Zero-Trust-Datenresilienz (ZTDR)

Sichere Architektur für die Sicherung und Wiederherstellung von Daten

Ein pragmatischer Ansatz zur Implementierung von Zero Trust

Überblick

Unternehmen aller Größen und Branchen wissen, wie wichtig Zero Trust für die Sicherheit ihrer Daten und ihres Geschäfts ist. Das aktuelle Zero-Trust-Modell wurde jedoch noch nicht umfassend auf die Datensicherung und -wiederherstellung angewendet. Die Ausweitung der Zero-Trust-Prinzipien auf die Sicherung und Wiederherstellung von Daten steht im Einklang mit dem ganzheitlichen Wesen der Cybersicherheit. Zum Schutz sensibler Informationen gehört mehr als nur Perimetersicherheit.

Angesichts dieser Herausforderung hat Veeam gemeinsam mit dem Zero-Trust-Experten Jason Garbis von Numberline Security das Zero Trust Data Resilience Framework entwickelt, um die Risiken zu minimieren, die Datensicherung zu stärken und die Sicherheitslage eines Unternehmens massiv zu verbessern. Dieses Framework baut auf dem Zero Trust Maturity Model (ZTMM) der Cybersecurity and Infrastructure Security Agency (CISA) auf und weitet die Grundprinzipien des ZTMM auf ein Sicherungs- und Wiederherstellungsszenario aus. Das Zero Trust Data Resilience Framework geht davon aus, dass niemals Vertrauen vorausgesetzt wird und während des gesamten Datenlebenszyklus — einschließlich Datensicherung und -wiederherstellung — konsequent Sicherheitsmaßnahmen angewendet werden. Es handelt sich hier um ein praxisorientiertes Modell, mit dessen Hilfe IT- und Sicherheitsteams die Risiken erheblich reduzieren, die Datensicherung optimieren und die Sicherheitslage jedes Unternehmens deutlich verbessern können.

Sie möchten mehr über Zero-Trust-Datenresilienz erfahren? Laden Sie das Whitepaper herunter

Das Zero-Trust-Konzept von Veeam: Zero-Trust-Datenresilienz (ZTDR)

Zero Trust ist grundlegender Bestandteil der Sicherheitsstrategie eines Unternehmens. Beim Schutz von Backup-Umgebungen sind zentrale Grundsätze wie die Segmentierung kritischer Datenbestände, der Zugriff mit minimalen Rechten sowie die kontinuierliche Authentifizierung und Autorisierung unter Verwendung von Best Practices für Identity and Access Management (IAM) besonders relevant. Durch die Integration einer Funktion für Zero-Trust-Datenresilienz können Unternehmen die besonderen Herausforderungen von Datensicherungslösungen bewältigen und für eine umfassende Sicherheitsstrategie sorgen — unabhängig davon, ob sie lokal, in der Cloud oder in hybriden Umgebungen arbeiten.

Ein wesentliches Zero-Trust-Konzept besteht darin, unabhängig von der Sicherheit einer Umgebung stets von einer Sicherheitsverletzung auszugehen. Eine wichtige Vorgehensweise zur Bekämpfung dieses Risikos besteht bei der ZTDR-Methodik in der Trennung von Backup-Management-Software und Backup-Speicher in separate Resilienzzonen oder Sicherheitsdomänen. Auf diese Weise werden die Backup-Daten von Bedrohungen der Backup-Management-Software isoliert, unabhängig davon, ob diese Bedrohungen von innen oder außen kommen. Veeam unterstützt mehrere Technologien, um Resilienzzonen mit hochsicherem, unveränderlichem Speicher zu schaffen (siehe Abbildung 1).

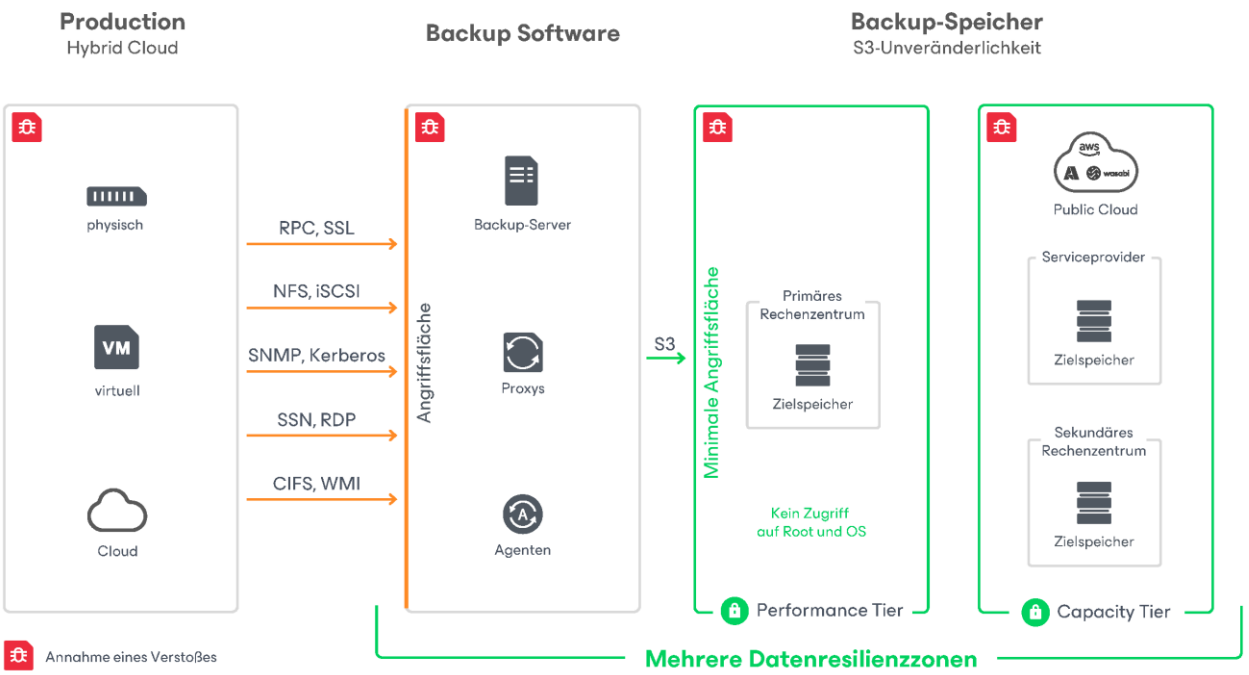

Abbildung 1

Da Datensicherungslösungen zu den Lösungen mit den meisten Lese- und Schreibzugriffen auf Produktionsdaten im gesamten Unternehmen und oft auch auf die wichtigsten Daten gehören, muss die Backup-Umgebung eines Unternehmens sicher sein und mithilfe von Zero Trust Best Practices geschützt werden.

Grundsätze der Zero-Trust-Datenresilienz

Aufbauend auf dem CISA Zero Trust Maturity Model (siehe Abbildung 2) sollten Unternehmen speziell auf die Datensäule zusätzliche Überlegungen anwenden.

CISO Zero Trust Maturity Model

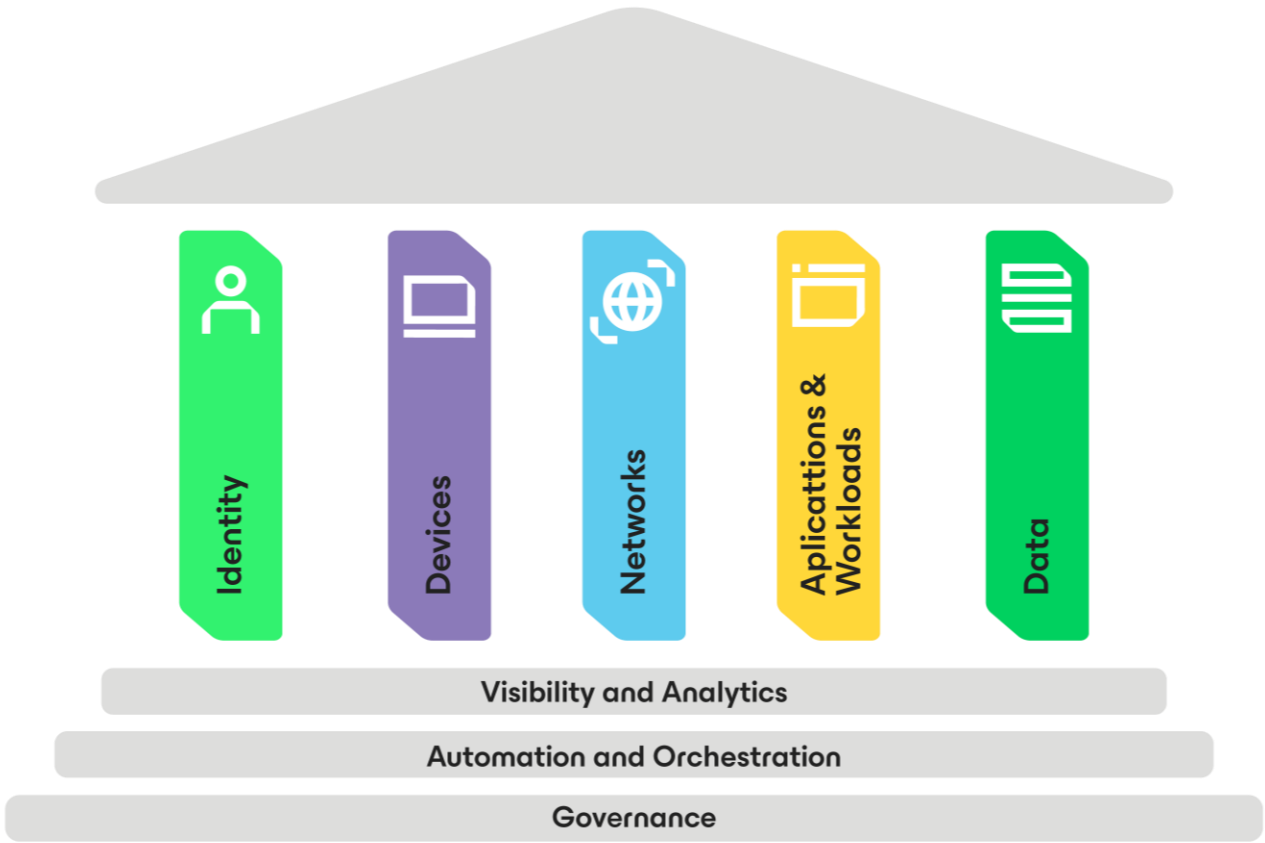

Abbildung 2

Die Studie zur Zero-Trust-Datenresilienz hebt 5 zentrale Grundsätze der Zero-Trust-Datenresilienz (ZTDR) hervor, die Unternehmen bei ihrer allgemeinen Strategie für Cyberresilienz unterstützen und den Schutz kritischer Datenbestände angesichts sich entwickelnder Cyberbedrohungen sicherstellen sollen.

Zugriff nach dem Prinzip der geringsten Rechte

Bei diesem Prinzip geht es darum, einer Person, einem Prozess, einem Gerät oder einer Workload nur den Zugriff zu gewähren, der für die beabsichtigte Funktion erforderlich ist.

Kontrollierter Zugriff auf die Backup-Infrastruktur:

- Durch die Implementierung von Zero-Trust-Richtlinien zur Kontrolle des Zugriffs auf die Backup-Infrastruktur wird sichergestellt, dass nur validierte Benutzer Verbindungen zur Backup-Lösung herstellen können. Dies ist ein entscheidender Schritt, um unbefugten Zugriff und potenzielle Datenschutzverletzungen zu verhindern.

Granulare Self-Service-Rollen und eingeschränkte Backup-Admin-Rollen:

- Mit granularen Self-Service-Rollen und eingeschränkten Backup-Admin-Rollen setzt sich Veeam für die Umsetzung des Prinzips der geringsten Rechte ein. Auf diese Weise wird sichergestellt, dass Benutzer nur Zugriff auf die spezifischen, für ihre Aufgaben erforderlichen Funktionen haben, und die Wahrscheinlichkeit eines versehentlichen oder vorsätzlichen Missbrauchs wird verringert.

Best Practices für Identity and Access Management (IAM)

- Die Durchsetzung von IAM Best Practices wie der Multifaktorauthentifizierung (MFA) stellt eine zusätzliche Sicherheitsebene für die Backup-Umgebung dar. Dies ist eine wichtige Maßnahme, um unbefugten Zugriff zu verhindern, insbesondere angesichts der hohen Berechtigungen im Zusammenhang mit Backup-Lösungen.

„Vier Augen"-Prinzip bei kritischen operativen Entscheidungen:

- Durch die Einbeziehung des „Vier Augen"-Prinzips bei kritischen operativen Entscheidungen wird sichergestellt, dass für wichtige Aktionen die Genehmigung oder Verifizierung durch mindestens zwei autorisierte Personen erforderlich ist. Dies fügt eine zusätzliche Kontrollebene hinzu und senkt das Risiko böswilliger oder fehlerhafter Aktivitäten.

Unveränderlichkeit

Selbst bei einem sicheren Netzwerkperimeter besteht ein wichtiges Zero-Trust-Konzept darin, von einer Sicherheitsverletzung auszugehen. Die Unveränderlichkeit von Backups ist ein leistungsstarker Schutzmechanismus, da sie dafür sorgt, dass interne oder externe Bedrohungsakteure kritische Backup-Daten nicht ändern oder löschen können.

Segmentierung zur Minimierung der Angriffsfläche und des Auswirkungsbereichs:

- Die Segmentierung von Backup-Software und Backup-Speicher in separate Resilienzzonen ist das Kernkonzept von ZTDR. Durch die Isolierung kritischer Komponenten werden dabei die potenziellen Auswirkungen interner oder externer Bedrohungen minimiert. Ein zusätzlicher Schutz besteht darin, sicherzustellen, dass die Backup-Software keine Berechtigungen auf Betriebssystem-/Verwaltungsebene für den Backup-Speicher hat.

Mehrere Resilienzzonen und 3-2-1-1-Backup-Regel:

- Mehrere Datenresilienzzonen oder Sicherheitsdomänen sorgen für mehrstufige Sicherheit. Darüber hinaus ist die 3-2-1-1-Backup-Regel eine Best Practice für die Backup-Strategie im Einklang mit den Grundsätzen der Datenresilienz. Wenn mindestens drei Kopien der Daten auf zwei verschiedenen Medientypen unterhalten werden und mindestens eine externe Kopie und mindestens eine durch ein Air-Gap getrennte oder unveränderliche Kopie vorhanden ist, bietet dies mehrstufige Sicherheit und reduziert das Risiko von Datenverlusten.

Resilienzzonen

Ein zentrales Zero-Trust-Konzept für Netzwerke ist die Mikrosegmentierung. Sicherheitsperimeter werden in kleinere Zonen aufgeteilt, um die Angriffsfläche, den Auswirkungsbereich einer kompromittierten Zone und die laterale Bewegung eines Angreifers zu reduzieren. Für ZTDR kann dieses Konzept durch die Verwendung von Datenresilienzzonen angewendet werden. Resilienzzonen trennen den Backup-Speicher und isolieren die Steuerungsebene des Speichers von der Backup-Software und ihrer Steuerebene. Dadurch entsteht eine kritische Grenzlinie, die die Überlebensfähigkeit der Backup-Daten auch bei einer Kompromittierung der Backup-Software sicherstellt. Dies kann aus verschiedensten Gründen geschehen, einschließlich interner Bedrohungsakteure. Ein Backup-System muss sicherstellen, dass Backup-Daten einfach und schnell von einer Neuinstallation der Backup-Software wiederhergestellt werden können.

Produktions-
infrastruktur

Veeam-
Infrastruktur

Autonome
Backup-Daten

Unveränderlich | Verschlüsselt | 3-2-1-1-0

Datenintegrität und verbesserte Sicherheit:

- Die Konfiguration eines kompatiblen Backup-Repositorys und die Festlegung eines Aufbewahrungszeitraums für unveränderliche Backups stellen eine proaktive Maßnahme für Datenintegrität und verbesserte Sicherheit dar. Unveränderliche Backups dienen als Schutz vor Ransomware-Angriffen und anderen Arten der Datenmanipulation.

Systemresilienz

Ein ganzheitlicher Ansatz für die IT-Sicherheit umfasst die Resilienz des gesamten Ökosystems, einschließlich Plattformen, Tools, Technologien und Prozessen. Mit den vielfältigen Resilienzoptionen von Veeam stehen den Unternehmen Tools zur Verfügung, mit denen sie gegen verschiedene Arten von Störungen, einschließlich eines kompletten Systemausfalls, gewappnet sind.

Timeshift-Erkennung für unveränderliche Backups:

- Die Implementierung der Timeshift-Erkennung ist eine proaktive Maßnahme, um die Löschung unveränderlicher Backups zu verhindern, selbst bei kompromittiertem NTP (Network Time Protocol). Dieses Feature erhöht die Sicherheit und Zuverlässigkeit von Backup-Repositorys und stellt die Integrität kritischer Backup-Daten sicher.

Flexible Wiederherstellungsoptionen:

- Veeam bietet flexible Wiederherstellungsoptionen, auch für unterschiedliche Umgebungen, und unterstützt physische und virtuelle Bereitstellungen sowie hybride Umgebungen, um den vielfältigen IT-Infrastrukturen der Unternehmen gerecht zu werden. Diese Flexibilität ermöglicht den Unternehmen eine schnelle Wiederherstellung: beispielsweise von lokaler VMware in AWS oder Azure oder von AWS in Azure, falls die ursprüngliche Umgebung nicht verfügbar ist.

Optionen für die granulare Datenwiederherstellung:

- Die flexible Möglichkeit zur Wiederherstellung von Daten in verschiedenen Umgebungen und mit unterschiedlichen Granularitäten verbessert die allgemeine Datenresilienz. Dank dieser Anpassungsfähigkeit können Unternehmen ihre Wiederherstellungsprozesse an die spezifischen Anforderungen unterschiedlicher Szenarien anpassen.

Proaktive Validierung

Eine kontinuierliche Validierung funktionaler Aspekte und Prozesse ist entscheidend, damit Daten geschützt bleiben und Anomalien erkannt und umgehend behoben werden.

Kontinuierliche Überwachung und Validierung:

- Die Bedeutung, die einer Systemüberwachung rund um die Uhr beigemessen wird, spiegelt die Erkenntnis wider, dass Cybersicherheitsbedrohungen jederzeit auftreten können. Durch Echtzeiteinblicke in den Zustand der Umgebung können Administratoren Anomalien frühzeitig erkennen und Unternehmen können Situationen untersuchen und reagieren, bevor ein potenzieller Cyberangriff oder Datenverlust auftritt.

- Mit Tools wie Veeam ONE für das Monitoring kann die Integrität und Sicherheit von Backup- und Wiederherstellungsumgebungen proaktiv aufrechterhalten werden. Durch die Überwachung verschiedener Parameter wie CPU-Auslastung, Datastore-Schreibrate, Netzwerk-Übertragungsrate und die Größe inkrementeller Backups liefert Veeam ONE wertvolle Einblicke in potenzielle Probleme.

Durchgängige Transparenz:

- Das Konzept der durchgängigen Transparenz über die gesamte Datensicherungsinfrastruktur hinweg ist von entscheidender Bedeutung. Es stellt sicher, dass Unternehmen einen umfassenden Einblick in den Zustand und Status ihrer Systeme für Sicherung und Wiederherstellung erhalten und somit fundierte Entscheidungen treffen und bei Bedarf umgehend handeln können.
- Als Teil der neuen Version 12.1 von Veeam fasst das neue Threat Center Informationen aus der gesamten Plattform und Infrastruktur in einer einzigen Konsole zusammen, in der Bedrohungen aufgezeigt und Risiken identifiziert werden. Die Sicherheit der gesamten Datensicherungsumgebung der Unternehmen wird in einer einfachen und leistungsstarken Scorecard bewertet.

Einfache Abläufe

Die Bedeutung einfacher Abläufe bei Katastrophen oder Cybersicherheitsereignissen zeigt, wie wichtig ein einfaches Vorgehen für eine effektive Wiederherstellung ist. Je länger die Ausfallzeit, desto stärker die Auswirkungen auf den Geschäftsbetrieb und das Geschäftsergebnis eines Unternehmens.

Durchschnittliche Ausfallzeit bei Ransomware-Angriffen:

- Laut Ransomware Trends Report 2023 von Veeam beträgt die durchschnittliche Ausfallzeit nach einem Ransomware-Angriff drei Wochen. Dies macht deutlich, wie wichtig eine schnelle Wiederherstellung ist, insbesondere in Belastungssituationen, in denen jeder Moment zählt.

Gleichgewicht zwischen Tools, Mitarbeitern und Prozessen:

- Die richtige Balance zwischen Tools, Mitarbeitern und Prozessen zu finden, ist besonders bei Katastrophen oder Cyberangriffen eine große Herausforderung. Einfache Abläufe beinhalten die Rationalisierung von Workflows, die Optimierung von Prozessen und die Bereitstellung der richtigen Tools für eine effiziente Wiederherstellung.

Investition in einfachere Wiederherstellungsfunktionalitäten:

- Branchenführer wie Veeam investieren vorausschauend in Wiederherstellungsfunktionalitäten und befassen sich mit der Komplexität der Wiederherstellung. Die Möglichkeit, Daten einer Plattform auf einer anderen wiederherzustellen und Tools wie den Veeam Recovery Orchestrator zu nutzen, zeigt, wie wichtig es für uns ist, komplexe Wiederherstellungsszenarien zu vereinfachen. Failover-Pläne werden aktualisiert, automatisiert und umfassend getestet, um für Belastungssituationen bereit zu sein.

Erfahren Sie mehr über die neuesten Sicherheitsfunktionalitäten in Version 12.1

Fazit

Mit der Weiterentwicklung und Ausweitung unserer digitalen Landschaft nehmen auch Cyberangriffe und die Möglichkeiten der Bedrohungsakteure zu. Daher ist es dringend erforderlich, die IT- und Sicherheitsteams zusammenzubringen und ihre Zusammenarbeit und Effektivität zu stärken, um die Daten, Geräte und Mitarbeiter der Unternehmen besser zu schützen und zu verteidigen. Ein höherer Reifegrad kann nicht über Nacht erreicht werden, dies muss jedoch eher früher als später geschehen. Der erste Schritt ist Zero Trust. Das Zero-Trust Maturity Model (ZTMM) von CISA umfasst wichtige Prinzipien für die Sicherheit und den Schutz eines Unternehmens, deckt jedoch nicht alles ab. Die Einführung von Zero Trust Data Resilience (ZTDR) als Erweiterung des Zero Trust Maturity Model (ZTMM) von CISA ist ein strategischer und zukunftsorientierter Ansatz, um der sich entwickelnden Landschaft der Cyberbedrohungen zu begegnen.

Die Berücksichtigung der ZTDR-Prinzipien, einschließlich Zugriff mit minimalen Rechten (Least Privileged Access), Unveränderlichkeit, Systemresilienz, proaktiver Validierung und einfacher Abläufe, stellt eine umfassende Strategie für die Sicherung und den Schutz von Unternehmensdaten dar. Mit der Einführung von ZTDR steht den Unternehmen eine klare und konkrete Möglichkeit zur Stärkung ihrer Sicherheitsposition zur Verfügung. Dies bedeutet effizientere Abläufe und eine bessere Abstimmung zwischen IT- und Sicherheitsteams, was letztendlich zu einer schnelleren und sichereren Wiederherstellung führt.

Über Veeam Software

Veeam®, weltweit führender Anbieter im Bereich Datensicherung und Wiederherstellung nach Ransomware-Angriffen, möchte allen Unternehmen helfen, sich nach einem Datenausfall oder Datenverlust nicht nur wieder zu erholen, sondern auch Fortschritte zu machen. Mit Veeam erreichen Unternehmen maximale Ausfallsicherheit 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. IT- und Sicherheitsverantwortliche haben somit die Gewissheit, dass ihre Anwendungen und Daten stets geschützt und verfügbar sind. Veeam hat seinen Hauptsitz in Columbus, Ohio, und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 450.000 Kunden, darunter 73 % der Global 2000-Unternehmen, die auf Veeam vertrauen, um ihren Geschäftsbetrieb aufrechtzuerhalten. Profitieren Sie mit Veeam von maximaler Ausfallsicherheit. Weitere Informationen erhalten Sie unter www.veeam.com/de. Sie können Veeam auch auf LinkedIn unter @veeam-software und auf X unter @veeam folgen.