SOPHOS

RANSOMWARE-REPORT 2025: ENTERPRISE-UNTERNEHMEN

Ergebnisse einer unabhängigen Befragung von 1.733 IT- und Cybersicherheits-Verantwortlichen aus Enterprise-Unternehmen, die im letzten Jahr von Ransomware betroffen waren.

Sophos-Whitepaper, Dezember 2025

Einführung

Willkommen beim ersten Sophos Ransomware-Report zu Enterprise-Unternehmen, der die aktuelle Bedrohungslage durch Ransomware für Enterprise-Unternehmen (mehr als 1000 Mitarbeitende) im Jahr 2025 aufzeigt.

Der Report geht darauf ein, wie sich die Erfahrungen von Enterprise-Unternehmen mit Ransomware im vergangenen Jahr verändert haben – sowohl bei den Ursachen als auch den Folgen. Außerdem werden die betrieblichen Rahmenbedingungen, die Angriffe auf Enterprise-Unternehmen ermöglichen, sowie die Auswirkungen auf Mitarbeitende in IT- und Cybersicherheits-Teams näher beleuchtet.

Für den Report wurden 1.733 IT- und Cybersicherheits-Verantwortliche aus 17 Ländern befragt, deren Unternehmen im letzten Jahr Opfer von Ransomware waren. Der Report bietet damit fundierte Einblicke in folgende Bereiche:

- Warum Enterprise-Unternehmen Opfer von Ransomware werden
- Auswirkungen auf Daten
- Lösegeldforderungen und -zahlungen

Informationen zu den Ergebnissen

Der Report basiert auf den Ergebnissen einer unabhängigen Befragung, die von Sophos in Auftrag gegeben wurde und die Erfahrungen von Unternehmen und Organisationen mit Ransomware untersucht. Die Befragung wurde zwischen Januar und März 2025 von einem spezialisierten Drittanbieter durchgeführt. Die Befragten arbeiten alle in Enterprise-Unternehmen mit 1.000 bis 5.000 Mitarbeitenden und wurden gebeten, die Fragen basierend auf ihren Erfahrungen der letzten 12 Monate zu beantworten.

Die 1.733 Befragten aus Enterprise-Unternehmen, die zum Report beigetragen haben, stammen aus 17 Ländern und 14 Branchen, sodass die Umfrageergebnisse ein breites und vielfältiges Spektrum an Erfahrungen widerspiegeln. Der Report beinhaltet zudem Vergleiche mit Ergebnissen vorheriger Erhebungen, wodurch eine direkte Gegenüberstellung über die Jahre hinweg ermöglicht wird. Alle Finanzdaten sind in US-Dollar angegeben.

Hinweis zu den Datumsangaben im Report

Um einen einfachen Vergleich der Daten unserer jährlichen Umfragen zu ermöglichen, benennen wir den Report nach dem Jahr, in dem die Studie durchgeführt wurde, in diesem Fall 2025. Uns ist bewusst, dass die Befragten ihre Erfahrungen aus dem vergangenen Jahr schildern, daher ereigneten sich viele der erwähnten Angriffe und deren Auswirkungen im Jahr 2024.

Wichtigste Erkenntnisse

Warum Enterprise-Unternehmen Opfer von Ransomware werden

- **Ausgenutzte Schwachstellen** sind die häufigste technische Ursache von Angriffen. Sie wurden in 29 % der Vorfälle zum Einfallstor. **Phishing** und **kompromittierte Zugangsdaten** folgten dicht dahinter und wurden jeweils bei 21 % der Vorfälle als Ursache genannt.
- Mehrere betriebliche Faktoren tragen dazu bei, dass Enterprise-Unternehmen Opfer von Ransomware werden. Die häufigste Ursache sind **unbekannte Sicherheitslücken**, die 40 % der Befragten als Grund nannten. Fast ebenso häufig wurden sowohl **zu wenig Personal/Kapazitäten** als auch **mangelnde Expertise** genannt, die bei jeweils 39 % der Angriffe zu den ursächlichen Faktoren zählten.

Auswirkungen auf Daten

- Die Datenverschlüsselungs-Quote in Enterprise-Unternehmen befindet sich auf dem niedrigsten Stand seit fünf Jahren: Nur noch **49 % der Angriffe führen zu einer Datenverschlüsselung**, verglichen mit einem Höchststand von 64 % im Jahr 2022.
- 30 % der Enterprise-Unternehmen, deren Daten verschlüsselt wurden, waren auch von einer Datenexfiltration betroffen.
- 96 % der Enterprise-Unternehmen, deren Daten verschlüsselt wurden, konnten sie wiederherstellen.
- Der Einsatz von Backups zur Wiederherstellung verschlüsselter Daten ist in Enterprise-Unternehmen auf dem niedrigsten Stand seit vier Jahren und erfolgt in 53 % der Vorfälle.
- **48 % der betroffenen Enterprise-Unternehmen zahlten das Lösegeld**, um ihre Daten zurückzuerhalten. Dies ist eine der niedrigsten Raten, die in der diesjährigen Umfrage verzeichnet wurden.

Lösegeldforderungen und -zahlungen

- Die durchschnittliche **Lösegeldforderung** (Medianwert) an Enterprise-Unternehmen ist im letzten Jahr um ein Drittel gesunken (56 %) und liegt 2025 bei **1.20 Mio. US$**, im Vergleich zu 2.75 Mio.US$ im Jahr 2024. Der Hauptgrund für diesen signifikanten Rückgang ist ein Rückgang der Lösegeldforderungen von 5 Mio. US$ oder mehr um 24 %: 2024 wurden noch 38 % der Lösegeldforderungen in dieser Höhe gestellt, im Jahr 2025 nur noch 29 %. Hierbei ist jedoch zu beachten, dass die Forderungen im Bereich zwischen 1 Mio. und 5 Mio. US$ um 17 % gestiegen sind.
- Auch die durchschnittliche **Lösegeldzahlung** von Enterprise-Unternehmen ist gesunken und liegt im Jahr 2025 bei **1 Mio. US$**, verglichen mit 1,26 Mio. US$ im Jahr 2024. Der Rückgang ist im Wesentlichen auf einen um 37 % gesunkenen Anteil der Lösegeldzahlungen von 5 Mio. US$ oder mehr zurückzuführen. Es sollte jedoch betont werden, dass es in nahezu allen Zahlungskategorien unter 5 Mio. US$ zu Steigerungen gekommen ist.
- Der **Anteil der von Enterprise-Unternehmen gezahlten Lösegeldforderung** sank von 95 % im Jahr 2024 auf 86 % im Jahr 2025.
- Bei genauer Gegenüberstellung **der Forderungen und Zahlungen** gaben knapp ein Drittel (31 %) der Enterprise-Unternehmen an, dass ihre Zahlung der ursprünglichen Forderung entsprach. 51 % zahlten weniger als die ursprüngliche Forderung, 18 % mehr.

Geschäftliche Folgen von Ransomware

- Die durchschnittlichen **Wiederherstellungskosten für Enterprise-Unternehmen** nach einem Ransomware-Angriff sanken im letzten Jahr um 41 % und liegen nun bei **1,84 Mio. US$**, im Vergleich zu 3,12 Mio.US$ im Jahr 2024.
- Betrachtet man die **Zeit bis zur kompletten Wiederherstellung**, so erholen sich Enterprise-Unternehmen immer schneller: 2025 war genau die Hälfte innerhalb einer Woche wieder komplett funktionsfähig, gegenüber 36 % im Jahr 2024.

Auswirkungen auf Mitarbeitende

Alle Enterprise-Unternehmen, deren Daten im letzten Jahr im Rahmen eines Angriffs verschlüsselt wurden, berichteten von direkten Auswirkungen auf das IT-/Cybersicherheits-Team:

- 40 % der IT- und Cybersicherheits-Teams berichteten von **erhöhtem Druck** seitens der Führungskräfte, 31 % von **mehr Anerkennung**.
- 39 % berichteten sowohl von einer anhaltenden **Zunahme der Arbeitsbelastung** als auch **von verstärkter Angst oder Stress** im Zusammenhang mit zukünftigen Angriffen.
- 37 % berichteten von **Veränderungen der Prioritäten/Fokusbereiche im Team**.
- Mehr als ein Drittel der Befragten (35 %) nannte sowohl **Schuldgefühle** darüber, dass der Angriff nicht gestoppt wurde, als auch **Veränderungen in der Team-/Organisationsstruktur** als Folgen des Vorfalls.
- In 31 % der Teams kam es zu **Fehlzeiten bei Mitarbeitenden** aufgrund von **Stress oder psychischen Problemen**, die direkt mit dem Angriff in Zusammenhang standen.
- In über einem Viertel der Fälle (27 %) wurde als Folge des Angriffs **die Teamführung ausgetauscht**.

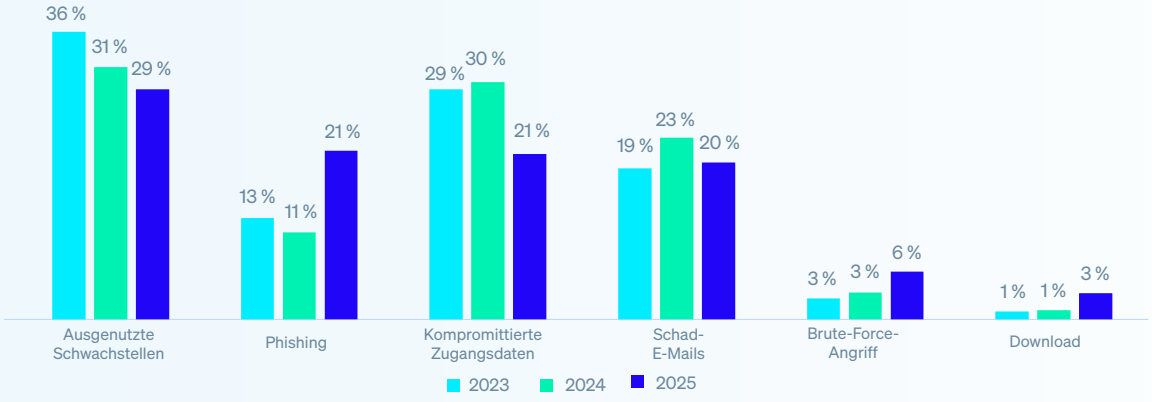
Warum Enterprise-Unternehmen Opfer von Ransomware werden

Technische Ursache von Angriffen auf Enterprise-Unternehmen

Zum dritten Mal in Folge identifizierten Enterprise-Unternehmen **ausgenutzte Schwachstellen** als Hauptursache für Ransomware-Angriffe; sie sind für 29 % der Vorfälle verantwortlich. **Phishing-E-Mails** belegten den zweiten Platz, wobei ihr Anteil von 11 % im Jahr 2024 auf 21 % im Jahr 2025 anstieg.

Auf ausgenutzten Zugangsdaten basierende Angriffe stellen weiterhin ein erhebliches Risiko dar. Die Meldungen von solchen Vorfällen sind jedoch deutlich zurückgegangen – von 30 % im Jahr 2024 auf 21 % im Jahr 2025. Im Gegensatz dazu nannten **kleine und mittlere Unternehmen** (mit 100 bis 250 Mitarbeitenden) auf ausgenutzten Zugangsdaten basierende Angriffe als Hauptursache für Ransomware-Angriffe; diese sind für fast ein Drittel (30 %) der Vorfälle verantwortlich.

Abbildung 1: Technische Ursachen von Ransomware-Angriffen auf Enterprise-Unternehmen, 2023–2025

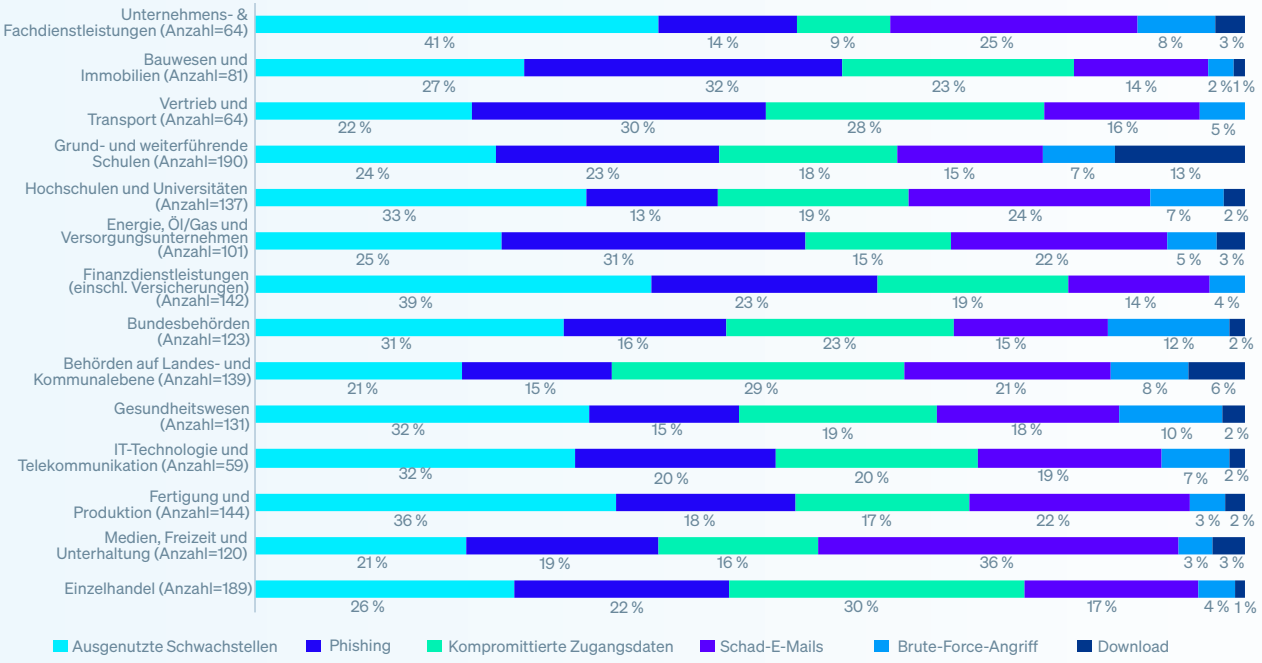


Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ja. Anzahl=1.733 (2025), 1.409 (2024), 1.045 (2023).

Die Untersuchung zeigt, dass die Ursachen zwar nach Branche variieren, ausgenutzte Schwachstellen jedoch für Enterprise-Unternehmen in nahezu allen Branchen ein wesentlicher Angriffsvektor sind. Erwähnenswerte Ausnahmen:

- **Phishing** war die am häufigsten genannte Ursache sowohl im **Bauwesen und Immobiliengewerbe** (32 %), **im Vertriebs- und Transportwesen** (30 %) als auch in **Energie, Öl/Gas und Versorgungsunternehmen** (31%).
- **Kompromittierte Zugangsdaten** wurden von Enterprise-Unternehmen im **Einzelhandel** als häufigster Angriffsvektor genannt, der für fast ein Drittel der Vorfälle (30 %) verantwortlich war.

Abbildung 2: Technische Ursache von Ransomware-Angriffen nach Branche

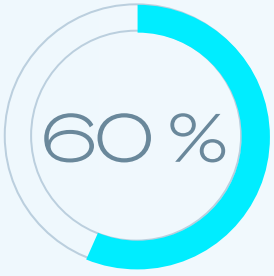


Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ja. Anzahl der erhaltenen Antworten jeweils in Klammer.

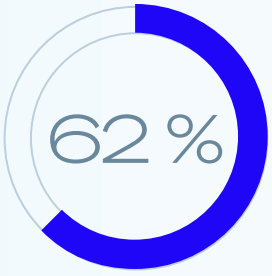
Organisatorische Ursachen von Vorfällen in Enterprise-Organisationen

Neben den technischen Ursachen der Vorfälle ist es auch wichtig, die organisatorischen Faktoren zu verstehen, die Enterprise-Unternehmen Angriffen ausgesetzt haben. Die Ergebnisse zeigen, dass die Opfer in Enterprise-Unternehmen typischerweise mit mehreren organisatorischen Herausforderungen konfrontiert sind. Die Befragten nannten im Durchschnitt drei Faktoren, die dazu beigetragen haben, dass sie Opfer eines Ransomware-Angriffs wurden.

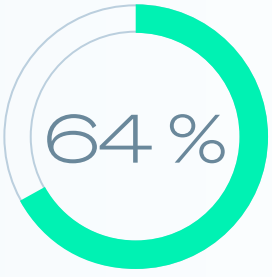
Dabei lässt sich keine einzelne Hauptursache ausmachen: Die Ursachen sind nahezu gleich häufig unzureichender Schutz, fehlende Ressourcen und Sicherheitslücken. Bei Enterprise-Unternehmen ist es jedoch etwas wahrscheinlicher, dass eine (bekannte oder unbekannte) Sicherheitslücke als Hauptgrund genannt wird.



MANGELHAFTER/ SCHLECHTER SCHUTZ
Mangelnder Schutz oder unzureichende Schutzlösungen, die den Angriff nicht stoppen konnten



MANGEL AN PERSONAL/ EXPERTISE
Fehlende menschliche Expertise (Fachwissen oder Kapazitäten) zur rechtzeitigen Erkennung und Abwehr des Angriffs



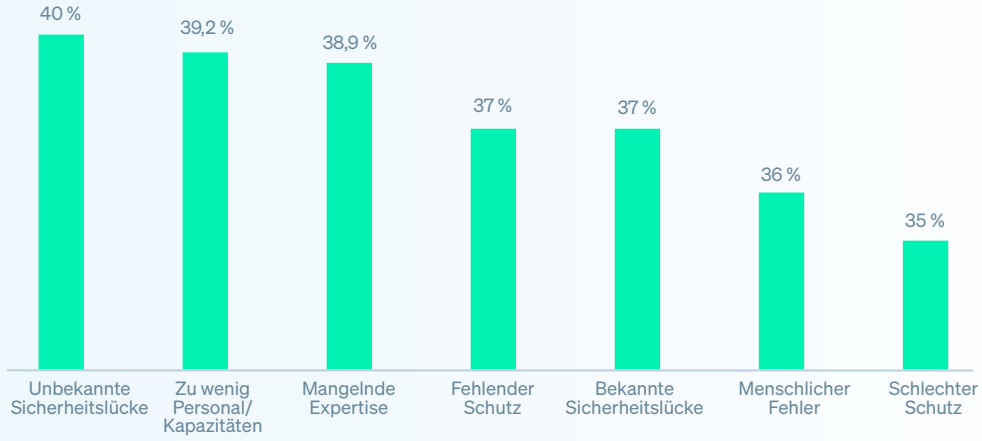
SICHERHEITSLÜCKE (BEKANNT/UNBEKANNT)
Bekannte oder unbekannte Schwachstelle in ihrer Abwehr

Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Anzahl=1.733 Zusammengefasste Antworten.

Unbekannte Sicherheitslücken (d. h. Schwächen in den Abwehrmechanismen, die den Befragten nicht bewusst waren) sind der am häufigsten genannte individuelle Grund; 40 % der Befragten aus Enterprise-Unternehmen nannten ihn. Mit jeweils 39 % wurden von Enterprise-Unternehmen fast ebenso häufig sowohl **zu wenig Personal/Kapazitäten** (d. h. eine unzureichende Anzahl von Cybersecurity-Experten, die die Systeme zum Zeitpunkt des Angriffs überwachten) als auch **mangelnde Expertise** (d. h. unzureichende Fähigkeiten oder Kenntnisse, um den Angriff rechtzeitig zu erkennen und zu stoppen) als ursächliche Faktoren genannt.

Interessanterweise nannten auch **KMUs zu wenig Personal/Kapazitäten** als häufigen Faktor: 42 % gaben dies als Hauptgrund dafür an, Opfer eines Angriffs geworden zu sein. Dies unterstreicht, dass Ressourcenengpässe unabhängig von der Unternehmensgröße eine weit verbreitete Herausforderung darstellen.

Abbildung 3: Operative Ursache von Ransomware-Angriffen auf Enterprise-Organisationen



Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Anzahl=1.733

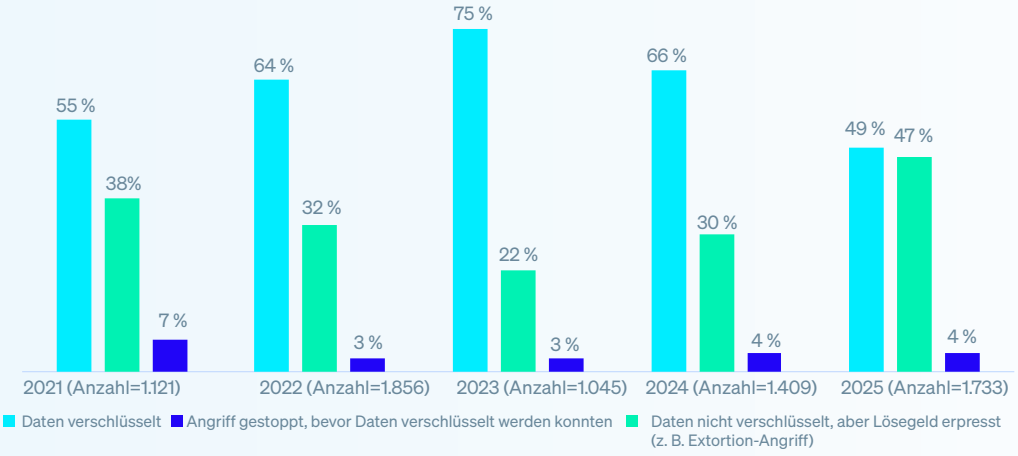
Auswirkungen auf Daten

Datenverschlüsselung in Enterprise-Unternehmen

Erfreulicherweise ist die Datenverschlüsselungs-Quote in Enterprise-Unternehmen so niedrig wie nie zuvor in den fünf Jahren unserer Ransomware-Studie: Bei weniger als der Hälfte (49 %) der Angriffe werden Daten verschlüsselt, im Vergleich zu 66 % im Jahr 2024.

Der Anteil der Ransomware-Angriffe, die vor der Datenverschlüsselung gestoppt werden konnten, hat sich in den letzten zwei Jahren mehr als verdoppelt und ist von 22 % im Jahr 2023 auf 47 % im Jahr 2025 gestiegen. Diese Entwicklung lässt darauf schließen, dass es Enterprise-Unternehmen immer besser gelingt, Angriffe zu erkennen und zu stoppen, bevor diese ernsthaften Schaden anrichten.

Abbildung 4: Datenverschlüsselungs-Quote bei Ransomware-Angriffen auf Enterprise-Unternehmen, 2021–2025

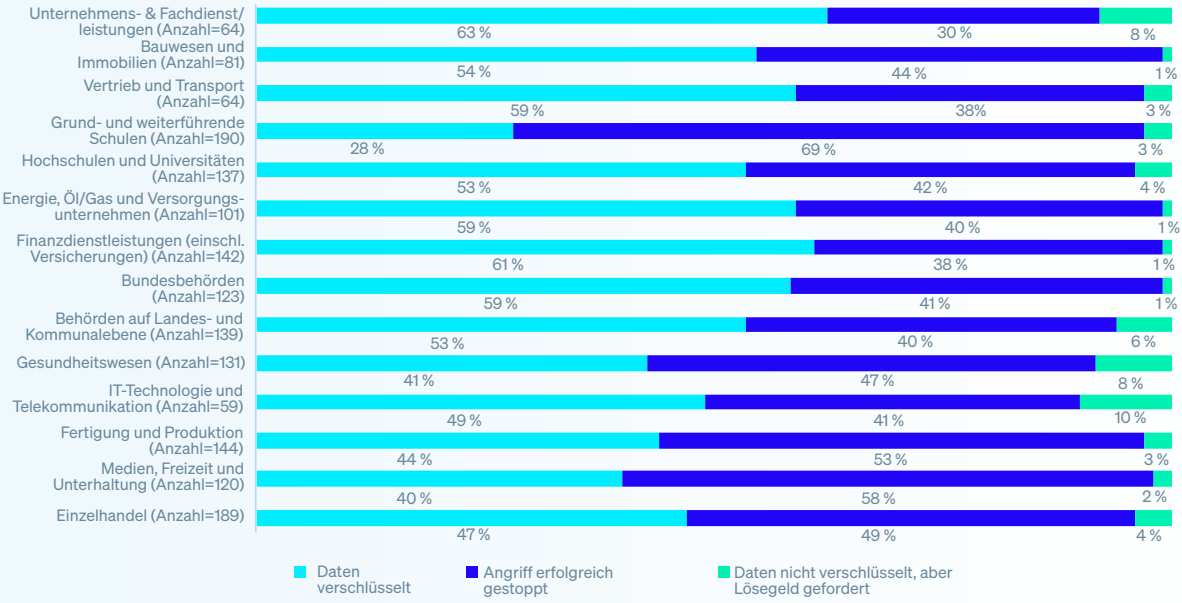


Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Anzahl der erhaltenen Antworten jeweils in Klammer.

Datenverschlüsselungs-Quote nach Branche

Bei Enterprise-Unternehmen im Bereich **Unternehmens- & Fachdienstleistungen** ist die Wahrscheinlichkeit am höchsten, dass Daten verschlüsselt werden (63%). Dies deutet darauf hin, dass Unternehmen in dieser Branche geringere Erfolgsquoten bei der Erkennung und Verhinderung von Angriffen vor der Verschlüsselung aufweisen und/oder weniger in der Lage sind, schädliche Verschlüsselungen zu blockieren und rückgängig zu machen. Im Gegensatz dazu meldeten **Grund- und weiterführende Schulen** die niedrigste Datenverschlüsselungs-Quote von lediglich 28 %.

Abbildung 5: Datenverschlüsselungs-Quote in Enterprise-Unternehmen nach Branche



Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Anzahl der erhaltenen Antworten jeweils in Klammer.

Datendiebstahl

Cyberkriminelle verschlüsseln nicht nur Daten – sie stehlen sie. In Enterprise-Unternehmen erlebten 15 % aller Ransomware-Opfer und 30 % derjenigen, deren Daten verschlüsselt wurden, einen Datendiebstahl. Eine Aufschlüsselung der Daten nach Branche liefert folgendes Ergebnis:

- Mit 52 % waren Enterprise-Unternehmen aus der **Medien-, Freizeit- und Unterhaltungsbranche** besonders häufig von Datenverschlüsselung betroffen, die gleichzeitig mit Datendiebstahl einherging.
- Im Gegensatz dazu waren nur 11 % der Enterprise-Unternehmen im **Bauwesen und Immobiliengewerbe** neben Verschlüsselung auch von Datendiebstahl betroffen.

Extortion-Angriffe

Wie aus Abbildung 4 hervorgeht, blieb der Anteil der Enterprise-Unternehmen, deren Daten nicht verschlüsselt wurden, von denen jedoch trotzdem Lösegeld gefordert wurde, im Jahresvergleich konstant bei 4 %. Betrachtet man die einzelnen Branchen, so waren Unternehmen aus dem Bereich **IT-Technologie und Telekommunikation** mit 10 % am stärksten von dieser Angriffsart betroffen, während Enterprise-Unternehmen aus **den Bereichen Bauwesen und Immobilien, Energie, Öl und Gas sowie Versorgungsunternehmen, Finanzdienstleistungen und Bundesbehörden** am wenigsten betroffen waren und jeweils nur 1 % meldeten.

Insgesamt waren **Grund- und weiterführende Schulen** am besten in der Lage, die Folgen eines Ransomware-Angriffs erfolgreich zu verhindern (d. h. die Verschlüsselung von Daten zu stoppen, Datenexfiltration zu verhindern und sich vor Erpressung zu schützen). Dies lässt darauf schließen, dass sich Grund- und weiterführende Schulen als überraschend effektiv bei der Erkennung und Intervention erweisen – selbst mit begrenzten Budgets.

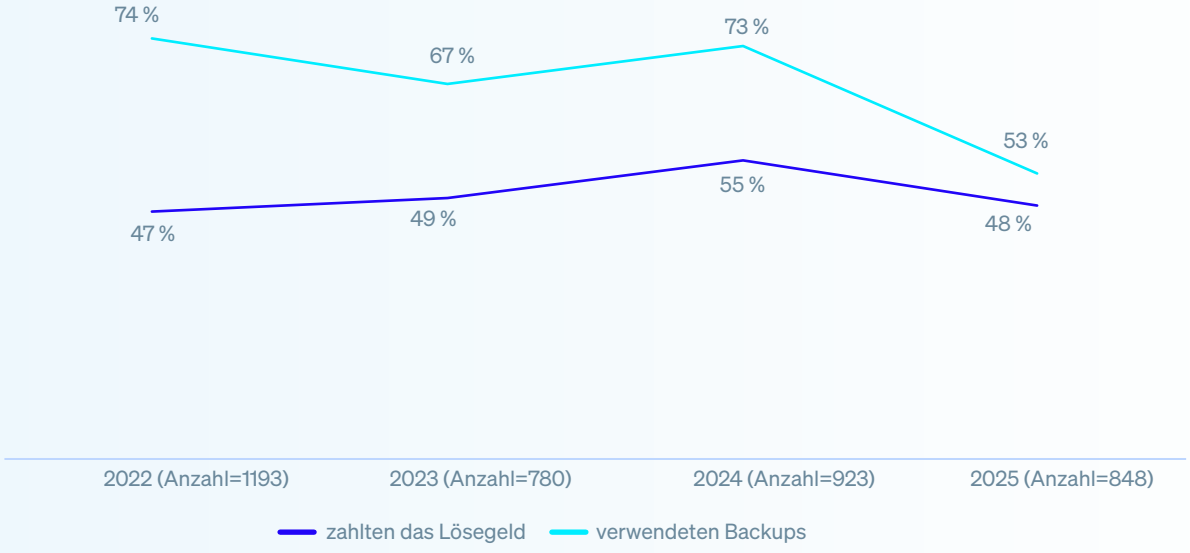
Wiederherstellung verschlüsselter Daten in Enterprise-Organisationen

96 % der Enterprise-Unternehmen, deren Daten verschlüsselt wurden, konnten diese wiederherstellen.

Im Jahr 2025 **zahlten 48 % der Enterprise-Unternehmen das Lösegeld, um ihre Daten zurückzuerhalten** – ein Rückgang gegenüber 55 % im Jahr 2024. Gleichzeitig sank **die Nutzung von Backups** deutlich auf den niedrigsten Stand seit vier Jahren (53 %, gegenüber 73 % im Jahr 2024). Zusammengenommen deuten diese Ergebnisse auf eine stärkere Widerstandsfähigkeit gegenüber den Forderungen hin, verbunden mit Schwächen und mangelnder Resilienz.

Darüber hinaus deutet die sich verringernde Kluft zwischen Enterprise-Unternehmen, die Lösegeld zahlen, um Daten wiederherzustellen, und solchen, die Backups zur Datenwiederherstellung nutzen, auf eine zunehmende Abhängigkeit von mehreren/alternativen Wiederherstellungsmethoden hin. Als Beleg dafür stellten wir fest, dass fast ein Drittel (30 %) der Enterprise-Unternehmen, deren Daten verschlüsselt wurden, angaben, **andere Methoden zur Wiederherstellung ihrer Daten verwendet zu haben.** Alternative Methoden können beispielweise die Wiederherstellung aus Schattenkopien, die Nutzung von Rollback-Funktionen in Endpoint-Schutz-Lösungen oder die Datenwiederherstellung von nicht betroffenen Systemen umfassen.

Abbildung 6: Wiederherstellung verschlüsselter Daten in Enterprise-Unternehmen, 2021–2025



Erhielt Ihr Unternehmen Daten wieder zurück? Ja, wir haben das Lösegeld gezahlt und unsere Daten zurückerhalten; Ja, wir haben Backups genutzt, um die Daten wiederherzustellen. Anzahl der erhaltenen Antworten jeweils in Klammer.

Lösegeldforderungen

Lösegeldforderungen an Enterprise-Unternehmen

Die durchschnittliche Lösegeldforderung (Medianwert) an Enterprise-Unternehmen sank im letzten Jahr um ein Drittel (56 %) und liegt 2025 bei 1.20 Mio. US$, im Vergleich zu 2.75 Mio.US$ im Jahr 2024. Sinkende Lösegeldforderungen an Enterprise-Unternehmen sind im Wesentlichen auf einen Rückgang von Lösegeldforderungen in Höhe von 5 Mio. US$ oder mehr um 24 % im letzten Jahr zurückzuführen. Allerdings ist zu beachten, dass der Anteil von Lösegeldforderungen zwischen 1 Mio. US$ und 5 Mio. US$ um 17 % gestiegen ist – und insgesamt 27 % aller Lösegeldforderungen ausmacht – gegenüber 23 % im Jahr 2024.

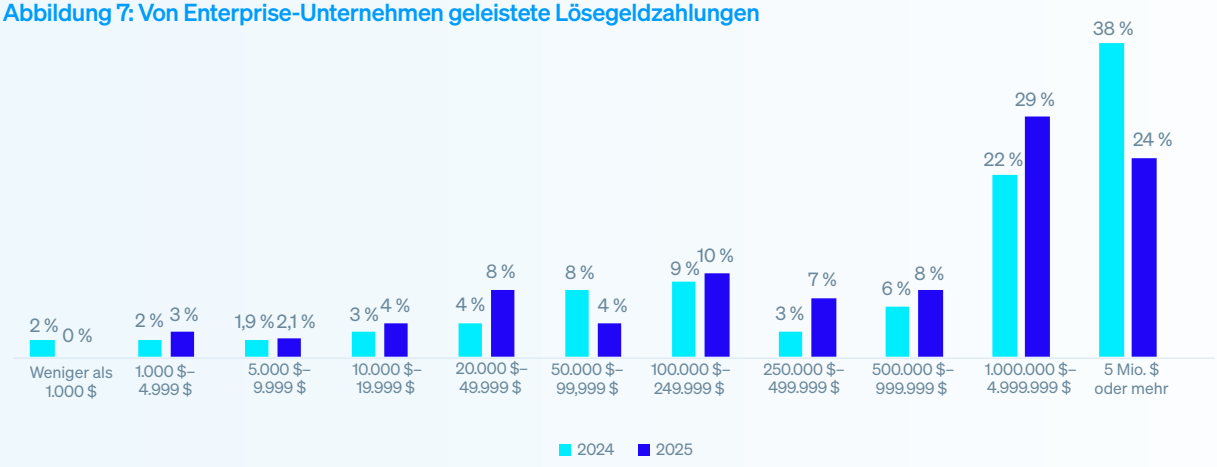
Lösegeldzahlungen von Enterprise-Unternehmen

Diesem Trend folgend sank auch das durchschnittliche Lösegeld (Medianwert), das von Enterprise-Unternehmen gezahlt wurde, von 1,26 Mio. US$ im Jahr 2024 auf nur noch 1 Mio. US$ im Jahr 2025. Dies ist vor allem auf einen 37%igen Rückgang der Zahlungen von 5 Mio. US$ oder mehr im letzten Jahr zurückzuführen. Der Report zeigte jedoch, dass es in fast allen Zahlungskategorien unter 5 Mio. US$ jährliche Steigerungen gab.

Diese Muster lassen darauf schließen, dass die Angreifer von den höchsten Lösegeldforderungen abrücken und stattdessen Enterprise-Unternehmen mit moderateren Forderungen ins Visier nehmen, wobei sie Beträge wählen, die zwar immer noch Schaden anrichten, aber realistischerweise auch bezahlt werden können.

Bei KMUs war ein ähnliches Muster zu beobachten, allerdings war der Rückgang bei den Forderungen und Zahlungen noch signifikanter. Die durchschnittlichen Lösegeldforderungen und -zahlungen sanken deutlich von 2 Mio. US$ im Jahr 2024 auf 126.000 US$ bzw. 200.000 US$ im Jahr 2025. Dies unterstreicht den allgemeinen Trend, dass Angreifer ihren Fokus auf Summen verlagert haben, die für Unternehmen und Organisationen jeder Größe erschwinglich sind.

Abbildung 7: Von Enterprise-Unternehmen geleistete Lösegeldzahlungen

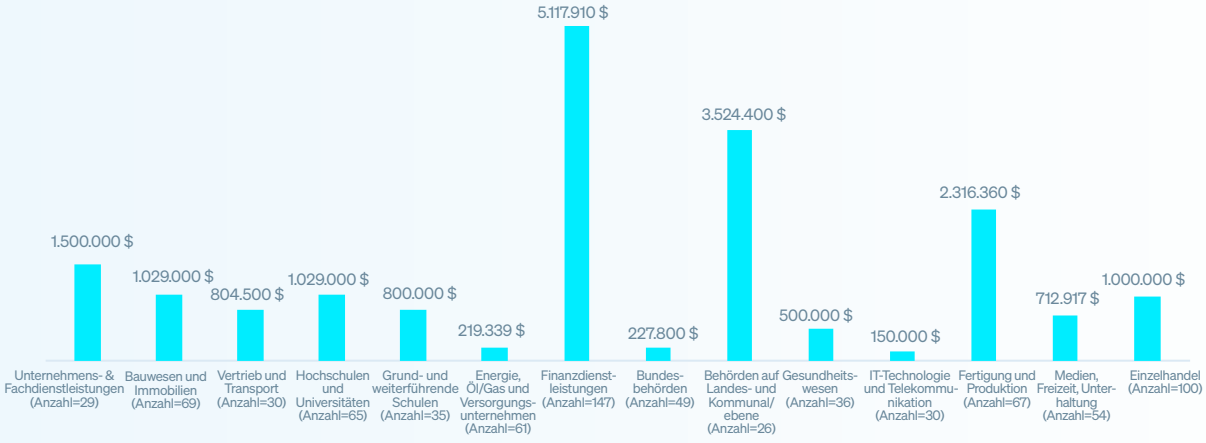


Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl=414 (2025), 470 (2024)

Lösegeldzahlungen nach Branche

Die Lösegeldzahlungen variierten je nach Branche erheblich, wobei Enterprise-Unternehmen im Finanzdienstleistungssektor mit durchschnittlich 5,1 Mio. US$ den höchsten Betrag (Medianwert) an Angreifer zahlten. Dies könnte an den hohen operativen Risiken und der geringen Toleranz gegenüber Störungen in dieser Branche liegen, wodurch Angreifer darauf vertrauen können, dass höhere Zahlungen eher in Betracht gezogen werden.

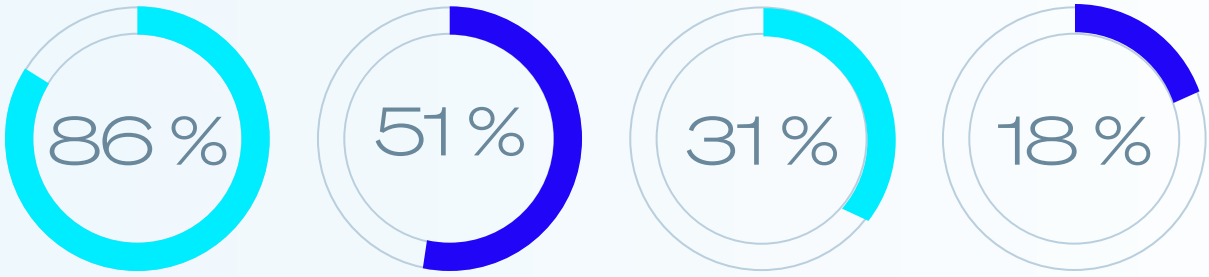
Abbildung 8: Lösegeldzahlungen nach Branche



Wie viel Lösegeld wurde den Angreifern gezahlt? Anzahl der erhaltenen Antworten jeweils in Klammer. Hinweis: Bei Zahlen unter 30 sollten die Ergebnisse nur als Richtwerte betrachtet werden.

Ursprüngliche Forderungen an Enterprise-Unternehmen und tatsächliche Zahlungen

414 Enterprise-Unternehmen, die Lösegeld zahlten, gaben sowohl die Höhe der ursprünglichen Forderung als auch der tatsächlichen Zahlung an: Im Durchschnitt zahlten sie 86 % der ursprünglichen Forderung. Ein erfreulicher Rückgang ggü. 95 % im Jahr 2024. Insgesamt zahlten 51 % weniger, als ursprünglich gefordert wurde. 18 % zahlten mehr und knapp ein Drittel (31 %) zahlte exakt das geforderte Lösegeld.



Gründe für die Differenz zwischen Lösegeldzahlung und ursprünglicher Forderung

Im Rahmen der Befragung wird auch untersucht, warum einige Enterprise-Unternehmen mehr zahlen als ursprünglich gefordert und andere weniger – eine wichtige Frage bei der Analyse von Ransomware-Angriffen.

72 Enterprise-Unternehmen, die **mehr zahlten** als ursprünglich gefordert, sagten Folgendes:

- 61 % Die Angreifer dachten, dass wir es uns leisten konnten, mehr zu zahlen.
- 49 % Die Angreifer erkannten, dass wir ein wertvolles Ziel sind.
- 42 %: Unsere Backups sind fehlgeschlagen oder waren kaputt.
- 39 % Die Angreifer waren verärgert und haben ihren Preis erhöht.
- 31 % Wir haben nicht schnell genug gezahlt und der Preis wurde erhöht.

Enterprise-Unternehmen nannten üblicherweise zwei Faktoren dafür, dass sie sich entschieden, mehr zu zahlen. Das zeigt die verschiedenen Herausforderungen, die die Opfer bei ihrer Datenwiederherstellung haben.

214 Enterprise-Unternehmen, die **weniger zahlten** als ursprünglich gefordert, gaben Folgendes als Grund an:

- 49 % Wir konnten mit den Angreifern einen geringeren Betrag aushandeln.
- 46 %: Wir zahlten das Lösegeld besonders schnell und bekamen einen Rabatt.
- 45 %: Die Angreifer verringerten ihre Forderung, um uns zu einer Zahlung zu bewegen.
- 43 %: Die Angreifer verringerten ihre Forderung aufgrund Druck von außen (Medien oder Strafverfolgungsbehörden)
- 38 %: Eine Drittpartei konnte mit den Angreifern einen geringeren Betrag aushandeln.

Diese Gruppe berichtet außerdem von durchschnittlich zwei Faktoren, die zu einem geringeren Lösegeld führten. Das unterstreicht die komplexe Situation von Ransomware-Opfern.

Geschäftliche Folgen von Ransomware

Wiederherstellungskosten in Enterprise-Unternehmen

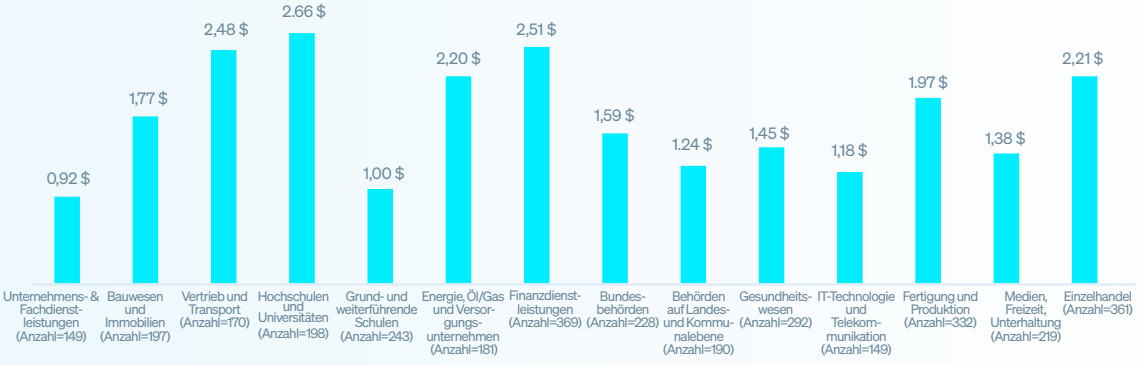
Die durchschnittlichen Wiederherstellungskosten für Enterprise-Unternehmen nach einem Ransomware-Angriff (ohne Lösegeldzahlung) sind auf den niedrigsten Stand seit drei Jahren gefallen und sanken im vergangenen Jahr um 41 % auf 1,84 Mio. US$, gegenüber 3,12 Mio. US$ im Jahr 2024. Dieser Wert liegt auch 330.000 US$ unter den 2023 gemeldeten 2,17 Millionen US$.

2023	2024	2025
2,17 Mio. $	3,12 Mio. $	1,84 Mio. $

Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwerwiegendsten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.), ohne Berücksichtigung gezahlter Lösegeldforderungen? Anzahl=1.733 (2025), 1.409 (2024), 1.045 (2023)

Bei Betrachtung der einzelnen Branchen fallen die Wiederherstellungskosten sehr unterschiedlich aus. **Grund- und weiterführende Schulen** meldeten mit 2,66 Mio. US$ die höchsten durchschnittlichen Kosten für die Behebung von Vorfällen. Im Gegensatz dazu meldeten Enterprise-Unternehmen im Bereich **Unternehmens- & Fachdienstleistungen** mit 0,92 Mio. US$ die niedrigsten Kosten. Diese Differenz dürfte zum Teil auf Unterschiede beim Aufwand zur Wiederherstellung der IT-Infrastruktur nach dem Angriff zurückzuführen sein. Grund- und weiterführende Schulen nutzen in der Regel ältere Lösungen als private Dienstleister.

Abbildung 9: Aufschlüsselung der Ransomware-Wiederherstellungskosten nach Branche (in Mio. US$)

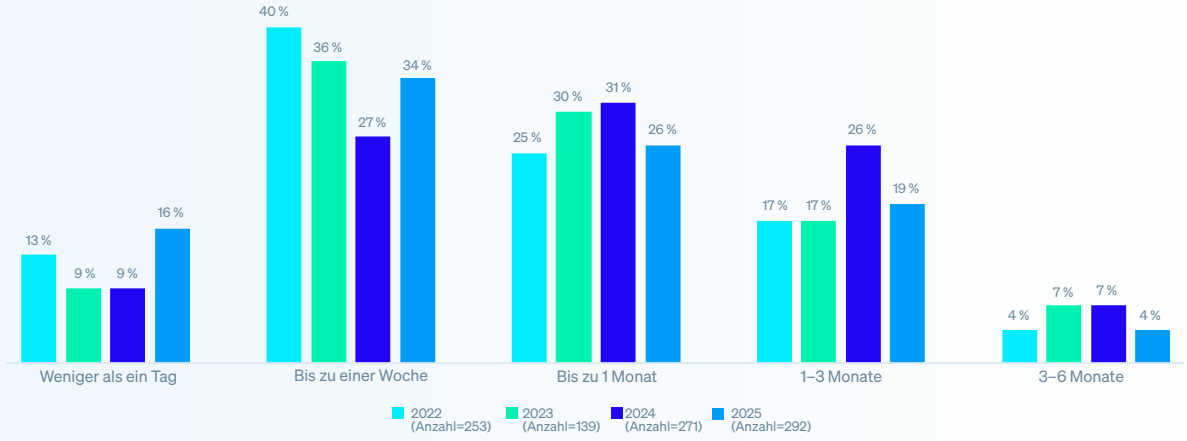


Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwerwiegendsten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.), ohne Berücksichtigung gezahlter Lösegeldforderungen? Anzahl der erhaltenen Antworten jeweils in Klammer.

Ausfallzeiten in Enterprise-Unternehmen

Die Daten zeigen, dass Enterprise-Unternehmen 2025 in der Lage waren, sich schneller von Ransomware-Angriffen zu erholen. Die Hälfte erholte sich innerhalb einer Woche, im Vergleich zu 36 % im Jahr 2024. Gleichzeitig sank der Anteil derer, die ein bis drei Monate zur kompletten Wiederherstellung benötigten, auf 19 %, gegenüber 26 % im Jahr 2024. Insgesamt erholten sich 95 % der betroffenen Enterprise-Unternehmen innerhalb von drei Monaten vollständig, was die wachsende Resilienz und die verbesserten Wiederherstellungsmöglichkeiten im gesamten Sektor unterstreicht.

Abbildung 10: Ausfallzeiten in Enterprise-Unternehmen nach Ransomware-Angriffen, 2022–2025



Wie lange hat es gedauert, bis sich Ihr Unternehmen vollständig von dem Ransomware-Angriff erholt hat? Anzahl der erhaltenen Antworten jeweils in Klammer.

Auswirkungen auf Mitarbeitende

Die Umfrage verdeutlicht, dass die Verschlüsselung von Daten durch einen Ransomware-Angriff erhebliche Auswirkungen auf die IT- und Cybersicherheits-Teams in Enterprise-Unternehmen hat. Alle Befragten gaben an, dass ihr Team in irgendeiner Weise betroffen war.

Abbildung 13: Auswirkungen verschlüsselter Daten auf IT- und Cybersicherheits-Teams

Welche Auswirkungen hatte der Ransomware-Angriff auf die Mitarbeitenden in Ihrem IT-/Cybersicherheits-Team (falls zutreffend)? Anzahl=848.

Empfehlungen

Obwohl sich die Erfahrungen von Enterprise-Unternehmen mit Ransomware im letzten Jahr mehrfach verändert haben, bleibt Ransomware eine erhebliche Bedrohung. Da Cyberkriminelle ihre Angriffe ständig weiterentwickeln, ist es unerlässlich, dass die Verteidiger und ihre Cyberabwehr mit Ransomware und anderen Bedrohungen Schritt halten. Nutzen Sie die Erkenntnisse des Reports, um Ihre Abwehr zu stärken, Ihre Reaktionsfähigkeit zu verbessern und die Auswirkungen von Ransomware auf Ihr Unternehmen und Ihre Mitarbeitenden zu minimieren. Konzentrieren Sie sich auf diese vier zentralen Handlungsfelder, um Angreifern einen Schritt voraus zu bleiben:

- **Prävention**. Die erfolgreichste Verteidigung gegen Ransomware ist es, wenn der Angriff gar nicht erst stattfindet – weil die Angreifer nicht in Ihr Unternehmen eindringen können. Ergreifen Sie Maßnahmen, um die im Report aufgezeigten technischen und betrieblichen Ursachen zu beseitigen.
- **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.
- Detection and Response. 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. Sorgen Sie für hochwertige Backups und üben Sie die Wiederherstellung von Daten, um im Fall der Fälle schnell wieder betriebsbereit zu sein.**

Sie möchten mehr darüber erfahren, wie Sophos Sie bei der Optimierung Ihrer Ransomware-Abwehr unterstützen kann? Kontaktieren Sie uns oder informieren Sie sich auf www.sophos.de

Erfahren Sie hier mehr über Ransomware und effektiven Schutz durch Sophos.

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.

2025-12-08 WP (MP)

SOPHOS