SOPHOS

RANSOMWARE-REPORT 2025

Ergebnisse einer unabhängigen Umfrage unter 3.400 IT- und Cybersicherheits-Verantwortlichen aus 17 Ländern, deren Unternehmen* im letzten 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

Einleitung

Die hier vorliegende sechste Ausgabe des jährlichen Sophos Ransomware-Reports gibt einen umfassenden Einblick in die aktuelle Bedrohungslage durch Ransomware im Jahr 2025.

Der Report zeigt, wie sich die Erfahrungen von Unternehmen mit Ransomware in den letzten zwölf Monaten verändert haben – sowohl bei den Ursachen als auch den Folgen. Außerdem werden bislang wenig untersuchte Aspekte näher beleuchtet, etwa betriebliche Rahmenbedingungen, die Angriffe ermöglichen, sowie die Auswirkungen auf Mitarbeitende in IT- und Cybersicherheits-Teams.

Für den Report wurden 3.400 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:

- Gründe, warum Unternehmen Opfer von Ransomware werden
- Auswirkungen auf Daten
- Lösegeldforderungen und -zahlungen
- Geschäftliche Folgen von Ransomware
- Auswirkungen auf Mitarbeitende

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 Umfrage durchgeführt wurde, in diesem Fall 2025. Da sich die Antworten der Befragten auf ihre Erfahrungen im vergangenen Jahr beziehen, fanden viele der erwähnten Angriffe bereits im Jahr 2024 statt.

Informationen zu den Ergebnissen

Der Report basiert auf den Ergebnissen einer von Sophos in Auftrag gegebenen unabhängigen Befragung zu Erfahrungen mit Ransomware in Unternehmen. Sie wurde von Januar bis März 2025 von einem spezialisierten Drittanbieter 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.

Die Befragung wurde mit Teilnehmenden in 17 Ländern und verschiedenen Branchen durchgeführt, sodass die Ergebnisse eine große Bandbreite unterschiedlicher Erfahrungen sowohl aus dem privaten als auch dem öffentlichen Sektor abbilden. Der Report beinhaltet zudem Vergleiche mit Ergebnissen aus den Reports der vorherigen Jahre. Alle Finanzdaten sind in US-Dollar angegeben.

Wichtigste Erkenntnisse

Gründe, warum Unternehmen Opfer von Ransomware werden

- Zum dritten Mal in Folge wurden als häufigste technische Angriffsursache **ausgenutzte Schwachstellen** genannt (in 32 % der Fälle).
- Mehrere betriebliche Faktoren tragen dazu bei, dass Unternehmen Opfer von Ransomware werden. Am häufigsten verantwortlich ist **mangelnde Expertise**, die 40,2 % der Befragten als Grund nannten. Fast ebenso häufig genannt wurden **unbekannte Sicherheitslücken**. Diese spielten in 40,1 % der Angriffe eine Rolle. Auf dem dritten Platz folgen mit 39,4 % **fehlendes Personal/fehlende Kapazitäten** als Grund für die Angriffe.

Auswirkungen auf Daten

- Die **Verschlüsselung von Daten** ist auf dem niedrigsten Stand seit sechs Jahren und spielt nur noch in 50 % der Angriffe eine Rolle – im Vergleich zu 70 % im Jahr 2024.
- 28 % der Unternehmen, deren Daten verschlüsselt wurden, hatten auch mit **Datenexfiltration** zu tun.
- 97 % derjenigen, deren Daten verschlüsselt wurden, konnten sie wiederherstellen.
- Der Einsatz von **Backups** zur Wiederherstellung verschlüsselter Daten ist auf dem niedrigsten Stand seit sechs Jahren und erfolgt in nur 54 % der Vorfälle.
- 49 % der Opfer **zahlten das Lösegeld**, um ihre Daten zurückzubekommen. Das ist zwar ein leichter Rückgang gegenüber dem Vorjahr (56 %), bleibt aber die zweithöchste Quote seit sechs Jahren.

Lösegeldforderungen und -zahlungen

- Die durchschnittliche **Lösegeldforderung** (Medianwert) ist im letzten Jahr um ein Drittel gesunken (34 %) und liegt 2025 bei 1.324.439 $, im Vergleich zu 2 Millionen $ im Jahr 2024.
- Die durchschnittliche **Lösegeldzahlung** (Medianwert) ist im letzten Jahr um 50 % gesunken und beträgt statt 2 Millionen $ im Jahr 2024 nur noch 1 Million $ im Jahr 2025. Dieser Rückgang ist primär darauf zurückzuführen, dass der Prozentsatz der Lösegeldzahlungen von 5 Millionen $ oder mehr von 31 % im Jahr 2024 auf 20 % im Jahr 2025 gesunken ist.
- Bei einem Vergleich der **Lösegeldforderungen und -zahlungen** sagten nur 29 %, dass ihre Zahlung der ursprünglichen Forderung entsprach. 53 % zahlten weniger als die ursprüngliche Forderung, 18 % mehr.

Geschäftliche Folgen von Ransomware

- Ohne Berücksichtigung gezahlter Lösegelder sanken die durchschnittlichen **Wiederherstellungskosten** nach einem Ransomware-Angriff im letzten Jahr um 44 % und liegen nun bei 1,53 Millionen $, im Vergleich zu 2,73 Millionen $ im Jahr 2024.
- Betrachtet man die **Zeit bis zur kompletten Wiederherstellung**, zeigt sich: Die Unternehmen werden schneller. 53 % waren nach einer Woche wieder vollständig arbeitsfähig, im Vergleich zu nur 35 % im Jahr 2024.

Auswirkungen auf Mitarbeitende

- Alle Unternehmen, deren Daten im letzten Jahr im Rahmen eines Angriffs verschlüsselt wurden, berichten von **direkten Auswirkungen** auf das IT-/Cybersicherheits-Team:
  - 41 % der IT-/Cybersicherheits-Teams sagen, dass sie unter **mehr Stress oder Angst** vor künftigen Angriffen leiden.
  - Ein Drittel (34 %) berichtet, dass das Team **sich schuldig fühlt**, den Angriff nicht rechtzeitig gestoppt zu haben.
  - 40 % erleben **mehr Druck** von ihren Führungskräften, während 31 % berichten, dass sie jetzt **mehr Anerkennung** erfahren.
  - 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 einem Viertel der Fälle wurde als Folge des Angriffs **die Teamführung ausgetauscht**.

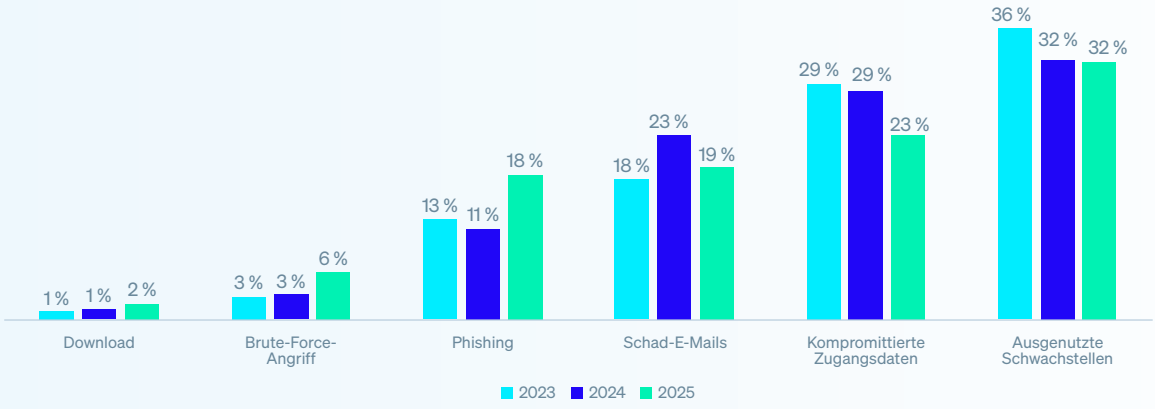
Gründe, warum Unternehmen Opfer von Ransomware werden

Technische Ursachen

Zum dritten Mal in Folge wurden **ausgenutzte Schwachstellen** als häufigste technische Ursache für Ransomware-Vorfälle genannt. Diese führten in 32 % der Fälle zu einem erfolgreichen Eindringen ins Unternehmen .

Der zweithäufigste Angriffsvektor sind weiterhin **kompromittierte Anmeldedaten**, auch wenn der Prozentsatz dieser Angriffsart von 29 % im Jahr 2024 auf 23 % im Jahr 2025 gesunken ist. Auch E-Mails bleiben weiterhin ein wichtiger Angriffsvektor: 19 % der Opfer nennen **schädliche E-Mails** als Ursache und weitere 18 % **Phishing**. Letzteres ist ein beachtlicher Anstieg im Vergleich zu 11 % im Vorjahr.

Abbildung 1: Technische Ursachen von Ransomware-Angriffen 2023–2025

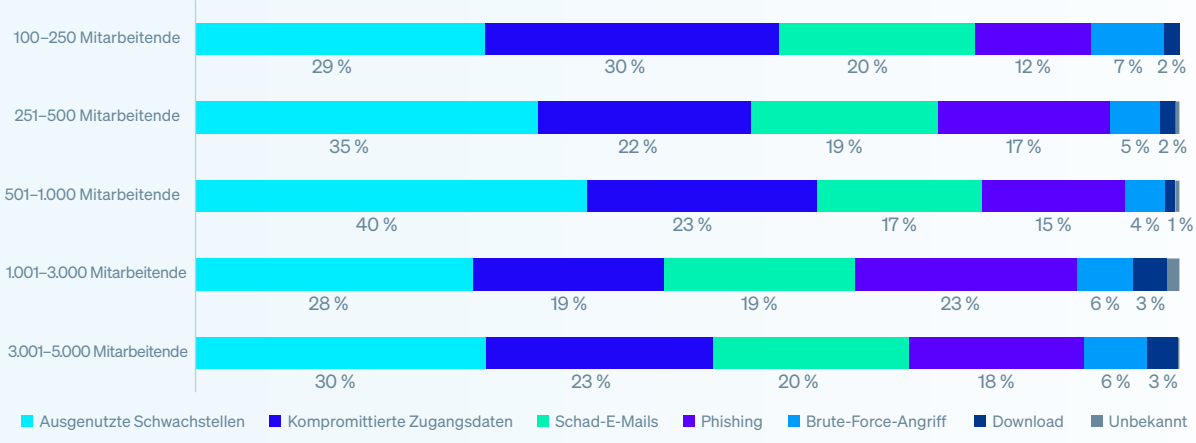


Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ja. Anzahl=3.400 (2025), 2.974 (2024), 1.974 (2023).

Die Untersuchungen zeigen Unterschiede in den Angriffsvektoren je nach Unternehmensgröße:

- **Kompromittierte Anmeldedaten** waren die häufigste Angriffsursache in Unternehmen mit 100 bis 250 Mitarbeitenden. Sie wurden in 30 % der Fälle zum Einfallstor.
- 40 % der Angriffe in Unternehmen mit 501 bis 1.000 Mitarbeitenden begannen mit einer **ausgenutzten Schwachstelle**.
- Fast ein Viertel (23 %) der Angriffe auf Unternehmen mit 1.001 bis 3.000 Mitarbeitenden begannen mit einer **Phishing-E-Mail**.

Abbildung 2: Technische Ursachen von Ransomware-Angriffen nach Unternehmensgröße

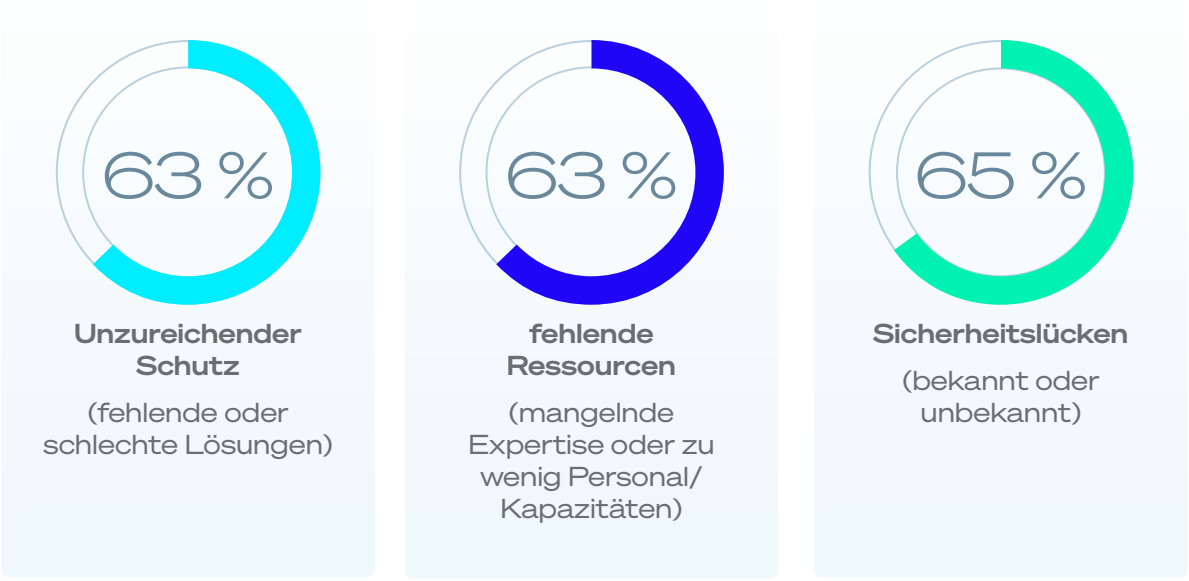


Kennen Sie die Ursache des Ransomware-Angriffs auf Ihr Unternehmen im vergangenen Jahr? Ja. Anzahl=3.400

Betriebliche Ursachen

Der diesjährige Report untersucht erstmals die betrieblichen Faktoren, die Unternehmen anfällig für Angriffe gemacht haben. Die Ergebnisse zeigen: Betroffene Unternehmen kämpfen in der Regel mit mehreren betrieblichen Herausforderungen – im Durchschnitt nannten die Befragten 2,7 Faktoren, die dazu beitrugen, dass sie Opfer des Angriffs wurden.

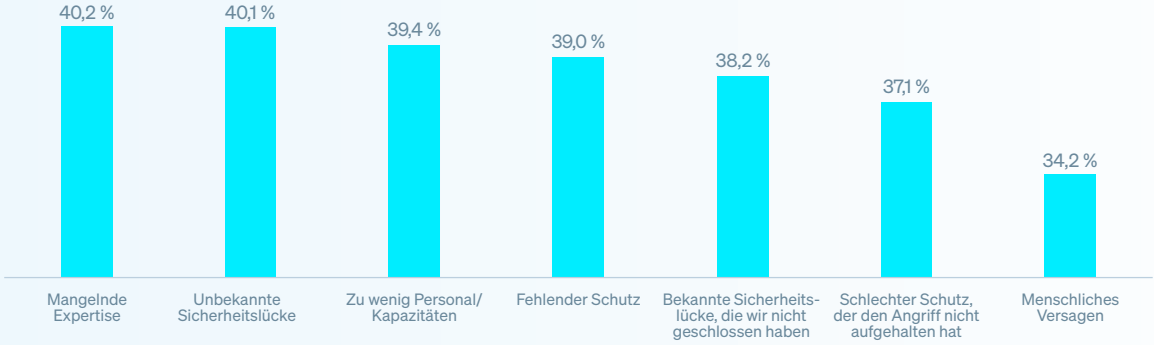
Dabei lässt sich keine einzelne Hauptursache ausmachen: Die Ursachen sind nahezu gleich häufig unzureichender Schutz, fehlende Ressourcen und Sicherheitslücken.



Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer des Ransomware-Angriffs? Anzahl=3.400

Mangelnde Expertise (nicht genug Fähigkeiten oder Kenntnisse zum rechtzeitigen Erkennen und Stoppen des Angriffs) wird als häufigste betriebliche Ursache genannt (von 40,2 % der Befragten). Fast ebenso häufig nannten die Befragten **Sicherheitslücken, von denen das Unternehmen nichts wusste**. In 40,1 % der Angriffe spielten diese eine Rolle. An dritter Stelle stehen **fehlendes Personal/ fehlende Kapazitäten** (nicht genug Cybersicherheits-Experten, die das System zum Zeitpunkt des Angriffs hätten überwachen können). Das trug in 39,4 % der Fälle zu den Angriffen bei.

Abbildung 3: Betriebliche Ursachen für Ransomware-Angriffe

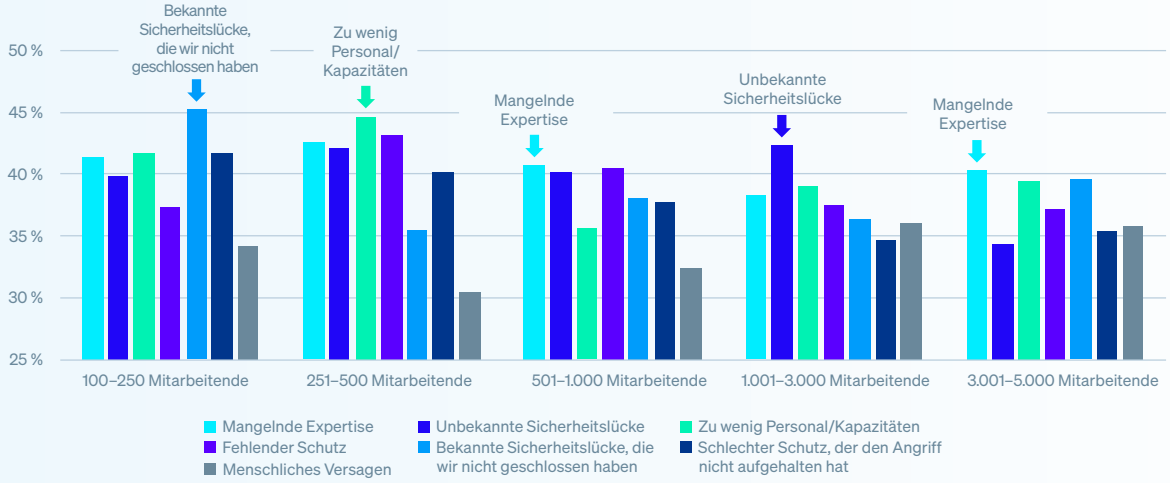


Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Anzahl=3.400

Betriebliche Ursachen nach Unternehmensgröße

Welcher betriebliche Faktor am häufigsten dazu führt, dass Unternehmen Opfer von Ransomware werden, hängt stark von der Unternehmensgröße ab – und spiegelt die jeweils unterschiedlichen Herausforderungen wider. In den fünf in diesem Report untersuchten Unternehmensgrößen nach Mitarbeitendenzahl standen vier verschiedene Herausforderungen an der Spitze der genannten Faktoren für erfolgreiche Angriffe, wie die folgende Abbildung zeigt.

Abbildung 4: Betriebliche Ursachen von Ransomware-Angriffen nach Unternehmensgröße



Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Anzahl=3.400 Aufgeteilt nach Unternehmensgröße (Mitarbeitendenzahl)

Betriebliche Ursachen nach Branche

Gleichermaßen variiert die häufigste betriebliche Ursache auch je nach Branche – und spiegelt damit die unterschiedlichen Herausforderungen der Unternehmen wider. Bemerkenswert ist: In keiner der untersuchten Branchen wurde menschliches Versagen als Hauptgrund für den erfolgreichen Angriff genannt.

Abbildung 5: Wichtigste betriebliche Ursachen für Ransomware-Angriffe nach Branche

MANGELNDE **EXPERTISE**	UNBEKANNTE **SICHERHEITSLÜCKE**	ZU WENIG **PERSONAL/KAPAZITÄTEN**	FEHLENDER **SCHUTZ**	BEKANNTE **SICHERHEITSLÜCKE**	SCHLECHTER **SCHUTZ**
Wir hatten nicht ausreichend Fähigkeiten oder Wissen, um den Angriff rechtzeitig zu erkennen und zu stoppen.	Wir hatten eine Schwachstelle in unserer Abwehr, die uns nicht bewusst war.	Wir hatten nicht ausreichend Cybersicherheits-experten, die unsere Systeme überwacht haben.	Wir hatten nicht die richtigen Cybersicherheits-Produkte und -Services.	Wir hatten mindestens eine Schwachstelle in unserer Abwehr, die wir kannten, aber nicht behoben hatten.	Unsere Cyber-sicherheits-Produkte und -Services konnten den Angriff nicht aufhalten.
Energie, Öl/Gas und Versorgungs-unternehmen (43 %)	Hochschulen (49 %)	Schulen (42 %)*	Finanzdienstleistungen, einschl. Versicherungen (44 %)*	Bundesbehörden (45 %)	Medien, Freizeit und Unterhaltung (41 %)
Schulen (42 %)*	Unternehmens- und Fachdienstleistungen (46 %)	Gesundheitswesen (42 %)	Behörden auf Landes- und Kommunalebene (40 %)	IT, Technologie und Telekommunikation (42 %)	Vertrieb und Transport (41 %)
Fertigung und Produktion (42 %)	Einzelhandel (46 %)			Bauwesen und Immobilien (41 %)*	
Bauwesen und Immobilien (41 %)*	Finanzdienstleistungen, einschl. Versicherungen (44 %)*				

* Gemeinsame wichtigste Angriffsursache

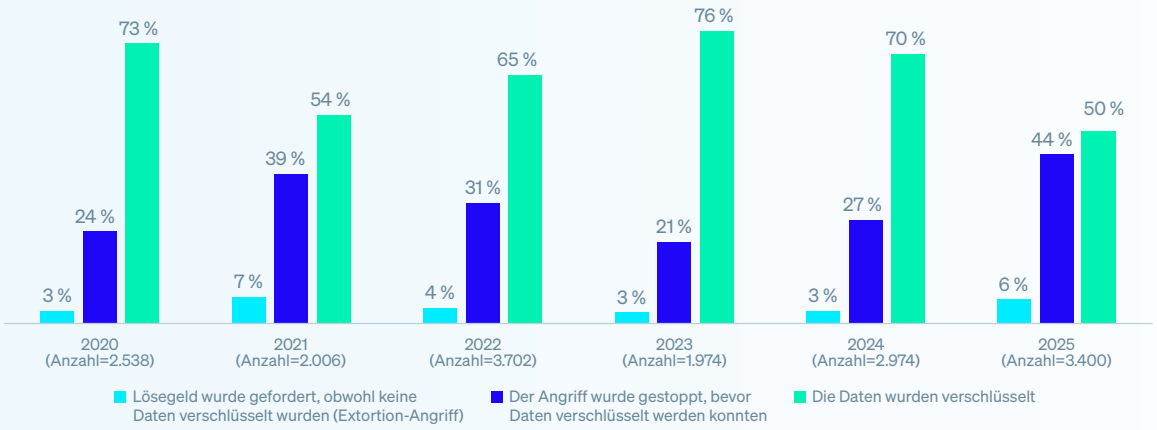
Warum wurde Ihr Unternehmen Ihrer Meinung nach Opfer eines Ransomware-Angriffs? Anzahl=3.400 Aufgeteilt nach Branche

Auswirkungen auf Daten

Datenverschlüsselung

Erfreulicherweise liegt der Anteil der Angriffe, bei denen Daten verschlüsselt wurden, so niedrig wie noch nie seit Beginn unserer Erhebung vor sechs Jahren: 50 % der Angriffe führten zu einer Verschlüsselung der Daten. Im Verlauf des letzten Jahres zeigt sich ein beachtlicher prozentueller Rückgang bei den Angriffen mit Datenverschlüsselung: Im Jahr 2024 lagen sie bei 70 %, im Jahr 2025 nur noch bei 50 %. Das lässt vermuten, dass die Unternehmen immer besser wissen, wie sie Angriffe stoppen, bevor es zu einer Verschlüsselung kommt.

Abbildung 6: Datenverschlüsselungs-Quote bei Ransomware-Angriffen 2020–2025



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

Die größten Unternehmen, die an unserer Umfrage teilnahmen, waren am häufigsten von Datenverschlüsselungen betroffen. In Unternehmen mit 3.001 bis 5.000 Mitarbeitenden kam es in 65 % der Angriffe zu einer Verschlüsselung – der höchste Wert unter allen untersuchten Unternehmensgrößen. Das deutet darauf hin, dass größere Unternehmen schlechter in der Lage sind als kleine, Angriffe rechtzeitig zu erkennen und zu stoppen und/oder Verschlüsselungen weniger gut zu blockieren und rückgängig zu machen.

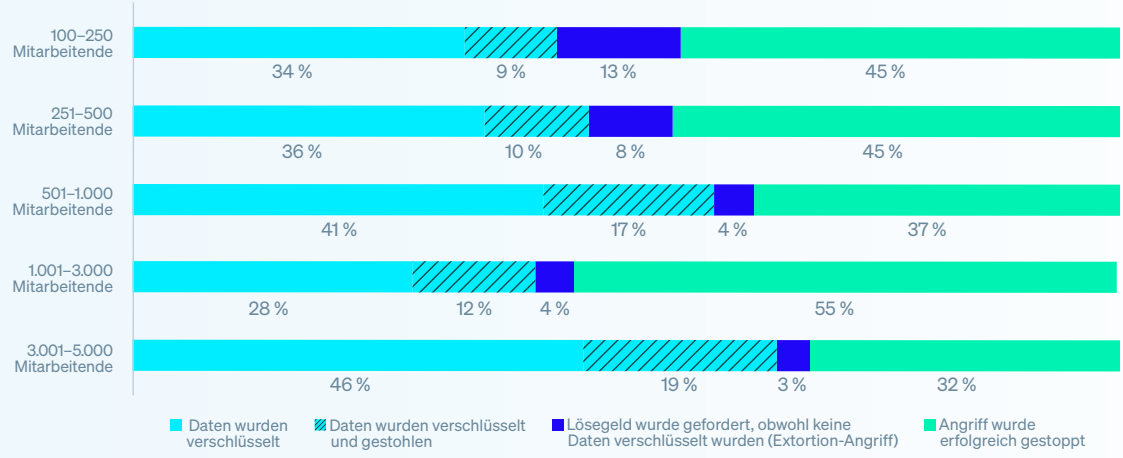
Datendiebstahl

Cyberkriminelle verschlüsseln Daten nicht nur – sie stehen sie auch. 14 % aller Ransomware-Opfer und 28 % derjenigen, deren Daten verschlüsselt wurden, erlebten einen Datendiebstahl. Sieht man sich die Daten nach Unternehmensgröße an, wird deutlich, dass in kleinen Unternehmen die Wahrscheinlichkeit eines Datendiebstahls um fast 40 % geringer ist.

- In 22 % der Unternehmen mit 100 bis 500 Mitarbeitenden, deren Daten verschlüsselt wurden, wurden auch Daten gestohlen.
- In 30 % der Unternehmen mit 501 bis 5.000 Mitarbeitenden, deren Daten verschlüsselt wurden, wurden auch Daten gestohlen.

Es ist zwar möglich, dass kleinere Unternehmen Datendiebstahl besser verhindern können als größere – wahrscheinlicher ist es jedoch, dass Angreifer in großen Unternehmen eher versuchen, Daten zu exfiltrieren und/oder dass kleinere Unternehmen weniger gut erkennen, dass Daten gestohlen wurden.

Abbildung 7: Datenverschlüsselungs-Quote bei Ransomware-Angriffen nach Unternehmensgröße



Konnten Cyberkriminelle bei dem Ransomware-Angriff Ihre Unternehmensdaten verschlüsseln? Anzahl=3.400

Extortion-Angriffe

Wie in Abbildung 6 zu sehen, hat sich der Prozentsatz der Unternehmen, deren Daten nicht verschlüsselt wurden, bei denen aber trotzdem Lösegeld erpresst wurde (Extortion), im letzten Jahr verdoppelt: 2024 war das nur bei 3 % der Unternehmen der Fall, im Jahr 2025 bereits bei 6 %. Bei kleineren Unternehmen ist die Wahrscheinlichkeit größer, nach Lösegeld gefragt zu werden, ohne dass die Daten verschlüsselt werden (Extortion-Angriff), als bei größeren Unternehmen:

- 13 % der Opfer mit 100 bis 250 Mitarbeitenden erlebten einen Extortion-Angriff.
- 3 % der Opfer mit 3.001 bis 5.000 Mitarbeitenden erlebten einen Extortion-Angriff.

Insgesamt gelingt es Unternehmen mit 1.001 bis 3.000 Mitarbeitenden am besten, die Folgen eines Ransomware-Angriffs erfolgreich abzuwehren – also Datenverschlüsselung zu verhindern, eine Datenexfiltration und Erpressungsversuche zu unterbinden. Möglicherweise sind diese Unternehmen aufgrund ihrer Größe gut aufgestellt: Sie sind so groß, dass sie über stärkere Sicherheitstools und mehr Expertise verfügen, haben aber nicht so komplexe Strukturen wie noch größere Unternehmen.

Wiederherstellung verschlüsselter Daten

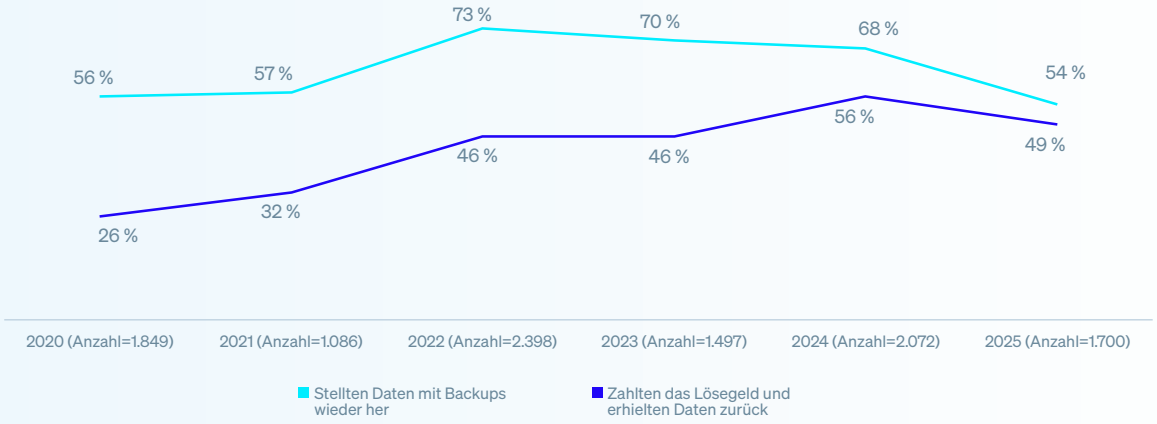
97 % der Unternehmen, deren Daten verschlüsselt wurden, konnten sie wiederherstellen.

Gut der Hälfte (54 %) gelang das mit Backups – im dritten Jahr in Folge ist diese Zahl gesunken. Insgesamt war die Zahl der Datenwiederherstellungen über Backups so niedrig wie seit sechs Jahren nicht.

Knapp die Hälfte (49 %) bezahlten das Lösegeld und erhielten ihre Daten zurück. Das ist zwar ein leichter Rückgang gegenüber dem Vorjahr (56 %), bleibt aber die zweithöchste Quote seit sechs Jahren.

29 % der Unternehmen, deren Daten verschlüsselt wurden, sagten, sie hätten zur Wiederherstellung der Daten andere Methoden genutzt. Dazu gehören vermutlich bereits veröffentlichte Entschlüsselungsschlüssel.

Abbildung 8: Datenwiederherstellung über Backups und Lösegeldzahlungen 2020–2025



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

Lösegeld

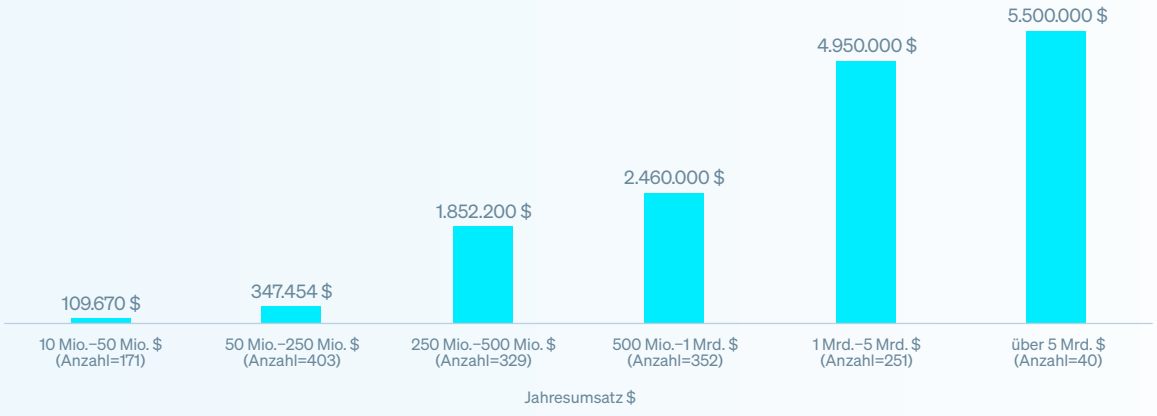
Lösegeldforderungen

Die durchschnittliche Lösegeldforderung (Medianwert) ist im letzten Jahr um ein Drittel gesunken (34 %) und liegt 2025 bei 1.324.439 $, im Vergleich zu 2 Millionen $ im Jahr 2024. Dieser Rückgang ist primär darauf zurückzuführen, dass der Prozentsatz der Lösegeldzahlungen von 5 Millionen $ oder mehr von 30 % auf 24 % gesunken ist. So erfreulich dieser Rückgang auch ist – man darf nicht außer Acht lassen, dass 57 % der Lösegeldforderungen bei einer Million US-Dollar oder mehr lagen.

Die Forderungen wachsen gemeinsam mit dem Umsatz des Unternehmens, was darauf hindeutet, dass die Angreifer die Höhe des Lösegelds daran festmachen, wie sicher sie sich sind, dass die Unternehmen wirklich zahlen können:

- 109.670 $: Lösegeldforderung (Medianwert) bei Unternehmen mit 10 bis 50 Millionen $ Jahresumsatz
- 5.500.000 $: Lösegeldforderung (Medianwert) bei Unternehmen mit über 5 Milliarden $ Jahresumsatz

Abbildung 9: Lösegeldforderungen nach Jahresumsatz der Unternehmen



Wie viel Lösegeld forderten die Angreifer? Anzahl der erhaltenen Antworten jeweils in Klammer.

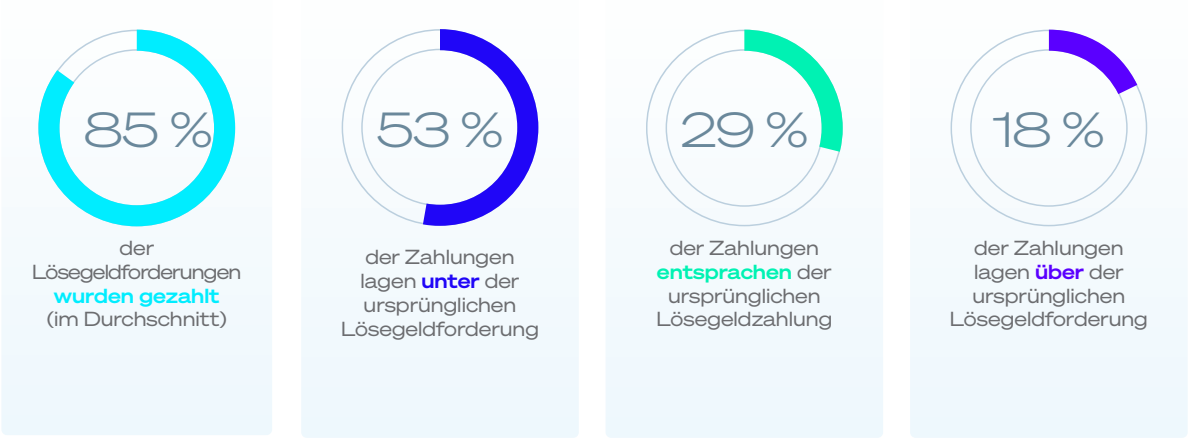
Lösegeldzahlungen

Die durchschnittliche Lösegeldzahlung (Medianwert) ist im letzten Jahr um 50 % gesunken – von 2 Millionen US-Dollar im Jahr 2024 auf 1 Million US-Dollar im Jahr 2025. Wie bei den Lösegeldforderungen ist der Hauptfaktor für den niedrigeren Medianwert der Rückgang bei besonders hohen Zahlungen: Der Anteil der Fälle mit Zahlungen von 5 Millionen US-Dollar oder mehr ging von 31 % im Jahr 2024 auf 20 % im Jahr 2025 zurück.

Damit ist sowohl die Höhe der Lösegeldforderungen als auch die Höhe der Zahlungen im letzten Jahr gesunken. Erfreulich ist die Tatsache, dass sich die Zahlungen am stärksten verringert haben. Dennoch: 1 Million US-Dollar bleibt eine beträchtliche Summe – mit weitreichenden Folgen für die meisten Unternehmen.

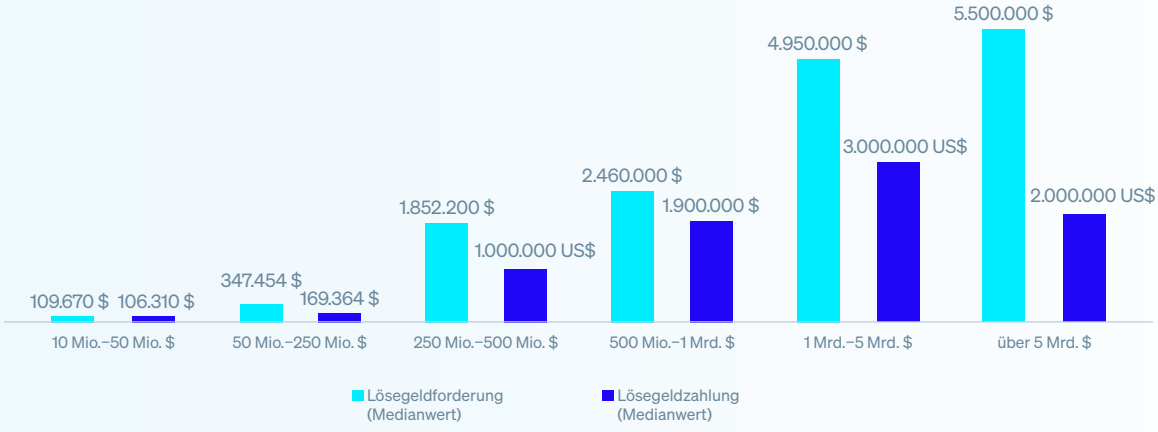
Ursprüngliche Forderungen und tatsächliche Zahlungen

826 Unternehmen, die Lösegeld zahlten, gaben sowohl die Höhe der ursprünglichen Forderung als auch der tatsächlichen Zahlung an: Im Durchschnitt zahlten sie 85 % der ursprünglichen Forderung. Insgesamt zahlten 53 % weniger, als ursprünglich gefordert wurde. 18 % zahlten mehr und 29 % zahlten exakt das geforderte Lösegeld.



Bei einer Aufschlüsselung der Daten nach Jahresumsatz zeigt sich, dass alle Umsatzgrößen im Durchschnitt weniger zahlten als ursprünglich gefordert. Am deutlichsten verringert war die Summe bei Unternehmen mit einem Jahresumsatz von 5 Milliarden US-Dollar oder mehr: Ihre durchschnittliche Zahlung lag – bei Ausschluss extremer Einzelwerte – bei 2 Millionen US-Dollar und damit bei lediglich 36 % der ursprünglichen Forderung von 5,5 Millionen US-Dollar. Am geringsten fiel die Differenz bei Unternehmen mit einem Jahresumsatz zwischen 10 und 50 Millionen US-Dollar aus: Deren Median-Zahlung entsprach 97 % der geforderten Summe.

Abbildung 10: Lösegeldforderung versus Lösegeldzahlung, aufgeteilt nach Jahresumsatz des Unternehmens



Wie viel Lösegeld forderten die Angreifer? Wie viel Lösegeld wurde den Angreifern gezahlt? (Anzahl=1.552/836)

Gründe für die Differenz zwischen Lösegeldzahlung und ursprünglicher Forderung

Dieses Jahr haben wir zum ersten Mal untersucht, warum einige Unternehmen mehr zahlen als ursprünglich gefordert und andere weniger – eine wichtige Frage bei der Analyse von Ransomware-Angriffen.

151 Unternehmen, die **mehr zahlten** als ursprünglich gefordert, sagten Folgendes:

- 50 %: Die Angreifer dachten, dass wir es uns leisten konnten, mehr zu zahlen.
- 48 %: Die Angreifer erkannten, dass wir ein wertvolles Ziel sind.
- 38 %: Die Angreifer waren verärgert und haben ihren Preis erhöht.
- 38 %: Unsere Backups sind fehlgeschlagen oder waren kaputt.
- 32 %: Wir haben nicht schnell genug gezahlt und der Preis wurde erhöht.

Die 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.

445 Unternehmen, die **weniger zahlten** als ursprünglich gefordert, gaben Folgendes als Grund an:

- 47 %: Wir konnten mit den Angreifern einen geringeren Betrag aushandeln.
- 45 %: Die Angreifer verringerten ihre Forderung aufgrund Druck von außen (Medien oder Strafverfolgungsbehörden).
- 45 %: Die Angreifer verringerten ihre Forderung, um uns zu einer Zahlung zu bewegen.
- 43 %: Wir zahlten das Lösegeld besonders schnell und bekamen einen Rabatt.
- 40 %: 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

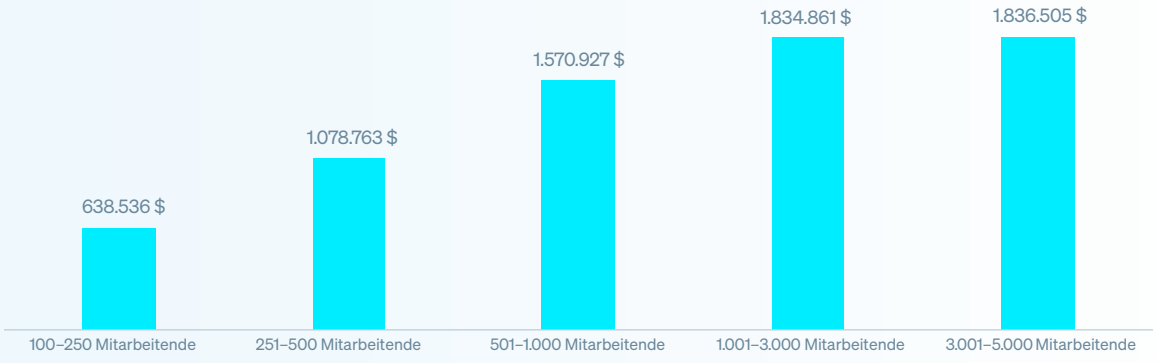
Die durchschnittlichen Kosten (Mittelwert) für die Wiederherstellung nach einem Ransomware-Angriff (neben Lösegeldzahlungen) sind im letzten Jahr um 44 % gesunken und betragen nun 1,53 Millionen $ im Vergleich zu 2,73 Millionen $ im Jahr 2024. Sie betragen gut 300.000 $ weniger als 2023.

2023	2024	2025
1,82 $ Millionen	2,83 $ Millionen	1,53 $ Millionen

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=3.400 (2025), 2.974 (2024), 1.974 (2023)

Die Wiederherstellungskosten steigen mit der Unternehmensgröße – bis sie sich bei Unternehmen mit 1.000 bis 5.000 Mitarbeitenden auf einem gleichbleibenden Niveau einpendeln. Unternehmen mit 100 bis 250 Mitarbeitenden melden durchschnittliche Wiederherstellungskosten von 638.536 $. Bei Unternehmen mit 1.000 bis 5.000 Mitarbeitenden entstanden Kosten in Höhe von 1,83 Millionen $.

Abbildung 11: Wiederherstellungskosten nach Ransomware-Angriff, aufgeteilt nach Unternehmensgröße

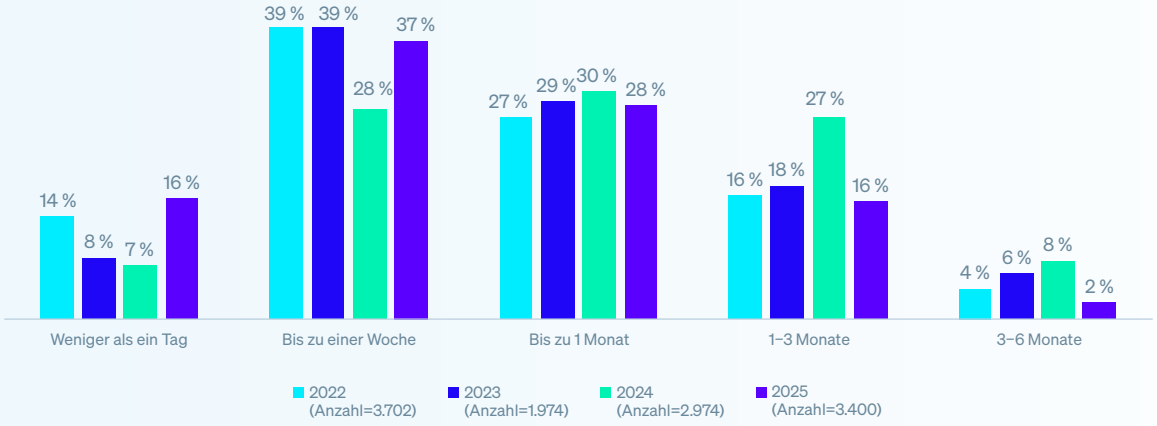


Wie hoch waren die ungefähren Kosten, die Ihrem Unternehmen durch den schwerwiegendsten Ransomware-Angriff entstanden sind (unter Berücksichtigung von Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangenen Geschäftschancen usw.), ohne Berücksichtigung gezahlter Lösegeldforderungen? Anzahl=3.400

Ausfallzeiten

Die Daten zeigen, dass Unternehmen ihre Daten immer schneller wiederherstellen können. Bei 16 % ist die vollständige Wiederherstellung nach einem Tag erfolgt, im Vergleich zu 7 % im Jahr 2024 und 8 % im Jahr 2023. Über die Hälfte (53 %) konnten all ihre Daten innerhalb einer Woche wiederherstellen. Auch hier handelt es sich um einen deutlichen Anstieg im Vergleich zu 35 % im Jahr 2024. Insgesamt hatten fast alle Opfer (97 %) ihre Daten drei Monate nach dem Angriff wiederhergestellt. Dieses schnellere Tempo bei Wiederherstellungen könnte darauf hindeuten, dass Unternehmen im letzten Jahr verstärkt in die Vorbereitung auf Cybervorfälle und in ihre Fähigkeiten im Bereich Wiederherstellung investiert haben.

Abbildung 12: Wiederherstellungszeit nach Ransomware-Angriffen 2022–2025



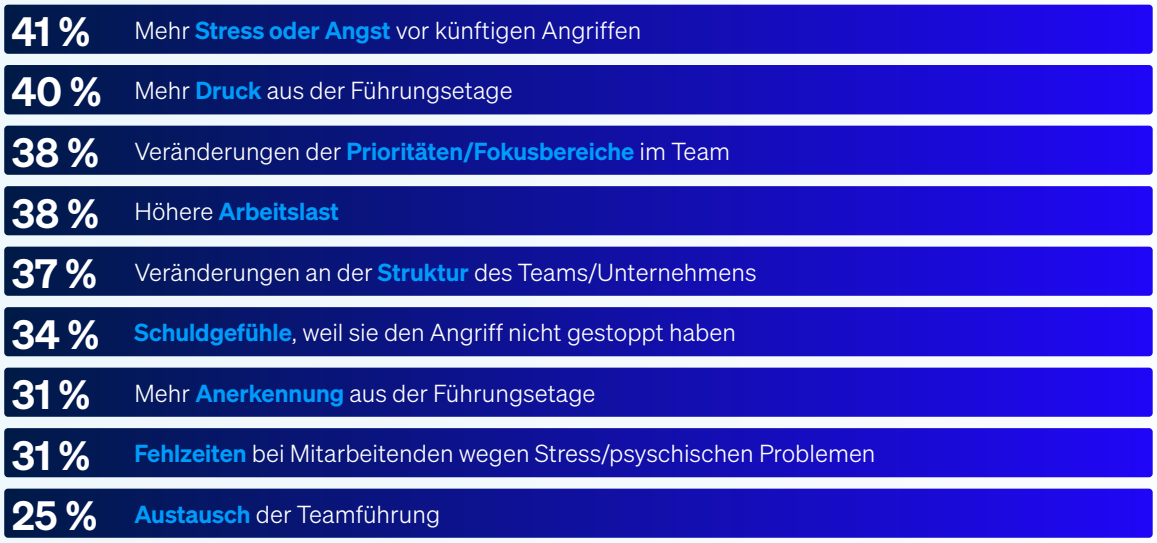
Wie lange hat es gedauert, bis sich Ihr Unternehmen vollständig von dem Ransomware-Angriff erholt hat? Anzahl der erhaltenen Antworten jeweils in Klammer

Wenig überraschend: Unternehmen, deren Daten verschlüsselt wurden, benötigten in der Regel mehr Zeit für die Wiederherstellung als solche, die eine Verschlüsselung rechtzeitig abwehren konnten: Nur 9 % der Unternehmen, deren Daten verschlüsselt wurden, hatten sie innerhalb eines Tages vollständig wiederhergestellt, im Vergleich zu 24 %, deren Daten nicht verschlüsselt wurden.

Auswirkungen auf Mitarbeitende

Die Umfrage zeigt deutlich, dass eine Datenverschlüsselung im Rahmen eines Ransomware-Angriffs beträchtliche Folgen für die IT-/Cybersicherheits-Teams hat: Alle Befragten gaben an, dass ihr Team auf irgendeine Weise beeinträchtigt wurde.

Abbildung 13: Die Auswirkungen einer Datenverschlüsselung auf die IT-/Cybersicherheits-Teams



Welche Auswirkungen hatte der Ransomware-Angriff auf die Mitarbeitenden in Ihrem IT-/Cybersicherheits-Team (falls zutreffend)? Anzahl=1.700

Empfehlungen

Auch wenn sich die Erfahrungen von Unternehmen mit Ransomware im letzten Jahr verändert haben, bleibt Ransomware eine ernstzunehmende Bedrohung für alle Unternehmen. Da Angreifer ihre Angriffsmethoden ständig weiterentwickeln, ist es entscheidend, dass auch die Abwehrmaßnahmen und Schutzstrategien der Unternehmen Schritt halten – sowohl gegen Ransomware als auch gegen andere Bedrohungen. 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 Sicherheitsfundament ist ein Muss. Endpoints (einschließlich Server) sind das Hauptziel von Ransomware-Akteuren. Stellen Sie daher sicher, dass diese umfassend geschützt sind, unter anderem 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 ausgearbeiteten Incident-Response-Plan, d. h. einem Plan für die Reaktion auf Vorfälle, reduzieren Sie die Auswirkungen eines schwerwiegenden Vorfalls deutlich. 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 aller Größen 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.

2025-06-26 (WP-DD)

SOPHOS