Erweitern des Zero-Trust-Konzepts auf die Sicherung und Wiederherstellung von Daten

Ein praktischer Leitfaden für
IT- und Sicherheitsexperten

Contents

Executive Summary	**3**
Zero Trust: Eine kurze Einführung	**4**
Einführung in die Zero-Trust-Datenresilienz (ZTDR)	**5**
ZTDR-Referenzarchitektur	**6**
Erste Schritte mit ZTDR	**7**

Executive Summary

Zero Trust ist eine moderne und hochwirksame Strategie zum besseren Schutz der IT-Infrastruktur unseres Unternehmens vor Ransomware und anderen Bedrohungen. Datensicherungs- und Wiederherstellungssysteme sind für unsere Unternehmen von entscheidender Bedeutung und müssen in jede Zero-Trust-Initiative einbezogen werden.

Die Architektur und Implementierung von Zero Trust ist jedoch mitunter kompliziert. Bislang herrschte kein Konsens darüber, wie dieser Ansatz am besten auf Sicherungs- und Wiederherstellungssysteme angewendet werden sollte.

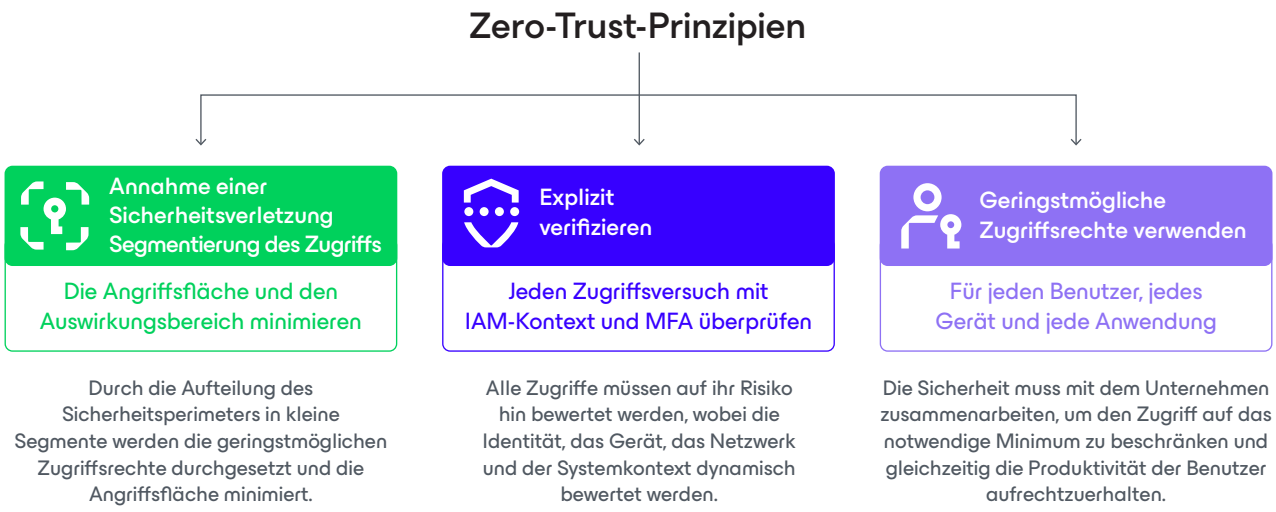
Zero-Trust-Datenresilienz (ZTDR) ist ein neues Modell von Veeam und Numberline Security und baut Zero-Trust-Reifegradmodell der US-amerikanischen Behörde CISA (Cybersecurity and Infrastructure Security Agency). ZTDR erweitert die Prinzipien von Zero Trust auf Backup und Wiederherstellung und stellt so sicher, dass Unternehmen Risiken mindern und ihre Sicherheits- und Resilienzziele erreichen können.

Wenn Sie dem in diesem Leitfaden erläuterten Zero-Trust-Ansatz für Datenresilienz folgen, erfahren Sie, worauf es bei einer Plattform und Architektur für die Sicherung und Wiederherstellung von Daten ankommt, und wie Sie in Ihrer Umgebung schnell und effektiv damit beginnen können.

Zero Trust: Eine kurze Einführung

Zero Trust ist eine moderne Sicherheitsstrategie, die auf dem Gedanken basiert, dass kein Benutzer, kein Gerät und kein Netzwerkpaket implizit vertrauenswürdig sein sollte. Damit die Datensicherheit gewährleistet bleibt, sollte der Zugriff auf kritische Datenbestände segmentiert und die gesamte Kommunikation authentifiziert, ausgewertet und autorisiert werden, bevor ein Zugriff gewährt wird. Dies gilt für jedes Segment und seine Daten, Anwendungen, Ressourcen oder Services.

Dies ist eine signifikante Veränderung gegenüber herkömmlichen Architekturen zur Informationssicherheit, die auf statischen, netzwerkbasierten Perimetern basierten — und die eindeutig nicht in der Lage waren, unsere Unternehmen vor Ransomware und böswilligen Akteuren zu schützen.



Einführung in die Zero-Trust-Datenresilienz (ZTDR)

Systeme zur Datensicherung und -wiederherstellung sind wichtige Elemente der Unternehmens-IT und häufiges Ziel von Angriffen. Sie müssen sachgerecht und ganzheitlich gesichert werden.

Durch die Einhaltung der ZTDR-Prinzipien und die Auswahl von Backup- und Speicheranbietern anhand der ZTDR-Richtlinien profitiert Ihr Unternehmen von stärkeren Schutzmaßnahmen, einem effizienteren Betrieb sowie einer schnelleren und zuverlässige Wiederherstellung.

ZTDR erweitert zentrale Zero-Trust-Prinzipien

LÖSUNGSANFORDERUNGEN

Trennung von Backup-Software und Backup-Speicher

Die Angriffsfläche und den Auswirkungsbereich minimieren

Achten Sie auf Lösungen für Datensicherung und Wiederherstellung, bei denen Backup-Software und -Speicher voneinander getrennt sind und die im Idealfall den Zugriff von Root oder OS auf den Backup-Speicher verhindern.

Diese Funktionalitäten ermöglichen es Ihnen, Zugriffskontrollen über Zero-Trust-Richtlinien strikt durchzusetzen.

Mehrere Resilienzzonen

3-2-1-Backup-Regel

Achten Sie auf Lösungen für Datensicherung und Wiederherstellung, die mehrere Resilienzzonen unterstützen, sodass Ihr Unternehmen den Verlust oder die Kompromittierung eines einzelnen Backup-Systems oder einer einzelnen Speicherumgebung übersteht.

So können Sie die 3-2-1-Regel für Backups problemlos einhalten.

Unveränderlicher Backup-Speicher

Schutz von Backup-Daten vor Änderung oder Löschung

Achten Sie auf Lösungen für Datensicherung und Wiederherstellung, die einen robusten, zuverlässigen unveränderlichen Backup-Speicher einfach und effizient unterstützen.

So können Sie darauf vertrauen, dass Ihre gesicherten Daten vor Löschung und Änderung geschützt sind, selbst in Anwesenheit eines böswilligen Akteurs.

Die 3-2-1-Regel für Best Practices beim Backup:

3

3 Kopien der Daten, einschließlich Produktionsdaten.

2

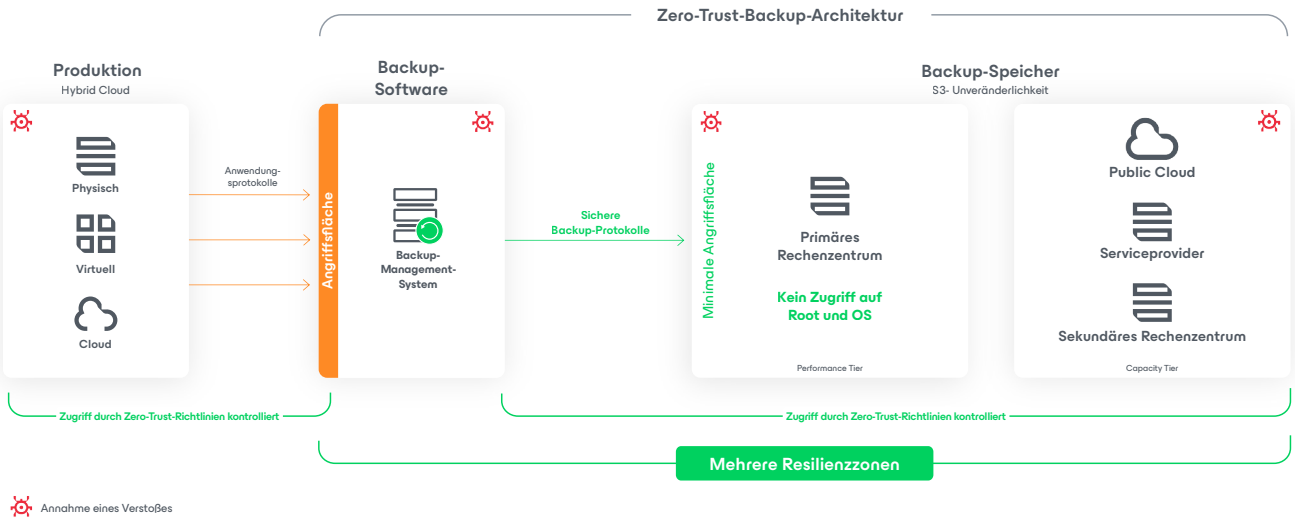
2 Kopien der Backup-Daten in unveränderlichem Speicher in separaten Resilienzzonen.

1

1 Kopie extern.

ZTDR-Referenzarchitektur

Diese ZTDR-Referenzarchitektur zeigt Ihnen, wie eine Zero-Trust-Plattform zusammen mit Ihren Backup-Management- und Speichersystemen bereitgestellt werden sollte.



Erste Schritte mit ZTDR

Zero Trust ist zwar ein langer Weg, aber es gibt unmittelbare und wirkungsvolle Maßnahmen, die Sie ergreifen können, um die Sicherheitsresilienz Ihrer Infrastruktur für Sicherung und Wiederherstellung zu verbessern.

Diese Woche:

Finden Sie heraus, wie gut Ihre Backup- und Wiederherstellungssysteme die ZTDR-Anforderungen erfüllen.

Aufgabe	Zu stellende Fragen
Sprechen Sie mit Ihren Netzwerk- und IT-Infrastrukturteams über Ihre Netzwerksegmentierung.	• Wie ist unser Netzwerk segmentiert? • Sind Backup-Software und Backup-Speicher in getrennte Sicherheitszonen unterteilt? • Wie werden die Zugriffe auf und von den einzelnen Segmenten der Backup-Infrastruktur gesteuert?
Prüfen Sie, ob Ihre Backup-Datenspeicher in mehrere Resilienzzonen unterteilt sind.	• Befolgen wir die Branchenrichtlinien in Bezug auf 3-2-1? • Was passiert mit unseren Backup- und Wiederherstellungsprozessen, wenn eine unserer Backup-Zonen nicht verfügbar ist? • Was geschieht mit unseren Backup- und Wiederherstellungsprozessen, wenn zwei unserer Backup-Zonen nicht verfügbar sind?
Bestimmen Sie, ob Ihre Backup-Speichersysteme ordnungsgemäß unveränderlich sind	• Wie dokumentiert und garantiert Ihr Speicheranbieter die Unveränderlichkeit? • Kann ein böswilliger Administrator Einstellungen bezüglich Unveränderlichkeit oder Aufbewahrung durch Root- oder OS-Zugriff auf den Speicher ändern? • Was passiert, wenn die Systemzeit böswillig vorgeschoben wird?
Ihre Wiederherstellungsprozesse validieren	• Wie sieht unser DR-Reaktionsplan aus? Wann haben wir es zuletzt getestet? • Wie viele Personen aus dem IT- oder Speicher-Team können ein System erfolgreich wiederherstellen, indem sie die aufgeführten Schritte befolgen? • Was passiert, wenn (wichtige Person X) während eines Vorfalls nicht verfügbar ist?

Nächste Woche:

Überprüfen Sie Ihre Prozesse und Tools und planen Sie dann kurz- und mittelfristige Veränderungen an Ihrer Infrastruktur und den Prozessen für die Sicherung und Wiederherstellung.

Aufgabe	Zu stellende Fragen
Bewerten Sie Ihr Vertrauen und die Wiederholbarkeit Ihrer Wiederherstellungsprozesse durch regelmäßige (wöchentliche/ monatliche) Tests.	• Wie oft führen wir unsere Wiederherstellungstests durch? • Was haben wir über Dokumentations- oder Prozesslücken gelernt? • Wann können wir diese beheben?

Aufgabe	Zu stellende Fragen
Netzwerkkonfiguration, -segmentierung oder Firewall-Regeländerungen planen	• Mit wem aus dem IT- oder Sicherheitsteam kann ich mögliche Änderungen besprechen? • Wer im Sicherheitsteam leitet unsere Zero-Trust-Initiative und wie kann ich sie unterstützen? • Welche Änderungen an der Netzwerksegmentierung oder Infrastruktur werden derzeit durchgeführt?
Berücksichtigen Sie Änderungen an der Speicherkonfiguration oder die Evaluierung neuer Anbieter, um Lücken bei der Unveränderlichkeit zu schließen.	• Wie gehen wir bei der Evaluierung und Beschaffung von zusätzlichem Backup-Speicher vor? • Welche Art von Begründung müssen wir in den Bereichen Finanz, Effizienz oder Risiko anstellen? • Wie erhalte ich die Genehmigung für die Einleitung eines Prozesses zur Anbieterbewertung?
Verantwortliche Eigentümer für alle Prozess- und Dokumentationsverbesserungen zuweisen	• Wer ist an der Genehmigung und Umsetzung der Änderungen an (Prozess X) beteiligt? • Wie können wir einen für beide Seiten akzeptablen Implementierungstermin festlegen?

Nächster Monat:

Beginnen Sie mit der Implementierung kurzfristiger Änderungen und identifizieren Sie alle erforderlichen längerfristigen Änderungen.

Aufgabe	Zu stellende Fragen
Verbesserte Disaster Recovery-Prozesse bereitstellen und erneut testen	• Wie stark haben sich unsere DR-Prozesse verbessert? • Haben wir alle Prozess- und Dokumentationslücken geschlossen?
Netzwerksegmentierung validieren und wiederholen	• Welche Bereiche des Netzwerks gewähren noch breiten Netzwerkzugriff auf unsere Backup-Systeme und von dort? • Wie können wir diese Sicherheitsmaßnahmen verschärfen, um unsere Resilienz gegenüber Ransomware zu verbessern?
Verbesserungen bei Speicherkapazität, Speicherort und Unveränderlichkeit durchführen	• Wie zufrieden sind wir mit unseren Backup-Speicherkapazitäten? • Wie sicher sind wir, dass unsere Backup-Speichersysteme unveränderlich sind? • Wie gut befolgen wir die 3-2-1-Regel der Best Practices? • Wie nutzen wir mehrere Resilienzzonen?

Worauf sollten Sie sonst noch achten?

Proaktive Disaster-Recovery-Validierung

Vorfälle, bei denen gesicherte Daten wiederhergestellt werden müssen, ereignen sich häufig zu unerwarteten Zeitpunkten und wahrscheinlich unter sehr stressigen Umständen. Es ist wichtig, dass Ihre Organisation über gut verstandene, gut dokumentierte und eingespielte Disaster-Recovery-Pläne und -Prozesse verfügt. Außerdem sollten Sie sicherstellen, dass Sie der Integrität und Gültigkeit der gesicherten Daten ein hohes Maß an Vertrauen entgegenbringen.

Einfache Abläufe

Stellen Sie sicher, dass Sie ein System auswählen, das einfach genug ist, damit Ihr Unternehmen leicht und zuverlässig betrieben werden kann, und das gleichzeitig genügend Funktionalität, Skalierbarkeit und Raffinesse bietet, um die Anforderungen Ihres Unternehmens vollständig zu erfüllen. Arbeiten Sie daran, die Kapazität und Fähigkeiten Ihrer Mitarbeiter klar zu verstehen, damit der Betrieb nicht von einer einzelnen Person oder einem „Superhelden“ abhängt.

FAQ

Ist Zero Trust etwas, das Sie von einem Anbieter kaufen können?

Nein — Zero Trust ist etwas, das Sie **tun** — es ist eine Sicherheitsstrategie, die die IT-, Sicherheits- und Geschäftsergebnisse verändert und verbessert.

Geht es bei Zero Trust nur darum, den Zugriff einzuschränken und die Benutzerproduktivität zu verringern?

Nein — Bei Zero Trust geht es darum, **unnötigen** Zugriff zu eliminieren und gleichzeitig die Produktivität der Benutzer zu gewährleisten. Viele Unternehmen **verbessern** mit Zero Trust sogar die Benutzerproduktivität und das Benutzererlebnis.

Warum ist Zero Trust wichtig?

Zero Trust ist der effektivste Weg, um unsere Unternehmen vor Risiken wie Ransomware, böswilligen Akteuren und anderen Risiken zu schützen. Angesichts der aktuellen Bedrohungslage sehen wir uns in der Verantwortung, diese Möglichkeit zu nutzen.

Können Sie Ihre derzeitige Sicherheitsinfrastruktur für Zero Trust nutzen?

Höchstwahrscheinlich ja! Bei richtiger Anwendung können moderne Firewall-, Identitäts- und Infrastruktursysteme Sie bei Ihrem Weg zu Zero Trust unterstützen. Um einen optimalen Zero-Trust-Reifegrad zu erreichen, sind möglicherweise zusätzliche Investitionen erforderlich, die durch Tools wie die ZTDR-Referenzarchitektur gesteuert werden können.

Zusätzliche Ressourcen

Sie möchten mehr über Zero Trust und ZTDR erfahren?

- Auf der Veeam-Website finden Sie die vollständige ZTDR-Studie, und Sie erfahren mehr über den Veeam-Ansatz für Datensicherheit und Cyberresilienz.
- Um das vollständige ZTDR-Forschungs-Whitepaper zu lesen und die Perspektive von Numberline Security zu diesem Thema zu erfahren, besuchen Sie die Numberline-Website.

Über Veeam Software

Veeam, der #1 Weltmarktführer im Bereich Datenresilienz, ist der Ansicht, dass Unternehmen die Kontrolle über all ihre Daten behalten sollten, jederzeit und überall, wenn sie sie benötigen. Veeam bietet Datenresilienz durch Daten-Backup, Datenwiederherstellung, Datenfreiheit, Datensicherheit und Datenintelligenz. Veeam mit Hauptsitz in Seattle hat weltweit mehr als 550.000 Kunden, die auf Veeam vertrauen, um ihren Geschäftsbetrieb aufrechtzuerhalten. Weitere Informationen finden Sie unter www.veeam.com/de. Sie können Veeam auf LinkedIn unter @veeam-software und auf X unter @veeam folgen.

Weitere Informationen:
veeam.com