Ransomware in 2022:

7 erforderliche Funktionalitäten für schnelle und zuverlässige Wiederherstellung

Dave Russell,

Vice President, Enterprise Strategy, Veeam Software

Jeff Reichard,

Senior Director, Enterprise Strategy, Veeam Software

Chris Hoff,

Data Protection & Ransomware Marketing Manager, Veeam Software

Inhalt

Unternehmen 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. 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.

Koordinierte Maßnahmen von Regierung und Industrie nehmen Zeit in Anspruch. Bis dahin müssen Organisationen aller Größenordnungen sich und ihre Kunden oder Teilnehmer schützen. Dabei können Sie konkrete Schritte mit bereits verfügbaren Tools und Sicherheits-Frameworks einsetzen.

Ransomware und andere moderne Cyberbedrohungen sind ausgefeilt und anpassbar und erfordern daher einen agilen, mehrschichtigen Abwehransatz. Dennoch nutzen viele Organisationen nach wie vor Standalone-Sicherheitsprodukte, die auf einen einzelnen Angriffsvektor abzielen und leicht umgangen werden können. Zu den Technologieproblemen kommt noch der Mangel an Sicherheitsexperten in der Belegschaft. Die Anzahl der offenen Cybersicherheitspositionen wurde kürzlich auf weltweit über 3 Millionen geschätzt. Das Personal benötigt nicht nur technische Kenntnisse, sondern muss auch Richtlinien aufstellen können, die Konsistenz schaffen und die Gesamteffektivität der Organisation messen.[i] Wenn diese erforderlichen Aspekte in Bezug auf Personen, Prozesse und Technologie nicht erfüllt sind, werden Ihre Daten anfälliger denn je für geschickte Cyberkriminelle.

Organisationen 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

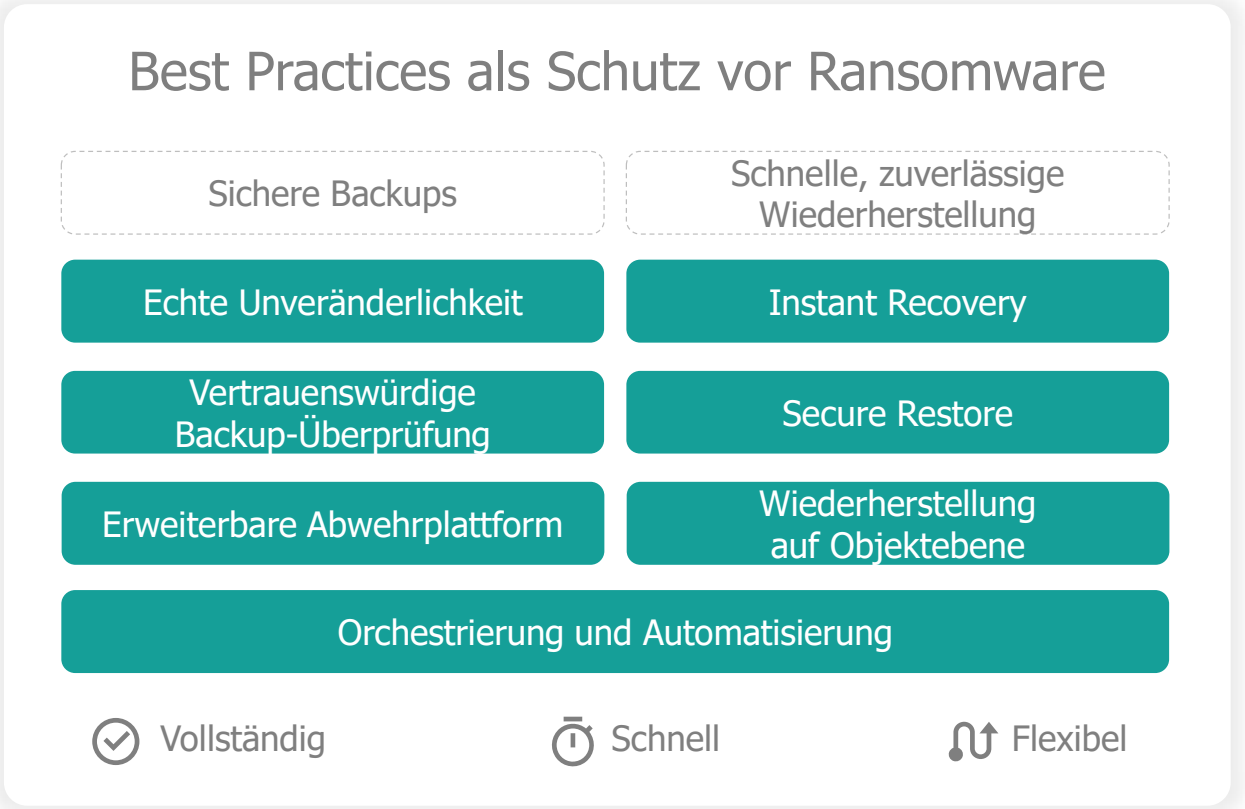
Häufigkeit: Alle 2 Minuten bis alle 11 Sekunden

Innovation: Bitcoin, Ransomware-as-a-Service, Double/Triple Extortion

Aufbau eines Frameworks für resiliente Wiederherstellung

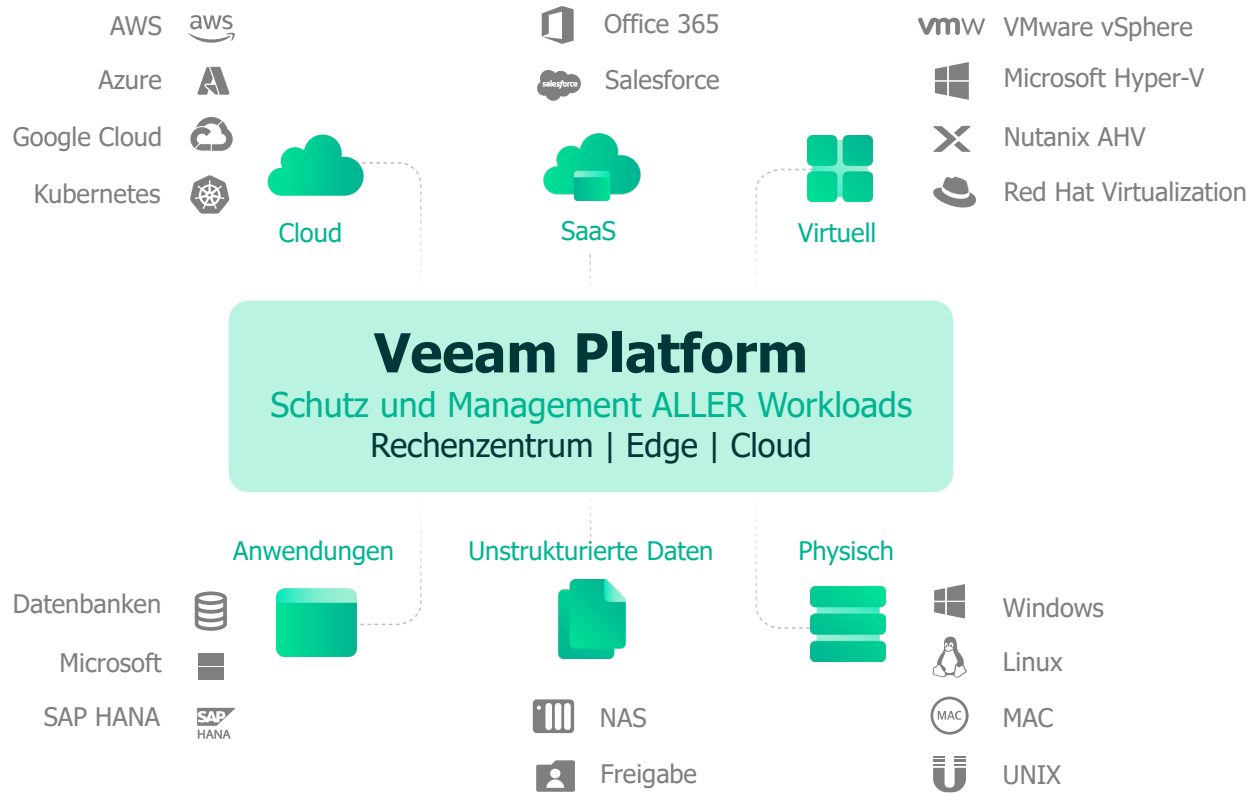
Für ein effektives Sicherheitsprogramm müssen Sie genau wissen, was geschützt werden muss und wie wertvoll eine Ressource für die Organisation ist. Nur dann können Sie bestimmen, wie der Schutz implementiert werden muss. Unabhängig von der gewählten Methodik muss das Framework messbare Ergebnisse definieren, anhand derer IT-Teams Angriffe abwehren und Daten nach einem erfolgreichen Angriff schnell wiederherstellen können. Das NIST Cybersecurity Framework (CSF) schafft beispielsweise eine gemeinsame Sprache für die verschiedenen Stakeholder und wird vielerorts eingesetzt und kontinuierlich aktualisiert. Das NIST CSF wird von vielen Cybersicherheitsexperten als Grundlage für den Aufbau ihrer Programme eingesetzt. Sie definieren damit Best Practices und erschaffen ein einheitliches Wörterbuch zum Verständnis und Management der Risiken moderner Infrastrukturen. Über diesen organisierten Ansatz können sie auch Investitionen in Cybersicherheit begründen, indem sie die Wirkung dieser Investitionen deutlich veranschaulichen. Der Prozess ist zudem iterativ und ermöglicht eine phasenweise Implementierung sowie die Gewinnung von Einblicken aus früheren Implementierungszyklen.

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.



Best Practices und ausgewählte Funktionalitäten von Veeam zum Schutz vor Ransomware

Seit 2019 hat jede Version der Veeam® Modern Data Protection-Plattform wesentliche Funktionalitäten für Cybersicherheit und Schutz vor Ransomware bereitgestellt, um Organisationen die zuverlässige Wiederherstellung nach jedem Cyberangriff in Minutenschnelle zu ermöglichen. Unser softwareorientierter Ansatz bietet flexible Verwaltungsoptionen für resilienten, unveränderlichen Speicher, ob lokal oder in der Cloud – ohne Bindung an proprietäre Hardware. Mit diesen Best Practices können Sie die geeigneten Schutzvorkehrungen für zuverlässige Datensicherung und Wiederherstellung für Ihre kritischen Infrastrukturservices einrichten und stets für verfügbare Daten sorgen.



1. Umfassende, erweiterbare Abwehrplattform

Die bereitgestellte Verfügbarkeitslösung sollte in der Lage sein, alle unternehmenskritischen Workloads zu schützen – ob physisch, virtuell oder containerbasiert. 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.

Veeam bietet eine horizontal skalierbare SDS-Architektur (Software Defined Storage). Am Front-End kann Veeam problemlos zur Aufnahme von Daten zusätzlich zu Ihren Backup-Volumes oder bei erforderlichen Leistungsänderungen erweitert werden. Am Back-End befindet sich ein Scale-out Backup Repository™ (SoBR). Hierbei handelt es sich um ein softwaredefiniertes Konstrukt, das verschiedene Typen von Speichergeräten für Backup-Daten in einem Pool vereint. Über die Richtlinien-Engine von Veeam können Daten auf den am besten geeigneten Geräten platziert werden, einschließlich lokaler Direct Attached Storage (DAS), Deduplizierungs-Appliances, Network Attached Storage (NAS), Objekt-Storage und Cloud. Diese können automatisch oder über einen Serviceprovider verwaltet werden.

Mit all diesen Funktionalitäten stellt die Veeam Platform eine skalierbare Lösung dar, die sich entsprechend Ihrer geschäftlichen Entwicklung und Anforderungen erweitern lässt. Der Ansatz von Veeam ist modular und erweiterbar. Sie sind an keine bestimmte Hardware gebunden und können sich darauf verlassen, dass die Lösung stets mit Ihnen mitwächst.

Die softwaredefinierten Veeam-Funktionalitäten für die Fehlerbehebung nach einem Ransomware-Angriff funktionieren mit jeder Infrastruktur – jetzt und in der Zukunft. Proprietäre Infrastruktur darf keine Voraussetzung sein, damit Unternehmen jede beliebige Hardware oder Cloud einsetzen 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.

2. Erfolgreiche Datensicherung mit automatisierter Überprüfung

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 anderes Backup mit den verfügbaren Production-Daten erstellt werden. 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.

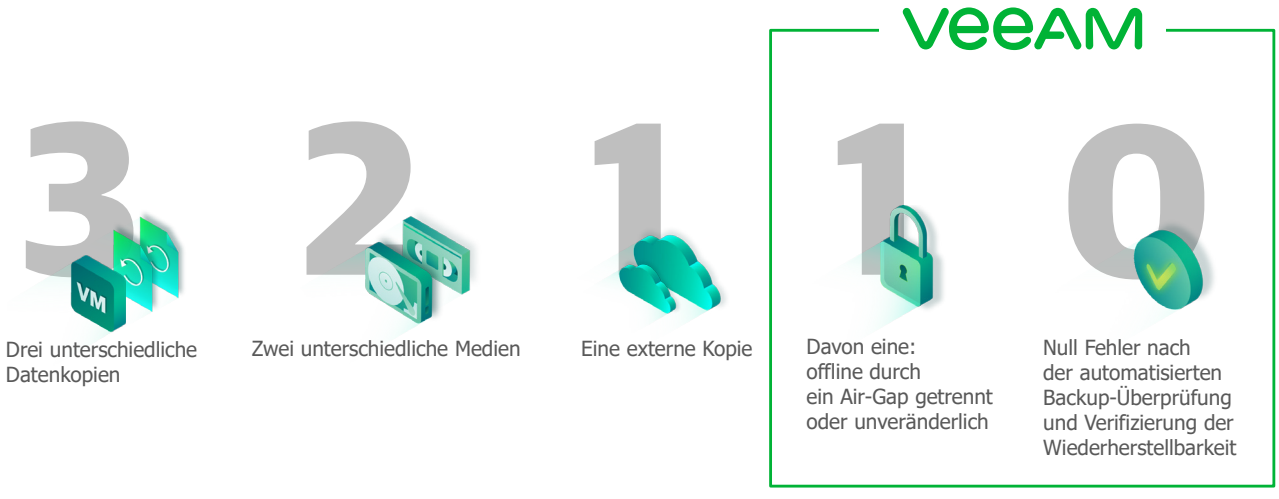
Veeam SureBackup® ist Vorreiter bei der automatisierten Backup-Überprüfung, einerwesentlichen Funktion in unseren Best Practices zur Ransomware-Resilienz. SureBackup startet Server und Anwendungen automatisch in einer vom Netzwerk isolierten Umgebung und führt Integritätsprüfungen mit zahlreichen integrierten 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.

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

Schon seit vielen Jahren ist Veeam ein Vertreter der 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. Für die 3-2-1-Regel wird keine bestimmte Hardware benötigt und sie ist so vielseitig, dass sie nahezu jedes Ausfallszenario abdeckt.

Da Ransomware mit immer fortschrittlicheren Methoden arbeitet, betont Veeam, dass mindestens eine Datenkopie resilient sein muss (z. B. 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.



3. Resiliente Backups — durch Air-Gap getrennt und unveränderlich

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.

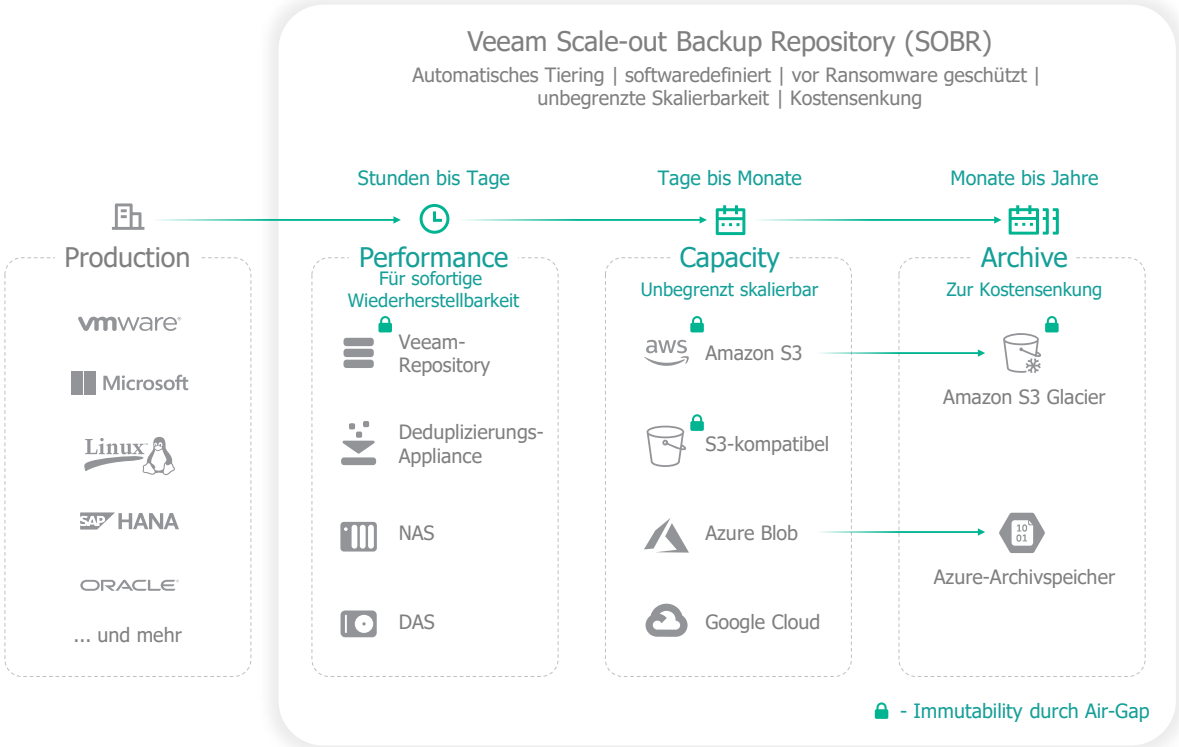
Resilienz können Sie ganz einfach erreichen, indem Sie Daten in Wechseldatenträgern oder Bändern sichern, die Sie dann aus der Bandbibliothek entfernen. Durch Air-Gap getrennte Offline-Backups stellen den ersten Schritt dar.

Veeam bietet einen zuverlässigen, richtliniengesteuerten Ansatz für das Datenmanagement mit verschiedenen resilienten Speicheroptionen. Zertifizierte Speicherlösungen[ii] von Veeam[iii] 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, erhalten 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 (z. B. Wechseldatenträger, Rotationsdatenträger)
- Backups in Veeam Cloud Connect mit Insider Protection (einer servicegesteuerten Funktion)
- Unveränderliche Backups in einem abgesicherten Repository

Die Veeam Platform beinhaltet alle Funktionen für die Fehlerbehebung nach einem Ransomware-Angriff in ihrem Kernprodukt. Diese können einfach vom Kunden bereitgestellt und flexibel mit jeder Infrastruktur, ob lokal oder in der Cloud, eingesetzt werden.



Richtliniengesteuertes Backupdaten-Lebenszyklusmanagement

4. Unveränderlichkeit ist erst der Anfang

Einige Veeam-Kunden möchten sich mit einem Double- oder Triple Immutability-Ansatz zusätzlich absichern. Dazu können sie das abgesicherte Repository von Veeam für lokale Backups der ersten Ebene nutzen und dann die Immutability-Funktion in der automatisch verwalteten Veeam Capacity Tier mit S3-Object-Lock für Cloud- oder lokale Objektspeicher einsetzen und/oder Backups automatisch in physische WORM-Bandmedien (Write One, Read Many) schreiben. Veeam unterstützt physische Bandmedien nativ, ohne dass Sie Integrationen von Drittanbietern benötigen.

Unveränderlichkeit ist sowohl als einfacher Ansatz als auch in Form von Double- oder Triple Immutability effektiv bei der Bewältigung von Cyberbedrohungen. Sie stellt aber erst den Anfang einer umfassenden Strategie für den Schutz vor Ransomware dar.

End-to-End-Verschlüsselung ist zur Abwehr von Datenexfiltration erforderlich. Eine der am schnellsten zunehmenden Cyberbedrohungen besteht derzeit aus Datenleck und Datenexfiltration. Dabei müssen Opfer ein Lösegeld zahlen, um zu verhindern, dass sensible Daten im Dark Web offengelegt werden.

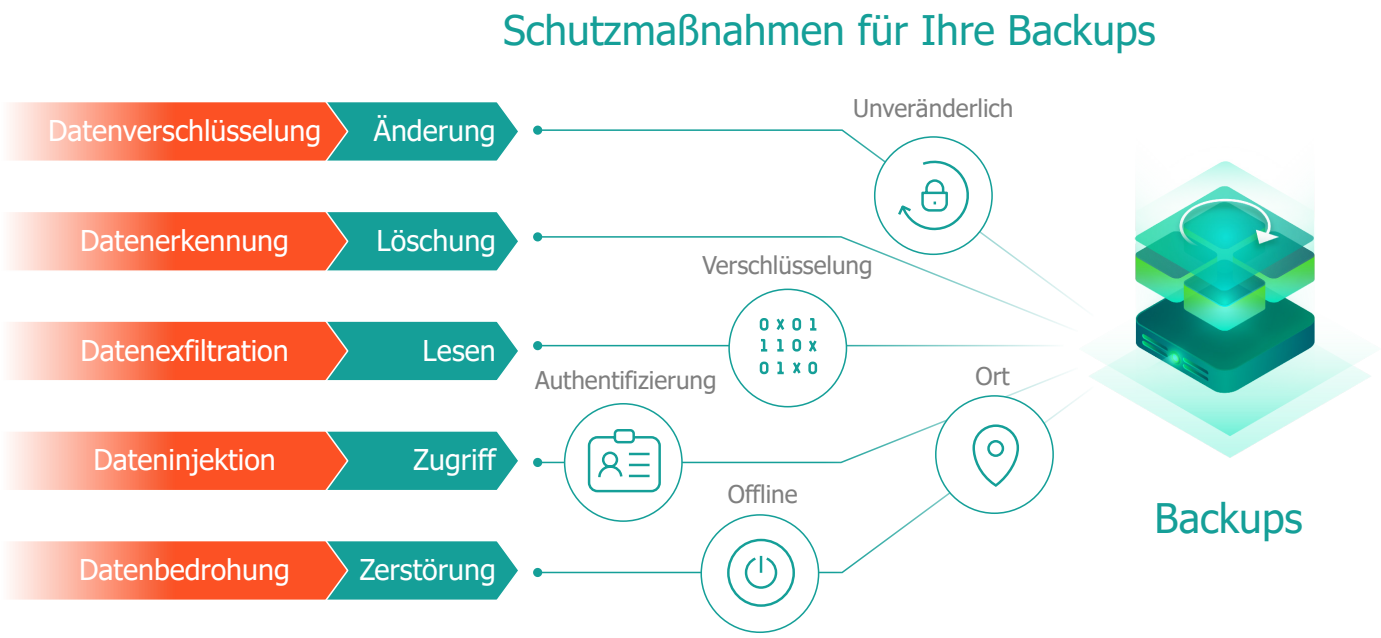
Angemessene Authentifizierung und „Digitalhygiene" bezüglich Least-Privilege-Zugriff sind erforderlich, um Dateninjektion zu verhindern. Außerdem müssen Sie Daten vor Änderung schützen, damit Sie sicher sein können, dass augenscheinlich gültige Datensätze und Einträge nicht böswillig geändert wurden.

Weitere Best Practices zur Digitalhygiene:

- Eindeutige Passwörter für jede Anmeldequelle. So können Sie sicherstellen, dass ein gestohlenes Passwort Hackern keinen Zugriff auf andere Konten gewährt.
- Passwortmanager. Ein robuster Passwortmanager erleichtert die Verwaltung all Ihrer Anmeldeinformationen, sodass Sie sichere, eindeutige Passwörter einfacher erstellen können.
- Multifaktorauthentifizierung (MFA). Sie können die Multifaktorauthentifizierung für höhere Sicherheit Ihrer Konten konfigurieren, sodass bei jeder Anmeldung eine zweite Validierung erforderlich ist.
- Entfernen Sie nicht genutzte Geräte, Anwendungen und nicht erforderliche Programme und Utilitys von allen Servern.
- Patch-Management – Stellen Sie sicher, dass jede verwendete Software, Hardware und Firmware die aktuellen Softwareversionen ausführt, die alle bekannten Schwachstellen abdecken.

Offline-Datenkopien sind unerlässlich, um Insider-Bedrohungen, einschließlich Datenzerstörung, abzuwehren. Insider-Bedrohungen werden zunehmend zur Gefahr. Laut einigen Analysten könnte der Großteil von Cyberbedrohungen in den nächsten drei Jahren von Mitarbeitern ausgehen.

Umfassende Fehlerbehebung nach einem Ransomware-Angriff: Implementieren Sie eine vollständige Strategie für die Fehlerbehebung nach einem Ransomware-Angriff. Mit Veeam erhalten Sie alle erforderlichen Funktionen für die Fehlerbehebung nach einem Ransomware-Angriff: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.



5. Sofortige Wiederherstellung von Daten

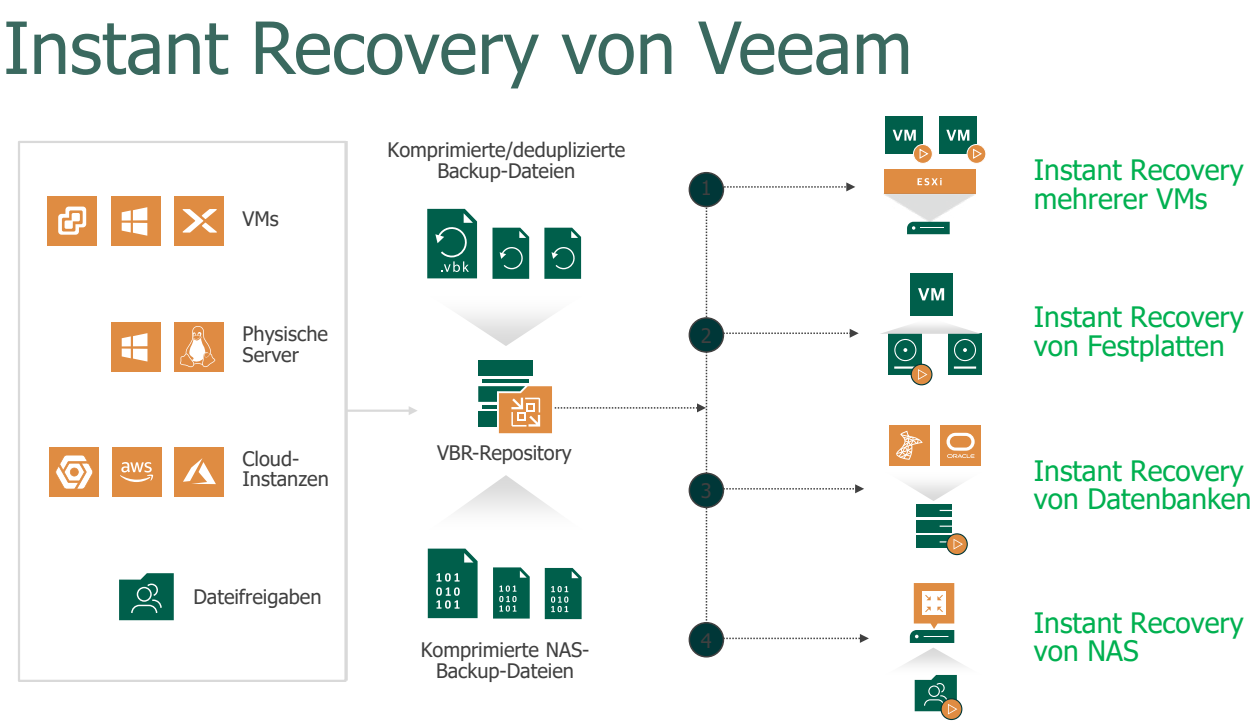
Vor dem Auftreten von Ransomware stellten Unternehmen in der Regel nur 3–5 % ihrer gesicherten Daten über einen Zeitraum von einem Jahr hinweg wieder her. Bei einem Ransomware-Angriff können aber 100 % Ihrer Production-Daten verschlüsselt oder mit Malware infiziert werden, und Sie müssen alle Daten schnell wiederherstellen. Der schnelle Zugriff auf Daten ist Voraussetzung, um 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
- Für die Wiederherstellung physischer und virtueller Dateien und Workloads in einer virtualisierten Umgebung (wie VMware vSphere, Microsoft Hyper-V und Nutanix AHV), sogar mit automatischer Migration von einem Hypervisor zu einem anderen mit nur zwei Mausklicks
- Für die Wiederherstellung physischer und virtueller Dateien und Server in einer Cloud-Umgebung (wie AWS, Azure und Google Cloud Platform), mit nur zwei Mausklicks
- Für die sofortige Wiederherstellung und Nutzung kritischer Unternehmensanwendungen, wie Oracle- und SQL Server-Datenbanken
- Für ein Rollback vollständiger Network Attached Storage-(NAS-) und Dateifreigaben zu einem bekanntermaßen fehlerfreien Zustand vor der Infizierung, damit Sie den normalen Geschäftsbetrieb schnell wiederaufnehmen können

Instant Recovery von Daten mit einem portierbaren Datenformat bietet plattformübergreifenden Datenzugriff für schnelle Wiederherstellung – jederzeit und überall. Von AHV, Hyper-V und vSphere zu physischen Windows- oder Linux-Systemen bis hin zu Azure, AWS oder GCP – die Veeam Platform schützt Sie in jedem Fall.



6. Sichere Wiederherstellung von Daten

Ransomware kann über Monate hinweg unbemerkt im Netzwerk eines Opfers vorhanden sein, bevor ein Angriff eingeleitet wird. Daher müssen Sie per Automatisierung sicherstellen, dass Sie nie Malware in einer bereinigten oder neuen Umgebung wiederherstellen.

Der vielseitige SureBackup-Job (oben unter Punkt 2 beschrieben) kann unter anderem kontinuierlich ausgeführt werden, damit Sie weitere Überprüfungen und forensische Untersuchungen im System nach dem Wiederherstellungspunkt des Backups ausführen können. Dabei kann es sich z. B. um eine manuelle Inspektion handeln, um herauszufinden, ob die Ransomware-Bedrohung weiterhin besteht, oder die Untersuchung bestimmter Dateien.

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

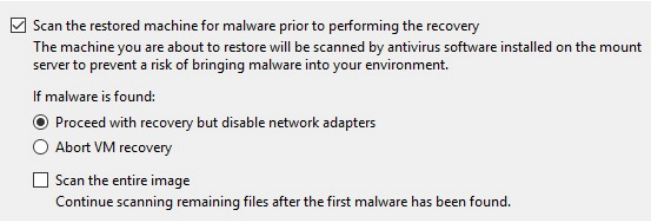
Veeam Secure Restore liefert eine voll integrierte Virenprüfung als optionalen Schritt jedes Wiederherstellungsprozesses. Dieses Feature löst die Probleme beim Malware-Management, da Sie damit stets sicherstellen können, dass alle gesicherten Daten, die Sie im Production-System wiederherstellen möchten 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.** Mit Secure Restore können Sie sich darauf verlassen, dass eine Bedrohung korrekt neutralisiert und gänzlich aus Ihrer Umgebung beseitigt wurde.

Secure Restore kann komplett über PowerShell konfiguriert werden. Wenn Sie also Wiederherstellungsprozesse über eine Drittanbieterintegration oder ein externes Portal automatisieren, können Sie diese Funktion ebenfalls nutzen, um die Wiedereinführung von Bedrohungen in Ihre Produktivumgebung zu verhindern.

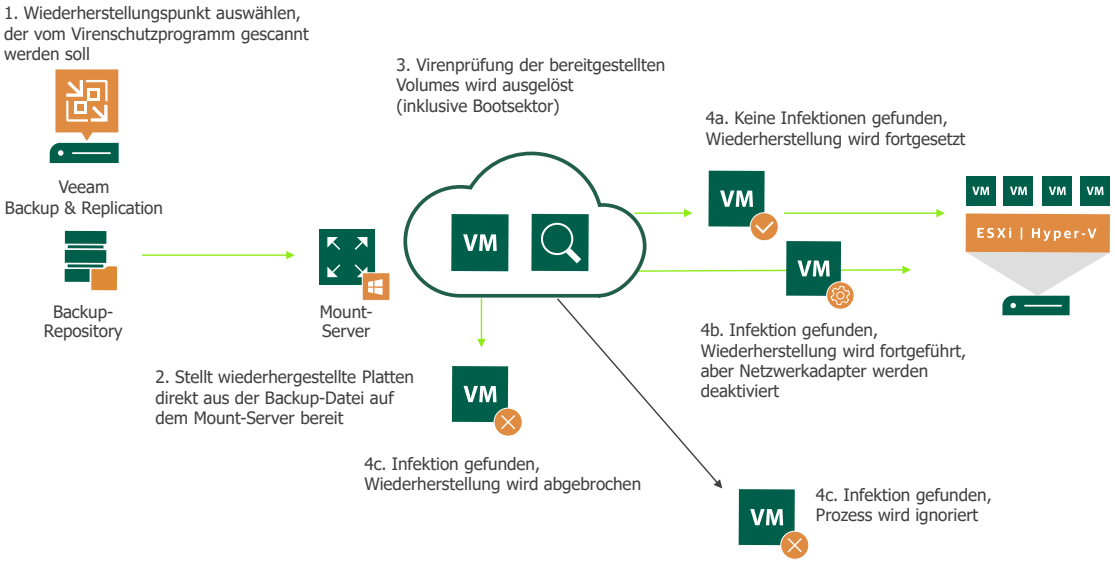
Diese leistungsstarke Funktionalität eignet sich für Folgendes:

- Erkennung „ruhender" Ransomware in Backup-Daten und Aufruf der Beseitigungsschritte des Virenschutzprogramms, um Daten vor der Wiedereinführung in die Produktivumgebung zu bereinigen
- Überprüfung von Backups aus Standorten mit weniger IT-Kontrollen, wie Remote-Standorte und Zweigstellen (ROBO), vor der Wiederherstellung in den Primärdaten
- Scan von Backup-Daten mit zusätzlichen Virenschutzlösungen, um seltene oder Zero-Day-Malware besser zu erkennen

Wie alle Funktionalitäten der Veeam Platform lässt sich Secure Restore schnell und einfach mit nur wenigen Mausklicks konfigurieren:



Veeam DataLabs: Secure Restore



7. Automatisierte Wiederherstellung

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 automatische 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** (VDRO) **können Sie komplexe Workflows komplett automatisieren und dokumentieren, darunter unterbrechungsfreie, groß angelegte Wiederherstellungstests mit dynamischer Dokumentation.** Die Dokumentation für Incident-Response/-Recovery kann auch mit Veeam-externen Informationen aktualisiert werden, wie Kontaktlisten und andere unternehmenskritische Reaktionsinformationen.

Zuverlässige Wiederherstellung

- Zuverlässige, skalierbare Orchestrierung
- Anwendungsbezogen

Automatische Tests

- Unterbrechungsfrei
- Geplant oder spontan
- Readiness Checks

Dynamische Dokumentation

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

Die meisten Organisationen nutzen viele Arten von Business Continuity-(BC-) und Disaster Recovery-(DR-)Plänen. Einige Beispiele:

- Fehler auf Anwendungsebene
- Fehler auf Site-Ebene
- Fehler von Infrastrukturkomponenten
- Geschäftskritische Anwendungen
- Entwicklungs-/Testanwendungen

Genauso wie die automatisierte Backup-Überprüfung, wie Veeam SureBackup, für den täglichen Backup-Betrieb entscheidend ist, sind auch regelmäßige Tests Ihres Wiederherstellungsplans für die Cyberresilienz notwendig. Wenn Sie einen Wiederherstellungsplan aufgestellt haben, müssen Sie diesen unbedingt testen. Nur so erfahren Sie, ob Ihr Plan auch wirklich funktioniert. Viele Disaster-Recovery-Pläne werden nur unzulänglich oder überhaupt nicht getestet. Die meisten Organisationen testen ihre DR-Pläne bestenfalls einmal oder zweimal im Jahr.

Kontinuierliche Tests sind aber wichtig, besonders da Anwendungen sich stets verändern. Um Änderungen und Konfigurationsabweichungen zu berücksichtigen, müssen Wiederherstellungspläne bei jeder Anwendungsänderung aktualisiert werden, z. B. wenn Sie die Kapazität mit zusätzlichen Servern erweitern oder ältere Server entfernen. Legen Sie bei den Tests besonderes Augenmerk auf das, was nicht wie geplant läuft. Nur so können Sie Ihren Disaster-Recovery-Plan verbessern. Der Test dient einzig dazu festzustellen, ob der Plan funktioniert oder nicht.

Cyberresilienz und erfolgreiche Fehlerbehebung nach einem Ransomware-Angriff müssen Teil Ihres Disaster-Recovery-Plans sein. Am besten bereiten Sie sich auf Cybersicherheitsvorfälle vor, indem Sie einen Notfallplan aufstellen. In einem klar umrissenen Notfallplan können Sie Verfahren zum Erkennen, Kommunizieren, Kontrollieren und Beseitigen von Sicherheitsvorfällen definieren, damit Mitarbeiter immer wissen, wie sie auf ein Cybersicherheitsereignis reagieren müssen.

Darüber hinaus muss dieser Plan automatisch getestet werden, die dynamische Aktualisierung der wichtigen Dokumentation ermöglichen und sich in andere notwendige Tools und Workflows integrieren lassen. Dann können Sie den kritischen Geschäftsbetrieb stets erfolgreich wiederaufnehmen.

1-Click Site Recovery und DR-Tests

Veeam Disaster Recovery Orchestrator

Fazit

Die Daten eines Unternehmens gehören zu seinem wertvollsten Gut. Ransomware ist aber eine wachsende Bedrohung für die kritischen Daten von Organisationen aller Größenordnungen aus allen Branchen und Regionen. Unternehmen müssen ihre Sicherheitsprogramme unbedingt kontinuierlich verbessern, um Daten effektiv zu schützen. Außerdem benötigen sie robuste Funktionalitäten für die schnelle und sichere Wiederherstellung nach einem Vorfall. Für ein umfassendes Sicherheitsprogramm müssen Sie Personen, Prozesse und Technologien so zusammenführen, dass das Programm stets verbessert wird und Sie sich gleichzeitig bestmöglich schützen. 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.

Die Implementierung einer vollständigen Fehlerbehebungsstrategie ist unerlässlich, um Bedrohungen wie Ransomware entgegenzuwirken. Mit Veeam erhalten Sie alle erforderlichen Funktionen für die Fehlerbehebung nach einem Ransomware-Angriff sowie umfangreiches Expertenwissen, sodass Daten bei einer Krise stets verfügbar bleiben. Unser softwareorientierter Ansatz bietet flexible Verwaltungsoptionen für resilienten, unveränderlichen Speicher, ob lokal oder in der Cloud – ohne Bindung an proprietäre Hardware. Mit unseren Best Practices und der modernen Datensicherungsplattform von Veeam erreicht Ihr Unternehmen digitale Resilienz. So minimieren Sie Ausfallzeiten nach einem Ransomware-Angriff anhand komplett automatisierter Prozesse für Ransomware-freie Wiederherstellung und DR-Orchestrierung an jedem Speicherort.

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.

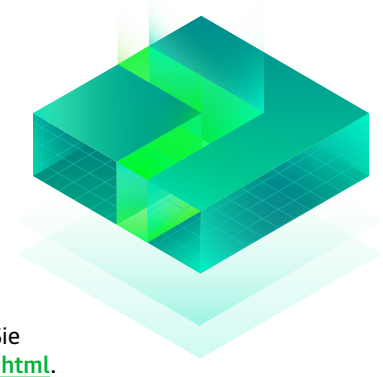
Informationen zu Veeam Software

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.

Veeam-Produkte für Ihre Fehlerbehebung nach Ransomware-Angriffen

Veeam-Produkte für Ihre Fehlerbehebung nach Ransomware-Angriffen

- Veeam Backup & Replication
- Veeam ONE
- Veeam Disaster Recovery Orchestrator
- Veeam Backup *for AWS*, *Azure* und *Google Cloud Platform*
- Veeam Backup *for Microsoft Office 365*
- Kasten K10 by Veeam



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

Ein detailliertes technisches White Paper zu den Best Practices im Hinblick auf Ransomware und eine ausführliche Beschreibung der Cybersicherheitsfunktionen von Veeam sind hier verfügbar: https://www.veeam.com/wp-protection-yourself-from-ransomware.html?wpty.

Autoren

Dave Russell verfügt über 32 Jahre Erfahrung in der Speicherbranche. Er ist als Vice President of Enterprise Strategy bei Veeam für die Entwicklung strategischer Produkt- und Markteinführungsprogramme, die Förderung des Engagements in der Branche und die Verbreitung der Vision von Veeam für moderne Datensicherung verantwortlich. Vor Veeam war er 13 Jahre lang Vice President und Distinguished Analyst bei Gartner und davor 15 Jahre bei IBM in der Produktentwicklung für die Datensicherung und Wiederherstellung von Mainframe und offenen Systemen zuständig.

Jeff Reichard ist Senior Director of Enterprise Strategy bei Veeam mit Schwerpunkt auf Risiken, Compliance und Partnerschaften. Er blickt auf über 25 Jahre Erfahrung in den Bereichen Datensicherung/Verfügbarkeit, Business Continuity und Lösungen zur Einhaltung gesetzlicher Vorschriften zurück. Seine früheren Aufgaben reichten von der Entwicklung von SAN- und Daten-Backup-Lösungen bis hin zu Systemtechnik und technischer Leitung für Kunden aus dem öffentlichen Sektor und Unternehmen. Vor seiner Tätigkeit bei Veeam leitete Jeff Reichard zuletzt das nationale nicht-militärische SE-Team von Commvault. Bei Veeam arbeitet er mit Partnern, Kunden und Branchenanalysten zusammen, um die Vision von Veeam für Cloud-Datenmanagement und Digital Transformation zu verbreiten.

Chris Hoff hat in mehr als 15 Jahren Tätigkeit im Bereich Cybersicherheit umfangreiche technische Erfahrungen gesammelt. Er leitet derzeit die Marketingaktivitäten für Sicherheit and Datensicherung bei Veeam. Zuvor war Chris in verschiedenen Ingenieurs-, Vertriebs- und Produktmanagementrollen tätig. Während seiner Laufbahn hat er zahlreichen Organisationen beim Management von Cyberrisiken geholfen und Lösungen für Branchen-Frameworks, Programme und Compliance-Vorschriften entwickelt.

i https://www.infosecurity-magazine.com/news/cybersecurity-skills-shortage-1/

ii Technische Zertifizierungen für unveränderlichen Speicher wurden aufgrund der Regulierung in der Finanzbranche eingeführt. Zahlreiche Regierungsregeln sollen sicherstellen, dass regulierte Organisationen unveränderte Kopien ihrer Finanzdaten für einen vorgeschriebenen Zeitraum beibehalten (in den USA beispielsweise SEC-Regel 17a-4(f), FINRA-Regel 4511 und CFTC-Regel 1.31 (c)-(d)). Die gleichen Kontrollzertifizierungen, die die Integrität von Finanzdaten garantieren, können auch für unlöschbare und unveränderliche Backup-Daten eingesetzt werden.

iii Die aktuellen Compliance-Zertifizierungen des abgesicherten Linux-Repositorys von Veeam finden Sie unter https://www.veeam.com/blog/hardened-repository-passes-compliance.html.