veeam Insights

Vom Risiko zur Resilienz

2025 Ransomware-Trends und proaktive Strategien

Executive Summary:

Bewertung von Ransomware-Bedrohungen und Abwehrmaßnahmen im Jahr 2025

Ransomware-Angriffe entwickeln sich weiter und werden schneller und raffinierter als je zuvor. Eines ist sicher: **Die allgegenwärtige Bedrohung durch Ransomware wird Unternehmen auch 2025 und darüber hinaus beschäftigen.** Unabhängig davon, ob diese Angriffe von etablierten Gruppen oder der zunehmenden Zahl von „einsamen Wölfen" ausgehen, kann eine unzureichende Vorbereitung eine Organisation viel Zeit und Geld sowie das Vertrauen der Beteiligten kosten.

Um diesen anhaltenden Cyber-Bedrohungen entgegenzuwirken, zeigt unser Risk to Resilience Report 2025 verschiedene Maßnahmen auf, die Unternehmen ergreifen können, um Risiken zu mindern und sich schneller von einem Angriff zu erholen. **Wir haben 1.300 Unternehmen weltweit befragt**, um herauszufinden, wie Chief Information Security Officers (CISOs), Sicherheitsexperten und IT-Führungskräfte dafür sorgen, dass sich ihr Unternehmen von Cyber-Bedrohungen erholt.

Die praxiserprobten Strategien von Unternehmen, die sich schneller von Angriffen erholt haben, spiegeln eine Reihe von Best Practices für die Cyberresilienz wider, deren Umsetzung alle Unternehmen in Betracht ziehen sollten.

Es gibt eine gute Nachricht. Im Vergleich zu unserer Umfrage von 2024[1] **ist der Prozentsatz der Unternehmen, die von mindestens einem Ransomware-Angriff betroffen waren, der zu einer Verschlüsselung oder Datenexfiltration führte, von 75 % auf 69 % leicht zurückgegangen.** Dieser Rückgang ist wahrscheinlich darauf zurückzuführen, dass die Unternehmen ihre Vorbereitungs- und Resilienzpraktiken sowie die Zusammenarbeit zwischen IT- und Sicherheitsteams weiter verbessert haben. Auch Regierungen haben sich zusammengetan, um große Ransomware-Gruppen auszuschalten, was die Bedrohungsakteure dazu veranlasst, sich anzupassen und ihre Angriffsdynamik zu verändern.

Unsere Analyse zeigt **sechs wichtige Trends, die die Ransomware-Bedrohungslandschaft 2025 prägen** sowie die datengestützten Erkenntnisse, die Unternehmen bei der Verbesserung ihrer Resilienz unterstützen können. Von Katz-und-Maus-Taktiken und der Zunahme der Exfiltration bis hin zu einem Rückgang der Lösegeldzahlungen und einer zunehmenden Zusammenarbeit zwischen den Beteiligten untersuchen wir die gegenwärtige Bedrohungslandschaft und fragen, wie erfolgreiche Unternehmen die Risiken und Auswirkungen von Ransomware reduzieren.

1.300

Organisationen auf der ganzen Welt wurden von Veeam befragt

6 %

Weniger Unternehmen, die von mindestens einem Ransomware-Angriff betroffen sind

Unternehmen müssen von reaktiver Sicherheit zu proaktiven **Cyberresilienz-Strategien** übergehen, um den Herausforderungen durch Ransomware-Angriffe zu begegnen, indem sie Bereitschaft, schnelle Reaktionsfähigkeit und sichere Wiederherstellungsmaßnahmen kombinieren, um das Risiko zu verringern.

Die 6 wichtigsten Ransomware-Trends, auf die Sie 2025 achten sollten

1 **Strafverfolgung zwingt Bedrohungsakteure zur Anpassung**

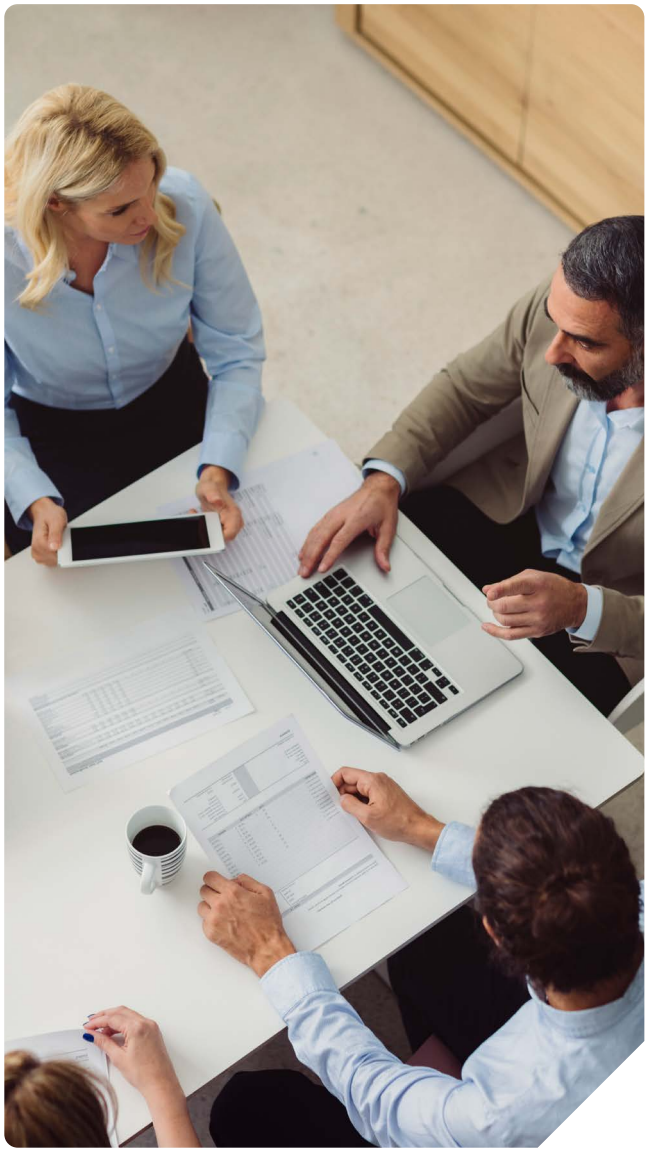
2 **Datenexfiltrationsangriffe nehmen zu**

3 **Ransomware-Zahlungen sind rückläufig**

4 **Neue rechtliche Konsequenzen von Lösegeld-Zahlungen**

5 **Zusammenarbeit stärkt die Resilienz in Bezug auf Ransomware**

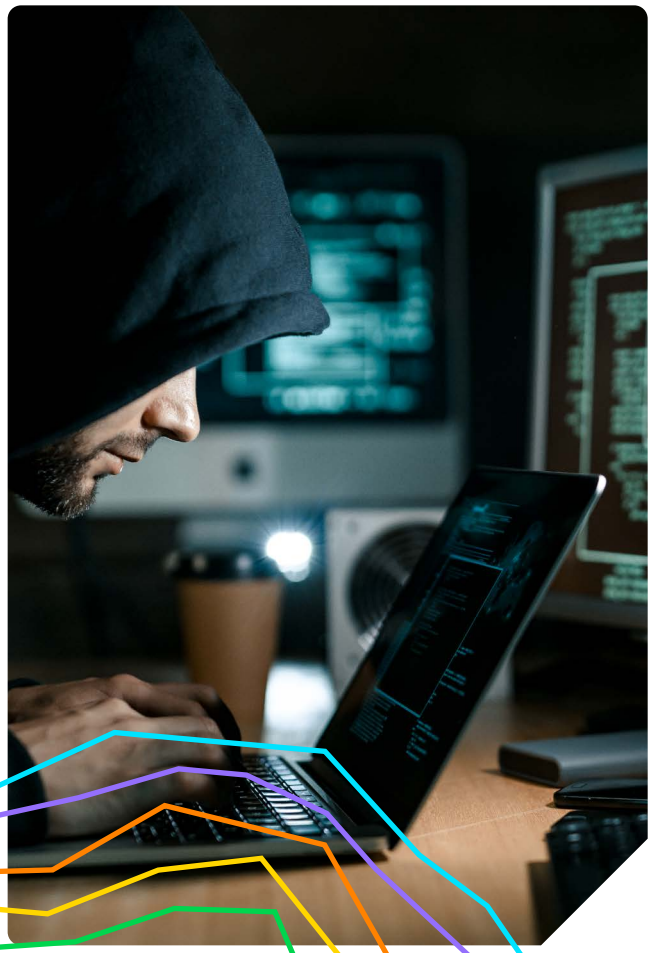
6 **Budgets für Sicherheit und Wiederherstellung steigen, aber dies ist nicht alles, worauf es ankommt**



Strafverfolgung zwingt Bedrohungsakteure zur Anpassung

TREND# 1

2024 starteten die Behörden mehrere erfolgreiche Operationen, um prominente Cyber-Bedrohungsgruppen auszuschalten. Die Eliminierung dieser größeren Gruppen ist natürlich eine positive Entwicklung für die Bedrohungsabwehr. Allerdings hat **die Zahl der kleineren Gruppen und „einsamen Wölfe", die Angriffe durchführen, zugenommen.** Einige Gruppen haben ihre Ziele auch „heruntergefahren", indem sie kritische Infrastrukturen meiden, um der Kontrolle durch Strafverfolgungsbehörden zu entgehen, und stattdessen kleine und mittlere Unternehmen (KMUs) ins Visier nehmen, die oft eine schwächere Cyberabwehr haben.



Einige der größeren Gruppen, die entweder geschlossen wurden, verschwunden sind oder ihre Tätigkeit eingestellt haben, sind:

- **LockBit**, eine Ransomware-as-a-Service (RaaS)-Gruppe, wurde durch Strafverfolgungsmaßnahmen unter der Leitung der britischen National Crime Agency in Zusammenarbeit mit dem FBI und Europol ausgeschaltet.[2]
- **BlackCat**, eine RaaS-Gruppe, die das FBI bereits 2023 stoppen konnte,[3] stellte den Betrieb im März 2024 nach einem erfolgreichen Angriff auf Change Healthcare und einer Lösegeldzahlung von über 22 Millionen US-Dollar ein.[4]
- **Black Basta** stellt offenbar 2025 seinen Betrieb ein, nachdem durchgesickerte Chatprotokolle zeigten, dass man dort nach einem Angriff auf das US-Gesundheitssystem Ascension, zu dem 140 Krankenhäuser in 19 Bundesstaaten gehören, wegen der Kontrolle durch die Strafverfolgungsbehörden besorgt war.[5]

Datenexfiltrationsangriffe nehmen zu

TREND# 2

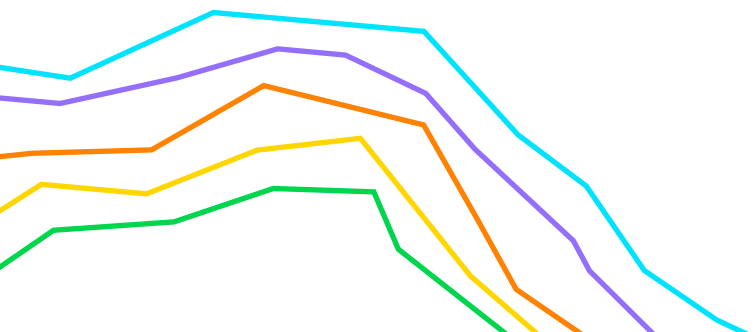
Da sich die Bedrohungslandschaft stetig weiterentwickelt, ändern die Bedrohungsakteure ihre Taktiken ständig. Obwohl Exfiltrationstaktiken in der Regel in Verbindung mit Datenverschlüsselungen eingesetzt werden, stieg die Zahl der Opfer, die nur aufgrund von Exfiltration ein Lösegeld gezahlt haben, im 4. Quartal an.[6]

Die Exfiltration ist eine Art „Smash-and-Grab"-Konzept, das bei herkömmlichen Ransomware-Angriffen vor der Verschlüsselung üblich ist. Sie kommt auch bei schlecht gesicherten cloudbasierten Anwendungen und Cloud-Infrastrukturen vor. Neben dieser Verlagerung hin zur Datenexfiltration — und zur doppelten Erpressung, bei der sowohl die Verschlüsselung zur Beschränkung des Zugriffs als auch die Veröffentlichung sensibler exfiltrierter Daten miteinander kombiniert werden — **hat sich auch die „Dwell Time" verkürzt, also die Zeitspanne zwischen der Kompromittierung selbst und dem Start des Angriffs, wobei viele Angriffe innerhalb weniger Stunden stattfinden.**

Im 2. Quartal 2024 stellte Coveware by Veeam fest, dass zwei der drei größten Ransomware-Angreifer in diesem Quartal eine durchschnittliche Dwell Time von weniger als 24 Stunden zeigten.[7] Dies ist ein deutlicher Rückgang im Vergleich zu den vorangegangenen Quartalen, und dieser Trend setzte sich auch im 4. Quartal fort.

Wenn sich Bedrohungsakteure Zugang zu den Netzwerken der Opfer verschaffen, verwenden sie in der Regel laterale Bewegungstechniken. Sie suchen nach einer einfachen Exfiltrationsmöglichkeit oder einem spezifischen Ziel, wie z. B. der Kompromittierung von VMware ESXi Hypervisoren, um die Opfer zur Zahlung von Lösegeld zu zwingen. Diese effizienten und gut eingespielten Strategien führen oft zu schnelleren Angriffen, die schwer zu entdecken und einzudämmen sind.

Allzu oft sind Unternehmen mit schwacher Cybersicherheit und komplexen Netzwerkarchitekturen besonders anfällig für Datenexfiltrationen und damit verbundene Cyber-Bedrohungen.



Ransomware-Zahlungen sind rückläufig

TREND# 3

Glücklicherweise ging der Gesamtwert der Ransomware-Zahlungen 2024 im Vergleich zu 2023 zurück.[8] Mehr als ein Drittel der von einem Ransomware-Angriff betroffenen Unternehmen (36 %) zahlten kein Lösegeld, und 25 % zahlten nicht, konnten ihre Daten aber trotzdem wiederherstellen.

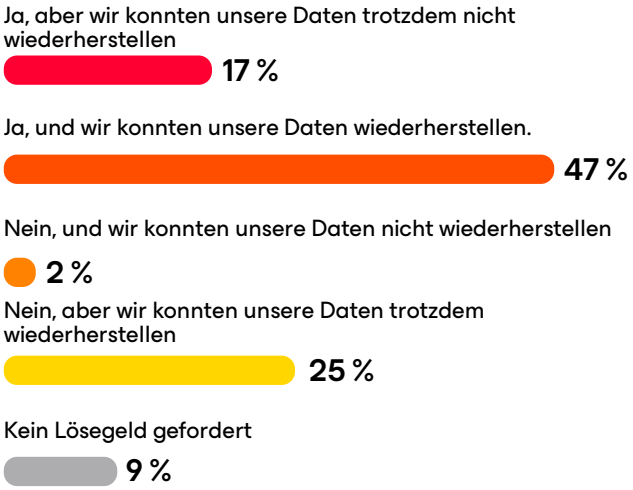
Von denjenigen, die zahlten, zahlten 82 % weniger als das ursprünglich geforderte Lösegeld, und 60 % zahlten weniger als die Hälfte dieser Summe. Diese Daten stimmen auch mit dem überein, was Coveware by Veeam während seiner Arbeit mit den betroffenen Unternehmen 2024 aus erster Hand erfahren hat: Der **Medianwert der Zahlungen sank im 4. Quartal um 45 %** auf ca. 110.000 USD, was einen historischen Tiefstand bedeutet.

Nur 25 % der Unternehmen, die mit Experten für die Reaktion auf Vorfälle von Coveware by Veeam zusammenarbeiten, zahlten ein Lösegeld, was einen „wichtigen Meilenstein im Kampf gegen Ransomware“ darstellt.[9]

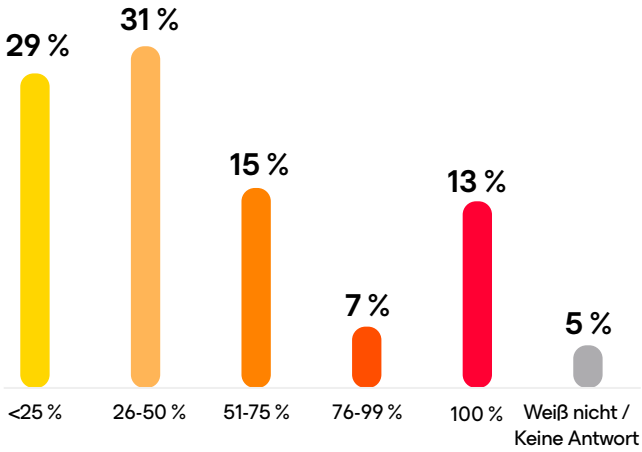
Im Vergleich zu den Unternehmen, die Services für die Reaktion auf Vorfälle von Coveware by Veeam nutzten, zahlten andere Unternehmen mit einer um 156 % höheren Wahrscheinlichkeit ein Lösegeld. Dies deutet darauf hin, dass **die Zusammenarbeit mit erfahrenen externen Anbietern für die Reaktion auf Vorfälle mit weniger Lösegeldzahlungen, niedrigeren Lösegeldzahlungen und insgesamt widerstandsfähigeren Praktiken korreliert.**

Opfer zögern zunehmend, Lösegeld zu zahlen, weil sie nicht darauf vertrauen können, dass die Angreifer dann ihre Daten auch wirklich freigeben. Unternehmen haben auch ihre eigenen Pläne für die Reaktion auf Vorfälle proaktiv verbessert, unter anderem durch den Einsatz unveränderlicher Backups.

Hat Ihr Unternehmen ein Lösegeld für die Wiederherstellung seiner Daten bezahlt?



Prozentsatz des gezahlten Lösegelds



Neue rechtliche Konsequenzen von Lösegeld-Zahlungen

TREND# 4

Die Zahlung eines Lösegelds kann sich als sehr kostspielig erweisen, da sie für Angreifer einen Anreiz darstellt und bestätigt, dass ein gefährdetes Unternehmen zu Zahlungen bereit ist. Tatsächlich **wurden von denjenigen, die ein Lösegeld gezahlt haben, 69 % mehr als einmal angegriffen.** Unternehmen, die keine Maßnahmen ergreifen, um ihre Verteidigungs- und Reaktionskapazitäten zu stärken, haben weniger Möglichkeiten, wenn ein Angriff stattfindet.

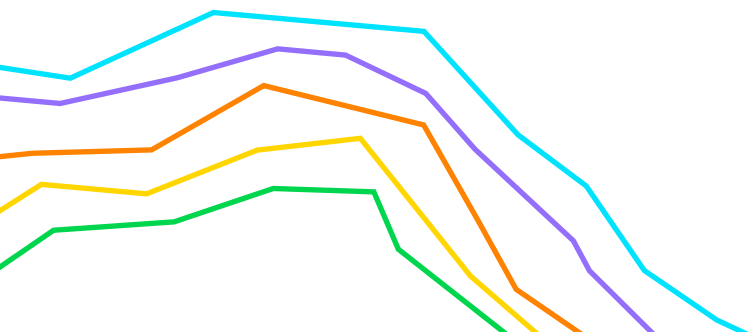
69%

der Organisationen, die ein Lösegeld gezahlt haben, wurden mehr als einmal angegriffen.

Sich entwickelnde Regulierungs- und Reporting-Initiativen sowie koordinierte Durchsetzungsmaßnahmen durch Behörden in verschiedenen Ländern haben ebenfalls zum Rückgang der Lösegeldzahlungen beigetragen. Die von der US-Regierung 2021 ins Leben gerufene International Counter Ransomware Initiative (CRI) und die ihr angeschlossene Task Force bringen 68 Länder mit dem Ziel zusammen, das Ransomware-Ökosystem zu stören und gemeinsame Konzepte für Richtlinien zu entwickeln.[10]

2023 unterzeichneten 40 CRI-Mitglieder eine gemeinsame Erklärung, in der sie sich dafür aussprachen „nachdrücklich davon abzuraten, eine Ransomware-Forderung zu bezahlen".[11] Einige Länder haben auch Gesetze vorgeschlagen, die es Organisationen des öffentlichen Sektors untersagen, Lösegeld zu zahlen — wie etwa Großbritannien im Januar 2025[12] — und zwei US-Bundesstaaten (Florida und North Carolina) haben solche Gesetze verabschiedet.[13]

Das FBI rät Organisationen davon ab, Lösegeld zu zahlen,[14] und das US-Finanzministerium weist darauf hin, dass bei Zahlungen an Einrichtungen, die vom Office of Foreign Asset Control (OFAC) gesperrt sind, Sanktionsrisiken bestehen können.[15] Weltweit tätige Unternehmen müssen auch andere Zahlungsrisiken und Compliance-Anforderungen berücksichtigen.



Zusammenarbeit stärkt die Resilienz in Bezug auf Ransomware

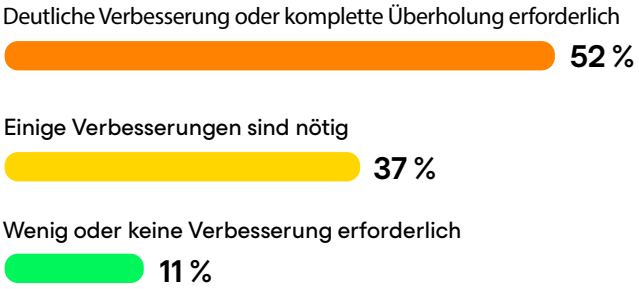
TREND# 5

Die Verbesserung der Zusammenarbeit und der Kommunikation zwischen IT-Betriebs- und Sicherheitsteams hat Unternehmen ebenfalls bei der Verbesserung ihrer Cyberresilienz unterstützt. Die Mehrheit der Befragten (52 %) gab jedoch an, dass erhebliche Verbesserungen oder eine vollständige Überarbeitung erforderlich sind, um diese Teams aufeinander abzustimmen. Und nur 11 % sagten, dass keine oder nur geringe Verbesserungen erforderlich sind.

Gleichzeitig schließen sich Plattform- und Technologieanbieter zusammen, um Ransomware-Informationen zu sammeln und Dienste anzubieten, die Unternehmen dabei unterstützen, ihre Abwehr zu verbessern. Die Meldung von Ransomware und anderen Cyberangriffen an Strafverfolgungs- und Regulierungsbehörden sowie an die entstehenden Partnernetzwerke und der Informationsaustausch in der Branche stärken die kollektive Abwehrfähigkeit.

> „Wir verfolgen den gemeinsamen Zweck der Sicherheit, und wir müssen unsere Ziele auf diesem Gebiet gemeinsam erreichen. Ich denke also nicht, dass wir eine cybersichere Zukunft erleben werden, wenn nicht sowohl öffentliche als auch private Organisationen mit ihren jeweiligen Werteversprechen gemeinsam Lösungen finden." [16]
>
> **Sue Gordon**
>
> früher Principal Deputy Director of U.S. National Intelligence
>
> Sehen Sie das vollständige Interview mit Sue Gordon und Veeam CISO Gil Vega hier

Gemeinsame Ausrichtung der IT-Betriebs- und Sicherheitsteams



Budgets für Sicherheit und Wiederherstellung steigen, aber dies ist nicht alles, worauf es ankommt

TREND# 6

Entscheidend ist dabei, dass dies Anbietern und Behörden ermöglicht, anderen im Ökosystem Anzeichen für Kompromittierungen und Strategien zur Schadensbegrenzung zur Verfügung zu stellen.

Obwohl viele Techniken zur Abwehr von Ransomware Anzeichen für Verbesserungen zeigen, **erhöhen einige Unternehmen ihre Budgets für Sicherheit und Wiederherstellung nicht schnell genug,** um mit der wachsenden Bedrohungslandschaft Schritt halten zu können. Auch Sicherheitsteams sind aufgrund der Vielzahl von Ransomware- und anderen Angriffsvektoren, mit denen sie konfrontiert sind, oft überfordert.

Insgesamt neigen Unternehmen dazu, etwas mehr Ressourcen für die Sicherheit (durchschnittlich 31 % des IT-Budgets) als für die Wiederherstellungsfähigkeit (durchschnittlich 28 %) aufzuwenden, was auf eine potenzielle Schwachstelle beim Aufbau proaktiver Resilienz hindeutet. Chief Information Officers (CIOs) und CISOs sollten bei der Zuteilung von Budgets für die einzelnen Bereiche ein angemessenes Gleichgewicht auf der Grundlage der Bedürfnisse ihrer Organisation finden. Die Ergebnisse der Umfrage **zeigen, dass zu geringe Investitionen in die Sicherheit oder die Wiederherstellung die Fähigkeit von Unternehmen schwächen können, sich vor Ransomware-Angriffen zu schützen und darauf zu reagieren.** Insbesondere die mangelnde Konzentration auf die Wiederherstellung kann wertvolle Zeit und Ressourcen kosten, vor allem, wenn Bedrohungsakteure es auf Backup-Repositorys abgesehen haben.

Positiv ist anzumerken, dass **94 % der Unternehmen 2025 ihr Budget für die Wiederherstellung 2025 und 95 % die Budgets für Vorbeugungsmaßnahmen erhöht haben,** was darauf hindeutet, dass der Stärkung der Cyberresilienz zunehmende Priorität eingeräumt wird.

94%

der Organisationen haben ihr Wiederherstellungsbudget für 2025 erhöht

95%

der Organisationen haben ihr Budget für Wiederherstellungen zur Prävention erhöht

Fragen, die Ihr Vorstand nach einer Ransomware-Attacke stellen wird

Wie kam es zu dem Angriff?

Geben Sie die Ursache und den Umfang des Angriffs an, sowie die Auswirkungen.

Was wurde getan, um die Bedrohung zu beseitigen?

Beschreiben Sie, ob ein Lösegeld gezahlt wurde (wenn ja, wie) und welche Schritte zur Beseitigung der Bedrohung und zur Wiederherstellung unternommen wurden.

Welche Systeme, Daten und Geschäftsabläufe waren betroffen?

Skizzieren Sie die Auswirkungen des Angriffs, einschließlich der finanziellen und rufschädigenden Folgen.

Was wurde getan, um die Cyberresilienz zu verbessern und zukünftige Angriffe zu verhindern?

Identifizieren Sie die Schritte, die zur Stärkung der Sicherheit und Wiederherstellungsfähigkeit unternommen wurden, wie z. B. Änderungen der Governance-Maßnahmen oder Investitionsprioritäten im Bereich der Cybersicherheit.

Wichtige Erfolgsfaktoren:

Was Organisationen mit besseren Resultaten gemeinsam haben

Wenn Unternehmen plötzlich mit einem Ransomware-Angriff konfrontiert werden, müssen sie sofort und koordiniert handeln. Da die Zeit drängt, ist es wichtig, das Ausmaß eines Angriffs abzuschätzen, die Bedrohung einzudämmen und innerhalb weniger Minuten eine Reaktion auf den Vorfall einzuleiten.

Die Analyse der gemeinsamen Merkmale von Unternehmen, die bei einem Ransomware-Angriff erfolgreicher oder weniger erfolgreich waren, kann Ihnen Erkenntnisse liefern, um Ihre Cyberabwehr zu verbessern.

Dieser große Unterschied beim Erfolg wirft die Frage auf:

Warum haben so viele Organisationen Schwierigkeiten, einer so weit verbreiteten Cyber-Bedrohung zu begegnen?

Die Untersuchung der Umfrageergebnisse zeigt, dass mehrere Schwachstellen mit einer geringeren Widerstandsfähigkeit gegen Ransomware korrelieren. Wenn Sie sich ansehen, welche Lehren Unternehmen nach eigenen Angaben im vergangenen Jahr aus den Angriffen gezogen haben, werden mehrere Muster deutlich, die für eine bessere Abwehr und Wiederherstellung von Ransomware genutzt werden können.

Eine Organisation galt als erfolgreicher, wenn fünf der neun folgenden Kriterien erfüllt waren.

- ✔ Das Unternehmen zahlte kein Lösegeld und konnte seine Daten wiederherstellen.
- ✔ Die Organisation wurde nicht mehrfach angegriffen.
- ✔ Die Organisation hat keine signifikanten Auswirkungen erfahren.
- ✔ Das Unternehmen hatte seine Produktionsdaten nicht verschlüsselt.
- ✔ Die Organisation wurde nach dem Angriff als vorbereitet oder vollständig vorbereitet eingestuft.
- ✔ Das Unternehmen konnte die Betriebsfähigkeit von mehr als 80 % seiner Server wiederherstellen.
- ✔ Mehr als 90 % der betroffenen Daten des Unternehmens konnten wiederhergestellt werden.
- ✔ Weniger als 20 % der Produktionsplattformen des Unternehmens waren betroffen.
- ✔ Weniger als 10 % der Backup-Repositorys wurden verändert oder gelöscht, als der Bedrohungsakteur dies versuchte.

Ransomware Playbooks verbessern die Vorbereitung auf potenzielle Angriffe

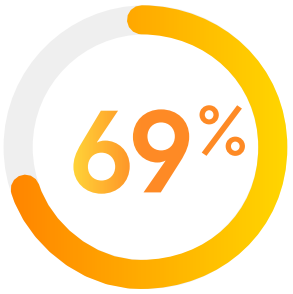
Die Zuversicht vor einem Angriff entspricht nicht immer der Realität: **69 % der Ransomware-Opfer gaben an, dass sie sich vor dem Angriff gut vorbereitet fühlten, diese Zuversicht sank jedoch nach dem Angriff um mehr als 20 %,** was kritische Lücken in der Planung aufzeigt.

Die Diskrepanz zwischen der Wahrnehmung der Bereitschaft und der Realität war auch bei bestimmten Rollen größer. Insbesondere die Bereitschaft der CIOs ging nach dem Angriff um 30 % zurück, während sie bei den CISOs nur um 15 % sank, was darauf hindeutet, dass CISOs ein besseres Verständnis der Sicherheitslage ihres Unternehmens haben.

Insgesamt ist es von entscheidender Bedeutung, die organisatorische Ausrichtung auf Cyberresilienz, Vorbereitungsmaßnahmen und Verfahren zur Reaktion auf Vorfälle zu unterstützen. Dies sollte Schulungen und Übungen für alle betroffenen Gruppen beinhalten, um eine einheitliche und koordinierte Reaktion während und nach einem Angriff zu ermöglichen.

Während 98 % der Befragten über ein Ransomware-Playbook verfügen, **verfügt weniger als die Hälfte der Unternehmen über wichtige technische Elemente,** wie z. B. Backup-Überprüfungen und -Frequenzen (44 %), Backup-Kopien und gewährleistete Reinheit (44 %), alternative Infrastrukturvorkehrungen (37 %), Eindämmungs- oder Isolierungspläne (32 %) und eine vordefinierte „Befehlsstruktur“ (30 %).

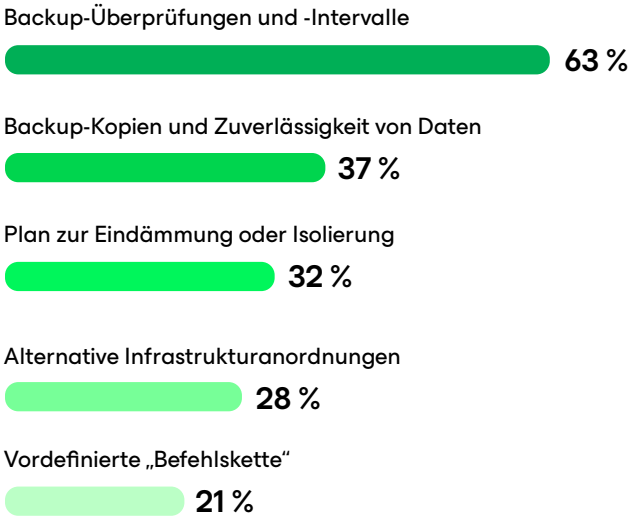
Organisationen mit **erfolgreicheren Ergebnissen hatten eine deutlich höhere Instanz mit diesen fünf technischen Schlüsselelementen in ihren Playbooks.**



waren zuversichtlich in Bezug auf ihre Vorbereitungen gegenüber potenziellen Ransomware-Angriffen

Rückgang des Vertrauens in die Vorbereitungen ihrer Organisation nach einem Angriff

Zentrale Playbook-Elemente für erfolgreichere Unternehmen



Proaktive Sicherung und Wiederherstellung stärkt die Resilienz

Sichere Backup-Wiederherstellung ist wichtig, aber schwieriger, als viele denken. Tatsächlich fanden **89 % der Unternehmen ihre Backup-Repositorys im Visier eines Bedrohungsakteurs.**

Schlimmer noch: Im Durchschnitt wurden 34 % der Backup-Repositorys verändert oder gelöscht. Weniger als 10 % schafften es, mehr als 90 % ihrer Server im Rahmen der Erwartungen wiederherzustellen, und nur 51 % gelang es, die Mehrheit ihrer Server wiederherzustellen.

Die Planung der Wiederherstellung ist entscheidend und umfasst mehrere Phasen. Sicherheits- und IT-Teams müssen die Cyberbedrohung eindämmen oder beseitigen und den Zugriff anschließend mit Tools wie Identity and Access Management und anderen Cybersicherheitslösungen sichern, bevor sie schließlich die Daten in einer sicheren Umgebung wiederherstellen.

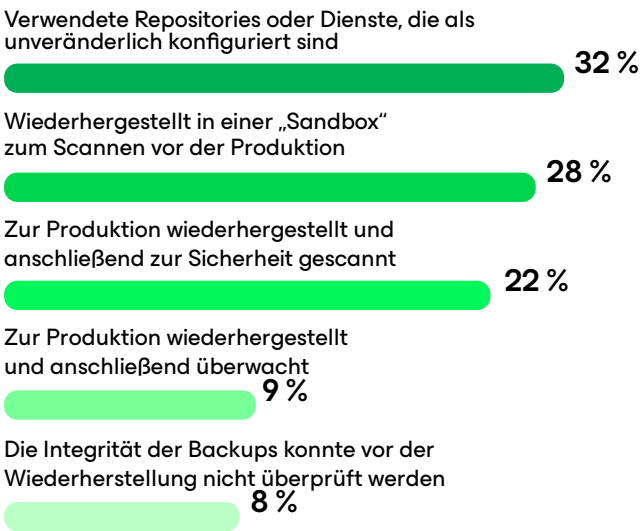
Sichere Backups wurden ebenfalls nicht ausreichend als proaktive Maßnahme genutzt. **Nur 32 % der Befragten nutzen Repositorys oder Services, die als unveränderlich konfiguriert sind,** während nur 28 % der Befragten die Daten in einer Sandbox-Umgebung wiederherstellten und auf ihre Integrität überprüften. **39 % der Befragten mussten ihre Daten direkt in der Produktivumgebung wiederherstellen, während 8 % die Integrität des Backups vor der Wiederherstellung nicht überprüfen konnten.**

Unternehmens- und IT-Führungskräfte müssen sicherstellen, dass Daten und Backups gescannt und frei von Malware sind, bevor sie in die Produktivumgebung zurückgebracht werden, um das Risiko für das Unternehmen zu minimieren. Andernfalls droht ihnen eine Reihe schwerwiegender Konsequenzen, unter anderem: Schnelle Wiederinfektionen, seitliche Bewegung, Persistenzmechanismen, verzögerte Detonation, anhaltende Geschäftsunterbrechung, Compliance-Verstöße und mehr.

89%

der Unternehmen fanden ihre Backup-Repositorys im Visier eines Bedrohungsakteurs.

Backup-Integritätsprüfungsmethode



„Die Macht der Menschen“ bei der Resilienz gegen Ransomware

Während diese technischen Aspekte der Wiederherstellung von entscheidender Bedeutung sind, vernachlässigen zu viele Unternehmen die entscheidenden „menschlichen“ Elemente in ihren Ransomware-Playbooks.

Nur 26 % der Unternehmen verfügen über einen Entscheidungsprozess für Lösegeldzahlungen, der eine schnelle Reaktion auf Zahlungsforderungen auf der Grundlage der möglichen Auswirkungen vorschreibt. In vielen Fällen gibt es auch keine Verfahren für die Benachrichtigung der Strafverfolgungsbehörden, was Wiederherstellung und Compliance unterstützen könnte.

Mehr als ein Drittel der Unternehmen nutzte interne Teammitglieder für die Kommunikation mit Bedrohungsakteuren. Der Rest verließ sich auf die Hilfe Dritter, darunter Spezialisten für die Reaktion auf Vorfälle und für Lösegeldverhandlungen. Diese Spezialisten sind unverzichtbar, um die Interaktion auf der Grundlage eines detaillierten Verständnisses des Verhaltens der Bedrohungsakteure anzuleiten, was zu erfolgreicheren Ergebnissen führt. Wenn interne Teammitglieder mit Bedrohungsakteuren kommunizieren, kann ein Unternehmen unbeabsichtigt zusätzlichen Risiken und Bedrohungen ausgesetzt werden.

Schließlich hatten nur 30 % der Unternehmen eine vordefinierte Befehlskette für den Umgang mit Angriffen. Die „Befehlskette“ trägt dazu bei, dass bei der Reaktion auf einen Vorfall die korrekten Autorisierungswege und Genehmigungen für kritische Entscheidungen sichergestellt werden, bis hin zur Kontaktaufnahme mit Bedrohungsakteuren oder der Zahlung von Lösegeld.

Egal, an welchem Tag oder zu welcher Uhrzeit, ein Ransomware-Angriff kommt immer ungelegen. Deshalb ist es so wichtig, einen Fahrplan für die Reaktion auf solche belastenden und zeitkritischen Bedrohungen zu haben.

26 %

der Unternehmen verfügten über einen Entscheidungsprozess für Lösegeldzahlungen

So kommt alles zusammen

Zusammengenommen deuten diese Maßnahmen auf einen zentralen Unterschie bei der Denkweise zwischen Unternehmen, die sich im vergangenen Jahr gegen Ransomware-Angriffe gewappnet haben, und solchen, bei denen dies nicht der Fall war:

Erfolgreiche Unternehmen machen Cyberresilienz zu einem Teil ihrer täglichen Praxis. Sie verankern proaktive Strategien in ihren täglichen IT-Betriebsabläufen.

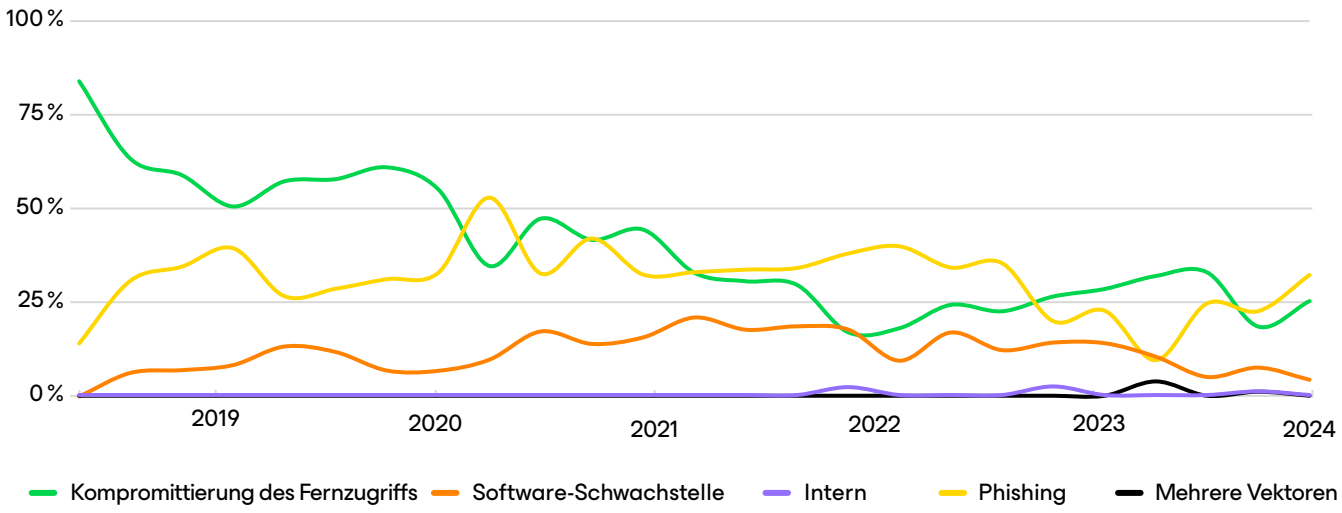
Erfolgreichere Unternehmen haben nach einem Angriff auch mit größerer Wahrscheinlichkeit größeren Wert auf Mitarbeiterschulungen und Sensibilisierungsprogramme gelegt, was dazu beitragen kann, Social-Engineering-Angriffe wie z. B. Phishing abzuwehren. Die Richtlinien für Software-Updates werden in der Regel auch nach einem Angriff verschärft, um die Ausnutzung von Softwareschwachstellen auf einer kontinuierlichen Basis zu verhindern. Insbesondere **haben viele Unternehmen nach dem Angriff neuere Sicherungs- und Wiederherstellungslösungen implementiert und auf Cloud- oder verwaltete Services umgestellt.** Diese Maßnahmen unterstützen Unternehmen dabei, sich vor häufigen Angriffsvektoren zu schützen und die Resilienz zu verbessern.

Erfolgreiche Unternehmen setzten mehr proaktive Wiederherstellungselemente nach einem Angriff ein. als weniger erfolgreiche Unternehmen.

Diese proaktiven Verteidigungspraktiken tragen auch dazu bei, die häufigsten anfänglichen Zugriffsvektoren zu bekämpfen, die Coveware by Veeam bei seiner Arbeit im vierten Quartal festgestellt hat, einschließlich Kompromittierung des Remote-Zugriffs, Phishing, Software-Schwachstellen und mehr.

Eine starke Verteidigung gegen Ransomware-Angriffe kann nicht einfach herbeigezaubert werden, wenn ein Angriff erfolgt. Sie muss ein grundlegender Bestandteil der täglichen Arbeit eines Unternehmens sein.

Anbieter im Bereich Ransomware-Angriffe



Quelle: Coveware by Veeam, „Werden die Erfolge der Strafverfolgungsbehörden gegen Ransomware auch 2025 noch anhalten?“

Bestandsaufnahme und Maßnahmen

Ransomware-Angriffe können den Ruf eines Unternehmens schädigen und das Vertrauen der Kunden und Endbenutzer untergraben. Die Kosten für den Umgang mit einem Angriff können auch erhebliche finanzielle Auswirkungen haben, einschließlich betrieblicher Ausfallzeiten, Produktivitätsverlust und möglicher Geldbußen oder Gerichtsverfahren.

Wenn es zu einem Angriff kommt, sollten sich Unternehmen auf Teamarbeit, Zusammenarbeit und Kommunikation konzentrieren und ruhig und gelassen bleiben, während sie die Reaktionsstrategien aus ihrem Ransomware-Angriffs-Handbuch umsetzen. Nach einem Angriff müssen Unternehmen eine Bestandsaufnahme durchführen, sich mit den eigentlichen Ursachen des Angriffs befassen und Maßnahmen ergreifen, um ihre Resilienz zu erhöhen, damit sich ein solcher Vorfall nicht wiederholt.

Organisationen, die erfolgreichere Wiederherstellungen hatten, folgten diesen Best Practices:

- ✔ Entwickeln Sie robuste Pläne für die Reaktion auf Vorfälle mit klaren Rollen und Verantwortlichkeiten.
- ✔ Erstellen Sie eine Backup- und Wiederherstellungsstrategie. Befolgen Sie die 3-2-1-1-0-Regel für die Datenresilienz, um Repositorys als unveränderlich oder anderweitig geschützt zu konfigurieren, und stellen Sie sicher, dass die Backups vor der Wiederherstellung frei von Malware sind.[17]
- ✔ Implementieren Sie proaktive Sicherheitsmaßnahmen und -prozesse, wie z. B. eine Zero-Trust-Architektur, Identitäts- und Zugriffsmanagement, Software-Update-Richtlinien, neuere Erkennungs- und Reaktionslösungen sowie Cloud- oder Managed Services.
- ✔ Erhöhen Sie die Aufwendungen für Tools zur Erkennung von Bedrohungen zur Prävention und für Backup-Lösungen zur Wiederherstellung. Plattformen für die Datenresilienz, die mit Sicherheitstools integriert sind und über Funktionen zur Verhinderung oder Erkennung von Bedrohungen verfügen — wie die Veeam Data Platform[18] — tragen erheblich zur Verbesserung von Cybersicherheit und Resilienz bei.
- ✔ Organisieren Sie Sicherheitsschulungsprogramme, und sensibilisieren Sie alle Mitarbeiter.

Über den Bericht

Der diesjährige Ransomware Report befragte 1.300 Unternehmen, von denen 900 in den letzten 12 Monaten mindestens einen Ransomware-Angriff mit Verschlüsselung oder Exfiltration erlebt hatten. Diee Befragten setzten sich aus Chief Information Security Officers (CISOs) oder Führungskräften mit ähnlicher Verantwortung sowie aus Sicherheitsexperten und IT-Leitern aus ganz Amerika, Europa und Australien zusammen.

Besuchen Sie unsere Homepage, um mehr über Sicherheitslösungen zu erfahren, die Ihre Cybersicherheitsposition verbessern und die Wiederherstellung beschleunigen können, oder um mit einem unserer Veeam-Experten zu sprechen.

Cyber-Verteidigungsstrategien sind ein Thema auf Vorstandsebene. Warten Sie nicht darauf, dass ein Cyberangriff stattfindet. Ergreifen Sie die erforderlichen Maßnahmen, um das Risiko zu minimieren und die Resilienz zu wahren.

Quellen

1 https://go.veeam.com/ransomware-trends-executive-summary-2024-us

2 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

3 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

4 https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

5 https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

6 https://www.veeam.com/blog/will-law-enforcement-success-against-ransomware-continue-in-2025.html

7 https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

8 https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

9 https://www.coveware.com/blog/2025/1/31/q4-report

10 https://counter-ransomware.org/aboutus

11 https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing

12 https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

13 https://www.databreachtoday.com/blogs/as-states-ban-ransom-payments-what-could-possibly-go-wrong-p-3273

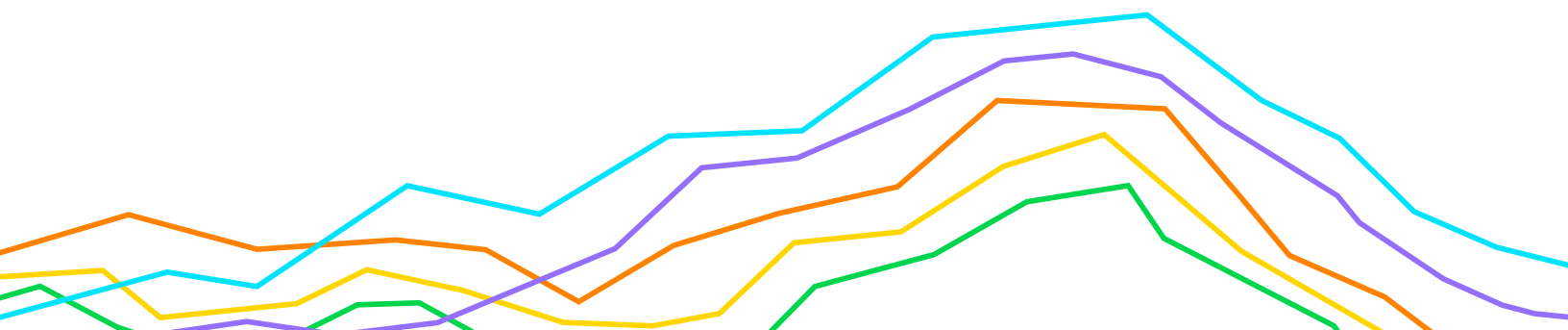
14 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

15 https://ofac.treasury.gov/media/912981/download?inline

16 https://www.youtube.com/watch?v=Fs2xq0pb7YQ

17 https://www.veeam.com/blog/321-backup-rule.html

18 https://www.veeam.com/products/veeam-data-platform.html



veeam Insights