7 Best Practices für die Wiederherstellung nach Ransomware-Angriffen

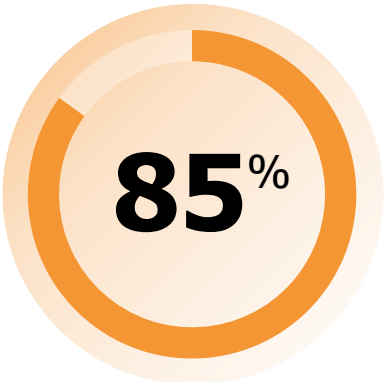
Wiederherstellung als Priorität behandeln

Inhalt

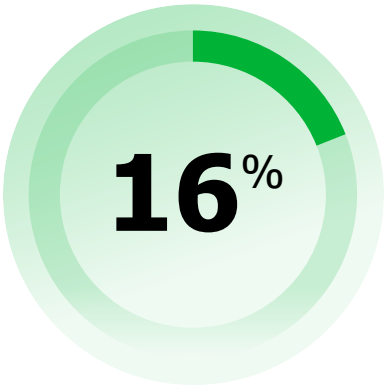
Einführung: Ein Ransomware-Angriff ist der schlimmste Katastrophenfall

Seit einigen Jahren häufen sich Ransomware-Angriffe und sie werden immer raffinierter. Damit sehen sich Unternehmen jeder Größe und Branche einem größeren Risiko gegenüber. Ransomware-Angriffe können verheerende Folgen haben: Betriebsunterbrechungen, finanzielle Verluste, Rufschädigung und sogar juristische und regulative Konsequenzen drohen. Deshalb braucht die Geschäftsleitung einen eindeutigen, umfassenden Plan für die Wiederherstellung nach einem Ransomware-Angriff, um die Folgen zu minimieren und den Geschäftsbetrieb so schnell wie möglich wieder aufzunehmen.

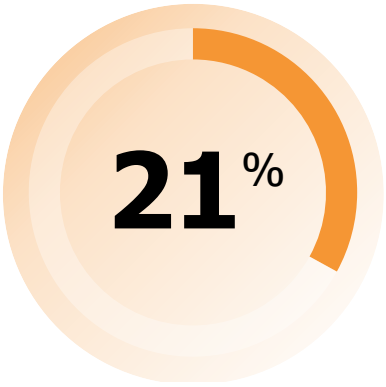
Aus den Veeam-Reports zu Datensicherungs- und Ransomware-Trends 2023:



der Unternehmen wurden im vergangenen Jahr mindestens einmal Opfer eines Ransomware-Angriffs.



der Unternehmen konnten ihre Daten ohne Zahlung eines Lösegelds wiederherstellen.



bezahlten das Lösegeld, konnten ihre Daten aber nicht wiederherstellen.

* Quelle: Data Protection Trends Report 2023, Ransomware Trends Report 2023

Nicht jeder Cyberangriff lässt sich verhindern, deshalb muss die Wiederherstellung nach dem Ernstfall zur Priorität werden. Backups werden weithin als eines der effektivsten Mittel bei Ransomware-Angriffen genutzt. Mit einem aktuellen, bestätigten und sicheren Backup steigt die Chance auf eine erfolgreiche Wiederherstellung nach kurzer Ausfallzeit und möglichst geringem Datenverlust.

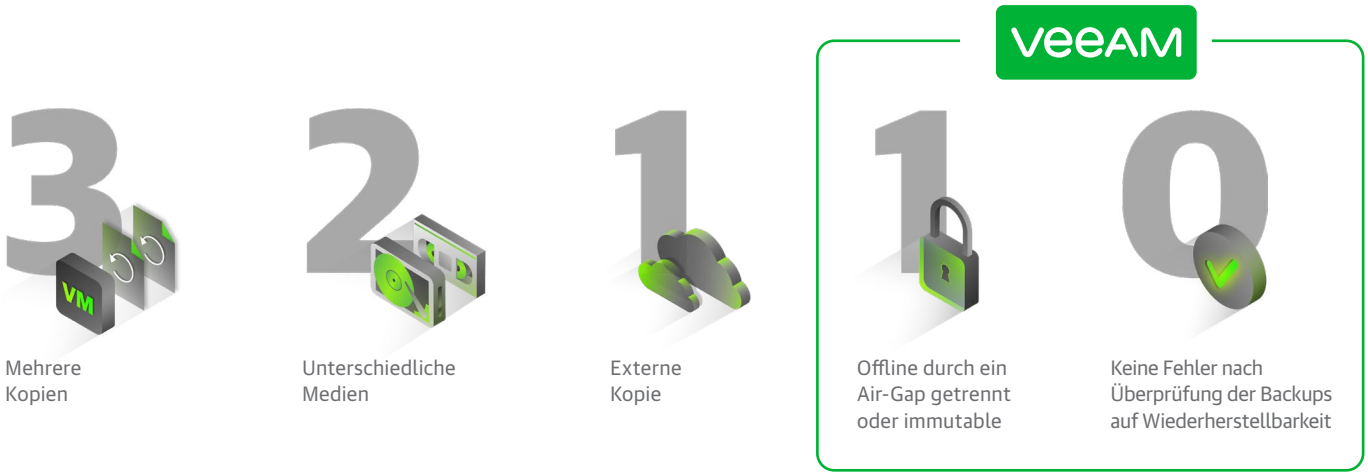
Disaster-Recovery-Planung gilt schon lange als Muss bei der gelungenen Infrastrukturplanung und verleitet zu Annahmen über die Integrität und Verfügbarkeit der Daten im Krisenfall. Die Risikoberechnung basiert auf einer veralteten Statistik für die Datenwiederherstellung, wonach nur **3** bis **5 Prozent** der Daten pro Jahr betroffen seien. Seitdem Ransomware allgegenwärtig ist, stimmt das aber nicht mehr. Unternehmen müssen sich heute darüber im Klaren sein, dass ein einziger Vorfall reichen kann, um 100% ihrer Daten zu verlieren.

Einen Ransomware-Angriff übersteht nur, wer mehrere Voraussetzungen erfüllt. In diesem White Paper nehmen wir das Framework unter die Lupe, das eine sichere, stabile Infrastruktur gewährleistet, in der sich Bedrohungen frühzeitig erkennen, Daten schnell wiederherstellen und alle Schritte im erforderlichen Umfang orchestrieren lassen.

1. Datenresilienz

Viele Unternehmen wenden zur Datensicherung standardmäßig die branchenübliche 3-2-1-Regel an. Viele Jahre war dies völlig ausreichend, doch seit dem Aufkommen von Ransomware ist diese Regel obsolet. Daher müssen Unternehmen mittlerweile einen Schritt weitergehen: Sie benötigen eine unveränderliche Kopie ihrer Daten (Immutability) und müssen umfangreiche Tests durchführen, wenn sie sichergehen wollen, dass ihre Daten fehlerfrei sind. Als Goldstandard gilt heute die 3-2-1-1-0-Regel, auch „Postleitzahl der Verfügbarkeit" genannt.

Die 3-2-1-1-0-Regel umsetzen



Jeder Kunde hat andere Anforderungen und Möglichkeiten, doch Veeam bietet so viele Optionen, dass sich die 3-2-1-1-0-Regel gut umsetzen lässt. So kann **Veeam Backup & Replication** diese Regel „out-of-the-box" einhalten, zum Beispiel wie in diesem Szenario: Drei Kopien der Daten (Produktions-Workloads, eine Kopie im Backup-Repository und eine Kopie auf Band) auf zwei unterschiedlichen Medien (Festplatten-Repository und Band), eines davon extern (Band) und eines unveränderlich (WORM-Bandmedium) — beide jedoch mit null Fehlern (geprüft mittels SureBackup).

Immutability im Datenlebenszyklus

Nicht ohne Grund wird Objektspeicher immer beliebter: Er ist langlebig, von Cloud-Providern wird er als Service angeboten und mit S3-Object-Lock-Technologie lässt sich Immutability leicht erreichen. Wenn Backups direkt in den Objektspeicher geschrieben werden können, profitieren Kunden über den gesamten Lebenszyklus der Daten hinweg von deren Unveränderlichkeit. Zusätzliche Kontrollmöglichkeiten sind zudem geboten, weil die Verwaltung der Backup-Ziele nun von der Steuerung des Backup-Servers getrennt ist. Ist für Immutability gesorgt, sind Ihre Backups auch dann sicher, wenn ein böswilliger Backup-Administrator oder ein externer Hacker auf den Backup-Server zugreift.

Wiederherstellungspunkte können automatisch zu einem sekundären Speicherort geleitet werden, der in unveränderlichem Speicher gesichert wird. Dabei ist es unerheblich, ob dies lokal oder cloudbasiert geschieht. Ist eine Langzeitaufbewahrung erforderlich, unterstützt die Archivierungsebene Immutability mittels Amazon S3 Glacier oder Microsoft Azure Archive-Blobspeicher.

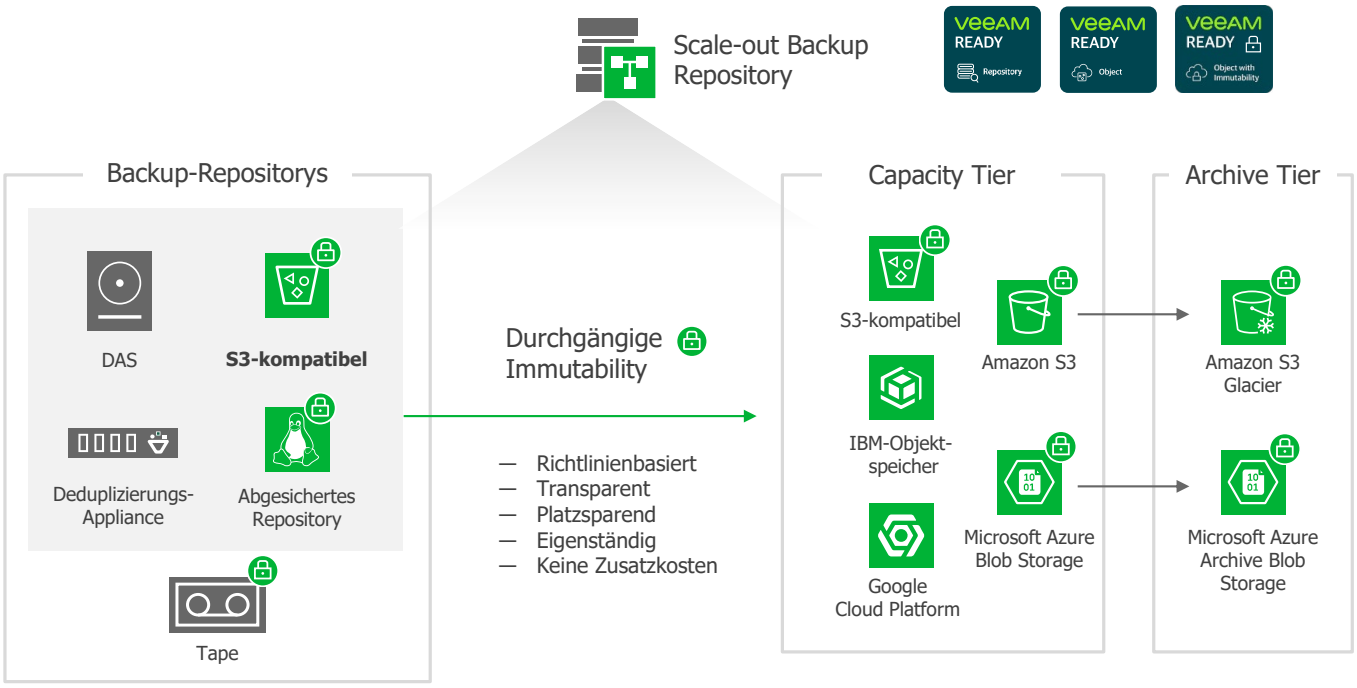
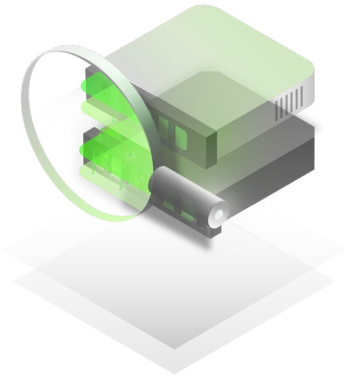


Abbildung 1 — Immutability während des gesamten Datenlebenszyklus



Falls **Objektspeicher** nicht zur Verfügung steht, kann auch das **abgesicherte Repository von Veeam** genutzt werden. Im Zuge der Bereitstellung verlangt das abgesicherte Repository Anmeldedaten zur einmaligen Anwendung. Danach bietet es native Funktionalitäten für Linux-Dateisysteme zu dem Zweck, Backup-Dateien als unveränderlich zu kennzeichnen. Wie bei allen anderen Systemen auch müssen Voraussetzungen und Best Practices für die Sicherheit bedacht werden. Am besten halten sich Anwender an Empfehlungen wie die, den physischen und netzwerkbasierten Zugriff einzuschränken sowie Hosts abzusichern.

2. Auslegung auf *schnelle* Wiederherstellung

Im Ernstfall ist der Rückgriff auf vorhandene Backups der erste Schritt zur Wiederherstellung. Denn ist Ihr Unternehmen handlungsunfähig, verlieren Sie Geld und Ihren guten Ruf. Um so schnell wie möglich weiterarbeiten zu können, benötigen Sie zwingend eine zuverlässige Lösung, die Ihnen dies ermöglicht.

2010 stellte Veeam das Feature **Instant VM Recovery** vor, mit dem sich VMs unverzüglich wiederherstellen und wieder in Betrieb nehmen lassen. Mittlerweile findet es nicht nur bei VMs Anwendung. Sofort wiederherstellen lassen sich auch Veeam Agent-Backups, physische Maschinen inbegriffen, Microsoft SQL Server- und Oracle-Datenbanken, cloudbasierte Workloads (z. B. Amazon EC2, Microsoft Azure und Google Compute Engine) und sogar NAS-Dateiserver. Sobald die Daten gemountet und zugänglich sind, können Nutzer direkt auf ihre Ressourcen zugreifen. Migrationen zum Kopieren von Daten zurück in den Produktivbetrieb können im Hintergrund ablaufen. Dies umfasst die Differenz zwischen dem ursprünglichen Backup und den Änderungen aus der Sofortwiederherstellung.

Replikatbasierte Wiederherstellung mit kurzem RPO

Die Replikations-Engine von **Veeam Data Platform** ist eine zusätzliche leistungsstarke Option und bietet größere Granularität, wenn es darum geht, kürzere RPOs zu erreichen. Ein Backup-Job kann alle 24 Stunden ausgeführt werden, ein Replikationsjob hingegen kann häufiger stattfinden (z. B. alle 2 Stunden). Dies kann den Abstand zwischen Wiederherstellungspunkten erheblich verkürzen.

Bei der Replikation wird ein Snapshot der zu schützenden VM erstellt und an einem speziellen Speicherort repliziert, meist einem DR-Standort. Das Erstreplikat ist eine vollständige Kopie der VM, alle nachfolgenden enthalten nur die Änderungen seit der letzten Replikation. Um den anfänglichen Prozess zu beschleunigen, bietet sich das Replikat-Seeding aus Backup-Dateien an. Zusätzlich kann auch der Veeam WAN Accelerator verwendet werden, um die Replikation zu beschleunigen.

Wenn virtuelle Workloads praktisch keinen Datenverlust hinnehmen können, empfiehlt sich die **kontinuierliche Datensicherung von Veeam (CDP)**. Mit der vSphere-API von Veeam für die E/A-Filterung sind Replikationen in Sekundenschnelle möglich, die die Leistung der betreffenden VM allerdings nicht schmälern.

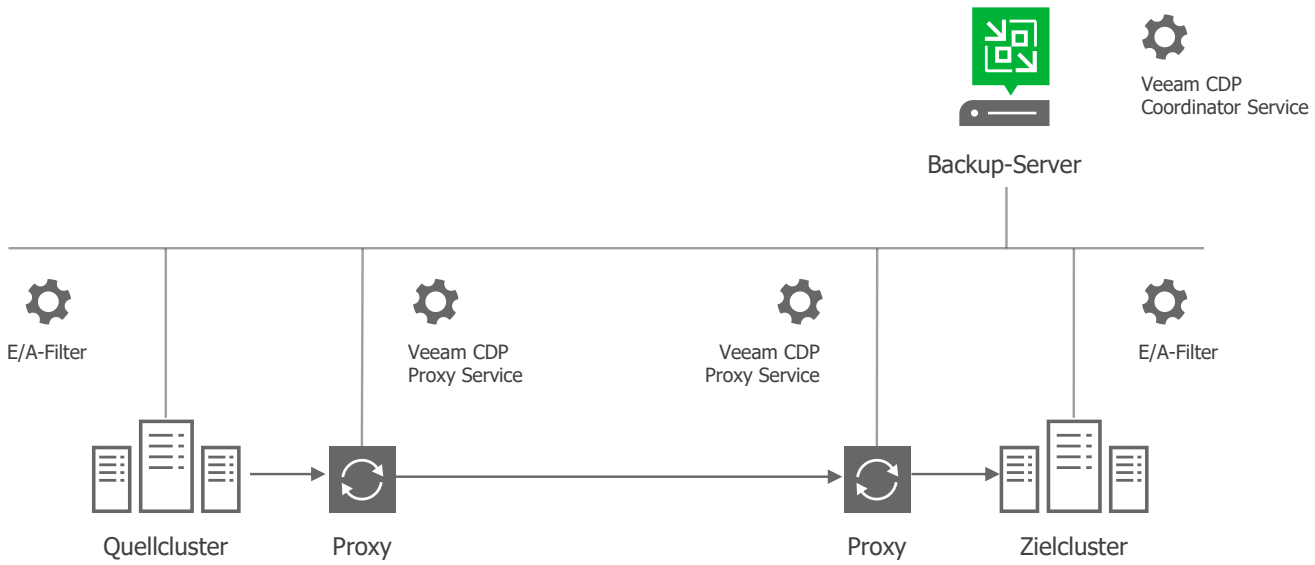
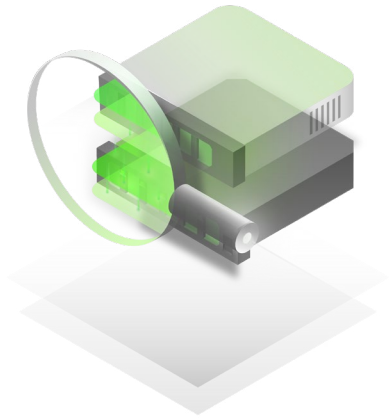


Abbildung 2 — Architektur von Veeam CDP

Leistungsstarke Storage-Snapshot-Integration



Veeam bietet zahlreiche Provider- und Speichersystem-Integrationen sowie die Systemintegration per Universal Storage API. Dank dieser einzigartigen API gelingt das Sichern und Wiederherstellen von Daten aus Snapshots mühelos. Expertenwissen zu Speicher-Arrays ist nicht notwendig.

Um die Auswirkungen auf den Produktivbetrieb so gering wie möglich zu halten, können arraybasierte Snapshots genutzt werden, um Backups zu erstellen. Darüber hinaus erhalten Anwender von **Veeam Explorer *for Storage Snapshots*** und **Instant VM Recovery *die Möglichkeit,*** anhand von Storage-Snapshots Wiederherstellung schnell und einfach durchzuführen — von ganzen VMs bis hinunter auf Datei- oder Anwendungsebene. Sie können die üblichen Backup-Jobs planen, aber auch Snapshot-Orchestrierung nutzen, um Ihre RPOs einzuhalten.

Backups vertrauen — aber nur getesteten

SureBackup ist eine Veeam-Technologie zum Testen von Backups, um sicherzustellen, dass diese später Datenwiederherstellungen ermöglichen. Wenn sich beispielsweise beim nächsten Systemstart eine Bedrohung zeigt, kann SureBackup erkennen, welches Problem den Start verhindert, oder eine Anwendung identifizieren, die nicht wie erwartet startet. SureBackup-Jobs können dazu beitragen, dass Anwendungen aus Backups (oder Replikate in VMware-Umgebungen) wie erwartet starten. Sie erhalten einen Report darüber, dass der Wiederherstellungspunkt tatsächlich wiederhergestellt werden konnte. Tests sind immer zu empfehlen, doch geradezu unverzichtbar ist die automatische Verifizierung für Wiederherstellungen nach Ransomware-Angriffen.

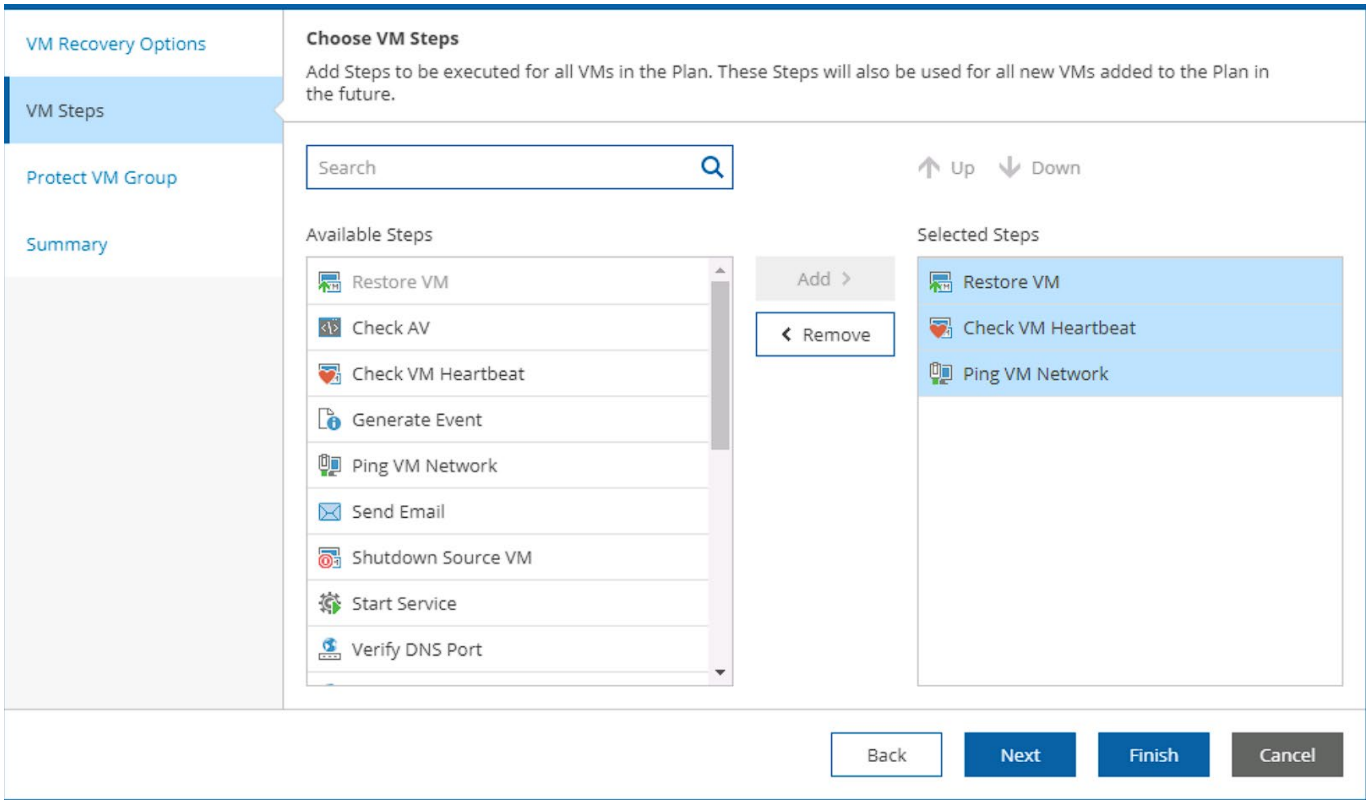
Zu den flexiblen Eigenschaften eines SureBackup-Jobs gehört, dass Sie ihn nach dem Start einfach weiter ausführen können. Der SureBackup-Job führt von alleine die konfigurierten Prüfungen durch. Wenn der Job so eingestellt ist, dass er weiter ausgeführt werden soll, können über den Wiederherstellungspunkt zusätzliche Prüfungen des Systems durchgeführt werden. Dabei kann es sich z. B. um eine automatisierte oder manuelle Inspektion handeln, um herauszufinden, ob die Ransomware-Bedrohung weiterhin besteht, zu überprüfen, ob bestimmte Dateien Anomalien aufweisen oder Daten verschlüsselt wurden, oder bestimmte Daten für weitere Analysen zu extrahieren.

Wiederherstellungen automatisieren und orchestrieren

Schafft es Ransomware doch in Ihr Netzwerk, werden Sie wahrscheinlich nicht nur eine Wiederherstellung durchführen müssen. In der Regel sind mehrere Workloads betroffen, und selbst solche, die verschont wurden, können aufgrund von Abhängigkeiten ausfallen. Umfassende Wiederherstellungen erfordern ein entsprechendes Maß an Geschwindigkeit, Automatisierung und Orchestrierung. Veeam Data Platform bietet Unternehmen alles Nötige, um Daten zügig wiederherzustellen.

Ob ein DR-Plan etwas taugt, zeigt sich erst im Ernstfall. **Veeam Recovery Orchestrator** liefert Nachweise, sodass Unternehmen Gewissheit haben und beruhigt sein können. Individuelle dynamische Dokumentationen und Reports bieten all jene Belege, die Unternehmen beim Risikomanagement benötigen. Genauso praktisch sind die automatischen Tests, die Administratoren planen können, um zu erfahren, ob Wiederherstellungen überhaupt durchführbar sind. Solche automatischen Tests stärken auch die Sicherheit, denn Wiederherstellungspunkte lassen sich auf Ransomware überprüfen. So wissen Administratoren mit Sicherheit, dass Viren nicht wieder eingeschleust werden.

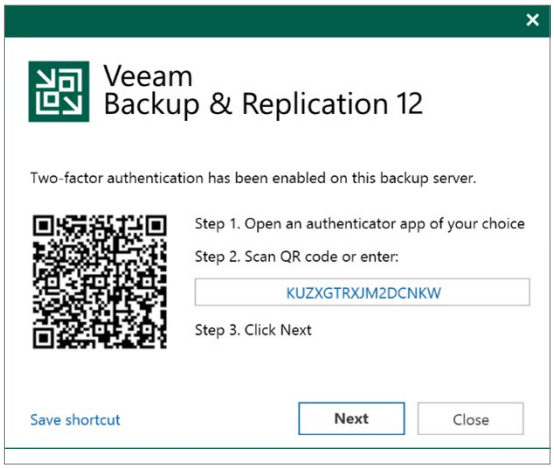
Immer häufiger schaffen es Unternehmen nicht, Wiederherstellungen zurück in die Produktivumgebung durchzuführen. Ungeachtet der möglichen Gründe, z. B. Ressourcenmangel, forensische Ermittlungen, Anforderungen des Versicherungsschutzes gegen Cyberangriffe – ohne einen Zielort für die Wiederherstellung geht es nicht. Mit Veeam Data Platform können Wiederherstellungen direkt in Microsoft Azure durchgeführt werden, was Unternehmen flexible Handlungsfähigkeit verleiht.



3. Anwendung mehrstufiger Sicherheit

Jeder Sicherheitsexperte hat einen grundlegenden Tipp für mehr Sicherheit: die Haustür abschließen. Egal, ob es sich um eine echte oder sprichwörtliche Tür handelt, die Gefahrenabwehrstrategie sollte noch mehr umfassen. Veeam bietet eine Reihe von Hilfsmitteln, mit denen es Unternehmen Angreifern sehr schwer machen können.

Angreifer fernhalten



Multifaktorauthentifizierung (MFA) sollte überall angewendet werden, wo es möglich ist. Vom Betriebssystem aus betrachtet, sollten infrastrukturelle Komponenten wie Proxies, Repositories und der Backup-Server selbst eine Form der MFA beim Anmelden erfordern. Zusätzlich sollten sich Benutzer der Veeam Backup & Replication-Konsole nur per MFA anmelden können. Dieses Feature ist auch offline nutzbar, falls der Backup-Server nicht mit dem Internet verbunden ist. Diese inhärente Sicherheitsvorkehrung sorgt für mehr Flexibilität.

Für die Interaktion mit Gastbetriebssystemen, z. B. im Fall eines Windows-Servers, der SQL Server ausführt, eignen sich Tools wie gMSAs (Group Managed Service Accounts) besonders gut. Diese Konten erfordern zufällig automatisch generierte 240-Byte-Passwörter, die automatisch alle 30 Tage wechseln. Insgesamt stellt dies eine äußerst robuste, zuverlässige Schnittstelle zu den Workloads dar.

Wenn Sie wissen möchten, wie sicher Ihre Backup-Umgebung wirklich ist, können Sie jederzeit den **Best-Practices-Analyzer für Sicherheit** anwenden. Dieses Tool liefert eine Übersicht der Best Practices für Sicherheit in der Serverkonfiguration von Veeam Backup & Replication. Bei Veränderungen an der Umgebung kann das Tool ausgeführt werden, um die Konsequenzen zu ermessen.

Daten während der Übertragung und bei der Speicherung schützen

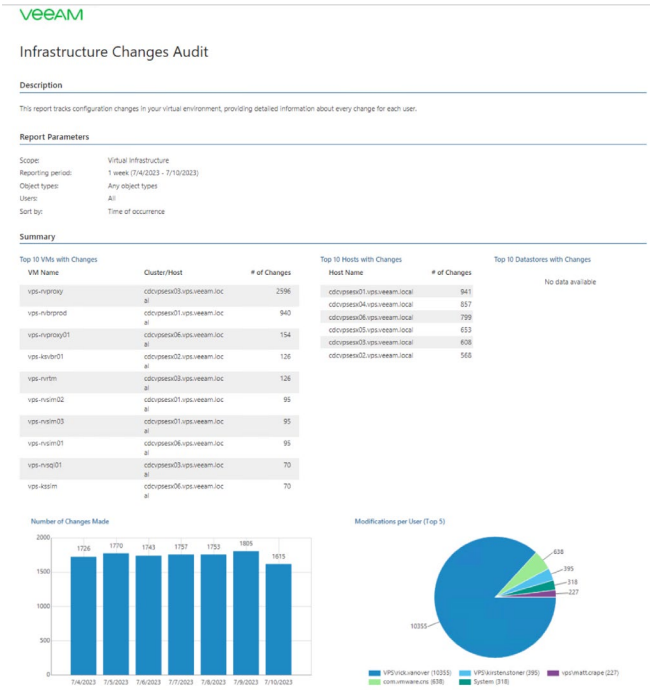
Unabhängig vom Speicherort der Backup-Daten ist Verschlüsselung ein Muss. Immutability schützt Backups zwar vor böswilligem und versehentlichem Löschen, allerdings verhindert sie nicht, dass die Daten kopiert und ausgeschleust werden können.

Durch seine Verschlüsselungstechnologie kann Veeam Backup & Replication Daten sowohl während der Übertragung zwischen Backup-Komponenten als auch bei der Speicherung am Zielort schützen. Kunden können diese beiden Verschlüsselungsmethoden auch miteinander kombinieren, sodass wichtige Daten an jedem Punkt des Datensicherungsprozesses vor unbefugtem Zugriff geschützt sind.

4. Überwachung auf neue Bedrohungen

Veeam ONE ist ein zentraler Bestandteil der Veeam Data Platform und dabei vorrangig zuständig für proaktive Überwachung und Analyse. Für beinahe alle Angriffe gibt es Vorzeichen. Sofern sie erkannt werden, sind schnelle Maßnahmen möglich, die im Kampf gegen Ransomware entscheidend sein können.

Unbefugte Zugriffe und Änderungen erkennen



Häufig hinterlassen Angreifer Spuren in der Umgebung. Wenn beispielsweise Anmeldedaten entwendet wurden, kann es zu ungewöhnlichen Anmeldungen bei den unterschiedlichsten Workloads im Netzwerk kommen. So testen die Angreifer die Gültigkeit der gestohlenen Anmeldedaten und den Umfang ihrer Berechtigungen.

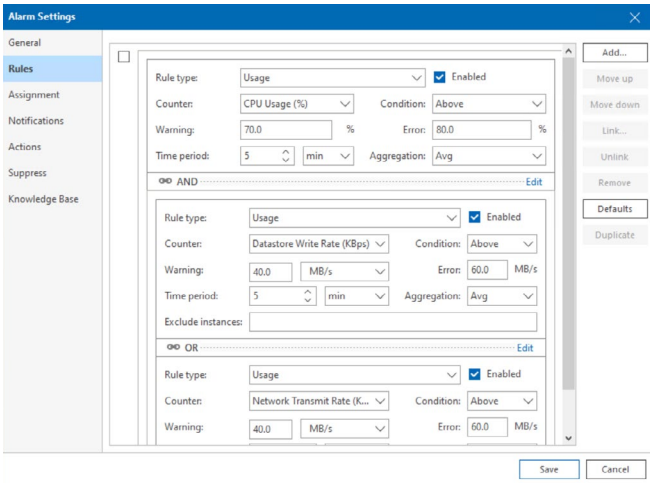
Um Veränderungen in der virtualisierten Umgebung auf die Spur zu kommen, sollte daher der Audit-Report zu infrastrukturellen Änderungen regelmäßig erstellt und gelesen. VMs, Hosts und Datastores lassen sich auf Änderungen überwachen. Aufgeführt ist die Anzahl und Art der Änderungen sowie die ausführende Person und der Zeitpunkt. Auf diese Weise wird unzulässiges Verhalten erkennbar und lässt sich stoppen.

Backup-Größenänderungen erkennen

Die Kernaufgabe von Ransomware ist das Verschlüsseln von Dateien. Somit werden neue Daten erzeugt, die auch ins Backup einfließen können. Wünschenswert ist dies zwar nicht, allerdings ergibt sich daraus eine weitere Überwachungsmöglichkeit: die Größe von Backup-Dateien.

Mittels der Konfiguration eines entsprechenden Alarms können **verdächtig große inkrementelle Backups** vom System gemeldet werden. Alarme wie dieser sind flexibel konfigurierbar und können Aufgaben beinhalten wie die Alarmierung per E-Mail, das Ausführen von Aufgaben- oder Informationserfassungsskripten und sogar das Starten von SureBackup-Jobs.

Potenzielle Bedrohungen in Echtzeit erkennen



Prozessor und Datenträger sind stark in den Verschlüsselungsvorgang eingebunden. Das Ergebnis ist eine neue verschlüsselte Datei. Dementsprechend kann sich ein Ransomware-Angriff durch Spitzen z. B. in der CPU-Auslastung, bei den Schreibvorgängen auf dem Datenträger und bei der Netzwerkübertragungsrate verraten. In Veeam ONE können Sie den Alarm für **potenzielle Ransomware-Aktivität** aktivieren und die auslösenden Grenzwerte individuell festlegen.

Hinsichtlich Veeam ONE-Alarmen hat es sich bewährt, den gewünschten Alarm zu duplizieren und auf die jeweilige Umgebung hin anzupassen. Beim oben genannten Beispiel ist zu beachten, dass einige Datenbank-Workloads den Prozessor generell stärker belasten als andere. Wenn Sie den Alarm kopieren, können Sie die Grenzwerte an den workloadspezifischen Umfang anpassen.

5. Automatisiertes Dokumentieren, Sichern und Testen

DR-Pläne sind eine kritische Komponente, doch Unternehmen jeder Größe tun sich schwer damit, sie auf dem neuesten Stand zu halten. Wenn der DR-Plan doch einmal ausgeführt werden muss, möchte kein IT-Team erleben, dass die Dokumentation veraltet, lückenhaft oder sogar komplett falsch ist. Veeam Recovery Orchestrator automatisiert die Dokumentation Ihrer Orchestrierungspläne und erleichtert Ihnen so diesen Teil der Arbeit.

Plan Steps & Default Parameters

Restore VM

Parameter	Description	Default Value
Description	This is a default step for every machine added to a Restore Plan. It restores machines from backup files into the specified recovery location.	None
Test Action	This step will always be executed in a Test DataLab environment only.	Execute
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Restore Timeout (minutes)	Timeout (in minutes) for the restore process. As soon as this timeout expires, Orchestrator will stop both the restore process and all the restore tasks currently running on the Veeam Backup & Replication server. If you set the parameter value to 0, the timeout will be disabled, but you will still be able to interrupt the restore process by halting the plan. This setting applies to Recovery, Migrate and Rename step independently.	0
Retries	Number of retries to perform in case the step fails on the first try.	2
Restored VM Name	A name for the newly created VM	%source_machine_name%

Check license and availability

Parameter	Description	Default Value
Description	This step checks whether Orchestrator is licensed to recover this system as a VM. If not, the check displays the ordinal number of the VM in the license queue.	None
Critical Step	Choose Yes or No to define whether this step is critical to the VM recovery. If critical step, then failure will cause the VM to be marked as failed	Yes
Timeout	Timeout (in seconds) for the step	300
Retries	Number of retries to perform in case the step fails on the first try.	1
Failback & Undo Failover Action	Choose Execute or Skip to define whether this step is executed during Undo Failover and Failback operations.	Execute
Test Action	Choose Execute or Skip to define whether this step is executed during plan testing in DataLab	Execute

Die Dokumentation ist von Menschen lesbar, leicht verständlich und kann jederzeit generiert werden, zum Beispiel nach einer Änderung.

Sichere Datenwiederherstellung

Gegen Ransomware-Angriffe sind Backups die letzte Verteidigung. Leider ist es in der Regel so, dass Malware schon eine Weile in der Umgebung lauert, ehe sie zuschlägt. Sie wartet sozusagen darauf, aktiviert zu werden. Deshalb kann sich die Bedrohung auch schon unerkannterweise in Ihren Backups befinden und im Zuge der Wiederherstellung erneut in die Umgebung gelangen.

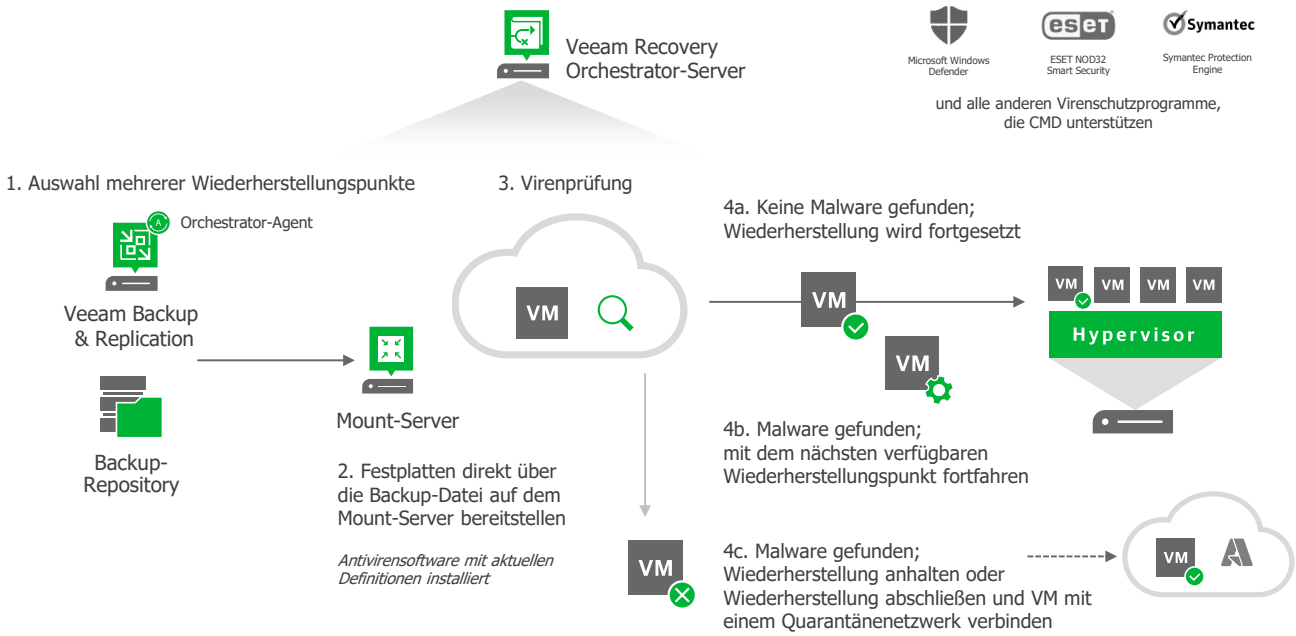
Secure Restore von Veeam Backup & Replication schafft Abhilfe. Diese Funktion für sichere Wiederherstellungen prüft währenddessen die Daten auf Malware. Die Datenträger mit den Backups werden in einen speziellen Server gemountet, der die Prüfung durchführt. Zeigen sich keine Bedrohungen, geht die Wiederherstellung wie gewohnt weiter. Wird aber Malware erkannt, kann der Anwender entscheiden, ob er die Wiederherstellung abbricht oder eingeschränkt weiterführt (d. h. die Netzwerkschnittstelle deaktiviert).

Saubere DR jeden Umfangs

Was ist, wenn es zur Katastrophe kommt und ganze Rechenzentren betroffen sind? Die Funktion **Clean DR** von Veeam Recovery Orchestrator erlaubt sichere, abgestimmte Wiederherstellungen in jedem Umfang. Ähnlich wie bei Secure Restore in Veeam Backup & Replication, der Grundlage für Clean DR, werden Datenträger automatisch gemountet und auf Malware durchsucht. Wird keine Bedrohung gefunden, kann der Wiederherstellungsvorgang plangemäß weiterlaufen.

Wird doch eine Bedrohung entdeckt, hat der Administrator folgende Wahl:

- Den neuesten Wiederherstellungspunkt nach Malware absuchen
- Die Wiederherstellung abbrechen
- Die Wiederherstellung mit dem verdächtigen Wiederherstellungspunkt abschließen und die VM mit einem Netzwerk in Quarantäne verknüpfen



Hinsichtlich Engines für die Malware-Erkennung haben Kunden eine große Auswahl aus zahlreichen Integrationen. Alternativ können sie eigene hinzufügen, indem sie XML-Konfigurationsdateien erstellen oder abwandeln. Mehr dazu erfahren Sie im KB-Artikel 3132 von Veeam.

Compliance des DR-Plans bestätigen

Selbst wenn sie wollen, weil sie wissen, dass sie es sollten: Viele Unternehmen schaffen es nicht, ihre DR-Pläne zu testen. Veeam Recovery Orchestrator nutzt Veeam **DataLabs**, um das Testen zu automatisieren, zu planen und somit zu optimieren.

RPO

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00 (HH:mm)
✓ Success	Target RPO Met	Yes
✓ Success	VMs not meeting RPO	None
✓ Success	Worst RPO failure	None

RTO

Result	Check	Details
[i] Info	RTO	Target RTO is 01:00 (HH:mm)
[i] Info	Duration	Test duration was 00:04:56 (HH:mm:ss)
✓ Success	Target RTO Met	RTO achieved

Nur dank DataLabs lassen sich Veeam Data Platform-Backups von agentenbasierten und virtuellen Workloads vollständig in einer Sandbox-Umgebung wiederherstellen. Dementsprechend wird bei einem DR-Test der gesamte Plan in einem separaten Netzwerk durchgespielt. Dadurch ist sichergestellt, dass der Plan wie erwartet funktionieren wird, und Sie erhalten praktisch umsetzbare RPOs und RTOs, mit denen Sie die Compliance nachweisen können.

6. Verwendung API-gestützter Bedrohungserkennung

Eine klassische Hürde für die Bedrohungserkennung ist die ressourcenintensive Prüfung von Produktions-Workloads. Die Suche nach Bedrohungen, deren Anzeichen sowie bekannten Schwachstellen kann den Prozessor stark belasten und die Leistung des Datenträgers herabsetzen. Zum einen lassen sich diese Einschränkungen vermeiden, zum anderen können Sie Ihre Backups auch offline auf Bedrohungen prüfen lassen.

Bedrohungen folgenlos auf die Spur kommen

Die mit Veeam Backup & Replication v10 eingeführte Veeam **Data Integration API** verschafft Kunden uneingeschränkten Offline-Zugriff auf ihre Daten. Mit dieser Funktionalität können sie die Daten von Backup-Dateien als gemounteten Ordner verfügbar machen und auf Daten zugreifen, die in Veeam Backup & Replication-Backups verfügbar sind. Diese Methode eignet sich insbesondere, um zu verhindern, dass Ransomware und andere Bedrohung durch die Wiederherstellung nicht in den Produktivbetrieb gelangen. Darüber hinaus können Sicherheitsteams die API für regelmäßige Prüfungen auf zusätzliche Bedrohungen konfigurieren und die Beseitigung in eine isolierte, abgesicherte Umgebung verlagern.

Da die Daten als Dateisystem gemountet sind und kein aktives System darstellen, werden Bedrohungen weder ausgeführt noch in den Systemspeicher geladen. Auf diese Weise können Audits, die forensischen Maßstäben genügen, und Suchen sicher und effektiv durchgeführt werden, mit minimalen Auswirkungen und ohne Bedrohung anderer Workloads.

Nicht konforme Daten und Änderungen erkennen

Ähnlich herausfordernd ist das Klassifizieren von Daten in diesen Systemen und die Einhaltung gesetzlicher Vorschriften. Prüfungen von Dateiinhalten und -änderungen können nicht im Produktivbetrieb vorgenommen werden, obwohl viele Unternehmen davon profitieren würden. Die Veeam Data Integration API nutzt **PowerShell**, sodass Unternehmen den für ihre individuellen Aufgaben erforderlichen Code selbst schreiben können. Eine solche Aufgabe kann sein, den Speicherort von personenbezogenen Daten zu bestimmen oder Änderungen an sensiblen Dateien festzustellen.

Dank diesen Analysen und der Aufzeichnung ihrer Ergebnisse behalten Unternehmen die Systeme, in denen sich ihre Daten befinden, mit beruhigender Zuverlässigkeit im Blick. Kunden ziehen daraus noch einen weiteren Nutzen: Anhand dieser Daten erstellen und prüfen sie Wiederherstellungspläne, die von vornherein dafür sorgen, dass Daten lokal vorgehalten und Vorschriften eingehalten werden. Somit müssen sie sich nicht erst im Ernstfall darum kümmern.

7. Absicherung des Rechenzentrums

Planen Sie rechtzeitig, wohin Ihre Workloads wiederhergestellt werden sollen. Diese kritische Entscheidung sollten Sie nicht aufschieben. Egal, ob die Produktionsserver im Zuge einer forensischen Ermittlung offline sind oder die Ressourcen zur Wiederherstellung zurück ins Rechenzentrum fehlen, Unternehmen müssen sicherstellen, dass sie so schnell wie möglich wieder online sind.

Als Teil der Veeam Data Platform Premium Edition versetzt Veeam Recovery Orchestrator Kunden in die Lage, Automatisierungen und Orchestrierungen zu planen, um Workloads möglichst flexibel und unter Einhaltung der SLAs wieder in Betrieb zu nehmen.

Wiederherstellung außerhalb des Rechenzentrums

Ein wichtiger Vorteil von Veeam Recovery Orchestrator ist die Funktion zur Wiederherstellung von VMware-Workloads und Veeam Agent-Backups in VMware-Umgebungen oder direkt in Microsoft Azure. Unternehmen können zur Begrenzung der Ausfallzeit Orchestrierungspläne aufstellen, um die Wiederherstellbarkeit zu gewährleisten. Ob der Ausfall nun durch Ransomware oder durch z. B. Auflagen der Strafverfolgungsbehörden eintritt, ist dabei unerheblich. Sobald die Pläne feststehen, können sie in einer Sandbox-Umgebung getestet werden. Dadurch ist nicht nur sichergestellt, dass alles wie erwartet ablaufen wird, sondern auch die RPOs und RTOs werden eingehalten. Somit erhalten Sie die beruhigende Gewissheit, dass die Wiederherstellung im Ernstfall gelingen wird.

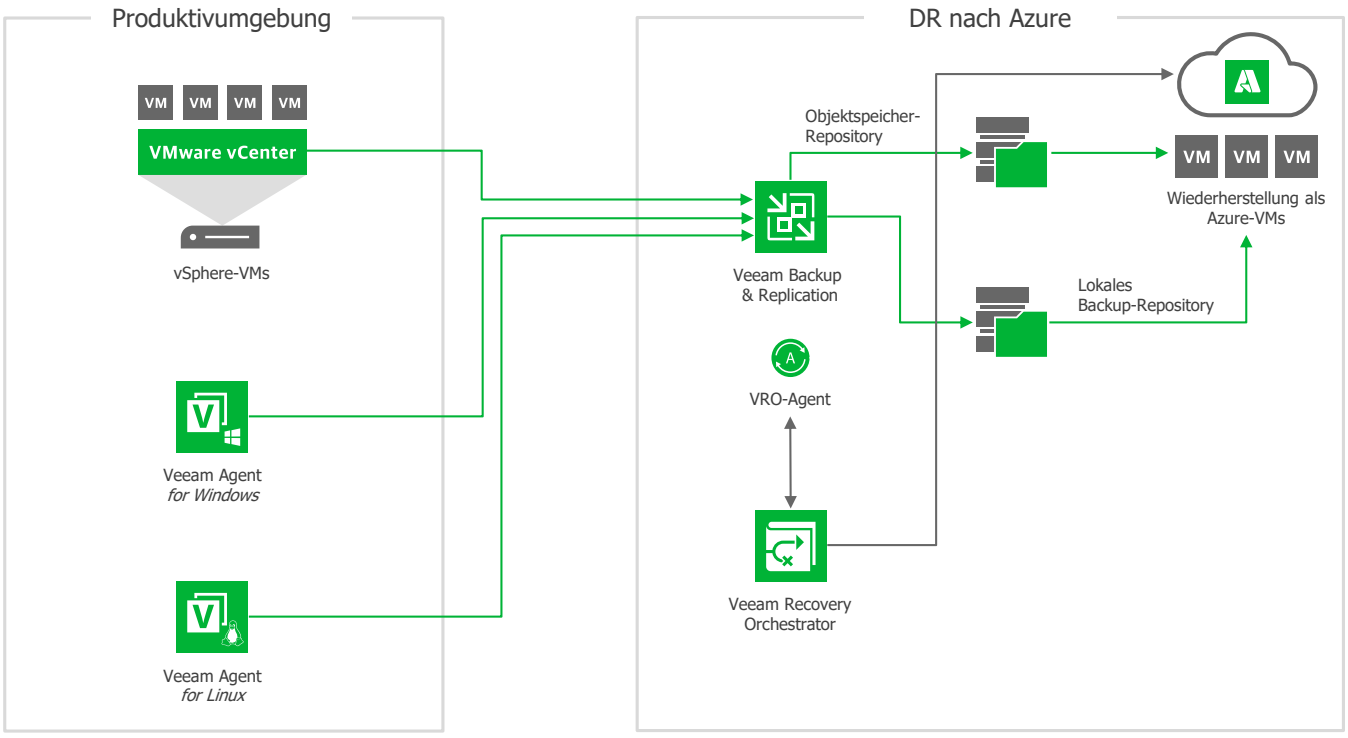
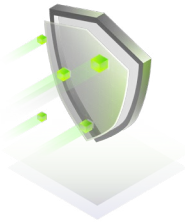


Abbildung 9 — Orchestrierte Wiederherstellung in Microsoft Azure

8. Fazit: Voraussetzungen für die schnelle Wiederherstellung nach Ransomware-Angriffen

Die Anzahl der Ransomware-Angriffe nimmt stark zu. Unternehmen und andere Organisationen melden immer wieder schwere Verluste. Die Angriffe zielen auf kritische Daten ab und machen sie für ihre Inhaber unzugänglich, bis ein Lösegeld gezahlt wird. Und selbst dann werden die Daten in vielen Fällen nicht wieder freigegeben; sie bleiben in Geiselhaft. Den besten Schutz vor Ransomware bietet ein zuverlässiger Backup-Plan.

Funktionierende Backups sind entscheidend, um Ransomware-Angriffe zu überstehen. Unternehmen müssen einfach wissen, dass sie ihre Daten nach einem Angriff – egal, wie umfangreich – zügig wiederherstellen können. Dazu ist es notwendig, dass noch mehr Unternehmen die Datensicherung und -wiederherstellung in ihr Sicherheitsprogramm aufnehmen und ihre Daten dadurch besser absichern und zuverlässiger bereitstellen.



Für ein umfassendes Sicherheitsprogramm müssen Sie Personen, Prozesse und Technologien so zusammenführen, dass das Programm stets verbessert wird und Sie gleichzeitig eine offensive statt reaktive Haltung einnehmen. Unabhängig von der gewählten Methodik müssen Sie messbare Ergebnisse definieren, anhand derer IT-Teams Angriffe abwehren und Daten nach einem erfolgreichen Angriff schnell wiederherstellen können.

Zweck eines Plans für die Wiederherstellung nach Ransomware-Angriffen ist es, Betriebsunterbrechungen so kurz wie möglich zu halten und den Prozess durch Automatisierung von Risiken zu befreien. Schon vor einem Angriff sollte der komplette Satz an Funktionalitäten bereitstehen, den der Markt zur Abwehr potenzieller Bedrohungen zu bieten hat.

Diese Tipps zu beherzigen, sorgt dafür, dass Unternehmen gut auf Ransomware-Angriffe vorbereitet sind und ihre Daten schnell wiederherstellen können, ohne Lösegeld zu zahlen. Zwar gibt es keine absolut zuverlässige Methode, Ransomware-Angriffe zu verhindern, doch wer die Best Practices der Datensicherung und erfolgreichen Wiederherstellung nach Ransomware-Angriffen kennt, bietet eine geringere Angriffsfläche und behält neue Bedrohungen besser im Blick. Im Ergebnis verfügen Incident-Response-Teams über das richtige Know-how und die richtigen Tools, um Daten und damit Unternehmen vor den Gefahren durch Ransomware zu schützen.

Data Protection Trends Report 2023

Ransomware Trends Report 2023

Jetzt ansehen: 6 Kurzdemos zum Umgang mit Ransomware


veeam