Schutz vor Ransomware 2022

Backups der Enterprise-Klasse sind Ihr letzter Rettungsanker

Dave Russell,

Vice President, Enterprise Strategy, Veeam Software

Jeff Reichard,

Vice President, Public Sector & Compliance Strategy, Veeam Software

Chris Hoff,

Data Protection & Ransomware Marketing Manager, Veeam Software

Inhalt

Unternehmen der Enterprise-Klasse können Cyberangriffe nicht verhindern

Die Zunahme und Entwicklung von Ransomware zählt zu den schädlichsten Trends der letzten 10 Jahre. Dadurch ist Ransomware von einem Wirtschaftsverbrechen zu einer Gefahr mit enormen globalen Sicherheitsauswirkungen geworden. Die NATO, die Regierung und das Militär der USA sowie die G7 haben allesamt vor Kurzem die Schwere der Ransomware-Bedrohung bestätigt und sich für eine umfassende koordinierte Reaktion von Regierungen und Industrie ausgesprochen.

Unternehmen können Cyberangriffe nicht verhindern, müssen aber die notwendigen Maßnahmen ergreifen, um ihre Daten im Falle eines Angriffs effektiv zu schützen.

Ransomware-Zunahme 2016–2021

Globale Kosten:
325 Mio. bis

20 Mrd. USD

Häufigkeit:
Alle 2 Minuten bis alle

11 Sekunden

Innovation:

Bitcoin, Ransomware-as-a-Service, zwei-/dreifache Erpressungsangriffe

Sichere Backups sind Ihr Rettungsanker

Die bereitgestellte Verfügbarkeitslösung sollte in der Lage sein, alle unternehmenskritischen Workloads zu schützen.

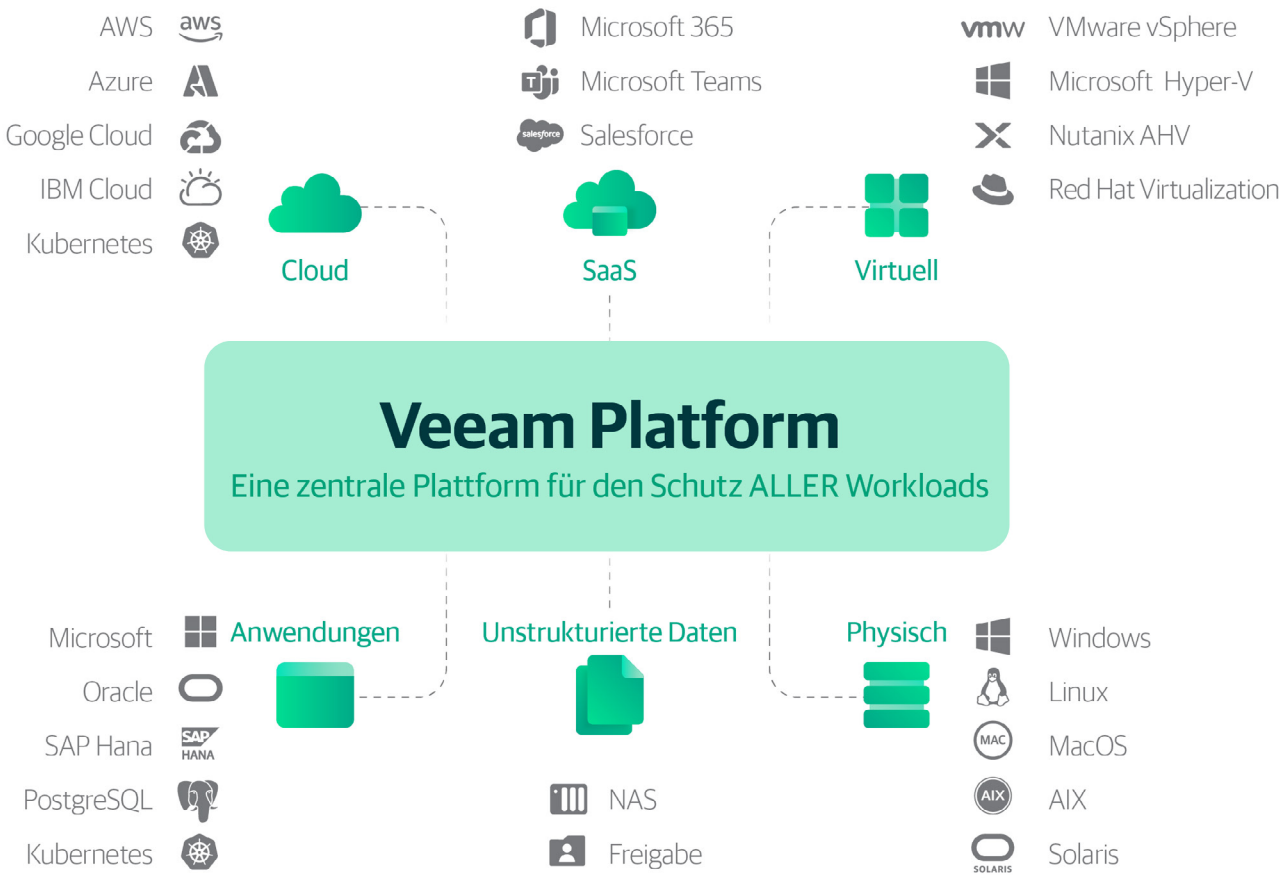
Ungeachtet dessen, ob Workloads lokal, in der Cloud mit IaaS oder als SaaS bereitgestellt sind — unternehmenskritische Daten befinden sich mittlerweile an vielen verschiedenen Speicherorten. Zudem müssen sie portierbar sein, um zukünftige Anforderungen zu erfüllen. Die Abwehrplattform muss entsprechend den Anforderungen und zu schützenden Workloads skalierbar sein. Die Backup-Lösung muss Daten mit zahlreichen Methoden erfassen können, darunter Backup, Replikation, kontinuierliche Datensicherung (CDP) and Speicher-Array-Integrationen.

Die Veeam® Platform erfüllt sämtliche dieser Voraussetzungen. Damit bietet sie eine Lösung, die mit Ihrem Geschäft mitwächst und sich an veränderte Anforderungen anpassen lässt.

Der Ansatz von Veeam ist modular und erweiterbar, Punktlösungen sind nicht erforderlich. Auch sind Sie damit nicht an einen Hardware-Anbieter gebunden und müssen sich keine Sorgen machen, dass Sie die Lösung nicht mehr nutzen können, wenn Ihr Unternehmen wächst.

Die softwaredefinierten Ransomware-Behebungsfunktionen von Veeam funktionieren in jeder beliebigen Infrastruktur — heute und in Zukunft.

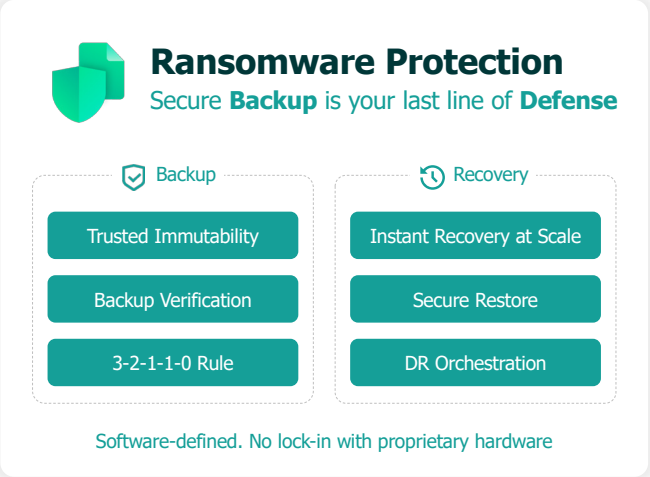
Eine proprietäre Infrastruktur ist dabei keine Voraussetzung, sodass Unternehmen sie auf der bevorzugten Hardware oder in der gewünschten Cloud bereitstellen können. Mit einer flexiblen Infrastruktur können Organisationen nicht nur selber entscheiden, auf welcher Hardware ihre Backup-Lösung ausgeführt wird, sondern auch ihre Backups vor Ransomware schützen — ganz egal, wo sich wichtige Daten befinden.



Aufbau eines Enterprise-Frameworks für resiliente Wiederherstellung

Für ein effektives Sicherheitsprogramm müssen Sie genau wissen, was geschützt werden muss und wie wertvoll eine Ressource für die Organisation ist. Nur dann können Sie bestimmen, wie der Schutz implementiert werden muss. Unabhängig von der gewählten Methodik muss das Framework messbare Ergebnisse definieren, anhand derer IT-Teams Angriffe abwehren und Daten nach einem erfolgreichen Angriff schnell wiederherstellen können.

Ohne ein strukturiertes Management der Cybersicherheitsrisiken werden Sie schnell dazu verleitet, sich auf erkennungsbasierte Abwehrmechanismen wie Firewalls und Virenschutzprogramme zu verlassen. Dabei könnten Sie die Prozesse und Tools vernachlässigen, die für eine effektive Reaktion auf einen erfolgreichen Angriff und die anschließende Wiederherstellung unerlässlich sind. Anders ausgedrückt: Der beste Ansatz ist eine solide Abwehr, einschließlich einer robusten Strategie für Sicherung und Schutz Ihrer Daten und Workloads. Erfolgreiche Backups sind der letzte Rettungsanker bei Cyberangriffen und können entscheidend sein, um erhebliche Ausfallzeiten, Datenverlust und Zahlung eines kostspieligen Lösegelds zu vermeiden. Daher haben wir diese Best Practices zur Sicherung Ihrer Daten zusammengestellt.



1. Zuverlässige Immutability

Cyberkriminelle versuchen im Rahmen von Ransomware-Angriffen jetzt regelmäßig, die Backups einer Organisation zu verschlüsseln oder zu löschen. Das ist entscheidend für den Angreifer, da die Opfer ohne Backups viel Geld für die Wiederherstellung ihrer Daten zahlen müssen.

Resiliente Backups sind ganz einfach Backups, die nicht von einem Angreifer zerstört werden können — selbst wenn dieser administrative Anmeldedaten erlangt hat.

Veeam bietet einen zuverlässigen, richtliniengesteuerten Ansatz für das Datenmanagement mit verschiedenen resilienten Speicheroptionen. Zertifizierte Speicherlösungen von Veeam oder unserem umfassenden Partnerökosystem verbessern die allgemeine Resilienz und garantieren *Immutability* (d. h. sie verhindern eine festgelegte Zeit lang, dass Daten gelöscht oder geändert werden können). **Zu diesen Optionen gehört das abgesicherte Repository von Veeam, eine robuste Lösung für unveränderliche lokale Backups.** Wenn Sie Ihre Daten lieber in der Cloud aufbewahren, erreichen Sie mit Veeam Immutability für AWS Amazon S3 und andere genehmigte S3-kompatible Objektspeicheranbieter mit der jeweiligen Objektsperre.

Backups in einem resilienten Speicher stellen eine der wichtigsten Schutzvorkehrungen für die Ransomware-Resilienz dar. Ein resilienter Backup-Speicher bedeutet, dass Sie mindestens eine Kopie Ihrer Backup-Daten auf einer beliebigen Kombination der folgenden Medien aufbewahren:

- Backups auf Band (die von der Bibliothek entfernt oder als WORM gekennzeichnet werden)
- Unveränderliche Backups in S3- oder S3-kompatiblem Objektspeicher
- Durch ein Air-Gap getrennte Medien und Offline-Medien (Wechseldatenträger, Rotationsdatenträger)
- Backups in Veeam Cloud Connect mit Insider Protection (einer servicegesteuerten Funktion)
- Unveränderliche Backups in einem abgesicherten Repository

2. Überprüfung von Backups

Eine robuste, umfassende Cybersicherheitsstrategie beginnt immer mit gültigen Backups. Zuverlässige, überprüfte und getestete Backups sind der erste Schritt zur erfolgreichen Wiederherstellung. IT-Teams haben viel zu tun und müssen einen Weg finden, die Integrität von Backup-Daten automatisch bei der Backup-Erstellung zu prüfen. Bei einem Problem kann ein weiteres Backup erstellt werden, während die Daten der Produktivumgebung verfügbar sind. So stellen Sie sicher, dass keine Probleme mit der Datenverfügbarkeit entdeckt werden, wenn die Production-Daten einmal nicht mehr verfügbar sind, kompromittiert wurden oder nicht mehr vertrauenswürdig oder fehlerfrei sind.

Veeam SureBackup® ist Vorreiter bei der automatisierten Backup-Überprüfung, einer wesentlichen Funktion in unseren Best Practices zur Ransomware-Resilienz. SureBackup startet Server und Anwendungen automatisch in einer vom Netzwerk isolierten Umgebung und führt Integritätsprüfungen mit zahlreichen integrierten Anwendungsprüfungsmethoden aus, darunter spezielle Active Directory- oder SQL-Befehle zum Prüfen der Anwendungsintegrität. Diese automatische Testfunktion kann Ihren Anforderungen entsprechend erweitert und angepasst werden. Außerdem können Sie die Ausführung nach Belieben planen und nach Abschluss der Tests einen Statusbericht an Ihre E-Mail-Adresse senden lassen.

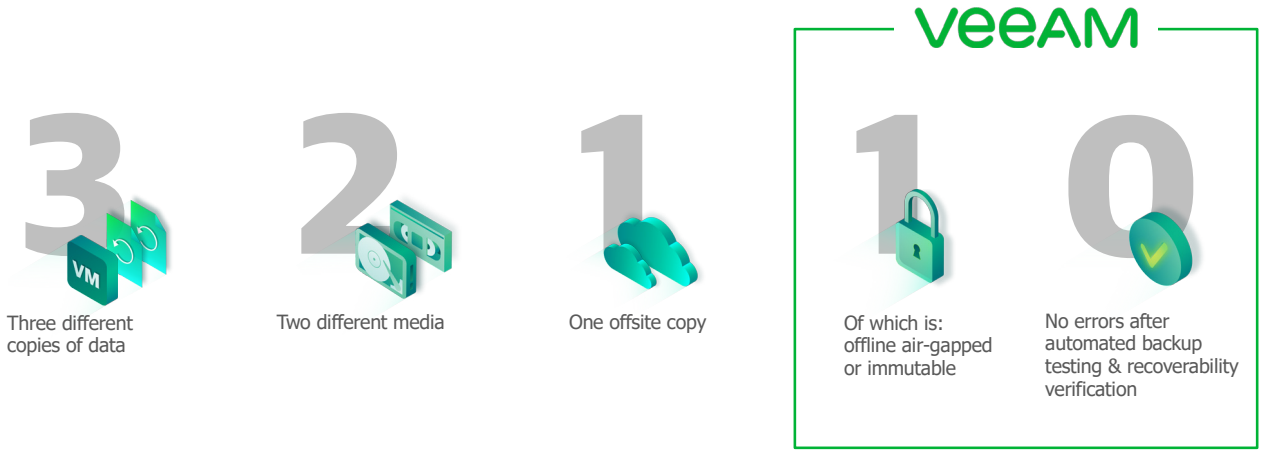
3. 3-2-1-1-0-Regel

Veeam empfiehlt die 3-2-1-1-0-Regel, bei der es sich um unsere Verbesserung der bekannten 3-2-1-Branchenregel handelt.

Schon seit vielen Jahren wirbt Veeam für die 3-2-1-Regel als allgemeine Datenmanagement-Strategie. Empfehlung der 3-2-1-Regel ist es, dass mindestens drei Kopien aller wichtigen Daten vorhanden sind, die sich auf mindestens zwei unterschiedlichen Medien befinden und von denen mindestens eine extern aufbewahrt wird.

Da Ransomware mit immer fortschrittlicheren Methoden arbeitet, betont Veeam, dass mindestens eine Datenkopie resilient sein muss (also durch ein Air-Gap getrennt, offline oder unveränderlich). Diese Empfehlung ist für Resilienz gegen Ransomware unumgänglich.

Die moderne 3-2-1-1-0-Regel erfüllt die Anforderung einer resilienten Kopie und stellt eines der wichtigsten Konzepte dar, mit denen Organisationen Cyberbedrohungen besser abwehren und bewältigen können.



4. Instant Recovery für alle Workloads

Vor dem Auftreten von Ransomware stellten Unternehmen in der Regel nur 3–5 % ihrer gesicherten Daten über einen Zeitraum von einem Jahr hinweg wieder her. Bei einem Ransomware-Angriff können aber 100 % Ihrer Production-Daten verschlüsselt oder mit Malware infiziert werden, und Sie müssen alle Daten schnell wiederherstellen. Der schnelle Zugriff auf Daten ist entscheidend — das Ziel ist hier eher, den kritischen Geschäftsbetrieb fortzusetzen, anstatt ihn im Nachhinein wiederherzustellen.

Veeam hat Instant Recovery 2010 als Vorreiter eingeführt und diese Funktionalität seitdem stets verbessert und erweitert.

Jetzt sind Sie mit Veeam optimal aufgestellt, um mehrere Computer gleichzeitig wiederherzustellen und selbst die höchsten Anforderungen an die Wiederherstellung in Unternehmen zu erfüllen.

Veeam bietet Instant Recovery von Daten:

- Ohne kostspielige, proprietäre Appliances oder Solid-State Drives
- Ohne Einschränkung auf die neuesten Backup-Daten

5. Sichere Wiederherstellung von Daten

Aufbauend auf der zuvor beschriebenen Instant Recovery-Funktion lässt sich Veeam in führende Anti-Malware-Lösungen integrieren, um den Wiederherstellungsprozess zu automatisieren. Dabei werden infizierte Backup-Daten geprüft und bereinigt, damit Sie ausschließlich Backup-Daten im Produktivsystem wiederherstellen, die frei von Cyberbedrohungen sind.

Veeam Secure Restore liefert eine voll integrierte Virenprüfung als optionalen Schritt jedes Wiederherstellungsprozesses. Dieses Feature löst die Probleme beim Malware-Management, da Sie damit stets sicherstellen können, dass alle gesicherten Daten, die Sie im Produktivsystem wiederherstellen möchten oder müssen, fehlerfrei sind und keine Malware aufweisen. **Secure Restore war eine weitere branchenweit erste, zum Patent angemeldete Methode für die Fehlerbehebung nach einem Angriff aus verborgener Malware in Ihren Backup-Daten.**

6. DR-Orchestrierung

Eins steht fest: Cyberangriffe sind Katastrophen. Bei einem Notfall benötigt Ihr Team automatisierte, wiederholbare Ergebnisse. Ihr gewähltes Tool muss regelmäßige Tests und Audits Ihrer Wiederherstellungszeit nach einem Ausfall ermöglichen, einschließlich automatischer Tests der Zugänglichkeit und Nutzbarkeit von Servern und Anwendungen nach der Wiederherstellung.Zudem müssen der Testprozess und die Ergebnisse automatisch dokumentiert werden, um die Anforderungen von Management und externen Sicherheitsauditoren zu erfüllen.

Mit der branchenführenden **Lösung Veeam Disaster Recover Orchestrator können Sie komplexe Workflows komplett automatisieren und dokumentieren, darunter unterbrechungsfreie, groß angelegte Wiederherstellungstests mit dynamischer Dokumentation.**

Zuverlässige Wiederherstellung

- Zuverlässige, skalierbare Orchestrierung
- Anwendungsbezogen

Automatische Tests

- Unterbrechungsfrei
- Geplant oder spontan
- Readiness Checks

Dynamische Dokumentation

- Prüfpfade
- Compliance-Reporting
- Integrierte Änderungsverfolgung
- Proaktive Fehlerbehebung

Fazit

Die Implementierung einer umfassenden Fehlerbehebung Strategie ist unerlässlich, um Bedrohungen wie Ransomware entgegenzuwirken. Mit Veeam erhalten Sie alle erforderlichen Funktionen für die Fehlerbehebung nach einem Ransomware-Angriff. Unser softwareorientierter Ansatz bietet flexible Verwaltungsoptionen für resilienten, unveränderlichen Speicher, ob lokal oder in der Cloud – ohne Bindung an proprietäre Hardware. Mit der modernen Datensicherungsplattform von Veeam erreicht Ihr Unternehmen digitale Resilienz. So minimieren Sie Ausfallzeiten nach einem Ransomware-Angriff.

Ob Ihre Daten lokal oder in der Cloud aufbewahrt werden – vollständige Funktionalitäten für die Fehlerbehebung nach einem Ransomware-Angriff sind unerlässlich. Binden Sie diese Best Practices in Ihr Sicherheitsprogramm ein, um die Reaktion auf Cyberangriffe zu vereinfachen und Datenverlust oder Zahlung eines hohen Lösegelds zu vermeiden.

Informationen zu Veeam Software

Veeam® ist ein führender Anbieter von Backup-, Wiederherstellungs- und Datenmanagement-Lösungen für die moderne Datensicherung. Wir bieten eine umfassende Plattform für cloudbasierte, virtuelle, physische sowie SaaS- und Kubernetes-Umgebungen. Dank unserer besonders unkomplizierten, flexiblen und zuverlässigen Plattform können sich Kunden darauf verlassen, dass Ihre Anwendungen und Daten gesichert und stets verfügbar sind. Veeam hat weltweit mehr als 400.000 Kunden, darunter über 82 % der Fortune 500-Unternehmen und über 60 % der Global 2000-Unternehmen. Das globale Ökosystem von Veeam umfasst mehr als 35.000 Technologiepartner, Händler und Serviceprovider sowie zahlreiche Alliance-Partner und Niederlassungen in über 30 Ländern. Weitere Informationen finden Sie unter www.veeam.com/de, auf LinkedIn unter @veeamsoftware und auf Twitter unter @veeam.

Autoren

Dave Russell ist ein Vice President of Enterprise Strategy.

Jeff Reichard ist Vice President of Public Sector and Compliance Strategy.

Chris Hoff ist ein Data Protection & Ransomware Marketing Manager.

Veeam-Lösungen für die Fehlerbehebung nach Ransomware-Angriffen

- Veeam Availability Suite
- Veeam Backup *for Microsoft 365*
- Veeam Disaster Recovery Orchestrator

Weitere Informationen zu den Ransomware-Funktionalitäten von Veeam finden Sie auf dieser Website:
https://www.veeam.com/de/ransomware-protection.html

Weitere Informationen zu Enterprise-Backup-Lösungen finden Sie hier:
eine ausführliche Beschreibung der Cybersicherheitsfunktionen von Veeam ist hier verfügbar
https://www.veeam.com/de/enterprise-backup-solutions-software.html