veeam

2023 EXECUTIVE SUMMARY

RANSOMWARE TRENDS

AUSGABE FÜR EUROPE

Laut dem Report „Datensicherungstrends 2023“ wurden 85 % der befragten Unternehmen in den vergangenen zwölf Monaten mindestens einmal Opfer eines Cyberangriffs — im Vorjahr waren es noch 76 %. Um ein genaueres Bild von den Vorkehrungen zum Schutz vor solchen Attacken und den Maßnahmen zur Wiederherstellbarkeit der Daten zu erhalten, führte ein unabhängiges Marktforschungsunternehmen eine Umfrage unter 1.200 IT-Entscheidungsträgern durch, in deren Unternehmen es 2022 mindestens einen Ransomware-Angriff gab. 350 Umfrageteilnehmer stammten aus der Region EMEA.

In dieser zweiten Befragung von Unternehmen, die von Cyberangriffen betroffen waren, ging es insbesondere um die Sichtweisen vier unterschiedlicher Rollen, die für den Schutz vor und/oder die Minderung von Cyberrisiken zuständig sind: Sicherheitsexperten, CISOs oder andere IT-Verantwortliche, für den IT-Betrieb zuständige Mitarbeiter und Backup-Administratoren.

Der ausführliche 2023 Ransomware Trends Report kann unter https://vee.am/RW23 abgerufen werden.

In der IT gibt es viele Teams, doch es mangelt an deren Abstimmung untereinander

Obgleich zahlreiche Unternehmen ***sagen***, dass Ransomware für sie eine Katastrophe darstellt und sie deshalb die Gefahr von Cyberangriffen in ihren Business-Continuity- und Disaster-Recovery-Plänen (BC/DR) berücksichtigen, lässt die ***tatsächliche*** Interaktion zwischen den Teams sehr zu wünschen übrig.

60 %

sind der Auffassung, dass die Abstimmung zwischen Cybersicherheits- und Backup-Teams „deutlich verbessert“ oder „komplett neu strukturiert“ werden muss.

45 %

sind der Meinung, dass ihr Risikomanagement-Programm gut funktioniert, während die übrigen Befragten noch kein Programm haben oder dieses verbessern möchten.

Dennoch kann eine Abstimmung in zwei Bereichen festgestellt werden: Budget und Strategien. Für die Abwehr von Cyberangriffen (Prävention) stehen Unternehmen 2023 um **5,3 %** höhere Budgets zur Verfügung und auch die Budgets für die Datensicherung (Wiederherstellung) sind um **5,4 %** gestiegen. Was das Vorhandensein von Incident Response Teams und die Vorkehrungen von Unternehmen zur Reaktion auf unvermeidbare Cyberangriffe betrifft, so umfassen die Strategien für die Wiederherstellung nach einer Attacke vor allem diese Aspekte:

- Saubere Backup-Kopien mit Daten, die nach einem Angriff wiederherstellbar sind und keinen schädlichen Code enthalten
- Regelmäßige Überprüfung von Backups auf Wiederherstellbarkeit

Eine Cyberversicherung kann Schutz bieten — wenn ein Abschluss möglich ist

Weltweit wurden **77 %** der geforderten Lösegelder von Versicherungen erstattet; in der Region EMEA lag der Anteil bei **82 %**. Es wird jedoch schwieriger und teurer, eine solche Cyberversicherung abzuschließen: **12 %** der befragten Unternehmen gaben an, dass Ransomware inzwischen in ihren Policen explizit ausgeschlossen ist. Unternehmen mit einer Cyberversicherung berichteten, dass sie diese zuletzt nur zu wesentlich ungünstigeren Konditionen verlängern konnten:

81 %

müssen höhere Beiträge bezahlen

38 %

haben höhere Selbstbeteiligungen

3 %

erhalten im Schadenfall weniger Leistungen

Lösegeldzahlung ist keine Garantie für die tatsächliche Wiederherstellung

Was vielleicht überrascht, ist die Tatsache, dass die meisten Befragten das geforderte Lösegeld bezahlt haben, obwohl dies vielen von ihnen vonseiten der Geschäftsführung oder durch den Gesetzgeber untersagt war. Dennoch sind auch Lösegeldzahlungen keine Garantie, dass eine Wiederherstellung der Daten möglich ist.

62 %

konnten nach Zahlung des Lösegelds ihre Daten wiederherstellen

20 %

konnten ihre Daten trotz Lösegeldzahlung nicht wiederherstellen

13 %

zahlten kein Lösegeld, da sie ihre Daten aus einem Backup wiederherstellen konnten

Statistisch waren weltweit gerade einmal **16 %** der Unternehmen in der Lage, ihre Daten ohne Zahlung eines Lösegelds wiederherzustellen. Im Vorjahr waren dies noch **19 %**.

Für eine Wiederherstellung ohne Lösegeldzahlung müssen Backups intakt bleiben

Mindestens **93 %** der Cyberangriffe hatten auch die Backup-Repositorys zum Ziel. Sind die Angreifer erfolgreich, bleibt Unternehmen gar keine andere Wahl, als das Lösegeld zu zahlen.

75 %

der Unternehmen konnten nach dem Angriff nur noch auf einen Teil ihrer Backup-Repositorys zugreifen

44 %

der Backup-Repositorys waren nach einem Angriff auf die Backup-Lösung nicht mehr verfügbar

Bei einem Angriff können Unternehmen entweder der Lösegeldforderung nachkommen oder ihre Daten aus einem Backup wiederherstellen. Nimmt ein Angreifer die Backup-Lösung ins Visier, ist eine Entscheidung zwischen diesen Optionen nicht mehr möglich.

Das Geheimrezept für intakte Backups ist Immutability

Neben weiteren Best Practices wie dem Schutz der Anmeldeinformationen für den Zugriff auf Backups, einer automatisierten Untersuchung von Backups auf Malware, einer automatischen Überprüfung der Backups auf Wiederherstellbarkeit usw. muss vor allem sichergestellt werden, dass die Backup-Repositorys nicht gelöscht oder beschädigt werden können. Diese sogenannte „Immutability“, d. h. die Unveränderlichkeit der gesicherten Daten, lässt sich über den gesamten „Lebenszyklus" des Datenschutzes hinweg umsetzen:

82 %

der Unternehmen nutzen immutable Cloud-Repositorys

64 %

der Unternehmen nutzen immutable Festplattenspeicher

Und was die Wiederherstellbarkeit der Medien betrifft, so gibt es kein besseres Air-Gap als ein Tape, das aus dem Laufwerk genommen und in einem Schrank aufbewahrt wird. Tatsächlich werden nach wie vor **47 %** aller Daten zu irgendeinem Zeitpunkt des Datensicherungsprozesses auf Tape geschrieben.

Das Geheimrezept für Wiederherstellbarkeit ist Portierbarkeit

Wie auch bei anderen Katastrophen (z. B. Brand, Überschwemmung oder Sturm) betrifft eine strategische Entscheidung die Frage, ***wo Daten wiederhergestellt werden*** sollen. Wurden beispielsweise die Produktivserver kompromittiert, benötigt das Unternehmen neue Server. In der Regel betreiben nur größere Unternehmen mehrere Rechenzentren mit Cold-Standby-Servern, die bei Bedarf hochgefahren werden können. Es überrascht daher nicht, dass die meisten Umfrageteilnehmer hybride Strategien verfolgen:

69 %

der Unternehmen planen die Wiederherstellung in eine cloudbasierte Infrastruktur oder mittels DRaaS

83 %

der Unternehmen planen die Wiederherstellung auf Server in einem Rechenzentrum

Zur Wiederherstellung von Servern im Rechenzentrum setzen Unternehmen unter anderen auf:

- den Einsatz von Cold-Standby-Servern (z. B. durch den Betrieb von zwei Rechenzentren)
- die Anschaffung neuer Server, sofern diese schnell genug lieferbar sind
- die einfache Löschung der Daten auf den ursprünglichen Servern und Weiterverwendung dieser Systeme, sofern sie nicht für forensische Untersuchungen oder zur Strafverfolgung benötigt werden

Da die beiden Prozentwerte zusammen mehr als 100 % ergeben, ist es ein positives Zeichen, dass die BC/DR- und Cybersicherheitsstrategien der meisten Unternehmen abhängig von der jeweiligen Situation beide Umgebungen beinhalten.

Erneute Infektionen bei der Wiederherstellung vermeiden

Entscheidend ist, bei der Wiederherstellung keinen weiteren Schaden anzurichten und keine Schadsoftware oder infizierten Daten in die Produktivumgebung einzuspielen. Bei anderen z. B. durch Brand oder Überschwemmung verursachten Katastrophen können die Daten aus Backups, Replikaten und Snapshots umgehend für die Wiederherstellung genutzt werden. Eines der zahlreichen Probleme bei Cyberangriffen besteht jedoch darin, dass die Daten sehr wahrscheinlich kompromittiert wurden, bevor die Lösegeldforderung eingeht.

Deshalb müssen sie während der Wiederherstellung sorgfältig überprüft werden.

Das ist nicht immer leicht und hängt davon ab, ob die Datensicherungslösung in Erkennungstechnologien integriert ist (die während der Sicherung und/oder Wiederherstellung zum Einsatz kommen) und ob es eine Staging- oder Sandbox-Umgebung gibt. Bei den von einem Cyberangriff betroffenen Umfrageteilnehmern zeigt sich folgendes Bild:

- **44 %** der Unternehmen stellten ihre Daten vor der Übertragung in die Produktivumgebung zunächst in einem isolierten Testbereich bzw. einer Sandbox wieder her.
- **35 %** stellten ihre Daten in der Produktivumgebung wieder her und untersuchten sie sofort danach auf Schadsoftware.
- **12 %** stellten ihre Daten wieder her und überwachten danach ihre Umgebung.
- **9 %** trafen keinerlei Vorkehrungen zur Vermeidung einer erneuten Infektion.

Abschließende Bemerkungen

Ein Großteil der **1.200** von einem Cyberangriff betroffenen Umfrageteilnehmer setzt inzwischen aufgrund seiner Erfahrungen verschiedene grundlegende Technologien ein, um sich für den nächsten Angriff zu wappnen:

- **Immutable Storage** auf Festplatten, in Cloud-Umgebungen und auf Air-Gap-Medien zur Gewährleistung der Wiederherstellbarkeit
- **Hybride IT-Architekturen** zur Wiederherstellung auf alternativen Plattformen wie bei anderen BC/DR-Strategien
- **Wiederherstellung in einer Staging-Umgebung** zur Vermeidung einer erneuten Infektion

Bei Fragen zu den Umfrageergebnissen 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 einer Lösung von Veeam profitieren Sie von umfassenden, branchenführenden Wiederherstellungsoptionen und echter Datenportabilität, um Ihre Daten aus der physischen in eine virtuelle Umgebung, zwischen verschiedenen Clouds oder auch aus der Cloud in ein lokales Rechenzentrum wiederherzustellen. 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 ermöglicht Unternehmen einen zuverlässigen Geschäftsbetrieb durch Datensicherheit, Datenwiederherstellung und Datenfreiheit in Hybrid-Cloud-Umgebungen. Die Veeam Data Platform ist eine zentrale Lösung für cloudbasierte, virtuelle, physische, SaaS- und Kubernetes-Umgebungen, sodass Unternehmen darauf vertrauen können, dass ihre Anwendungen und Daten zuverlässig geschützt und jederzeit verfügbar sind. Der Hauptsitz von Veeam befindet sich in Columbus, Ohio. Veeam ist zudem global mit Niederlassungen in über 30 Ländern vertreten. Weltweit hat Veeam mehr als 450.000 Kunden, darunter 82 % der Fortune 500- und 72 % der Global 2000-Unternehmen. Das globale Netzwerk von Veeam umfasst mehr als 35.000 Technologiepartner, Händler, Serviceprovider und Alliance Partner. Weitere Informationen finden Sie unter **www.veeam.com/de**, auf LinkedIn unter **@veeamsoftware** und auf Twitter unter **@veeam**.

Scannen Sie den QR-Code, um mehr über Veeam-Lösungen zum Schutz vor Ransomware zu erfahren.