergebnisse sind in folgenden Abschnitten zusammengefasst:

- Angriffs- und Abwehrmethoden
- Datenverschlüsselung und -wiederherstellung
- Lösegeldforderungen und -zahlungen
- Wirtschaftliche Folgen und Auswirkungen auf Mitarbeitende

Die Daten zeugen einerseits von kostspieligen Folgen, lassen andererseits jedoch auch echte Fortschritte erkennen:

- Die Kosten für die Wiederherstellung nach einem Ransomware-Angriff sind hoch; die durchschnittlichen Kosten belaufen sich mittlerweile auf 1,7 Mio. US$
- Bei über der Hälfte der Ransomware-Angriffe (56 %) gelingt es immer noch, Daten zu verschlüsseln, wobei die Rate ab 2025 steigt.
- Lösegeldforderungen und -zahlungen gehen jedoch zurück, und Unternehmen und Organisationen beweisen immer mehr Verhandlungsgeschick. In den letzten zwei Jahren sind die durchschnittlichen Lösegeldforderungen (Medianwert) um 65 % zurückgegangen, und die Zahlungen sind um 62 % gesunken.
- Nach drei Jahren an der Spitze sind ausgenutzte Schwachstellen nicht mehr die Hauptursache für Ransomware-Angriffe (18 %). E-Mail-basierte Angriffe (Phishing 24 % oder Schad-E-Mails 26 %) sind mittlerweile die häufigsten Angriffsvektoren.

2.158

IT- und Cybersicherheitsexperten aus 17 Ländern, deren Unternehmen und Organisationen im vergangenen Jahr von Ransomware betroffen waren, nahmen an einer unabhängigen weltweiten Befragung teil, die als Grundlage für unseren diesjährigen Ransomware-Report diente.

Informationen zu den Ergebnissen

Dieser Report basiert auf den Ergebnissen einer unabhängigen Befragung im Auftrag von Sophos. Im Rahmen der Befragung wurden Fragen zu den Erfahrungen von Unternehmen und Organisationen mit Ransomware-Angriffen und identitätsbasierten Angriffen gestellt, wobei die Lösegeldzahlungsraten, die Wiederherstellungskosten, die Wiederherstellungsdauer und viele weitere Kennzahlen im Jahresvergleich erfasst wurden. Die Antworten wurden von Januar bis März 2026 erhoben und basieren auf den Erfahrungen der Befragten aus den letzten 12 Monaten.

Die Befragten stammen aus 17 Ländern, einer Vielzahl von Branchen aus dem öffentlichen und privaten Sektor sowie aus Unternehmen und Organisationen unterschiedlicher Größe (zwischen 100 und 5.000 Mitarbeitenden), deren Verteilung einer Normalverteilung folgte und über die siebenjährige Laufzeit der Befragung hinweg proportional konstant blieb. Alle Finanzdaten sind in US-Dollar angegeben.

Wichtigste Erkenntnisse auf einen Blick

- **Identitätskompromittierung ist der primäre Ransomware-Bereitstellungsmechanismus**
  - Schad-E-Mails (26 %) und Phishing (24 %) sind die Hauptursachen für Ransomware-Angriffe geworden.
  - Ausgenutzte Schwachstellen — die Hauptursache von Ransomware der letzten drei Jahre – verzeichneten im letzten Jahr einen Rückgang um 14 Prozentpunkte auf 18 %.
  - Zwei Drittel der Ransomware-Opfer (67%) bestätigten, dass ihr Ransomware-Vorfall auch ihr bedeutendster Identitätsangriff war.
- **Schutz-, Sicherheits- und Ressourcenlücken erhöhen das Angriffsrisiko in Unternehmen und Organisationen**
  - Sicherheitslücken (bekannt und unbekannt) waren im zweiten Jahr in Folge mit 62 % die am häufigsten genannte operative Ursache, gefolgt von zu wenig Fachkräften und mangelnder Expertise (58 %) und fehlendem oder minderwertigem Schutz (57 %).
- **Multi-Faktor-Authentifizierung (MFA) allein reicht nicht aus, um Ransomware zu stoppen**
  - MFA war in 97 % der Fälle implementiert, in denen kompromittierte Zugangsdaten die Hauptursache für die Ransomware-Angriffe waren.
- **Bei mehr als der Hälfte der Vorfälle erkennen und stoppen Unternehmen und Organisationen Ransomware-Angriffe nicht rechtzeitig**
  - Bei über der Hälfte der Ransomware-Angriffe (56 %) gelang es, Daten zu verschlüsseln – bei 16 % davon wurden Daten sowohl verschlüsselt als auch gestohlen.
- **Wenn Daten verschlüsselt werden, haben Angreifer eine Chance von etwa 50:50, eine Lösegeldzahlung zu erhalten**
  - 48 % der Unternehmen und Organisationen, deren Daten verschlüsselt wurden, zahlten das Lösegeld.
  - Der Vierjahresdurchschnitt liegt nun bei 50 % Lösegeldzahlung nach Verschlüsselung.
- **Die Lösegeldforderungen sinken, aber Angreifer verlangen mehr, wenn sie schwer reparierbaren Zugriff auf ein privilegiertes System erhalten**
  - Die durchschnittliche Lösegeldforderung (Medianwert) sank auf 698.000 US$ und setzte damit einen mehrjährigen Abwärtstrend fort: Im Report von 2025 lag der Medianwert noch bei 1,3 Mio. US$ und im Report von 2024 bei 2 Mio. US$.
  - 59 % der Lösegeldforderungen bei Angriffen, die mit einer ausgenutzten Schwachstelle auf Firewall-Ebene begannen, betragen 1 Mio. US$ oder mehr. Für alle Lösegeldforderungen lag dieser Prozentsatz bei 48 %.
- **Lösegeldzahlungen sinken, Opfer können oft einen niedrigeren Betrag aushandeln als ursprünglich gefordert**
  - Die durchschnittliche Lösegeldzahlung (Medianwert) beträgt nun 769.000 US$, ein erheblicher Rückgang gegenüber den im Vorjahr gemeldeten 1 Mio. US$.
  - Knapp die Hälfte (48 %) der Zahlungen betrug mindestens 1 Mio. US$, verglichen mit 52 % im Vorjahr.
  - Fast die Hälfte (51 %) der Unternehmen und Organisationen, die Lösegeld zahlten, zahlten weniger als den geforderten Betrag; dieser Wert entspricht in etwa dem des Reports von 2025 (53 %) und liegt um 7 % über dem Report von 2024 (44 %).
- **Die Wiederherstellungskosten nach einem Ransomware-Angriff sind gestiegen**
  - Die durchschnittlichen (mittleren) Wiederherstellungskosten nach einem Ransomware-Angriff, ohne dass Lösegeld gezahlt wird, betragen jetzt 1.700.200 US$, was einem Anstieg von 11 % gegenüber dem Durchschnitt von 1.525.716 US$ im Report 2025 entspricht.
- **Die Verschlüsselung von Daten hat fast immer Auswirkungen auf das IT/Cybersecurity-Team**
  - 99 % der Ransomware-Opfer, deren Daten verschlüsselt wurden, gaben an, dass ihr IT/Cybersecurity-Team beeinträchtigt wurde.
  - Mehr Stress oder Angst vor zukünftigen Angriffen ist die häufigste Auswirkung (41 %), gefolgt von mehr Druck aus der Führungsetage (40 %).
  - Anerkennung aus der Führungsetage (36 % gegenüber 31 % im Report 2025) nahm als einzige Auswirkung im Jahresvergleich zu.

Angriffs- und Abwehrmethoden

Ursachen von Angriffen

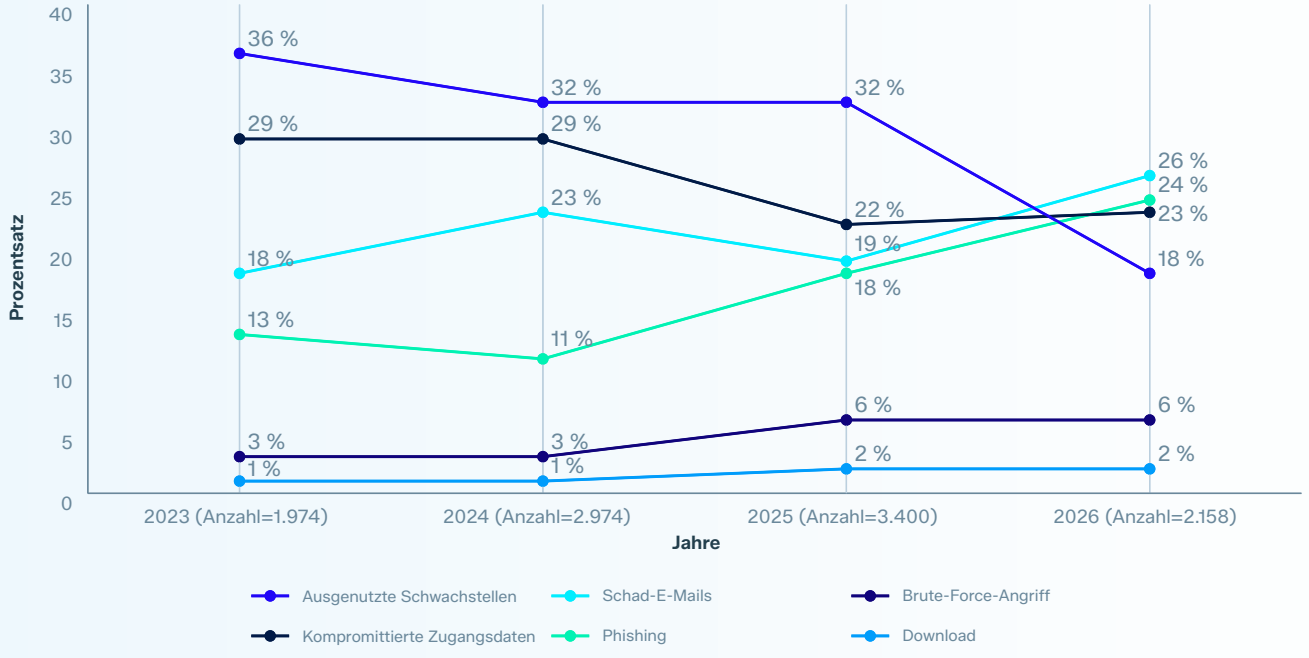
Die wichtigsten technischen Ursachen für Ransomware haben sich im diesjährigen Report geändert. Schad-E-Mails (26 %) und Phishing (24 %) waren die beiden Hauptursachen für Ransomware-Angriffe und machten die Hälfte aller Vorfälle aus. Dies stellt eine deutliche Veränderung gegenüber den Vorjahren dar, als ausgenutzte Schwachstellen die Ranglisten durchweg anführten.

Berichte über ausgenutzte Schwachstellen sanken von 32 % im Report 2025 auf 18 % im Report 2026. Angesichts der Geschwindigkeit und des Umfangs der Fähigkeiten von Frontier AI bei der Aufdeckung von Schwachstellen sollten Unternehmen und Organisationen jedoch weiterhin wachsam sein, da die Zahl der Ransomware-Angriffe mit ausgenutzten Schwachstelle als Ursache im kommenden Jahr zunehmen könnte.

Kompromittierte Zugangsdaten blieben mit 23 % die dritthäufigste Ursache, was mit den Vorjahren vergleichbar ist.

79 % der Angriffe begannen mit einem identitätsbasierten Ansatz, bei dem entweder Zugangsdaten für missbräuchliche Zwecke erlangt oder bereits erlangte Zugangsdaten ausgenutzt wurden. Dies verdeutlicht, warum Identitätssicherheit ein kritisches Element einer ganzheitlichen Sicherheitsstrategie sein muss.

Technische Ursachen von Ransomware-Angriffen (2023–2026)



Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Anzahl der erhaltenen Antworten jeweils in Klammer.

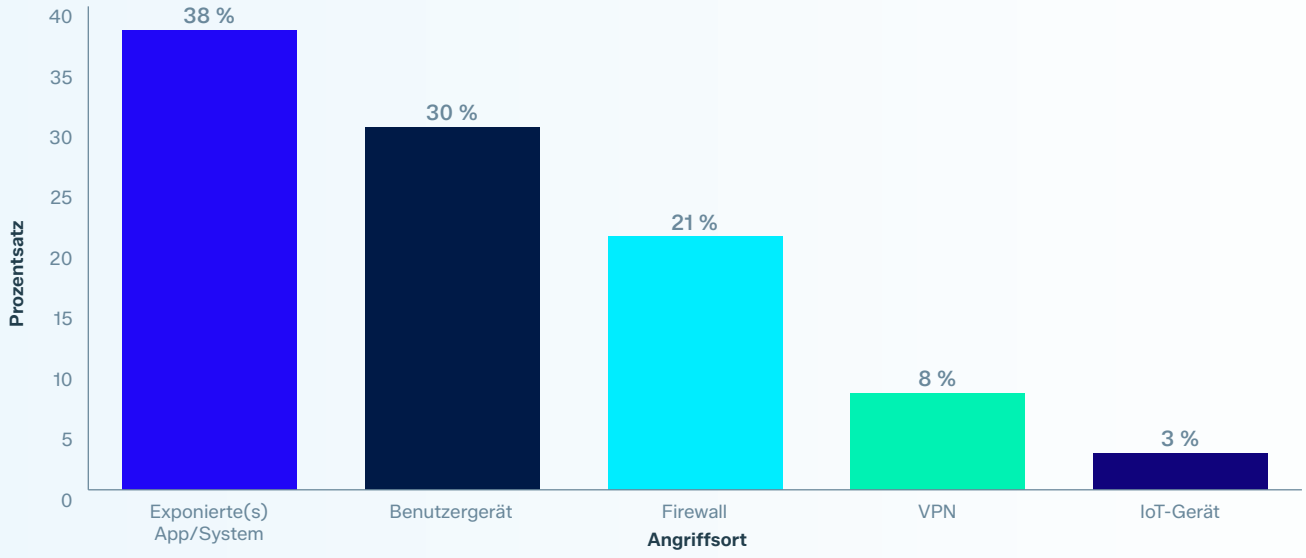
NEUE FORSCHUNG

Wo Angriffe beginnen

In diesem Jahr zeigen wir zum ersten Mal, wo genau innerhalb des organisatorischen Umfelds die eigentliche Ursache lag. Zu verstehen, wo Angriffe beginnen, ist eine wichtige Erkenntnis, um Strategien zur Risikominderung zu entwickeln. Bei allen Ransomware-Vorfällen, die mit einer ausgenutzten Schwachstelle, kompromittierten Zugangsdaten oder einem Brute-Force-Angriff begannen, waren **exponierte Anwendungen und Systeme der häufigste Angriffspunkt insgesamt (38 %)**, gefolgt von Benutzergeräten (30 %) und Firewalls (21 %).

Die zunehmende Bedeutung exponierter Anwendungen steht im Einklang mit dem allgemeinen Trend hin zu Cloud- und SaaS-Umgebungen, in denen internetgestützte Systeme eine große und stetig wachsende Angriffsfläche bieten.

Ransomware-Angriffsorte



Sie sagten, die Ursache war(en) eine ausgenutzte Schwachstelle, kompromittierte Zugangsdaten oder ein Brute-Force-Angriff – wo ist das in Ihrer Umgebung passiert? Anzahl=1.022

Die Daten zeigen, wie verbreitet kompromittierte Zugangsdaten in exponierten Apps und Systemen, Firewalls, VPNs und IoT-Geräten sind.

Häufigste Ursachen für jeden Ort

Ursache	In einer exponierten Anwendung oder einem exponierten System	In unserer Firewall	In unserem VPN	In einem IoT-Gerät
Kompromittierte Zugangsdaten	59 %	41 %	44 %	48 %
Ausgenutzte Schwachstelle	31 %	33 %	41 %	36 %
Brute-Force-Angriff	10 %	26 %	15 %	16 %

Sie sagten, die Ursache war(en) eine ausgenutzte Schwachstelle, kompromittierte Zugangsdaten oder ein Brute-Force-Angriff – wo ist das in Ihrer Umgebung passiert? Auswahl der Antworten. Anzahl=711

Kompromittierte Zugangsdaten waren besonders dominant in exponierten Anwendungen und Systemen (59 %), was zeigt, wie wichtig die Absicherung extern zugänglicher Ressourcen und Identitätskontrollen ist.

Eine erneute Auswertung desselben Datenvergleichs ergab, welche Ziele am häufigsten ins Visier von Angriffen mit kompromittierten Zugangsdaten und Brute-Force-Angriffen gelangten.

Wo Ransomware-Angriffe beginnen

Angriffsort	Gesamt %	Kompromittierte Zugangsdaten %	Brute-Force-Angriff %
In einer exponierten Anwendung oder einem exponierten System	38 %	46 %	30 %
Gerät eines Benutzers (im oder außerhalb des Netzwerks – z. B. Laptop, Desktop)	30 %	27 %	13 %
In unserer Firewall	21 %	18 %	44 %
In unserem VPN	8 %	7 %	9 %
In einem IoT-Gerät	3 %	3 %	4 %

Sie sagten, die Ursache waren kompromittierte Zugangsdaten oder ein Brute-Force-Angriff – wo ist das in Ihrer Umgebung passiert? Auswahl der Antworten. n=628

Verschiedene Angriffstypen zielten auf verschiedene Angriffsorte ab.

- Kompromittierte Zugangsdaten konzentrierten sich auf exponierte Anwendungen und Systeme (46 %), gefolgt von Benutzergeräten.
- Brute-Force-Angriffe zielten mit einer hohen Rate (44 %) auf Firewalls ab, was die Bedeutung von Richtlinien zur Ratenbegrenzung und Kontosperrung auf Geräten am Netzwerkperimeter unterstreicht.

NEUE FORSCHUNG

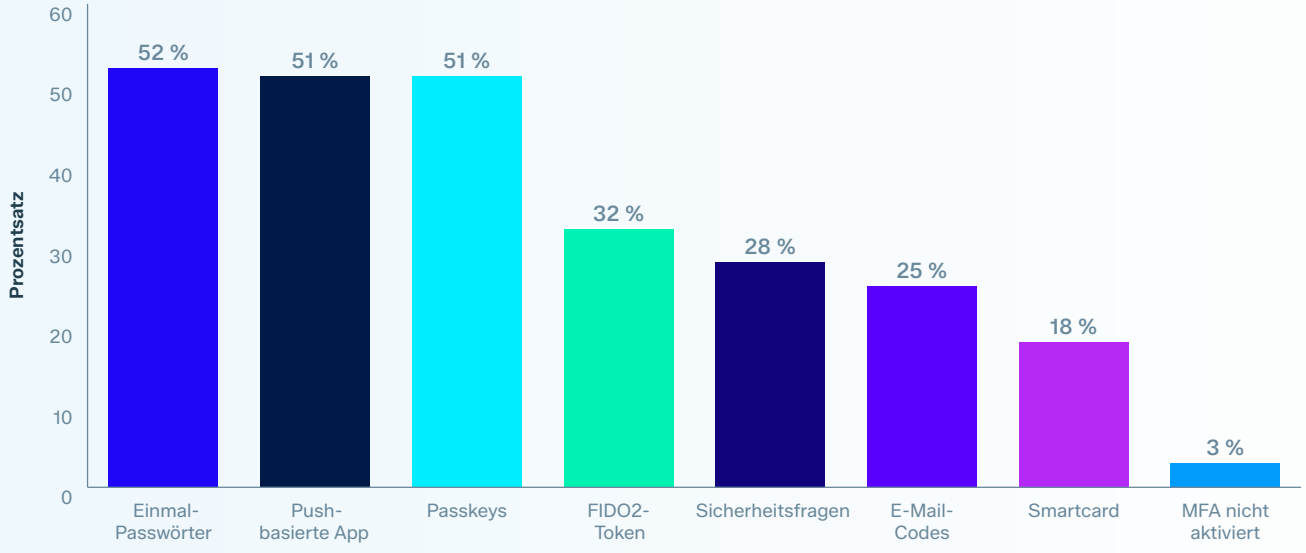
Die Rolle von Multi-Faktor-Authentifizierung (MFA)

Dieses Jahr bringt auch komplett neue Einblicke in die Rolle von MFA bei Ransomware-Angriffen.

Bei Unternehmen und Organisationen, in denen kompromittierte Zugangsdaten die Ursache für den Ransomware-Angriff waren, **hatten 97 % zum Zeitpunkt des Vorfalls in irgendeiner Form Multi-Faktor-Authentifizierung aktiviert**. Einmal-Passwörter (52 %), Push-basierte Anwendungen (51%) und Passkeys (51 %) waren die am weitesten verbreiteten Methoden, wobei die Befragten im Durchschnitt angaben, 2,5 MFA-Methoden zu nutzen.

Der hohe Anteil von Ransomware-Opfern, bei denen zum Zeitpunkt des Angriffs MFA eingerichtet war, deutet darauf hin, dass diese möglicherweise nicht auf allen relevanten Systemen vollständig implementiert war, wodurch Lücken entstanden sind, die Angreifer ausnutzen konnten. Dies lässt zudem darauf schließen, dass MFA zwar nach wie vor ein wesentlicher Bestandteil wirksamer Cyber-Abwehrstrategien ist, allein jedoch nicht ausreicht, um auf Zugangsdaten basierende Angriffe zu verhindern, da sich die Umgehungstechniken ständig weiterentwickeln.

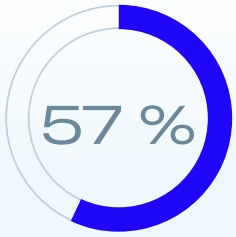
Zum Zeitpunkt des Angriffs aktivierte MFA-Methoden



Welche Art von Multi-Faktor-Authentifizierung war zum Zeitpunkt des Angriffs aktiviert? Basis: Der Angriff erfolgte aufgrund kompromittierter Zugangsdaten. Anzahl=503

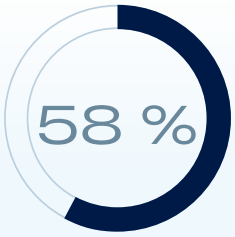
Was Unternehmen/Organisationen anfällig machte

Zum zweiten Mal gab es keinen einzelnen dominierenden organisatorischen Faktor, der Unternehmen und Organisationen für Angriffe anfällig machte; die Befragten nannten vielmehr ein breites Spektrum an Herausforderungen – von fehlenden oder unzureichenden Schutzmaßnahmen über Personal- und Kompetenzmangel bis hin zu Sicherheitslücken.



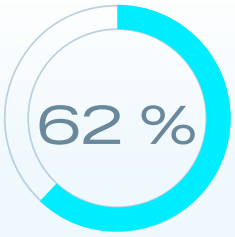
Unzureichender Schutz

(fehlende oder schlechte Lösungen)



fehlende Ressourcen

(mangelnde Expertise oder zu wenig Personal/ Kapazitäten)



Sicherheitslücken

(bekannt oder unbekannt)

Sicherheitslücken waren im zweiten Jahr in Folge mit 62 % die am häufigsten genannte Kategorie operativer Ursachen, gefolgt von zu wenig Fachkräften und mangelnder Expertise (58 %) und fehlendem oder minderwertigem Schutz (57 %).

Erfreulicherweise gingen alle Einzelfaktoren (bis auf einen) von Jahr zu Jahr zurück, wobei **menschliches Versagen (35 %) der einzige operative Faktor war, der im letzten Jahr zunahm**.

Wie schon 2025 berichteten Ransomware-Opfer von mehreren organisatorischen Herausforderungen, wobei im Durchschnitt **2,5 Faktoren genannt wurden**, gegenüber 2,7 im Vorjahr.

35 %

Menschliches Versagen: die eine Konstante. Die einzige operative Angriffsursache, die gegenüber dem Report von 2025 nicht zurückging.

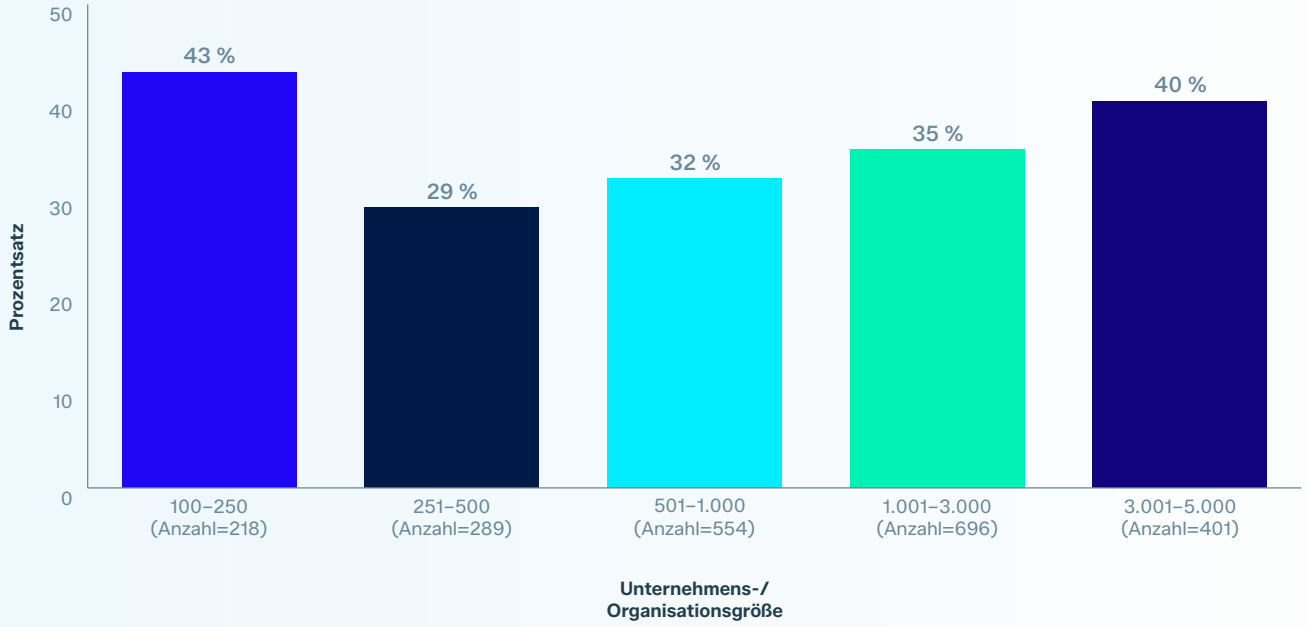
Die 7 häufigsten operativen Ursachen von Ransomware-Angriffen

Rang	2025	%	Rang	2026	%
1	Mangelnde Expertise	40,2 %	1	Fehlender Schutz	36,4 %
2	Unbekannte Sicherheitslücke	40,1 %	2	Unbekannte Sicherheitslücke	36,3 %
3	Zu wenig Personal/ Kapazitäten	39,4 %	3	Bekannte Sicherheitslücke	36,0 %
4	Fehlender Schutz	39,0 %	4	Zu wenig Personal/ Kapazitäten	35,3 %
5	Bekannte Sicherheitslücke	38,2 %	5	Menschliches Versagen	35,3 %
6	Schlechter Schutz	37,1 %	6	Mangelnde Expertise	35,1 %
7	Menschliches Versagen	34,2 %	7	Schlechter Schutz	32,6 %

Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Anzahl=3.400 (2025), Anzahl=2.158 (2026)

Wie zu erwarten, wurde der Mangel an Personal/Kapazitäten von kleinen Unternehmen und Organisationen mit 100 bis 250 Mitarbeitenden besonders häufig genannt. Allerdings geben vier von zehn Großunternehmen mit 3.001 bis 5.000 Mitarbeitenden ebenfalls Kapazitätsprobleme an – und zwar mit einer Quote, die nur 3 % unter der von Unternehmen mit 100 bis 250 Mitarbeitern liegt. Dies deutet darauf hin, dass die Personalbeschaffung mit zunehmender Unternehmensgröße nicht immer einfacher wird.

Zu wenig Personal/Kapazitäten trug zu Ransomware-Angriffen bei



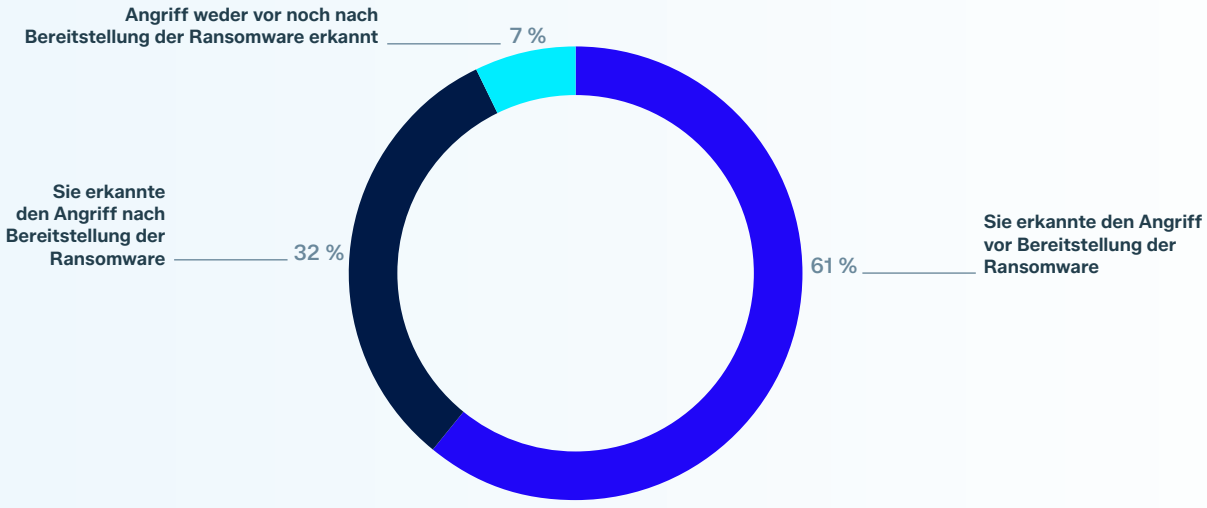
Warum wurde Ihr Unternehmen/Ihre Organisation Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Wir hatten nicht ausreichend Cybersicherheitsexperten, die unsere Systeme überwacht haben. Anzahl der erhaltenen Antworten jeweils in Klammer.

NEUE FORSCHUNG

Die Rolle von Firewalls bei der Ransomware-Abwehr

61 % der Opfer gaben an, dass ihre Firewall den Ransomware-Angriff erkannte, bevor der Payload ausgeführt wurde, und 32 % gaben an, dass die Firewall diesen nach der Bereitstellung der Ransomware identifizierte. Nur 7 % gaben an, dass ihre Firewall den Angriff überhaupt nicht erkannt hat.

Welche Rolle spielte Ihre Firewall bei der Identifizierung des Angriffs?



Welche Rolle spielte Ihre Firewall bei der Identifizierung des Angriffs? Anzahl=2.158

Die 7 % der Opfer, deren Firewall den Angriff nicht erkannt hatte, verzeichneten die schlimmsten Folgen hinsichtlich der Verschlüsselung: Bei 71 % von ihnen wurden Daten verschlüsselt, verglichen mit 50 % in den Fällen, in denen die Firewall den Angriff erkannte, bevor die Ransomware bereitgestellt wurde. Die Erkennung nach der Bereitstellung von Ransomware – also die Identifizierung von Anzeichen im Nachhinein, die später mit dem Ransomware-Angriff in Verbindung gebracht wurden – ging mit einer Verschlüsselungsrate von 65 % einher.

Die Ergebnisse machen deutlich, dass Firewalls eine Schlüsselrolle bei der Erkennung von Ransomware-Angriffen spielen. Telemetrie-Daten dieser Geräte liefern wertvolle frühe Signale von Angriffsaktivitäten. In Kombination mit Erkenntnissen aus der gesamten Sicherheitsumgebung, beispielsweise von Endpoint Protection- oder E-Mail-Security-Lösungen über ein XDR-Tool oder einen MDR-Service, kann Firewall-Telemetrie Bedrohungsexperten helfen, Ransomware-Angriffe zu erkennen und zu blockieren, bevor Daten verschlüsselt werden.

Auswirkungen der Firewall-gestützten Angriffserkennung auf die Verschlüsselung

	Angriff vor Bereitstellung der Ransomware erkannt	Angriff nach Bereitstellung der Ransomware erkannt	Angriff weder vor noch nach Bereitstellung der Ransomware erkannt
Cyberkriminelle konnten ihre Daten verschlüsseln	50 %	65 %	71 %
Cyberkriminelle konnten ihre Daten nicht verschlüsseln	50 %	35 %	29 %

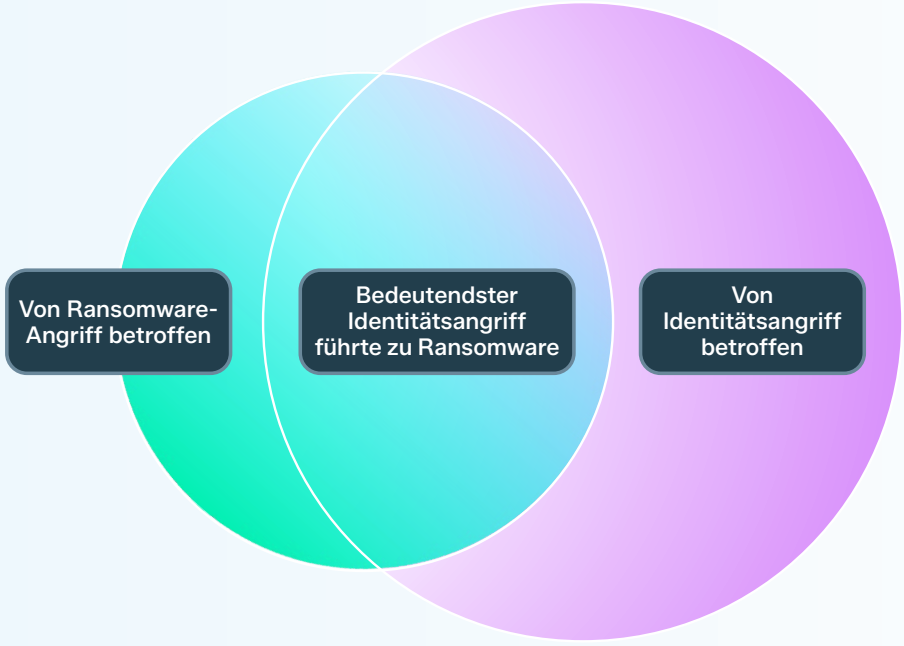
Welche Rolle spielte Ihre Firewall bei der Identifizierung des Angriffs? Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Daten verschlüsseln? Anzahl=2.158

Firewalls nehmen in der Infrastruktur von Unternehmen und Organisationen eine besonders wichtige Stellung ein, sodass eine Kompromittierung im Vergleich zu anderen Teilen der Umgebung weitaus schwerwiegendere Folgen nach sich zieht. Wenn Angreifer eine Schwachstelle in der Firewall erfolgreich ausnutzen, erhalten sie häufig weitreichenden Zugriff auf das gesamte Unternehmen. Die unterschiedlichen Lösegeldforderungen für diese Szenarien unterstützen diesen Punkt: **59 % der Lösegeldforderungen bei Angriffen, die mit einer ausgenutzten Schwachstelle auf Firewall-Ebene begannen, betragen 1 Mio. US$ oder mehr**. Für alle Ransomware-Angriffe lag dieser Prozentsatz bei 48 %.

NEUE FORSCHUNG

Verbindung zwischen Identität und Ransomware

Eines der auffälligsten Ergebnisse der diesjährigen Befragung ist die Bestätigung des direkten Zusammenhangs zwischen Identitätsangriffen und Ransomware. Von den Unternehmen und Organisationen, die im vergangenen Jahr von Ransomware betroffen waren, bestätigten zwei Drittel (67 %), dass es sich bei dem Ransomware-Vorfall um dasselbe Ereignis handelte wie bei ihrem bedeutendsten Identitätsangriff. Obwohl nicht alle Angriffe zu einer Datenverschlüsselung führten, belegt dies, dass die Identitätskompromittierung ein zentrales Einfallstor zur Verbreitung von Ransomware ist.



Datenaufteilung: War Ihr Unternehmen im letzten Jahr von Ransomware betroffen? (Anzahl=5.000). War Ihr Unternehmen in den letzten 12 Monaten von identitätsbezogenen Sicherheitsvorfällen betroffen? Anzahl=5.000. [Falls beides zutrifft] Entsprach dieser Ransomware-Vorfall Ihrem bedeutendsten identitätsbezogenen Angriff?

Datenverschlüsselung und -wiederherstellung

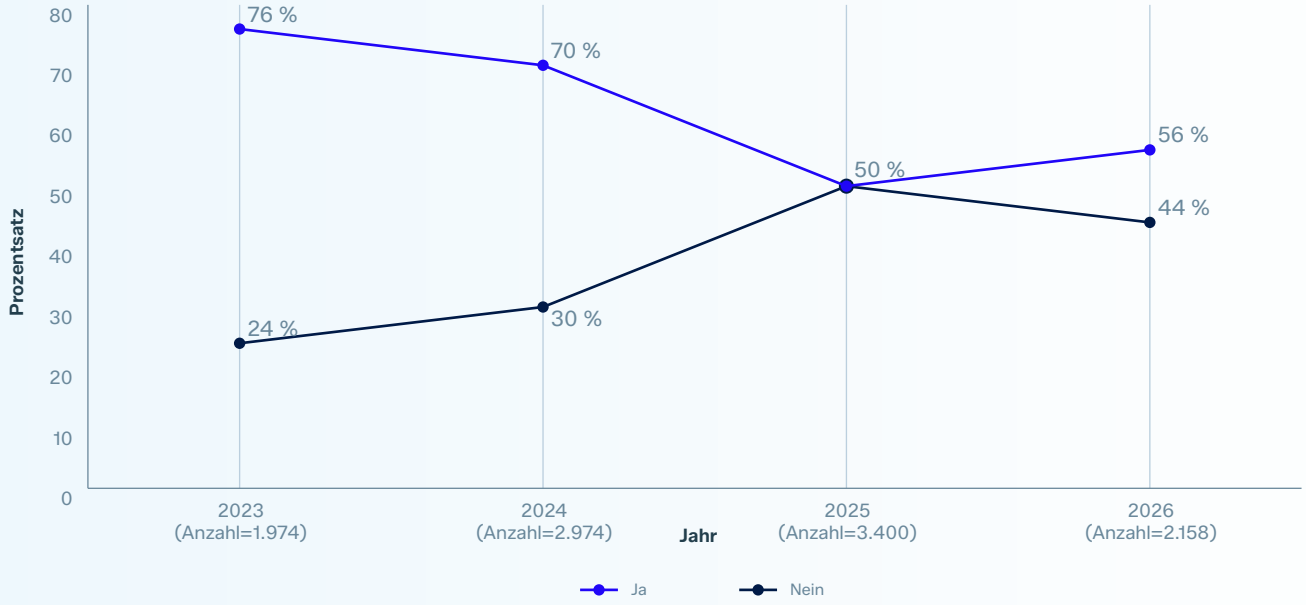
Datenverschlüsselungsrate

Bei über der Hälfte der Ransomware-Angriffe (56 %) gelang es, Daten zu verschlüsseln. In 40 % dieser Fälle wurden Daten lediglich verschlüsselt, in 16 % der Fälle wurden Daten sowohl verschlüsselt als auch gestohlen. 41 % der Angriffe wurden vor der Verschlüsselung abgewehrt, während es sich bei 2 % um Erpressungsangriffe ohne Verschlüsselung handelte.

+ 6 %

Der Anstieg der Ransomware-Verschlüsselungsrate gegenüber dem Vorjahrs-Report.

Wurden beim Angriff Daten verschlüsselt? (Zusammengefasst: Ja/Nein)

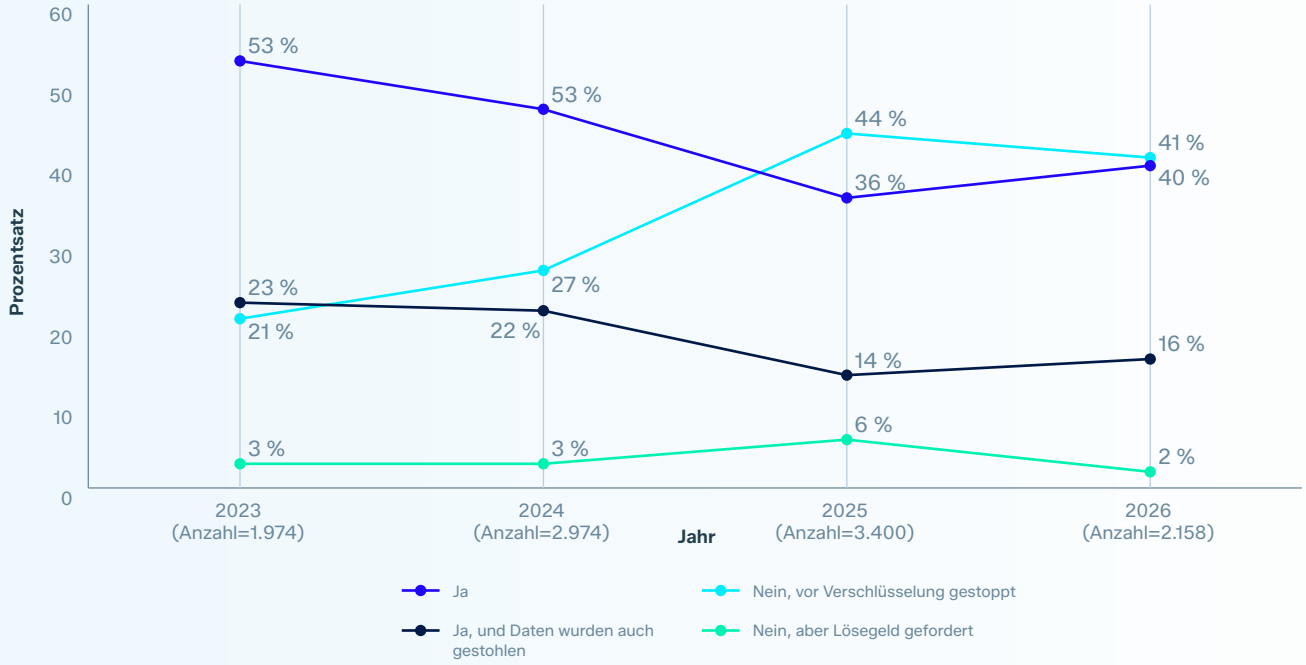


Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Zusammengefasste Antworten: Ja/Nein. Anzahl der erhaltenen Antworten jeweils in Klammer.

Die Verschlüsselungsrate bleibt zwar deutlich unter dem Höchstwert von 76 % im Report 2023, hat sie sich gegenüber dem Tiefststand von 50 % im Report 2025 leicht erhöht. Diese Kehrtwende verdient Aufmerksamkeit: Nach zwei Jahren rückläufiger Verschlüsselung scheinen Angreifer wieder Fuß zu fassen.

Besonders besorgniserregend sind die 16 % der Angriffe, die sowohl Verschlüsselung als auch Datendiebstahl beinhalten, da diese Angriffe mit doppelter Wirkung Angreifern mehrere Hebelpunkte für Erpressung bieten.

Wurden beim Angriff Daten verschlüsselt?

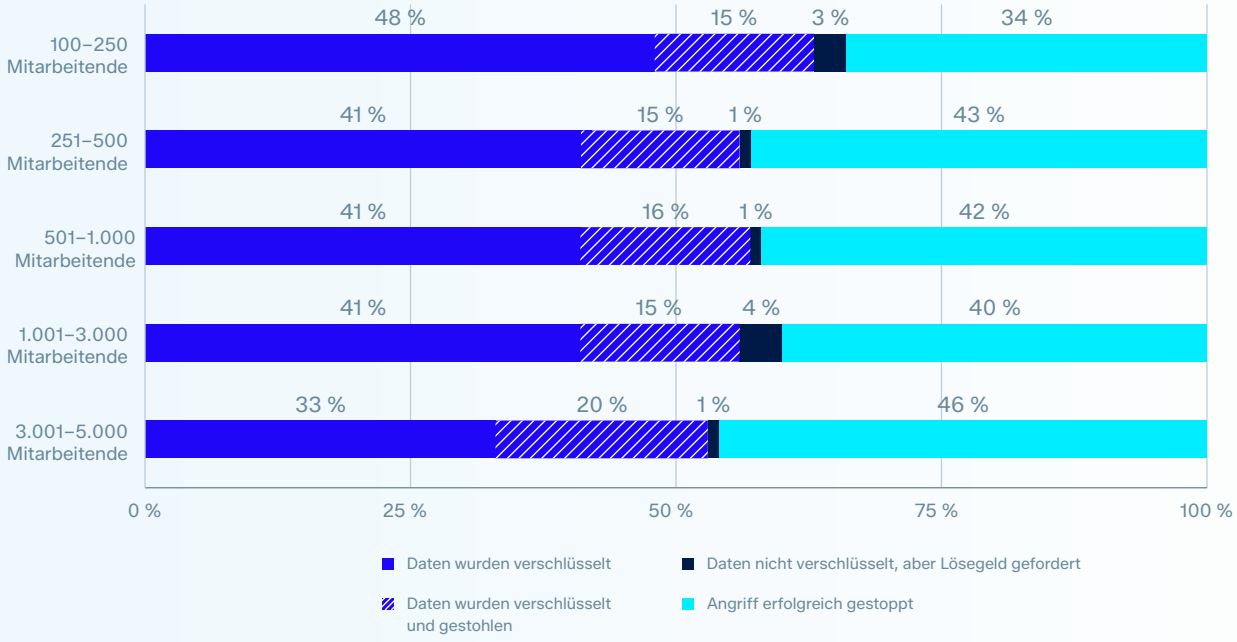


Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? (Vollständige Liste der Antwortmöglichkeiten)
Basis: Von Ransomware betroffene Unternehmen und Organisationen. Anzahl der erhaltenen Antworten jeweils in Klammer.

Die Folgen hinsichtlich der Verschlüsselung variierten je nach Organisationsgröße, wobei **die größten befragten Unternehmen und Organisationen (3.001 bis 5000 Mitarbeitende) Angriffe am ehesten vor einer Verschlüsselung oder Erpressung stoppen konnten (46 %)**, während dies bei den kleinsten Unternehmen und Organisationen (100–250 Mitarbeitende) nur bei 34 % der Fall war.

Wenn Angriffe in größeren Unternehmen und Organisationen jedoch tatsächlich zur Verschlüsselung von Daten führten, wurden mit höherer Wahrscheinlichkeit auch Daten gestohlen, wobei die Quote der „verschlüsselten und gestohlenen Daten“ in der Kategorie der größten Unternehmen und Organisationen 20 % erreichte, gegenüber 15 % bei den meisten anderen. Das Exfiltrieren von Daten zusätzlich zur Bereitstellung von Ransomware gibt Angreifern eine weitere Möglichkeit, den Angriff zu monetarisieren.

Datenverschlüsselungs-Quote bei Ransomware-Angriffen nach Unternehmensgröße



Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Daten verschlüsseln? Anzahl=2.158

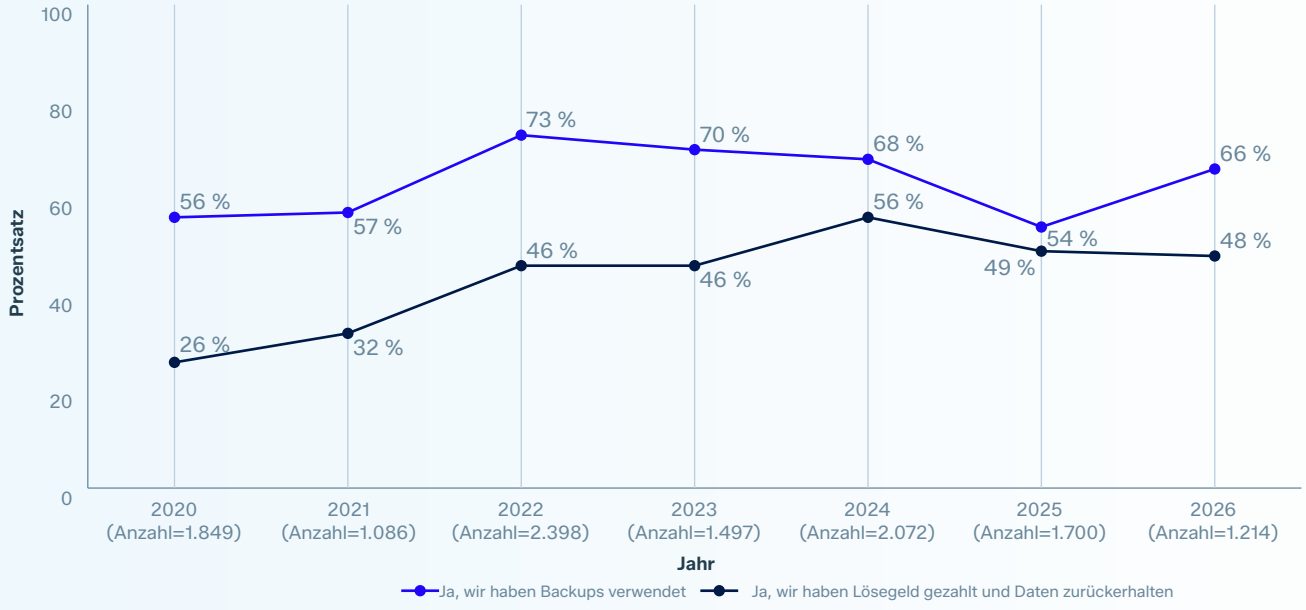
Wie Unternehmen und Organisationen verschlüsselte Daten wiederherstellen

Die Wiederherstellung auf Basis von Backups stieg bei Angriffen, bei denen Daten verschlüsselt wurden, auf 66 % – ein Anstieg gegenüber den 54 % im Report von 2025. Dieser deutliche Aufschwung deutet darauf hin, dass Unternehmen und Organisationen nach einem Rückgang der Nutzung im Jahr 2025 wieder verstärkt in ihre Backup-Infrastruktur investieren und ihre Resilienz gegenüber Lösegeldforderungen erhöhen.

+ 12 %

Die Zunahme der Nutzung von Backups zur Wiederherstellung von Ransomware-Angriffen von 2025 bis 2026.

Wie hat Ihr Unternehmen oder Ihre Organisationen Daten nach Ransomware-Angriffen wiederhergestellt?



Wie hat Ihr Unternehmen/Ihre Organisation die Daten zurückerhalten? Basis: Unternehmen/Organisationen, deren Daten verschlüsselt wurden. Anzahl der erhaltenen Antworten jeweils in Klammer. Mehrere Antworten erlaubt, sodass Prozentsätze 100 % überschreiten können.

Der Anteil der Unternehmen und Organisationen, die das Lösegeld für die Wiederherstellung von Daten zahlten, sank auf 48 %, die niedrigste Rate in den letzten 3 Jahren. Nur 2 % der Unternehmen und Organisationen gaben an, überhaupt keine Daten zurückerhalten zu haben, was darauf hindeutet, dass bei verschlüsselten Daten eine Wiederherstellung auf die eine oder andere Weise nahezu immer möglich ist.

Lösegeldforderungen und -zahlungen

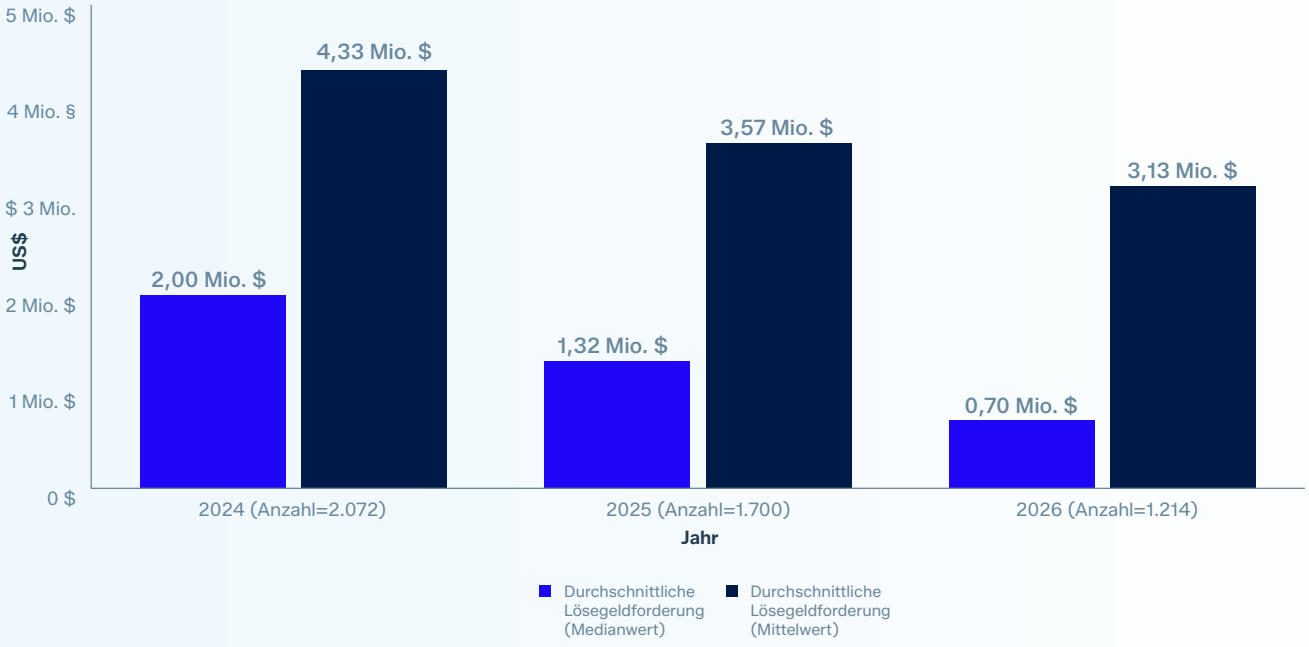
Lösegeldforderungen

**Der Medianwert der durchschnittlichen Lösegeldforderungen sank im diesjährigen Report auf 698.000 US$**und setzte damit einen mehrjährigen Abwärtstrend fort. Dies entspricht einem Rückgang von 65 % in den letzten zwei Jahren. Der Mittelwert der durchschnittlichen Lösegeldforderungen ist in diesem Zeitraum ebenfalls gesunken und liegt bei 3.126.372 US$, was einem Rückgang um 28 % seit dem Report 2024 entspricht.

698.000 US$

Die durchschnittliche Lösegeldforderung (Medianwert) im letzten Jahr.

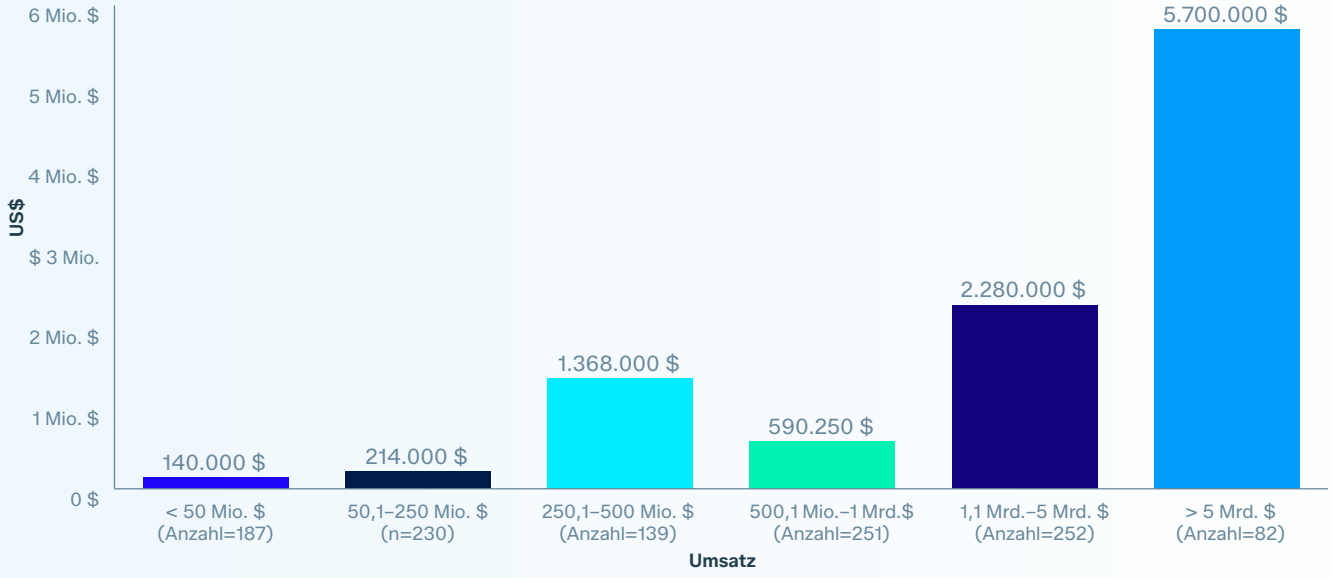
Lösegeldforderungen – Mittelwert und Medianwert



Wie viel Lösegeld forderten die Angreifer? Basis: Unternehmen/Organisationen, deren Daten verschlüsselt wurden. Anzahl der erhaltenen Antworten jeweils in Klammer. Ausreißerwerte ab 40 Mio.US$ wurden nicht berücksichtigt.

Die Lösegeldforderungen steigen stark mit dem Umsatz. Unternehmen mit einem Umsatz von unter 50 Mio. US$ sahen sich mit durchschnittlichen Lösegeldforderungen (Medianwert) von etwa 140.000 US$ konfrontiert, während dieser Wert bei Unternehmen mit einem Umsatz von über 5 Mrd. US$ bei 5,7 Mio. US$ lag. Dieses Muster deutet stark darauf hin, dass Angreifer Erkundungsmaßnahmen durchführen, um ihre Lösegeldforderungen auf die prognostizierte Zahlungsfähigkeit anzupassen.

Lösegeldforderung (Medianwert)



Wie viel Lösegeld wurde gefordert? Basis: Unternehmen/Organisationen, deren Daten verschlüsselt wurden. Anzahl der erhaltenen Antworten jeweils in Klammer. Ausreißerwerte ab 40 Mio.US$ wurden nicht berücksichtigt.

Lösegeldzahlungen

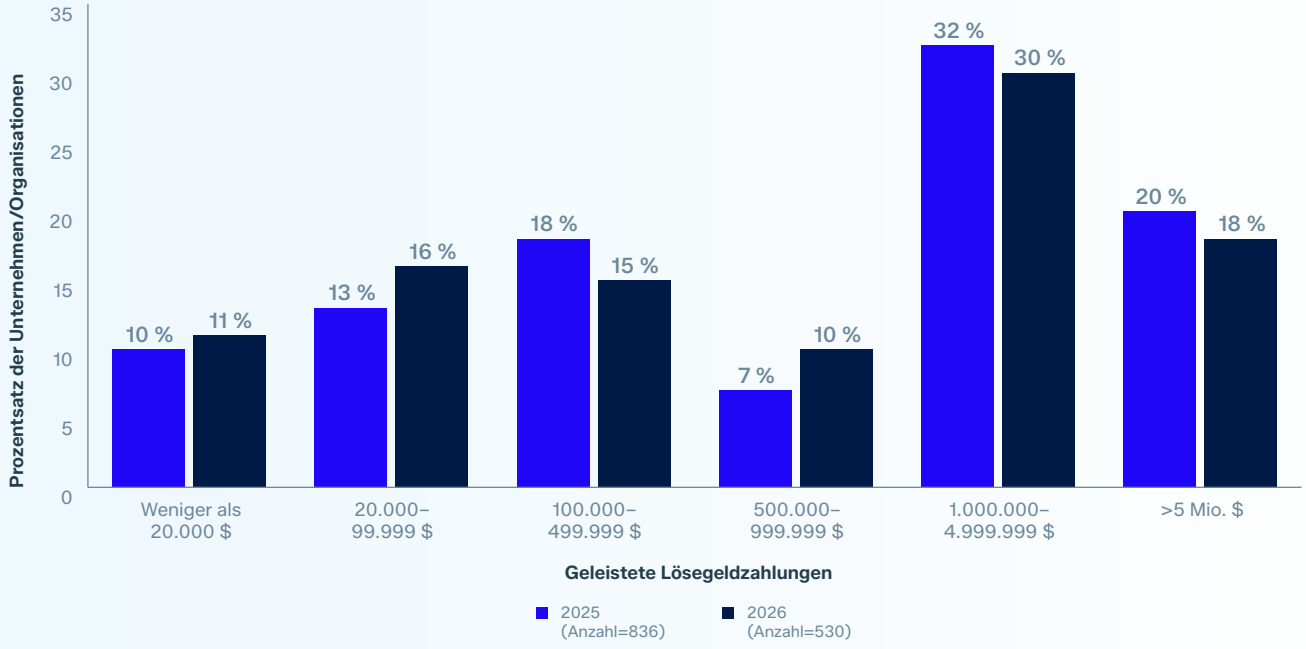
530 Unternehmen/Organisationen, die Lösegeld zahlten, teilten uns die Höhe der Zahlung mit. Daraus geht hervor, dass der Medianwert der Lösegeldzahlungen nun bei 769.000 US$ liegt – ein deutlicher Rückgang gegenüber den im Vorjahr gemeldeten 1 Mio. US$. Knapp die Hälfte (48 %) der Zahlungen entfielen auf 1 Mio. US$ oder mehr, verglichen mit 52 % im Vorjahr.

Betrachtet man die gesamte Verteilung der Zahlungen, so zeigt sich eine deutliche Verschiebung in Richtung der Mitte des Spektrums. Die beiden höchsten Betragsgruppen (1 Mio.–5 Mio. $ und >5 Mio. $) verzeichneten im Vergleich zum Vorjahres-Report Rückgänge, während die Betragsgruppen 20.000–99.999 $ und 500.000–999.999 $ jeweils zulegten, was darauf hindeutet, dass sich Angreifer und Opfer zunehmend im unteren bis mittleren Zahlungsbereich bewegen.

769.000 $

Die durchschnittliche Lösegeldzahlung (Medianwert) im letzten Jahr.

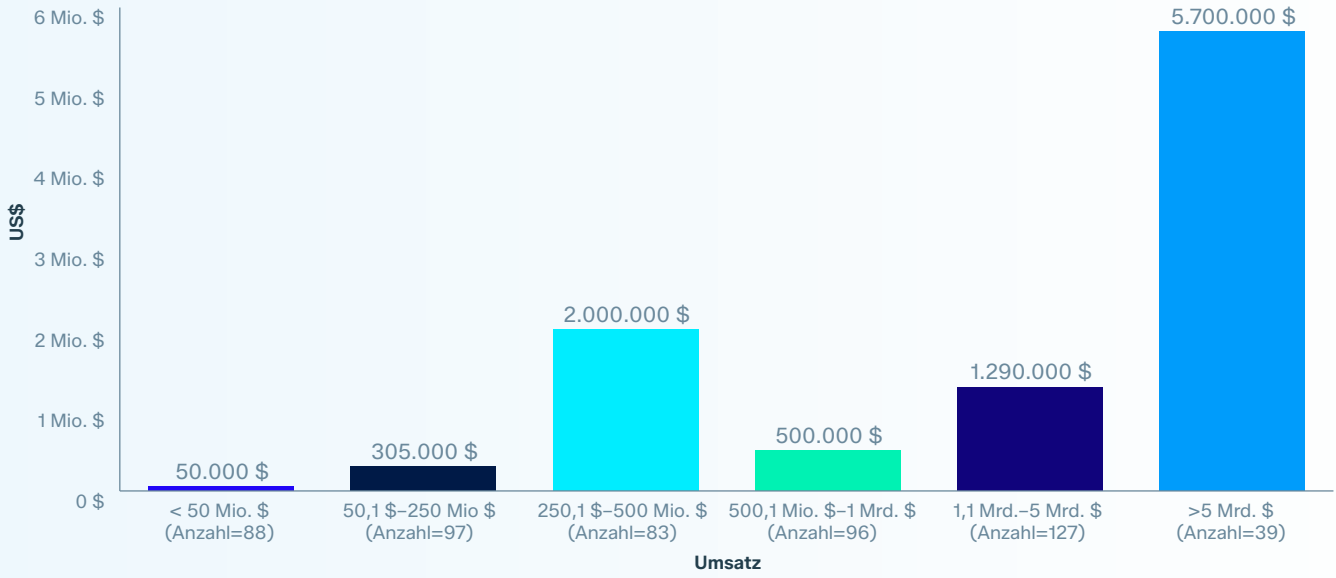
Geleistete Lösegeldzahlungen



Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl der erhaltenen Antworten jeweils in Klammer.

Bei der Aufschlüsselung der Lösegeldzahlungen nach Umsatz zeigte sich ein sprunghafter Anstieg im Bereich von 250,1 Mio.–500 Mio. US$, wobei die Opfer durchschnittlich 2 Mio. US$ (Medianwert) zahlten. Das ist mehr als in jedem anderen Segment – abgesehen von den allergrößten Unternehmen/Organisationen (mit einem Jahresumsatz von über 5 Mrd. US$) – und viermal so viel wie Unternehmen/Organisationen mit einem Umsatz zwischen 500,1 Mio. US$ und 1 Mrd. US$.

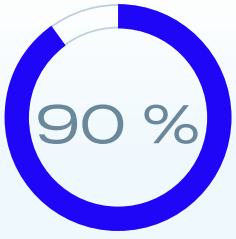
Mittlere Lösegeldzahlung



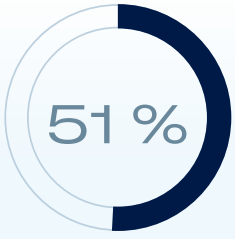
Wie viel Lösegeld wurde den Angreifern gezahlt? Basis: Unternehmen/Organisationen zahlten das Lösegeld. Anzahl der erhaltenen Antworten jeweils in Klammer.

Tatsächliche Zahlungen vs. ursprüngliche Forderungen

507 Unternehmen und Organisationen gaben sowohl ihre Lösegeldforderung als auch die Höhe der gezahlten Lösegeldsumme bekannt und zeigen damit, wie effektiv Unternehmen und Organisationen bei Verhandlungen mit Angreifern sind. **Die durchschnittliche Zahlung (Medianwert) betrug 90 % der Lösegeldforderung (Mittelwert: 85 %)**, wobei etwas mehr als die Hälfte (51 %) weniger als die ursprüngliche Lösegeldforderung zahlte, 30 % die tatsächliche Lösegeldforderung und 18 % mehr. Diese Zahlen liegen sehr nahe an den Zahlen des vergangenen Jahres, was zeigt, dass das Verhältnis zwischen Forderungen und tatsächlichen Zahlungen relativ stabil geblieben ist.

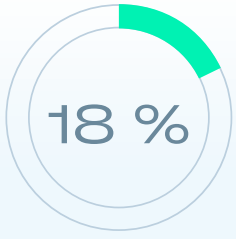


Durchschnittlicher Prozentsatz geleisteter Lösegeldzahlungen **(Medianwert)**



Zahlungen **unter** der ursprünglichen Lösegeldforderung

Zahlungen entsprachen der ursprünglichen Lösegeldzahlung



Zahlungen lagen **über** der ursprünglichen Lösegeldforderung

Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? Basis: Unternehmen/Organisationen, die sowohl Lösegeldforderung als auch gezahlte Summen nannten. Anzahl=507

Wie oben bereits erwähnt, steigen die durchschnittlichen Lösegeldforderungen (Medianwert) in der Regel mit zunehmendem Umsatz des betroffenen Unternehmens, doch je nach Umsatz variiert der Erfolg bei der Aushandlung niedrigerer Endzahlungen.

Unternehmen und Organisationen mittlerer Größe (50 bis 250 Mio. US$ Umsatz) sind am wenigsten erfolgreich bei der Reduzierung von Lösegeldzahlungen: 25 % zahlen mehr als die ursprünglich geforderte Summe. Die größten Unternehmen (mit einem Umsatz von über 5 Mrd. US$) sind am erfolgreichsten bei der Aushandlung niedrigerer Lösegeldsummen: 11 % zahlen mehr als die ursprüngliche Forderung, 57 % zahlen weniger – der höchste Anteil aller Gruppen.

Unternehmen mit höheren Umsätzen (über 500 Mio. US$) gelang es öfter, weniger als die ursprünglich geforderte Lösegeldsumme zu zahlen. Dies deutet darauf hin, dass die Angreifer bei höheren Lösegeldzahlungen eher bereit waren, Rabatte für insgesamt höhere Lösegeldsummen zu gewähren. Auch Unternehmen mit einem Umsatz von unter 50 Mio US$ konnten ihre Lösegeldzahlungen in bescheidenem Umfang senken.

Gezahlter Lösegeldprozentsatz (Medianwert) nach Umsatz

Umsatz	Gezahlter prozentualer Anteil der Lösegeldforderung (Medianwert)
< 50 Mio. $:	95 %
50,1 Mio.–250 Mio. $	100 %
250,1 Mio.–500 Mio. $	100 %
500,1 Mio.–1 Mrd. $	83 %
1,1 Mrd.–5 Mrd. $	83 %
5 Mrd. $ oder mehr	83 %

Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? Basis: Unternehmen/Organisationen, die sowohl Lösegeldforderung als auch gezahlte Summen nannten. Anzahl=507

Lösegeldzahlungen nach Branche

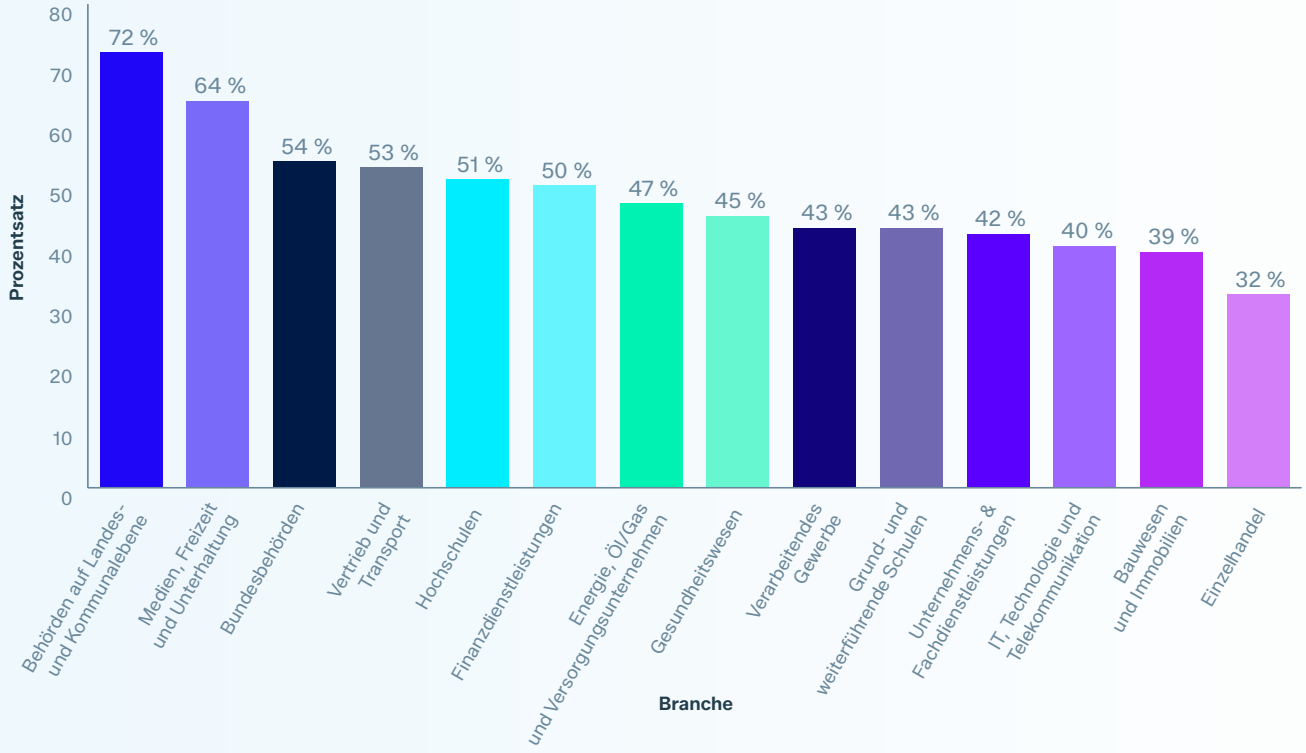
Die Zahlungsbereitschaft ist branchenabhängig **Behörden auf Landes- und Kommunalebene (72 %) und Medien, Freizeit und Unterhaltung (64 %) zahlten das Lösegeld am ehesten** – ihre Quote war mehr als doppelt so hoch wie die des Einzelhandels (32 %).

Organisationen des öffentlichen Sektors und Medienunternehmen stehen oft unter großem Druck, bürgerorientierte oder zeitkritische Services schnell wiederherzustellen, während Einzelhandelsunternehmen eher bereit sind, „die Krise auszusitzen".

Einzelhandel

Die Branche mit den geringsten Zahlungen an Ransomware-Angreifer (32 %).

Prozentsatz der Unternehmen/Organisationen, die das Lösegeld zahlten, nach Branche



Wie hat Ihr Unternehmen/Ihre Organisation die Daten zurückerhalten? Wir zahlten das Lösegeld. Basis: Unternehmen/Organisationen, deren Daten verschlüsselt wurden. Anzahl=1.214

Wirtschaftliche Folgen und Auswirkungen auf Mitarbeitende

Ransomware-Bereinigungskosten

Die durchschnittliche Wiederherstellung (Mittelwert) nach einem Ransomware-Angriff – exklusive Lösegeldzahlung – betrug im letzten Jahr 1.700.200 US$. Dies entspricht einem Anstieg von 11 % gegenüber dem Durchschnitt von 1.525.716 $ im Report 2025, bleibt aber 38 % unter dem Höchstwert von 2.730.684 $ im Report 2024. Die durchschnittlichen Kosten (Medianwert) liegen bei 375.000 US$ und sind damit gegenüber dem Vorjahres-

2024	2025	2026
2,73 $ Mio.	1,53 $ Mio.	1,70 $ Mio.

Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen/Ihrer Organisation durch den schwerwiegendsten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.), ohne Berücksichtigung gezahlter Lösegeldforderungen? Anzahl=2.158 (2026), Anzahl=3.400 (2025), 2.974 (2024)

Die Wiederherstellungskosten von Ransomware-Angriffen

Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen/Ihrer Organisation durch den schwersten Ransomware-Angriff entstanden sind? Anzahl=2.158

Ausfallzeiten

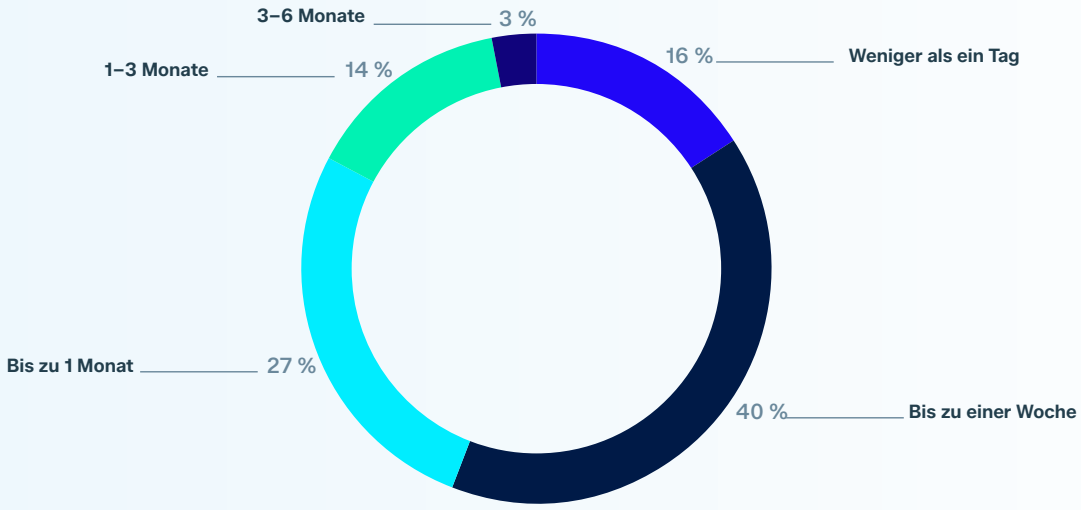
Über die Hälfte der Unternehmen und Organisationen (55 %) beseitigten die Folgen der Ransomware innerhalb von einer Woche (16 % innerhalb weniger als eines Tages) und 83 % innerhalb eines Monats. Nur 3 % benötigten länger als drei Monate.

Die 55%ige Wiederherstellungsrate innerhalb von einer Woche liegt um 3 % über dem Vorjahreswert. Die durchschnittliche Wiederherstellungsdauer blieb bei drei Wochen (Report 2026 und 2025) und lag damit unter den fünf Wochen, die im Report 2024 gemeldet wurden.

55 %

Prozentsatz der Unternehmen/ Organisationen, die sich innerhalb einer Woche von dem Ransomware-Angriff erholt haben.

Wie lange die Wiederherstellung dauerte



Wie lange hat es gedauert, bis sich Ihr Unternehmen/Ihre Organisation vollständig von dem Ransomware-Angriff erholt hat? Anzahl=2.158

Auswirkungen auf Mitarbeitende

Praktisch alle Unternehmen und Organisationen, deren Daten verschlüsselt wurden (99 %), berichteten von nachhaltigen Auswirkungen auf ihre IT- und Cybersecurity-Teams. Die am häufigsten genannten Auswirkungen waren mehr Stress oder Angst vor zukünftigen Angriffen (41 %) und mehr Druck aus der Führungsetage (40 %). Bei mehr als einem von fünf Opfern (21 %) wurde das Führungsteam als direkte Folge des Angriffs ersetzt.

„Mehr Anerkennung aus der Führungsetage" nahm als einzige Auswirkung im Jahresvergleich zu und stieg von 31 % auf 36 %. Alle anderen gemessenen Auswirkungen gingen zurück, darunter Änderungen der Team-Prioritäten (minus sieben Punkte), anhaltender Anstieg der Arbeitsbelastung (minus sieben Punkte) und Umstrukturierungen im Team (minus fünf Punkte).

21 %

Prozentsatz der IT-/Cybersecurity-Führungsteams, die aufgrund des Ransomware-Angriffs ersetzt wurden.

Wie Ransomware sich auf IT/Cybersecurity-Teams auswirkte

Auswirkungen	2026	Veränderung ggü. 2025
Mehr Stress oder Angst vor künftigen Angriffen	41 %	–
Mehr Druck aus der Führungsetage	40 %	–
Mehr Anerkennung aus der Führungsetage	36 %	↑ 5 Prozentpunkte
Veränderungen an der Struktur des Teams/Unternehmens	32 %	↓ 5 Prozentpunkte
Veränderungen der Prioritäten/ Fokusbereiche im Team	32 %	↓ 6 Prozentpunkte
Schuldgefühle, weil sie den Angriff nicht gestoppt haben	31 %	↓ 3 Prozentpunkte
Höhere Arbeitslast	31 %	↓ 7 Prozentpunkte
Fehlzeiten bei Mitarbeitenden wegen Stress/psychischen Problemen	29 %	↓ 2 Prozentpunkte
Austausch der Teamführung	21 %	↓ 4 Prozentpunkte

Welche Auswirkungen hatte der Ransomware-Angriff auf die Mitarbeitenden in Ihrem IT-/Cybersecurity-Team? Basis: Unternehmen/ Organisationen, deren Daten verschlüsselt wurden. Anzahl=1.214 (2026), Anzahl=1.700 (2025)

Die zunehmende Anerkennung durch die Führungsetage könnte selbst ein Faktor sein, der zu den positiven operativen Trends beiträgt, die an anderer Stelle in diesem Report beschrieben werden, da eine stärkere Aufmerksamkeit seitens der Führungsetage zu einer besseren Ressourcenausstattung und organisatorischen Unterstützung für Cybersecurity-Programme führen kann.

Empfehlungen

Stärken Sie die Identitätssicherheit zum Schutz vor Ransomware. Zwei Drittel der Ransomware-Opfer bestätigten, dass ihr Ransomware-Vorfall gleichzeitig ihr schwerwiegendster Identitätsangriff war, was den engen Zusammenhang zwischen Identitätskompromittierung und Ransomware unterstreicht. 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. Wie die Umfrageergebnisse zeigten (97 % der Unternehmen und Organisationen hatten zum Zeitpunkt ihres Angriffs in irgendeiner Form MFA aktiviert), reicht MFA allein nicht aus, um Angriffe zu stoppen, und diese muss umfassend aktiviert werden.

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.

Ziehen Sie fachliche Unterstützung oder MDR hinzu. Der Mangel an Kapazitäten, Fachwissen und Expertise ist sowohl für KMUs als auch für Großunternehmen ein immer wiederkehrendes Thema. Die Zunahme von KI-gestützten Bedrohungen wird diese Bereiche noch stärker belasten, da Sicherheitsexperten versuchen, mit der sich schnell verändernden KI-Technologie Schritt zu halten. Sofern Sie nicht in der Lage sind, ein eigenes Security Operations Team aufzubauen, sollten Sie die Lücke mit einem externen Spezialisten schließen – entweder direkt mit einem MDR-Anbieter mit 24/7-Abdeckung oder mit einem Managed Service Provider. Anbieter, die mithilfe von KI und Automatisierung mehr Vorfälle vollständig beheben können, werden zudem als Kraftmultiplikator wirken und dazu beitragen, Ihre Kompetenz- und Kapazitätslücken zu schließen.

Priorisieren Sie E-Mail Sicherheit. Da Phishing und Schad-E-Mails laut diesem Report mittlerweile die Hälfte aller Ursachen für Ransomware ausmachen, sollten Unternehmen und Organisationen moderne E-Mail-Filter einsetzen, DMARC-/DKIM-/SPF-Protokolle implementieren und in regelmäßige Phishing-Awareness-Trainings investieren. Der Wandel hin zu E-Mail-basierten Angriffen deutet darauf hin, dass technische Schwachstellen-Patches allein nicht ausreichen.

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.

Unterhalten Sie Exposure Management-Programme. Der Rückgang ausgenutzter Schwachstellen als Ursache um 14 % ist ermutigend, doch diese Angriffe bleiben ein wichtiger Angriffsvektor und werden wahrscheinlich zunehmen, da innovative KI-Modelle in der Lage sind, neue Schwachstellen schneller aufzuspüren. Unternehmen und Organisationen sollten einen straffen Zeitplan für die Installation von Patches einhalten und sich auf Schutzmaßnahmen wie Netzwerksegmentierung, Zero Trust Network Access sowie auf die Implementierung von MFA und kontinuierlicher Authentifizierung konzentrieren.

Reduzieren Sie die Exposition auf Firewall-Ebene und nutzen Sie Firewall-Telemetrie, um Angriffe frühzeitig zu erkennen. Stellen Sie sicher, dass Ihre Firewall schnelle – idealerweise automatisierte – Updates erhält, und minimieren Sie internetbasierte Dienste wie Admin-Zugriff und Benutzerportale. Verbinden Sie Firewalls mit XDR- und MDR-Lösungen, um Ransomware-Angriffe mithilfe von Firewall-Telemetriedaten zu erkennen, bevor Payloads ausgeführt werden.

Unterstützen Sie Cybersecurity-Teams bei der Bewältigung der Folgen. Da 99 % der betroffenen Teams Auswirkungen beklagten, sind die menschlichen Kosten von Ransomware nahezu allgegenwärtig. Unternehmen und Organisationen sollten klare Protokolle für die Unterstützung nach einem Vorfall festlegen und sicherstellen, dass die wachsende Anerkennung der Führungsetage zu nachhaltigen Investitionen in Mitarbeitende und nicht nur in Technologie führt.

Fazit

Der Ransomware-Report 2026 offenbart eine Bedrohungslandschaft im Wandel.

Es gibt echte Anzeichen für Fortschritte: Die Lösegeldforderungen und -zahlungen gehen zurück, die Wiederherstellung auf Basis von Backups hat ein nahezu rekordverdächtiges Niveau erreicht, und Unternehmen und Organisationen sind zunehmend erfolgreicher darin, die Bedingungen auszuhandeln, wenn sie doch zahlen. Der drastische Rückgang von Angriffen, bei denen Schwachstellen ausgenutzt werden, deutet darauf hin, dass sich die KI-gestützte Erkennung und die kontinuierlichen Investitionen in Patch-Management auszahlen.

Das vielleicht ermutigendste Signal, das sich aus den Daten ablesen lässt, ist die zunehmende Anerkennung von Cybersecurity-Teams durch die Führungsetage. Wenn die Führung Interesse zeigt, folgen Ressourcen. Die positiven operativen Entwicklungen in diesem Report – von einer verbesserten Backup-Nutzung bis hin zu besseren Verhandlungsergebnissen – könnten genau diese Dynamik widerspiegeln.

Gleichzeitig sind die verbleibenden Herausforderungen erheblich. Bei mehr als der Hälfte aller Ransomware-Angriffe gelingt es nach wie vor, Daten zu verschlüsseln; die Kosten für die Wiederherstellung belaufen sich im Durchschnitt auf 1,7 Mio. US$ pro Vorfall, und die Belastung für Cybersecurity-Teams ist nahezu allgegenwärtig.

Die Erkenntnis, dass zwei Drittel der Ransomware-Opfer ihren Vorfall auf eine Identitätskompromittierung **zurückführen konnten, unterstreicht, welche entscheidende Rolle Identitätssicherheit in der Abwehrkette gegen Ransomware spielt**. Unternehmen und Organisationen, die Identity als grundlegende Sicherheitsschicht und nicht als optional oder zweitrangig betrachten, sind besser in der Lage, Angriffe von vornherein zu verhindern.

Unternehmen und Organisationen müssen sich zudem auf **die entscheidendste Cybersecurity-Herausforderung des nächsten Jahrzehnts vorbereiten: KI-gestützte Bedrohungen**. Die Daten deuten bereits darauf hin, warum: 62 % der Opfer nannten eine bekannte oder unbekannte Sicherheitslücke als einen Faktor für ihren Angriff, und 58 % wiesen auf einen Mangel an Fachkräften oder Expertise hin. Beide Faktoren gewinnen zunehmend an Bedeutung, da KI die Geschwindigkeit und das Ausmaß von Angriffen erhöht und Angreifer KI nutzen, um Schwachstellen schneller aufzuspüren und Angriffe auf mehrere Kontrollpunkte in maschineller Geschwindigkeit zu koordinieren.

Die Tendenz, die sich aus den diesjährigen Ergebnissen abzeichnet – von den besseren Ergebnissen bei frühzeitiger Erkennung von Angriffen durch Firewalls bis hin zum starken Anstieg der auf Backups basierenden Wiederherstellung – weist in eine einheitliche Richtung: **Wenn Abwehrmaßnahmen nicht isoliert, sondern gemeinsam zum Einsatz kommen, verbessern sich die Ergebnisse**. Um die Lücke zu schließen, die durch Angriffe im KI-Zeitalter entstanden ist, kommt es weniger darauf an, weitere Tools hinzuzufügen, sondern vielmehr darauf, die bereits vorhandenen miteinander zu vernetzen, damit Kontextanalyse, Erkennung und Reaktion mit der Geschwindigkeit erfolgen können, die heutige Bedrohungen erfordern.

Unternehmen und Organisationen, die das Thema Ransomware kontinuierlich in den Fokus der Führungsetage rücken und gleichzeitig integrierte, KI-gestützte Abwehrsysteme einführen, werden in den kommenden Jahren am besten gegen Ransomware gewappnet sein – wobei sie nicht nur in Technologie und Prozesse investieren, sondern auch in die Mitarbeitenden, die diese Bedrohungen tagtäglich abwehren.

Methodologie

Diese Befragung wurde von Vanson Bourne im Auftrag von Sophos im ersten Quartal 2026 durchgeführt. 2.158 IT- und Cybersecurity-Verantwortliche aus Unternehmen und Organisationen, die in den letzten 12 Monaten von Ransomware betroffen waren, wurden in 17 Ländern befragt: USA, Brasilien, Chile, Kolumbien, Mexiko, Großbritannien, Frankreich, Deutschland, Italien, Spanien, Schweiz, Australien, Indien, Japan, Singapur, Südafrika und Vereinigte Arabische Emirate. Die Befragten stammten aus Unternehmen mit 100 bis 5.000 Mitarbeitern in 15 Branchen.

SOPHOS

Mehr über Ransomware und effektiven Schutz durch Sophos erfahren Sie auf unserer Website.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 58580
E-Mail: sales@sophos.de

2026-06-09 DE (DD)