veeam Insights Eurebis

Zusammenfassung

# Ransomware-Trends 2024

## Ausgabe für EMEA

Der 2024 Data Protection Trends Report, für den IT-Verantwortliche und -Implementierungsexperten in zehn Ländern weltweit befragt wurden, hat Folgendes ergeben:

- Nur 25% der Unternehmen gehen davon aus, dass sie 2023 nicht von Ransomware betroffen waren
- 49% bestätigten, dass sie in diesem Jahr zwischen einem und drei Mal betroffen waren
- 26% der Unternehmen gaben an, viermal oder öfter betroffen gewesen zu sein

Angesichts der hohen Angriffsraten, die dieser unabhängige Report jedes Jahr aufzeigt, wurde der Ransomware Trends Report in Auftrag gegeben, um die Angriffe, die Maßnahmen zur Wiederherstellung und die gewonnenen Erkenntnisse besser zu verstehen. In einer anonymen Doppelblindstudie wurden geprüfte IT-Verantwortliche befragt, die selbst Erfahrungen mit solchen Cyberattacken gemacht haben, um durch zusätzliche Recherchen mehr zu erfahren: Der 2024 Ransomware Trends Report.

# Einblicke in die Ransomware-Trends 2024

Der Ransomware Trends Report 2024 ist die dritte jährlich veröffentlichte Studie eines unabhängigen Analystenteams, das anonyme, aber geprüfte Unternehmen befragt, die in den letzten 12 Monaten mindestens einem erfolgreichen Cyberangriff ausgesetzt waren. Jedes Jahr werden für diesen Bericht 1.200 Antworten zusammengestellt. Dabei werden bewusst rund 400 Personen in drei Schlüsselpositionen befragt, die für einen Teil der Unternehmensstrategie zum Schutz vor Cyberangriffen verantwortlich sind:

- **CISO oder hochrangige Führungskraft:** Verantwortlich für die Cyberresilienzstrategie eines Unternehmens
- **Experte für Informationssicherheit:** Verantwortlich für die Verhinderung und Erkennung von Cyber-Ereignissen
- **Backup-Administrator:** Verantwortlich für die laufende Sicherung und Wiederherstellung von IT-Daten

Ransomware ist für alle in der IT-Branche ein wachsendes Problem. Gartner prognostiziert für 2024 eine weltweite geplante Erhöhung des gesamten IT-Budgets um 3,5%. Die Umfrageteilnehmer aus EMEA erwarten Budgeterhöhungen von:

**6,9%**

Erhöhung des Budgets für Technologien zur Prävention und Erkennung von Cyberangriffen

**5,7%**

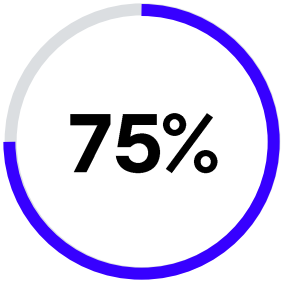
Aufstockung des Budgets für Wiederherstellungstechnologien wie Backup und Business Continuity/Disaster Recovery (BCDR)

Die IT-Ausgaben sind insgesamt gestiegen, wobei die Budgets für Cyberresilienz fast doppelt so stark gestiegen sind wie die allgemeinen IT-Ausgaben. Somit machen Backup- und Cyber-Investitionen "mehr als ihren Anteil" an den gestiegenen IT-Investitionen aus, während andere Bereiche zur Bekämpfung von Cyberbedrohungen weniger priorisiert werden. Saubere Backup-Kopien mit Daten, die nach einem Angriff wiederherstellbar sind und keinen schädlichen Code enthalten.

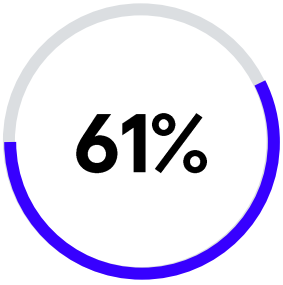
# In 63% der Unternehmen sind die Teams nicht aufeinander abgestimmt

Bereits das dritte Jahr in Folge ist mehr als die Hälfte der Unternehmen (66% in EMEA) der Auffassung, dass entweder eine "signifikante Verbesserung" oder eine "vollständige Überarbeitung" erforderlich ist, um ihre Backup- und Cybersicherheitsteams aufeinander abzustimmen.

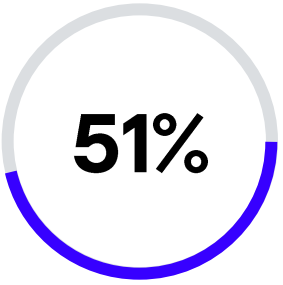
Von den drei untersuchten Rollen waren Backup-Administratoren mit der Ausrichtung ihrer Teams am wenigsten zufrieden.




der Backup-Administratoren halten eine komplette Generalüberholung ihres Systems für erforderlich




der Sicherheitsexperten halten nach Veränderungen in ihrem Unternehmen Ausschau




der CISOs or oder anderen vergleichbaren Führungskräfte haben Bedenken hinsichtlich der Abstimmung in ihrem Unternehmen

# Die Wiederherstellung erfordert eine gemeinsame Anstrengung

den Umfrageteilnehmern zufolge werden die für Prävention und Fehlerbehebung zuständigen Führungskräfte und das IT-Backup-Team am häufigsten benachrichtigt, um die Fehlerbehebung einzuleiten. Kurz darauf folgen Cybersicherheitsexperten und das gesamte Risikomanagementteam des Unternehmens.

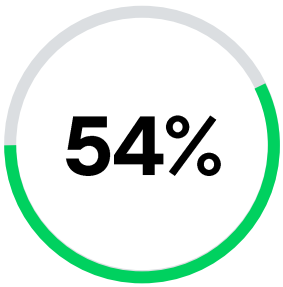
95% der befragten Unternehmen gaben an, dass sie bei der Wiederherstellung auch auf Dritte zurückgreifen. Am häufigsten werden diese vier Arten von Experten einbezogen:

- **Anbieter von Sicherheitssoftware**
- **Anbieter von Backup-Software**
- **Sicherheitsspezialisten für Forensik**
- **Händler, Partner oder Serviceprovider**

# Sie müssen damit rechnen, bei einem Cyberangriff 18% Ihrer Daten zu verlieren

Zwei der wichtigsten Statistiken aus den 1.200 globalen Lektionen, die wir im Jahr 2023 gelernt haben, sind:


der Produktionsdaten wurden bei den Angriffen im letzten Jahr erfolgreich von Cyberkriminellen verschlüsselt




der betroffenen Daten konnten wiederhergestellt werden, nachdem sie bei einem Ransomware-Angriff verschlüsselt wurden

Wenn nur 54% Ihrer Daten wiederherstellbar waren, bedeutet das leider, dass 46% nicht wiederhergestellt werden konnten. Somit waren 18% Ihrer Produktionsdaten nicht wiederherstellbar. An dieser Umfrage nahmen Unternehmen jeder Größe teil und stellten überraschenderweise fest, dass weder die Größe noch der Standort ihres Unternehmens einen signifikanten Einfluss auf die Angriffs- oder Wiederherstellbarkeitsraten hatte. Alle Organisationen wurden weltweit in etwa gleich stark betroffen und sahen sich mit einem ähnlichen Schadensumfang konfrontiert.

Die Unternehmen werden vielleicht auch überrascht sein, dass es keine signifikanten Unterschiede zwischen den Auswirkungen auf die Rechenzentren an Außenstellen und Zweigstellen und nicht einmal zwischen den in einer Public Cloud und einer Private Cloud gehosteten Daten gab.

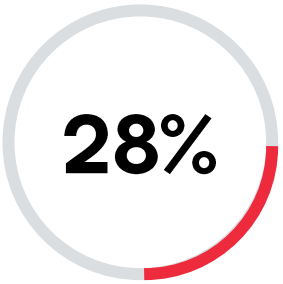
# Haben Sie bezahlt? Hat es funktioniert?

Die zwei wichtigsten Fragen, die jedes Jahr in dieser Umfrage gestellt werden, sind:

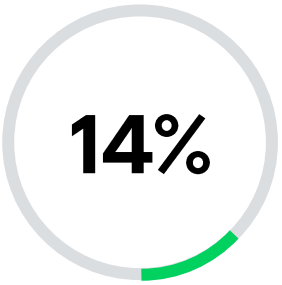
- **Haben Sie das Lösegeld bezahlt?**
- **Waren Sie in der Lage, Ihre Daten wiederherzustellen?**

## Die Ergebnisse 2023 für EMEA:


Haben gezahlt und konnten ihre Daten nach dem Angriff wiederherstellen




Haben gezahlt, konnten die bei dem Angriff verlorenen Daten jedoch nicht wiederherstellen




Konnten die Daten wiederherstellen, ohne das geforderte Lösegeld zu zahlen

Die globalen Ergebnisse waren ähnlich:

- 54% haben gezahlt und konnten ihre Daten nach dem Angriff wiederherstellen
- 27% haben gezahlt, konnten die bei dem Angriff verlorenen Daten jedoch nicht wiederherstellen
- 15% konnten die Daten wiederherstellen, ohne das geforderte Lösegeld zu zahlen

Von den restlichen 4% wurde kein Lösegeld gefordert. Diese Zahlen sind vor allem deshalb bemerkenswert, da sie zeigen, dass etwa **jedes vierte Unternehmen, das Lösegeld gezahlt hat, seine Daten auch nach der *Zahlung*** *nicht wiederherstellen konnte.*

# Angriffe bedeuten mehr als nur Lösegeldforderungen

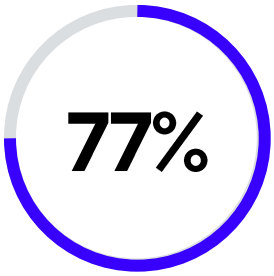
84% der Unternehmen glauben, eine Versicherung zu haben, wobei 25% dieser Versicherungen Ransomware ausdrücklich ausschließen. Die Kosten für Services zur Prävention, Erkennung und Wiederherstellung und das Lösegeld selbst sind jedoch bei Weitem nicht die einzigen finanziellen Faktoren, die Ihr Unternehmen im Falle eines Ransomware-Angriffs treffen könnten. Tatsächlich hat in der diesjährigen Umfrage nur eines von neun Unternehmen (11 %) angegeben, dass die Lösegeldzahlung den überwiegenden Teil der gesamten finanziellen Belastung ausgemacht hat. Bei den übrigen Opfern von Cyberangriffen waren die finanziellen Auswirkungen wesentlich höher als "nur" das Lösegeld an sich.

# 68% der Unternehmen haben ihr Lösegeld mit Versicherungsgeldern gezahlt

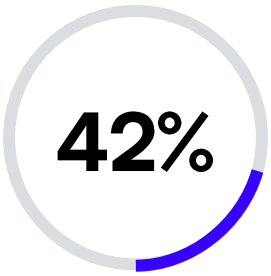
Was die internen Richtlinien der Unternehmen im Jahr 2023 betrifft, so hatten nur wenige Unternehmen (19%) nicht in einer Richtlinie festgelegt, ob gezahlt werden soll oder nicht. Die Mehrheit der Unternehmen verfügte zwar über eine Richtlinie, es gab jedoch ***annähernd so viele Befürworter (43%) wie Gegner einer Zahlung (38%)***.

Es sollte niemanden überraschen, dass zwar nur eine Minderheit der Unternehmen eine Richtlinie zur Zahlung von Lösegeld hatte, letztendlich aber 82% gezahlt haben. 68% haben über eine Versicherung gezahlt und weitere 22% hatten zwar eine Versicherung, entschieden sich aber für eine Lösegeldzahlung, ohne die Versicherung in Anspruch zu nehmen. Das bedeutet, dass im Jahr 2023 90% der Unternehmen über eine Versicherung verfügten, die sie bei einem Cybereereignis hätten nutzen können.

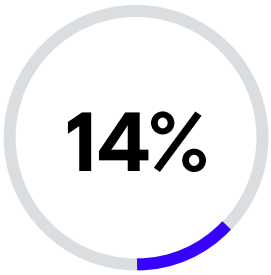
Diese Möglichkeiten werden abnehmen, da sich die Cyberversicherung infolge ständig zunehmender Schadensfälle weiter verändert. Bei letzter Verlängerung:




der Unternehmen haben als Reaktion auf die sich wandelnde IT-Landschaft eine Prämie erhalten




mussten angesichts immer häufigerer Ransomware und Cyberangriffe eine höhere Selbstbeteiligung tragen




mussten eine Verringerung der Versicherungsleistungen hinnehmen, da die Versicherungsunternehmen versuchten, sich vor der wachsenden Bedrohung durch Ransomware zu schützen.

# Cyberkriminelle wollen Ihre Backups

Ähnlich wie Ihr Präventionsteam saubere und wiederherstellbare Backups erwartet, möchten Cyberkriminelle verhindern, dass Sie Ihre eigenen Daten wiederherstellen können. Leider gelingt es den Angreifern bei viel zu vielen Angriffen, Ihnen die Möglichkeit zu nehmen, sich selbst zu retten. Demnach konnten nur 14% der Unternehmen ihre Daten ohne Lösegeldzahlung wiederherstellen. Durchschnittlich waren 33% der Backup-Repositorys von einem erfolgreichen Angriff betroffen.

# 69% haben keinen Plan zur Wiederherstellung

In 95 % aller Unternehmen, die ein Team mit einem Plan hatten, waren die beiden häufigsten Aspekte ihres Playbooks zur Reaktion auf Vorfälle die Sicherstellung von ***sauberen*** und ***wiederherstellbaren*** Daten.

Dies erklärt, warum 31 % der Unternehmen in EMEA eine alternative Infrastruktur in ihrem Plan haben, was leider bedeutet, dass die anderen 69 % nicht in einem Plan festgelegt haben, wo die Daten nach einem Krisenfall auf Standortebene wiederhergestellt werden sollen.

Cyberangriffe haben aber nicht nur Auswirkungen auf die Unternehmen und ihre Teams, sondern auch auf die Personen, die am stärksten involviert sind. Zu den wichtigsten persönlichen Auswirkungen der in diesem Jahr Befragten gehörten erhöhte Arbeitsbelastung, Stress und andere menschliche Faktoren, die die meisten Unternehmen selbst an "normalen" Tagen bereits schwer ausgleichen oder abmildern können.

# Der Angriff wird schlimmer, als Sie sich vorstellen können und mehr kosten, als Sie erwarten

Wenn 40 % der Daten bei einem Cyberangriff betroffen sind und nur 54 % dieser betroffenen Daten wiederhergestellt werden können, müssen Unternehmen realistischerweise mit Datenverlusten von 18 % pro Cyberangriff rechnen. Zudem machen die Lösegelder im Durchschnitt nur 29 % der gesamten finanziellen Auswirkungen aus, während nur 57 % der Gesamtkosten in irgendeiner Weise über Versicherungen oder auf anderem Wege zurückgefordert werden können. Dies kommt zu allem anderen hinzu, was die finanziellen Ressourcen des Unternehmens belastet.

# 2024 ist nicht unveränderlich genug

2024 ist es nicht unvernünftig, dass Unternehmen unveränderlichen Storage auf ihren lokalen Festplatten einsetzen, ergänzt durch unveränderliche Cloud-Repositories und durch ein Air-Gap getrennte Bänder. Leider nutzen selbst von den Unternehmen, die in der Vergangenheit mindestens einmal von einem Cyberangriff betroffen waren, nur 74% abgesicherte lokale Festplatten und nur 90% unveränderliche Clouds.

**Nur 45 % des gesamten Backup-Speichers von Unternehmen in EMEA ist unveränderlich.**

Dennoch ist es ermutigend, dass Unternehmen die branchenübliche 3-2-1-Regel befolgen und mehrere Medientypen verwenden – unabhängig davon, ob diese unveränderlich sind oder nicht. 2024 werden neben den lokalen Festplatten-Repositories 44% der Produktivdaten noch immer auf mindestens einem Band gespeichert und 49% auch in eine Cloud repliziert.

Dieser Forschungsbericht basiert auf der Auswertung von 1.200 Umfrageantworten, darunter 350 aus EMEA. Alle IT-Führungskräfte und Umsetzungsexperten waren für die Cyberresilienz-Strategien ihres Unternehmens verantwortlich. Zu ihnen gehörten CISOs, IT-Sicherheitsexperten und Backup-Administratoren.“ Diese Umfrage wurde Anfang 2024 durchgeführt und im Juni 2024 veröffentlicht. Die Daten wurden von zwei ehemaligen Branchenanalysten zusammengestellt, die zuvor für ESG und Gartner tätig waren und zusammen auf 70 Jahre Erfahrung im Bereich Datensicherung zurückblicken.

Bei Fragen zu dieser Umfrage und daraus veröffentlichten Erkenntnissen/Ressourcen senden Sie bitte eine Nachricht an StrategicResearch@veeam.com.

## Die Einschätzung von Veeam

Veeam® ist der Überzeugung, dass sichere Backups Ihr Rettungsanker bei Ransomware-Angriffen sind. Veeam unterstützt Unternehmen bei der Minimierung von Ausfallzeiten und Datenverlust und schützt sie so vor Lösegeldzahlungen. Mit Veeam profitieren Sie von umfassenden, branchenführenden Wiederherstellungsoptionen und echter Datenportabilität. So können Sie Ihre Daten überall wiederherstellen: Von physischen zu virtuellen Umgebungen, zwischen verschiedenen Clouds oder auch von der Cloud in ein lokales Rechenzentrum. Es gibt keinen magischen Schutz vor Ransomware. Deshalb verfolgt Veeam hinsichtlich Ransomwarebedrohungen und der Wiederherstellung nach einem Angriff einen mehrstufigen Ansatz.
Weitere Informationen finden Sie unter https://www.veeam.com/de/ransomware-protection.html

### Über Veeam Software

Veeam®, weltweit marktführender Anbieter von Lösungen für die Datensicherung und die Wiederherstellung nach Ransomware-Angriffen, hat es sich zum Ziel gesetzt, jedem Unternehmen nach einem Datenausfall oder -verlust nicht nur wieder auf die Beine zu helfen, sondern auch dessen zukünftigen Erfolg zu unterstützen. Mit Veeam erreichen Unternehmen umfassende Resilienz durch Datensicherheit, Datenwiederherstellung und Datenfreiheit für ihre Hybrid Cloud. Die Veeam Data Platform ist eine zentrale Lösung für cloudbasierte, virtuelle, physische, SaaS- und Kubernetes-Umgebungen, sodass Führungskräfte der IT- und Sicherheitsteams darauf vertrauen können, dass ihre Anwendungen und Daten zuverlässig geschützt sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 450.000 Kunden, darunter 74% der Global 2000-Unternehmen, die auf Veeam vertrauen, um ihren Geschäftsbetrieb aufrechtzuerhalten. Profitieren Sie mit Veeam von umfassender Resilienz.

Erfahren Sie mehr unter http://www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.