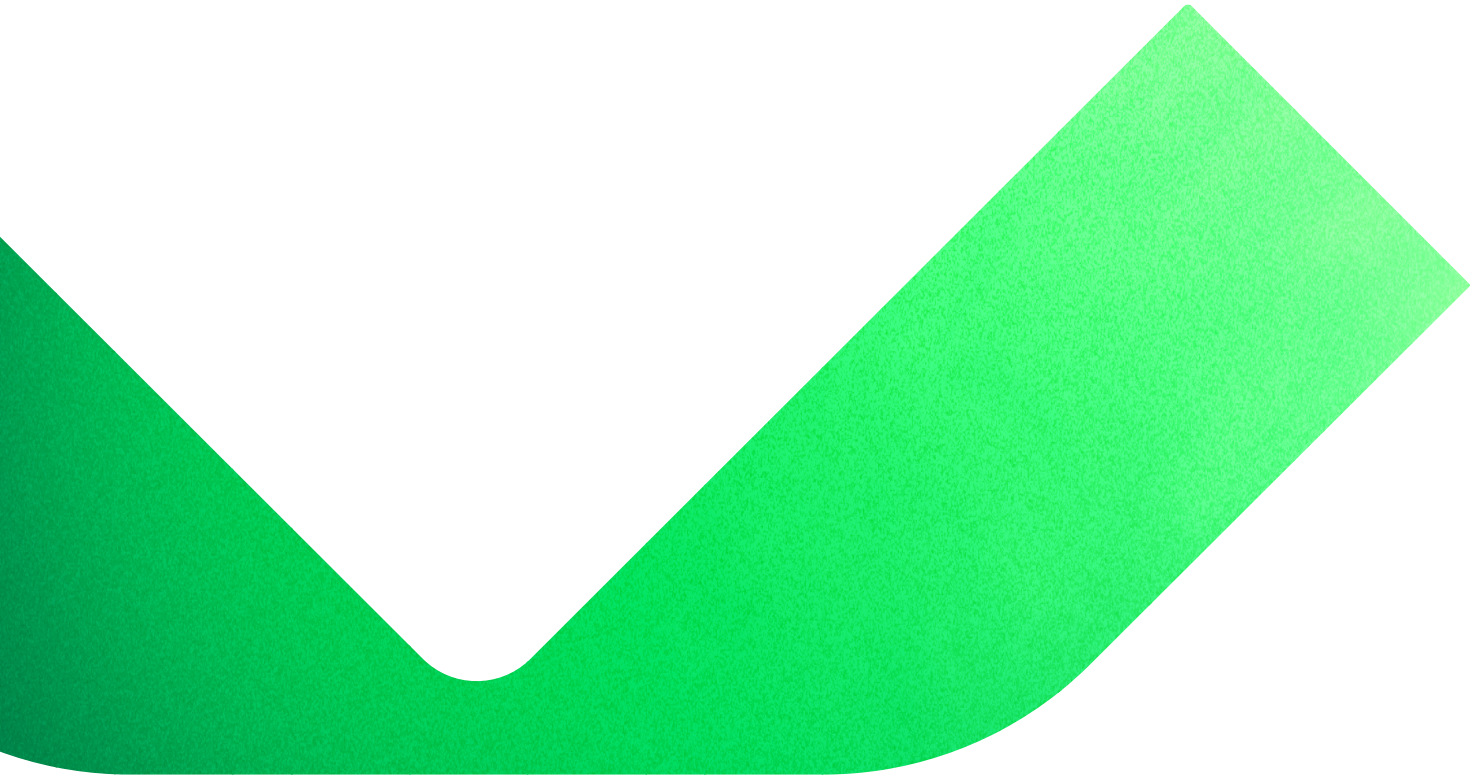
Zero-Trust-Datenresilienz

Ein Modell für die zuverlässige Sicherung und Wiederherstellung von Daten



Inhalt

Executive Summary	3
Einführung	4
Ansatz	5
Zero-Trust-Datenresilienz: Grundsätze	7
Zero-Trust-Datenresilienz: Referenzarchitektur	12
Zero-Trust-Datenresilienz: Erweitertes Reifegradmodell	14
Reifegradmodell — Zusammenfassung	19
Fazit	19

Executive Summary

Unternehmen werden beim Schutz ihrer Daten und Netzwerke mit immer größeren Herausforderungen konfrontiert, wozu insbesondere Ransomware und Datenexfiltrationsangriffe zählen. Um diesen Problemen zu begegnen, hat die so genannte „Zero Trust"-Strategie in der Informationssicherheitsbranche zuletzt erheblich an Akzeptanz gewonnen und wird von sehr vielen Unternehmen weltweit übernommen.

Doch selbst die am weitesten verbreiteten Zero-Trust-Modelle enthalten keine umfassenden Richtlinien in einigen wichtigen Bereichen, insbesondere im Hinblick auf die Sicherung und Wiederherstellung von Daten. Da es wichtig ist, diese Lücke zu schließen und die Zero-Trust-Prinzipien auf diesen Bereich anzuwenden, führen wir das Konzept der Zero-Trust-Datenresilienz ein. Diese besteht aus einer Reihe von Anforderungen, einer Architektur und einer Erweiterung bestehender Zero-Trust-Reifegradmodelle.

Insbesondere benötigen Unternehmen ein System zur Sicherung und Wiederherstellung von Daten, das eine unveränderliche Datenspeicherung und -konfiguration bietet und gleichzeitig einen kontextbezogenen und stark authentifizierten Zugriff auf die Quelldaten in der Produktivumgebung und in den gesicherten Daten ermöglicht. Dieses System muss zudem die in modernen Unternehmen üblichen Hybridarchitekturen nahtlos unterstützen und die Wiederherstellung in unterschiedlichen Umgebungen flexibel handhaben können.

Durch die Implementierung einer Zero-Trust-Architektur, die diese Anforderungen erfüllt, können Unternehmen ihre Daten, Netzwerke und Anwendungen besser vor böswilligen Akteuren schützen. Zero Trust bietet im Vergleich zu herkömmlichen Konzepten nachweislich höhere Sicherheit, und Organisationen sollten dies unbedingt übernehmen. Die neuen Anforderungen an die Datenresilienz, die in diesem Whitepaper vorgeschlagen werden, verbessern und erweitern Zero Trust und sollten als obligatorischer Teil der Sicherheitsstrategie eines jeden Unternehmens angesehen werden.

Einführung

Zero Trust ist eine Sicherheitsstrategie und notwendigerweise breit gefächert. Die weit verbreiteten Zero-Trust-Modelle und -Frameworks umfassen jedoch nicht alles. Dies kann zu entsprechenden Lücken oder Versäumnissen in den Sicherheitsarchitekturen von Unternehmen führen. Insbesondere sind Backup- und Wiederherstellungssysteme nicht Teil gängiger Zero-Trust-Frameworks. Dies ist bedauerlich, da Unternehmensdaten sehr häufig das primäre Ziel böswilliger Akteure sind, sowohl bei Ransomware- als auch bei Datenexfiltrationsangriffen.

Datensicherungs- und Wiederherstellungssysteme sind kritische Elemente der Unternehmens-IT und müssen auch als solche behandelt werden. Sie haben Lesezugriff auf alles, was wichtig ist, um es zu sichern. Außerdem müssen sie in der Lage sein, Daten in Produktivumgebungen zu schreiben, um ihre Datenwiederherstellung ausführen zu können. Sie enthalten auch eine vollständige Kopie der wichtigsten Daten des Unternehmens. All diese Eigenschaften zusammen unterstreichen die Wichtigkeit von Datensicherungs- und Wiederherstellungssystemen und verdeutlichen ihren Wert als Ziel für böswillige Akteure.

Sicherungs- und Wiederherstellungssysteme gehören zwar schon seit Jahrzehnten zum Verantwortungsbereich der IT-Abteilung, wurden jedoch häufig nicht in den Aufgabenbereich oder die Verantwortung der Sicherheitsteams einbezogen. Angesichts der massiven und raffinierten Sicherheitsbedrohungen, mit denen Unternehmen derzeit konfrontiert sind, reicht es jedoch nicht mehr aus, die Datensicherung und -wiederherstellung allein aus der Perspektive des Netzwerks und der IT-Infrastruktur zu betrachten. In der Praxis sind wir auf Unternehmen gestoßen, in denen diese Systeme schlecht konfiguriert und nicht überwacht wurden und daher ein erhebliches Risiko darstellten.

Moderne und effektive Sicherheit basiert auf dem Zero-Trust-Prinzip. Es ist also an der Zeit, Sicherungs- und Wiederherstellungssysteme unter diesem Gesichtspunkt neu zu betrachten. Dieses Whitepaper erreicht dies anhand eines neuen Konzepts der Zero-Trust-Datenresilienz. Mit diesem Konzept erhalten Unternehmen einen klaren und konkreten Weg zu stärkerem Schutz, effizienteren Betriebsabläufen und schnellerer Wiederherstellung.

[1] Im ZTMM-Dokument der CISA heißt es: „Während das ZTMM viele Aspekte der Cybersicherheit abdeckt, die für Unternehmen von entscheidender Bedeutung sind, geht es nicht auf andere Aspekte der Cybersicherheit ein, wie z. B. ... Wiederherstellung."

Ansatz

Die klassischen Grundelemente der Informationssicherheit — der „CIA"-Dreiklang aus Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) — lassen sich sämtlich auf die Sicherung und Wiederherstellung von Daten anwenden. Unternehmen müssen Datenexfiltrationen vermeiden (Vertraulichkeit), die Verschlüsselung von Daten durch Ransomware verhindern (Integrität) und sicherstellen, dass ihre Systeme vor Angriffen geschützt sind und nach einem Angriff schnell wiederhergestellt werden können (Verfügbarkeit).

Die zentralen Zero-Trust-Prinzipien sind dafür absolut relevant und sollten auf den Zugriff von Benutzern und Unternehmen auf IT-Systeme sowie auf Sicherungs- und Wiederherstellungssysteme für Daten angewendet werden. Zu diesen Prinzipien gehören die Eliminierung von implizitem Vertrauen und unsegmentierten Netzwerken, die Kontrolle aller Zugriffe durch dynamische und kontextsensitive Richtlinien über Policy Enforcement Points (PEPs), die Forderung nach einer angemessen starken Authentifizierung aller Subjekte, die Grundannahme, dass Verstöße vorliegen bzw. beabsichtigt sind, sowie die Gewährleistung und Validierung der System- und Datenintegrität. In diesem Whitepaper geht es darum, wie diese Prinzipien in die vorgeschlagenen neuen Anforderungen an Architekturen mit Zero-Trust-Datenresilienz einfließen.

Der De-facto-Standardrahmen für die Betrachtung des Zero-Trust-Reifegrads ist das in Abbildung 1 dargestellte CISA Zero Trust Maturity Model[2], das fünf Kernsäulen definiert: Identität, Geräte, Netzwerke, Anwendungen und Workloads sowie Daten. Dazu kommt die Definition von drei übergreifenden Funktionalitäten: Transparenz und Analysen, Automatisierung und Orchestrierung sowie Governance.

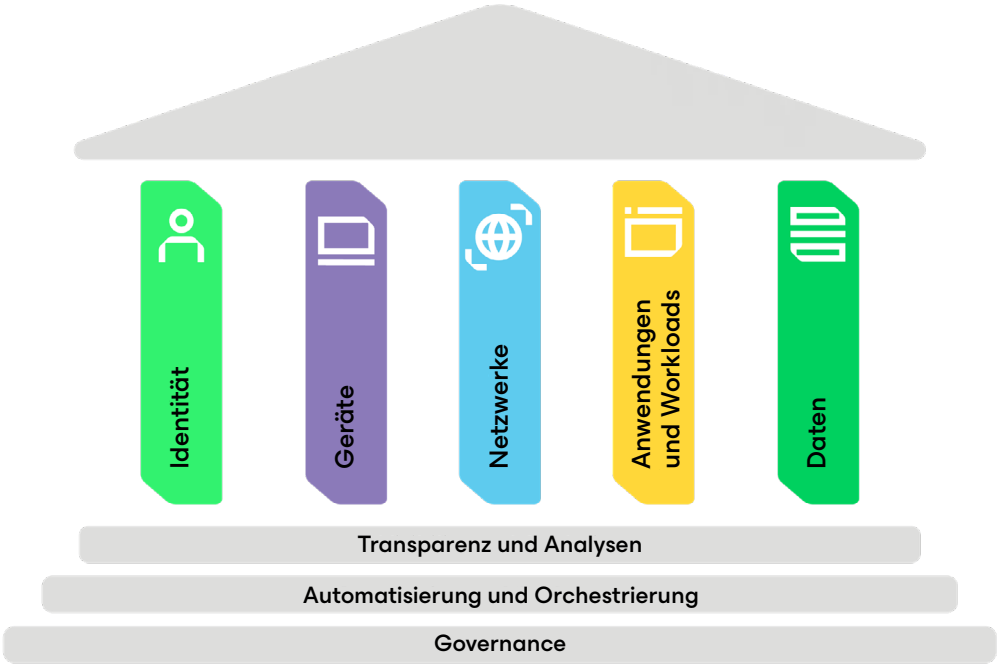


Abbildung 1: CISA Zero Trust Maturity Model

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

Im Bereich der Daten identifiziert das CISA-Modell fünf detaillierte Funktionen mit erwarteten Leistungen und Attributen für jeden Reifegrad.

Innerhalb dieser Funktionen spielt das Thema Integrität und Wiederherstellung von Datensicherungen jedoch nur eine kleine Rolle, und die CISA verweist auf ein NIST-Dokument von 2020, das nichts mit Zero Trust zu tun hat. Zusammenfassend lässt sich sagen, dass das CISA Zero Trust-Modell keine Angaben zu Anforderungen und Reifegraden für Datensicherungs- und -wiederherstellungssysteme macht. Da dieser Bereich für die Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmen so wichtig ist, muss diese Lücke geschlossen werden.

Um dies zu erreichen, führen wir das Konzept der Zero-Trust-Datenresilienz ein, das Prinzipien, eine Referenzarchitektur und eine neue Reihe von Funktionalitäten für das Zero Trust Maturity Model umfasst. Zusammengenommen stellen diese eine Erweiterung und Verbesserung von Zero Trust dar und werden zu einer stärkeren Unternehmenssicherheit führen.

Die Funktionen sind:

- Data Inventory Management
- Kategorisierung von Daten
- Datenverfügbarkeit
- Datenzugriff
- Datenverschlüsselung

Zero-Trust-Datenresilienz: Grundsätze

Die Grundprinzipien von Zero Trust Data Resilience (ZTDR) sind:

Zugriff nach dem Prinzip der geringsten Rechte

Immutability

Systemresilienz

Proaktive Validierung

Betriebliche Einfachheit

Sehen wir uns diese der Reihe nach an.

Zugriff nach dem Prinzip der geringsten Rechte

Dieses Prinzip ist für Zero Trust von zentraler Bedeutung und ein erforderlicher Bestandteil jeder Zero-Trust-Architektur. Es lohnt sich jedoch, sich seine Anwendbarkeit auf die Besonderheiten der Zero-Trust-Datenresilienz genauer anzusehen, da es auf mehreren Ebenen wirksam ist. Das Backup-Management-System selbst muss im Netzwerk isoliert werden, damit keine nicht autorisierten Benutzer oder Geräte ohne Authentifizierung darauf zugreifen können. Auch das Backup-Speichersystem muss isoliert werden. Dadurch wird verhindert, dass böswillige Akteure eines der Systeme durch Netzwerkaufklärung entdecken oder eine Schwachstelle ausnutzen.

Der rechtmäßige und autorisierte Zugriff auf das Backup-System darf nur über einen Zero-Trust-Richtliniendurchsetzungspunkt (Zero Trust Policy Enforcement Point, PEP) mit entsprechend starken Authentifizierungs- und Gerätestatusprüfungen erfolgen. Der Zero-Trust-PEP muss auch den Zugriff auf die Quelldaten (d. h. die Daten, die gesichert werden) kontrollieren, und zwar mit angemessenen Authentifizierungsverfahren und Geräte- oder Systemvalidierungen in gewissem Umfang, um sicherzustellen, dass nicht ein Angreifer-System/-Prozess, sondern das Backup-Management-System die Produktionsdaten liest.

Der Zugriff vom Backup-Management-System auf den Backup-Speicher muss ebenfalls über einen PEP gesteuert und durch eine entsprechend starke Authentifizierung vom übrigen Netzwerk getrennt sein. Beachten Sie, dass wir diese Anforderung im folgenden Architekturdiagramm noch einmal betrachten werden, da sie sehr wichtig ist: Das Backup-Speichersystem muss vom Backup-Management-System getrennt werden.

Immutability

Das Konzept und die Forderung nach unveränderlichen Backup-Daten haben sich in den letzten Jahren durchgesetzt, zusammen mit der zunehmenden Verbreitung und Raffinesse von Ransomware. Unter einem unveränderlichen Backup versteht man ein Backup mit einem Speichermechanismus, der nach seiner Erstellung nicht mehr verändert werden kann. Selbst wenn ein Angreifer im Netzwerk präsent wäre und die Kontrolle über das Backup-System übernehmen und auf den Backup-Speicher zugreifen könnte, wäre er dann nicht in der Lage, die gesicherten Daten zu löschen oder zu verändern (etwa zu verschlüsseln). Ein Teil dieser Unveränderlichkeit basiert auf den physischen Eigenschaften von Speichermedien, wie z. B. optischer „Write-Once-Read-Many"-Datenträger. Neuere Technologien verwenden hingegen Medien, bei denen die Unveränderlichkeit auf Hardware-, Firmware- oder Softwareebene erzwungen wird. In jüngster Zeit haben große Cloud-Serviceprovider Funktionalitäten für unveränderlichen Speicher eingeführt, um Unternehmen dabei zu unterstützen, Compliance- und Archivierungsanforderungen zu erfüllen.

ANMERKUNG

Anforderungen an Immutability gehen über die gespeicherten Daten hinaus und müssen auch die Aufbewahrungsfristen für Daten umfassen. Einige unveränderliche Daten können für die Speicherung auf unbestimmte Zeit konfiguriert werden, während andere einen bestimmten Aufbewahrungszeitraum haben, z. B. ein oder fünf Jahre. Daten, die ihren Aufbewahrungszeitraum überschritten haben, können gelöscht werden, weshalb das Datenspeichersystem auch den Aufbewahrungszeitraum der Daten unveränderlich machen muss. Dadurch wird eine böswillige Verkürzung der Aufbewahrungsfristen ausgeschlossen.

Systemresilienz

Wir betrachten die Systemresilienz in umfassender Weise und sich davon überzeugt, dass dieses Prinzip nicht nur auf die Backup-Infrastruktur selbst, sondern auf das gesamte Ökosystem aus Tools, Technologien und Prozessen im Zusammenhang mit der Sicherung und Wiederherstellung von daten angewendet werden muss. Insbesondere muss die Backup-Infrastruktur widerstandsfähig gegen Ausfälle und Angriffe sein, etwa wenn Komponenten oder Netzwerke nicht verfügbar sind oder NTP (Network Time Server)-Manipulationen den zeitlichen Ablauf gesicherter Daten auslösen. Auch die Nutzung von verteiltem und heterogenem Backup-Datenspeicher muss einfach zu konfigurieren sein, beispielsweise über geografische Standorte oder Infrastrukturtypen hinweg. Die Resilienz wird auch dadurch verbessert, dass die Backup-Daten vom Backup-Managementsystem getrennt werden, so dass eine Kompromittierung des Backup-Systems sich nicht auch auf den Datenspeicher auswirkt. Achten Sie daher auf ein Backup-Management-System, das im Falle einer Kompromittierung oder eines Ausfalls wiederhergestellt werden kann, ohne dass Sie beim Zugriff auf Ihre gesicherten Daten und deren Wiederherstellung eingeschränkt sind.

Zudem muss das System gegen erwartete und unerwartete Veränderungen in der Unternehmensumgebung resistent sein. Zu den erwarteten Änderungen gehören das geplante Hinzufügen oder Entfernen von Infrastrukturkomponenten und die Einführung hybrider oder cloudbasierter Anwendungen und Daten. Dies bedeutet, dass das Backup-System in der Lage sein muss, Unternehmensdaten unabhängig vom Standort oder der verwendeten Technologie effizient zu erfassen und zu speichern. Unerwartete Änderungen treten in der Regel bei Reaktionen auf Vorfälle oder bei Disaster Recovery (DR)-Maßnahmen auf und werden meist als Unterstützung für die Wiederherstellung in unterschiedlichen Umgebungen kategorisiert. Es ist durchaus möglich, dass die Wiederherstellungsumgebung bei der Datenwiederherstellung an einem anderen Standort oder auf einer anderen Infrastruktur betrieben wird. So kann beispielsweise eine Überschwemmung des lokalen Rechenzentrums eine Wiederherstellung in einer cloudbasierten Umgebung erforderlich machen, in der der laufende Betrieb über einen längeren Zeitraum hinweg aufrechterhalten werden muss. Daher muss das Backup-System sowohl die Wiederherstellung in diese andere Umgebung als auch zukünftig neue Backups aus dieser Produktionsumgebung unterstützen.

Das Backup-Datenspeichersystem selbst sollte nicht nur einen unveränderlichen Datenspeicher bieten, sondern sich zudem leicht absichern lassen. Dabei kann es sich um eine vorgehärtete Appliance oder ein vom Administrator konfigurierbares System mit klaren Härtungsempfehlungen handeln, das eher für anspruchsvolle Unternehmen geeignet ist.

Proaktive Validierung

Um einen ordnungsgemäßen Systembetrieb zu gewährleisten, muss das System überwacht und alle funktionalen Aspekte und Prozesse validiert werden. Das hat zwei Aspekte. Zunächst sollte das Backup-System in Bezug auf Netzwerk, Leistung und Sicherheit überwacht werden. Dies bedeutet, dass dieses System wie jedes andere hochwertige Produktionssystem behandelt werden sollte.

Zweitens, und das ist am wichtigsten, müssen die Gültigkeit der gesicherten Daten sowie die Zuverlässigkeit und Wirksamkeit der Wiederherstellungsprozesse regelmäßig überprüft werden. Die Wiederherstellung von gesicherten Daten erfolgt definitionsgemäß zu unerwarteten Zeitpunkten und sehr wahrscheinlich in einer von großem Stress geprägten Umgebung. Es ist wichtig, dass die Organisation über einen gut verstandenen, gut dokumentierten und gut einstudierten Prozess verfügt. Dazu kommt, dass mehrere Personen verfügbar sein müssen, die in der Lage sind, diese Aufgabe zu erfüllen, wobei Urlaub, Mitarbeiterfluktuation und andere Gründe für Abwesenheiten einzukalkulieren sind.

Denken Sie daran, dass dies zwar den Aufwand von Zeit und Energie erfordert, aber von operativer Reife zeugt und eine „Versicherung" für den Katastrophenfall darstellt. Beachten Sie auch, dass „Katastrophe" nicht immer wörtlich zu verstehen ist und nicht zwangsläufig für ein bedeutendes Ereignis wie etwa die Überflutung eines Rechenzentrums stehen muss. Beispielsweise geriet bei einem Unternehmen, mit dem wir zusammengearbeitet haben, aufgrund eines Programmierfehlers ein automatisierter Workflow außer Kontrolle, was dazu führte, dass erhebliche Mengen an Produktionsdaten im Finanzmanagementsystem gelöscht wurden. Dabei handelte es sich nicht um eine Katastrophe im Wortsinne, was vor allem durch die (validierten) Datenwiederherstellungsprozesse vermieden werden konnte.

Außerdem sollte das Backup-Management-System direkt oder indirekt in der Lage sein, Backups über den Zeitpunkt einer Malware-Infektion hinweg zu organisieren. Das heißt, es sollte Malware-Infektionen erkennen (oder darüber informiert werden) und Backups je nach dem Zeitpunkt ihrer Erfassung, als sauber, potenziell kompromittiert oder kompromittiert kategorisieren können.

ANMERKUNG

Bei der Datenvalidierung und -wiederherstellung müssen zudem alle Anforderungen an den Datenschutz und den Datenstandort eingehalten werden. Dies kann die Komplexität und Risiken erhöhen, weshalb eine sorgfältige Vorgehensweise sowohl unter Berücksichtigung des Dateninhalts als auch der gesetzlichen und Compliance-Verpflichtungen des Unternehmens erforderlich ist.

Betriebliche Einfachheit

Unser letztes Prinzip ist das der betrieblichen Einfachheit, definiert als System, das einfach genug ist, damit Ihr Unternehmen sicher arbeiten kann, und das gleichzeitig ausreichend Funktionalität, Skalierbarkeit und Verfeinerung bietet, um die Anforderungen Ihres Unternehmens vollständig zu erfüllen. Das heißt, ein System, das für Ihre Organisation geeignet ist.

Dies ist wichtig — wir haben erlebt, dass Unternehmen Schwierigkeiten hatten, Systeme zu nutzen und zu operationalisieren, die zu komplex für die Größe, das Team, die Fähigkeiten und die Anforderungen der Organisation waren. Dies führt zu eingeschränkten Vorteilen, Frustration und der Unfähigkeit, den erwarteten Sicherheitsreifegrad oder geschäftlichen Nutzen zu liefern. Ein Merkmal, auf das man bei einem Backup-Anbieter achten sollte, ist seine relative Stärke auf den Gebieten Orchestrierung und Automatisierung. Anbieter mit starken Funktionalitäten in ihren Plattformen werden schneller und einfacher zu operationalisieren sein.

Abschließend kann festgestellt werden, dass jedes dieser Prinzipien in die neuen Erweiterungen des Reifegradmodells eingegangen ist, die später in diesem Dokument erläutert werden; sie zeigen sich auch in der Referenzarchitektur, die wir anschließend besprechen werden.

Zero-Trust-Datenresilienz: Referenzarchitektur

Aufgrund der enormen Variabilität der Netzwerk-, Anwendungs- und Dateninfrastrukturen unterscheiden sich Daten-Backup-Architekturen unterschiedlicher Unternehmen zwangsläufig sehr. Dennoch gibt es gemeinsame Architekturelemente aufgrund gängiger Zero-Trust-Prinzipien, die in jeder Zero-Trust-Architektur für Datenresilienz vorhanden sein müssen.

Unsere Referenzarchitektur ist in Abbildung 2 dargestellt und veranschaulicht die wichtigsten Anforderungen in dieser Art von System. Hier wird die Umgebung aus der Perspektive des Backup-Management-Systems dargestellt. Auch der regelmäßige, alltägliche Zugriff von Anwendern und Systemen auf die Produktionssysteme würde von Zero Trust PEPs gesteuert, dies wird aber in dem Diagramm aus Übersichtlichkeitsgründen nicht gezeigt.

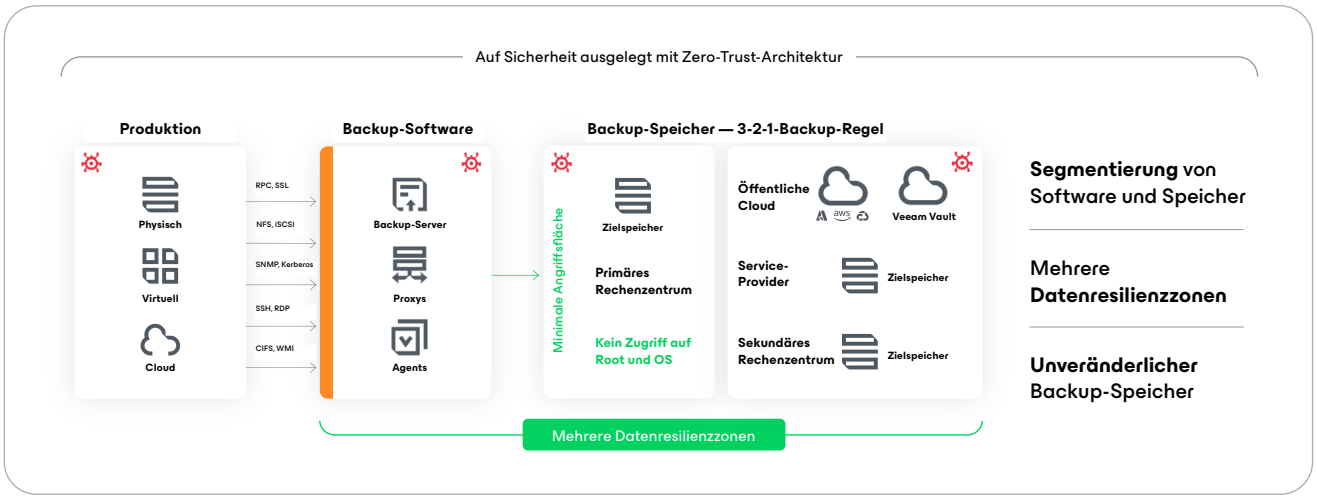


Abbildung 2 — Zero-Trust-Datenresilienz: Referenzarchitektur

Beachten Sie zunächst die Kernelemente jeder Zero-Trust-Architektur — den zentralen Policy Decision Point (PDP), der die Identitätsauthentifizierung an das IAM-System (Identity and Access Management) des Unternehmens delegiert. Der PDP stützt sich auf ihren Richtlinienspeicher, um Zugriffsentscheidungen für authentifizierte Identitäten zu treffen, einschließlich menschlicher und nicht menschlicher (System-)

Identitäten. In dieser Architektur trifft der PDP Zugriffsentscheidungen für das Backup-Management-System. Diese Entscheidungen werden über die Konsole (gestrichelte Linien) mit den Policy Enforcement Points (PEPs) weitergegeben, die sich logisch zwischen dem Backup-Management-System und den zu sichernden Datenquellen und den Backup-Zielorten befinden.

Die Architektur enthält auch eine empfohlene Struktur für die gesicherten Daten. Zusätzlich zur Anforderung der Unveränderlichkeit von Daten sollten Unternehmen dafür Sorge tragen, mindestens eine Kopie an einem primären Standort aufzubewahren, der über eine Netzwerkverbindung mit geringer Latenz zum vorgesehenen Wiederherstellungsstandort verfügt. Dies ermöglicht schnelle Backup-Snapshots, die häufigere Wiederherstellungspunkte und kürzere Wiederherstellungszeiten ermöglichen. Natürlich befindet sich der Primärstandort oft dort, wie auch die Produktionssysteme sind, so dass unsere Referenzarchitektur auch das Ziel unterstreicht, mindestens zwei Kopien der Daten an Sekundärstandorten aufzubewahren[3]. Diese müssen vom Primärstandort geographisch isoliert sein, um Resilienz gegen eine regionale Katastrophe zu erreichen. Der wahrscheinliche Nachteil ist eine langsamere Netzwerkverbindung, was zu Wiederherstellungspunkten mit niedrigerer Frequenz und längeren Wiederherstellungszeiten führen kann.

HINWEIS

Das Backup-Management-System wird bewusst von seinen Speicherebenen getrennt. Dadurch kann das Backup-System die gesicherten Daten nahtlos auf mehrere unveränderliche und geographisch verteilte Repositorys verteilen. Außerdem können Unternehmen damit Backup-Speicher-Repositorys auswählen, die die beste Kombination aus Leistung, Preis und betrieblicher Einfachheit für die jeweiligen Anforderungen bieten. Dazu kommt eine zusätzliche Sicherheitsebene, da die Kommunikation über einen PEP gesteuert wird.

[3] Es gibt unterschiedliche Auffassungen bezüglich der Anzahl der Backups an verschiedenen Speicherorten, die oft mit Merkformeln wie 3-2-1 oder 3-2-1-1-0 arbeiten.

Zero-Trust-Datenresilienz: Erweitertes Reifegradmodell

Die von uns vorgeschlagenen Prinzipien und Referenzarchitekturen für die Zero-Trust-Datenresilienz sind zwar universell anwendbar, lassen sich aber nicht vollständig und sofort auf die meisten Unternehmen anwenden. Wie bei den meisten Aspekten von Zero Trust müssen sie schrittweise geplant und umgesetzt werden. Dies wird standardmäßig anhand eines Reifegradmodells modelliert und kommuniziert. Wie bereits in der Einleitung erwähnt, folgen wir dem De-facto-Standard CISA Zero Trust Maturity Model und erweitern es um vier neue Funktionen, die unsere Prinzipien und Anforderungen umfassen.

Diese neuen Funktionen sind:

Zugriff auf Unternehmensdaten und -systeme

Zugriff auf Backup-Speicher und Daten

Systemresilienz

Systemüberwachung und -validierung

Diese ZTDR-Erweiterungen des Reifegradmodells sind in den Abbildungen 3 bis 6 dargestellt, die zeigen, wie jede der vier neuen Funktionen über die Standard-Reifegrade hinweg weiterentwickelt werden sollte: Traditional, Initial, Advanced, and Optimal (Traditionell, Anfänglich, Erweitert und Optimal).

Für jede der Funktionen haben wir erwartete Attribute für jeden Reifegrad identifiziert. Das Modell bildet dabei die Verbesserungen und Veränderungen ab, die eine Organisation vornehmen muss, um in der Reife für jede Funktion voranzukommen. Anschließend betrachten wir die einzelnen Funktionen einzeln, während wir die Reifegradstufen durchgehen.

Zugriff auf Unternehmensdaten und -systeme

Diese Funktion ist definiert als die Mittel und Mechanismen, mit denen das Backup-Management-System (BMS) auf die Quelldaten zugreifen kann, für deren Sicherung es verantwortlich ist.

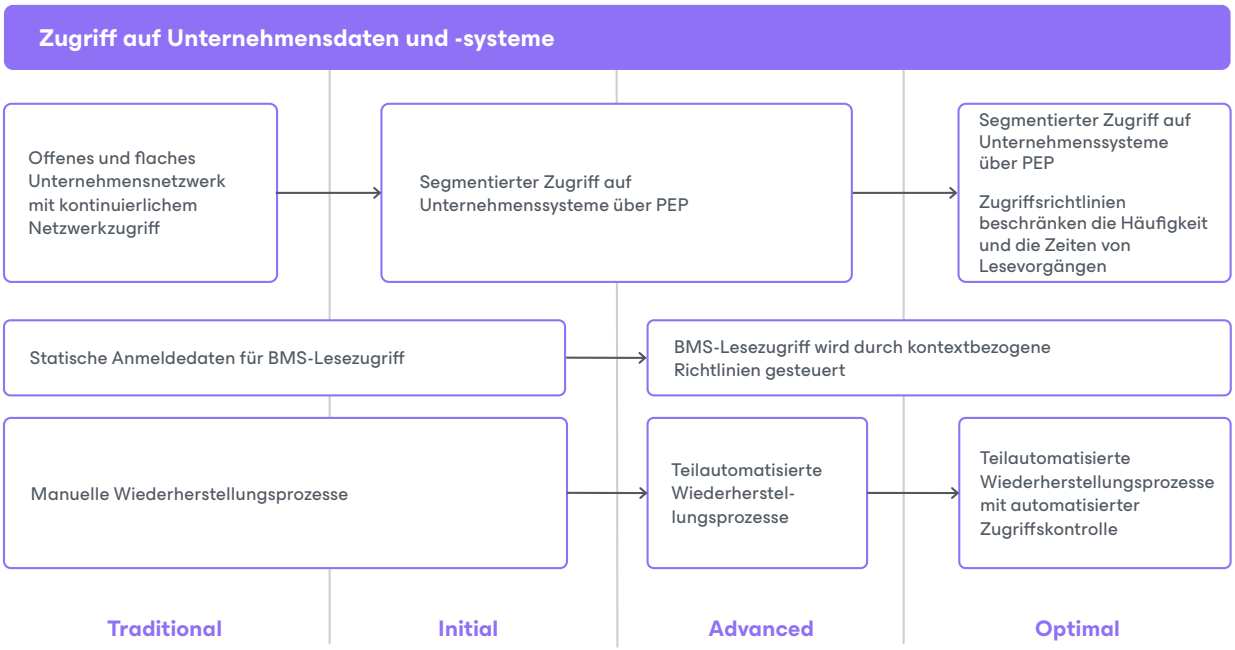


Abbildung 3 — Zugriff auf Unternehmensdaten und -systeme: Reifegradmodell

Beim Reifegrad **Traditional** (Traditionell) verfügt das Unternehmen über ein flaches, offenes Netzwerk, und das Backup-Management-System hat kontinuierlichen ungehinderten Netzwerkzugriff auf die Quellsysteme. Das BMS verwendet statische Anmeldeinformationen wie einen API-Schlüssel, einen gespeicherten Benutzernamen/ein Passwort oder ein Zertifikat, um die Quelldaten zu authentifizieren und zu lesen. Wenn Unternehmen das BMS zur Wiederherstellung eines Systems einsetzen, sind sie auf manuelle Prozesse angewiesen.

Um zur Stufe **Initial** (Anfänglich) überzugehen, muss das Unternehmen damit beginnen, eine bessere Netzwerksegmentierung durchzusetzen und den BMS-Zugriff auf Unternehmenssysteme über einen Zero Trust Policy Enforcement Point einzuschränken und das Prinzip der geringsten Privilegien einzuführen.

Auf der Stufe **Advanced** (Erweitert) hat das Unternehmen kontextsensitive Zugriffsrichtlinien für den BMS-Zugriff auf Unternehmensdaten und -systeme eingeführt und kann so die dynamischen Funktionen für die Zero-Trust-Richtliniendurchsetzung besser nutzen. Dazu hat es damit begonnen, automatisierte Wiederherstellungsprozesse mit einigen manuellen Schritten für die Initiierung und Prozessvalidierung einzusetzen.

Auf der Stufe **Optimal** hat das Unternehmen dann seine Nutzung von Zugriffsrichtlinien erweitert, um den BMS-Zugriff auf zulässige Zeiträume oder aktive Wiederherstellungsereignisse zu beschränken. Damit wird der Grundsatz der geringsten Privilegien weiter durchgesetzt.

Zugriff auf Backup-Speicher und Daten

Diese Funktion ist definiert als die Mittel und Mechanismen, mit denen das Backup-Management-System Schreib- und Lesezugriff auf den Backup-Speicher und die dort gespeicherten Daten hat.

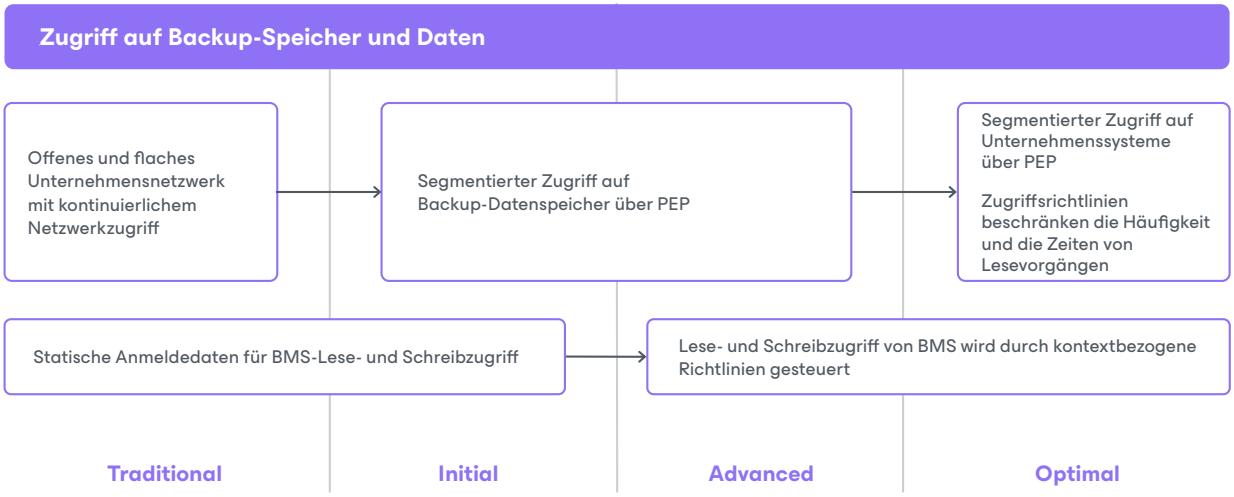


Abbildung 4 — Zugriff auf Backup-Speicher und -Daten: Reifegradmodell

Beim Reifegrad **Traditional** (Traditionell) verfügt das Unternehmen über ein flaches, offenes Netzwerk, und das Backup-Management-System hat kontinuierlichen und ungehinderten Netzwerkzugriff auf das Backup-Speichersystem und die dort gespeicherten gesicherten Daten. Das BMS verwendet statische Anmeldedaten, z. B. einen API-Schlüssel, einen gespeicherten Benutzernamen mit Passwort oder ein Zertifikat, für die Authentifizierung, zum Schreiben in den Speicher und zum Lesen der gespeicherten Daten.

Um die erste **Stufe** zu erreichen, muss das Unternehmen damit beginnen, eine bessere Netzwerksegmentierung durchzusetzen und den Zugriff des BMS auf den Backup-Speicher und die gespeicherten Daten über einen Zero-Trust-Richtliniendurchsetzungspunkt nach dem Prinzip der geringsten Rechte zu beschränken.

Auf der Stufe **Advanced** (Erweitert) hat das Unternehmen kontextsensitive Zugriffsrichtlinien für den BMS-Zugriff auf das Backup-Speichersystem und die gespeicherten Daten eingeführt. Dabei werden die dynamischen Richtliniendurchsetzungsfunktionen innerhalb des Unternehmens besser genutzt.

Auf der Stufe **Optimal** hat das Unternehmen dann seine Nutzung von Zugriffsrichtlinien erweitert, um den BMS-Zugriff auf den Speicher auf zulässige Zeiträume oder aktive Wiederherstellungsereignisse zu beschränken. Damit wird der Grundsatz der geringsten Privilegien weiter durchgesetzt.

Systemresilienz

Diese Funktion wird definiert als die Eigenschaften des Backup-Systems hinsichtlich seiner Widerstandsfähigkeit gegen Systemausfälle, Komponentenausfälle oder bösartige Aktivitäten.

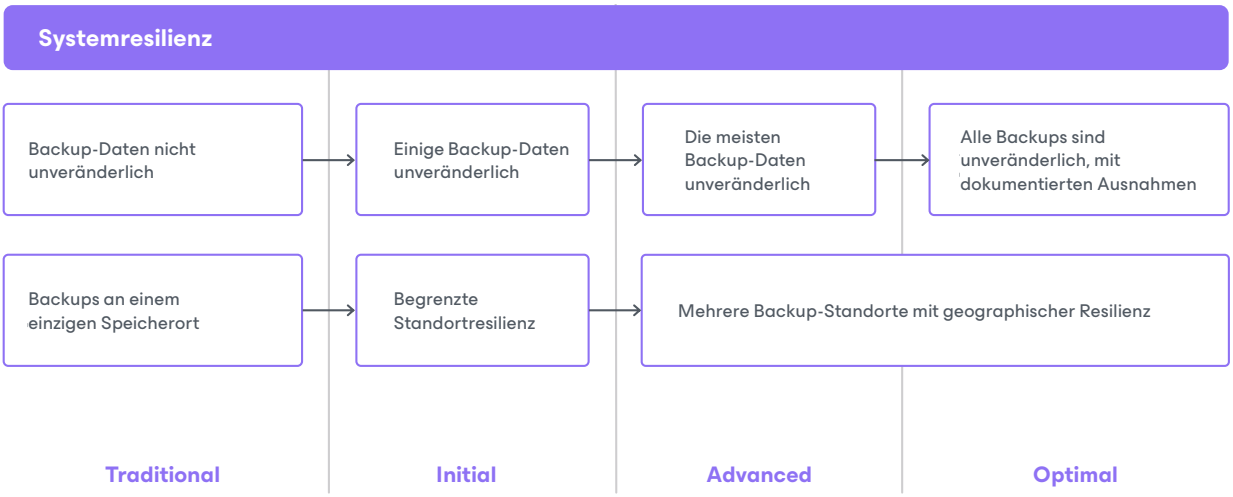


Abbildung 5 — Systemresilienz: Reifegradmodell

Beim **traditionellen** Reifegrad nutzt das Unternehmen veränderlichen Speicher für Backup-Daten, wodurch die Integrität und Verfügbarkeit der Daten gefährdet wird. Zudem werden Backups in der Regel nur an einem einzigen Ort gespeichert, wodurch das Unternehmen im Falle einer regionalen Katastrophe vollständig ausfallen könnte.

Beim Übergang zur Stufe **Initial** (Anfänglich) muss das Unternehmen beginnen, für einige seiner Daten-Backups unveränderlichen Speicher zu nutzen und für diese ein gewisses Maß an Standortresilienz einzuführen.

Auf der Stufe **Advanced** (Erweitert) verwendet das Unternehmens überwiegend unveränderlichen backup-Speicher, idealerweise priorisiert nach Sensibilität und Kritikalität der Daten. Hinzu kommen die Einführung und operationalisierte Nutzung mehrerer Backup-Speicherorte in verteilten Regionen.

Bei Erreichen der Stufe **Optimal** ist das Unternehmen vollständig zur Nutzung unveränderlichen Backup-Speichers übergegangen, wobei alle Ausnahmen davon dokumentiert und gesondert genehmigt werden müssen. Neue Datenquellen und Anwendungen nutzen standardmäßig unveränderliche Backups. Mit dieser Stufe verfügt das Unternehmen über ein Höchstmaß an Resilienz gegenüber regionalen Katastrophen und böswilligen Akteuren.

Systemüberwachung und -validierung

Diese Funktion umfasst die Tools und Prozesse, mit denen das Unternehmen sicherstellt, dass sein Backup-Management-System und sein Backup-Speicher ordnungsgemäß funktionieren und bei Bedarf einen Wiederherstellungsprozess durchführen können.

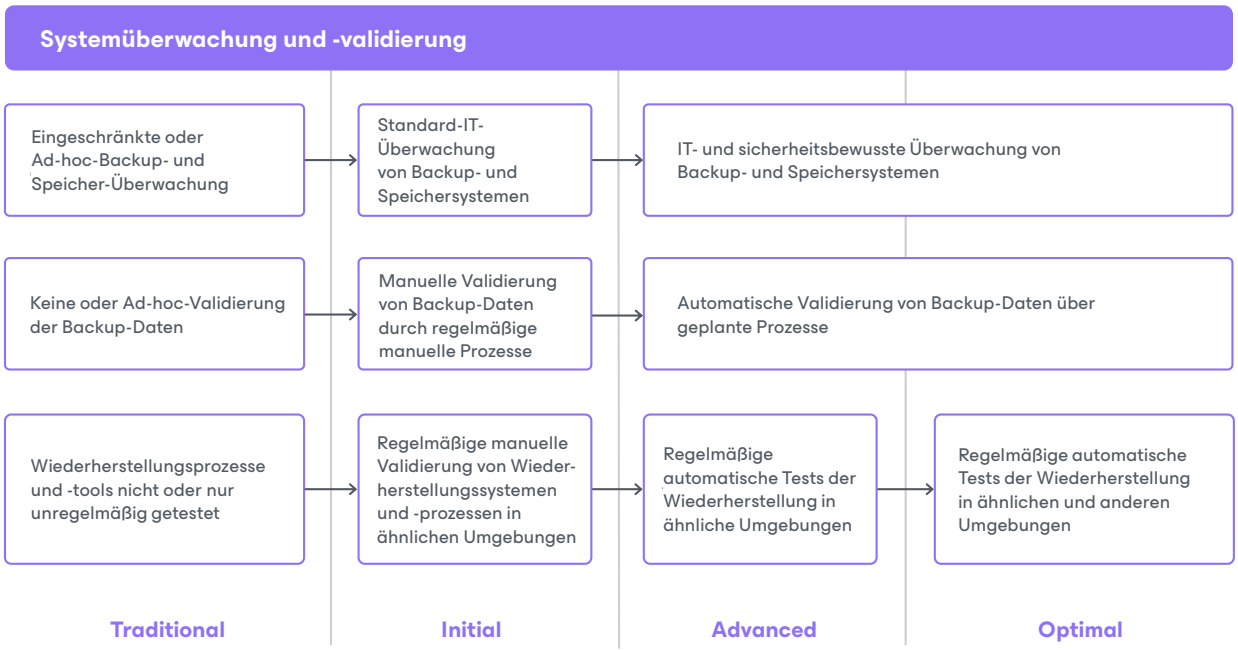


Abbildung 6 — Systemüberwachung und -validierung: Reifegradmodell

Beim Reifegrad **Traditional** (Traditionell) führt das Unternehmen nur ganz allgemeine Überwachungsfunktionen der Backup- und Speicherinfrastruktur durch, was oft dem allgemein noch niedrigen Reifegrad von IT und Betriebsabläufen entspricht. Die gesicherten Daten werden möglicherweise nicht validiert, oder es finden lediglich periodische (d.h. manuelle und seltene) Prüfungen statt. Außerdem wird das Unternehmen Wiederherstellungstools und -prozesse nicht regelmäßig testen, um sicherzustellen, dass sie gut verstanden, dokumentiert und wiederholbar sind.

Auf der Stufe **Initial** (Anfänglich) wird die IT- und Betriebsüberwachung des Backup- und Speichersystems auf standardisiertem Niveau durchgeführt. Außerdem führen sie eine regelmäßige manuelle Validierung der gesicherten Daten ein. Dazu wurde die regelmäßige (manuelle) Validierung von Wiederherstellungsprozessen implementiert, um institutionelles Wissen und die Vertrautheit mit diesen Prozessen sicherzustellen.

Auf der Stufe **Advanced** (Erweitert) haben Unternehmen IT- und Sicherheitsüberwachungstools und -pozesse für Backup- und Speichersysteme bereitgestellt. Außerdem validieren sie gesicherte Daten automatisch anhand geplanter Prüfungen, die alle anomalen Ergebnisse melden und eskalieren. Dazu gehört das automatische Testen von Wiederherstellungstools und -prozessen in Umgebungen, die Produktionsumgebungen ähneln.

Auf der Stufe **Optimal** hat das Unternehmen seine Testverfahren für Wiederherstellungen so verfeinert, dass auch die Wiederherstellung in unterschiedliche Umgebungen getestet werden kann.

Reifegradmodell — Zusammenfassung

In ihrer Gesamtheit definieren diese neuen Funktionen eine Reihe von Funktionalitäten und die erwarteten Kompetenzen über die vier Reifegradstufen des Zero-Trust-Konzepts hinweg. Sie bieten einen praktischen Fahrplan und Leitfaden für Unternehmen, die ihre Datensicherungs- und Wiederherstellungssysteme in ihre Zero-Trust-Initiative einbinden möchten.

Fazit

Zero Trust ist ein nachweislich besserer Weg, um die Informationssicherheit anzugehen, und als Sicherheitsverantwortliche haben wir die Pflicht, diese Strategie in unsere Unternehmen zu bringen. Derzeitige Zero-Trust-Architekturen und Reifegradmodelle sind solide Ausgangspunkte, aber unvollständig. Insbesondere fehlen in ihnen Anforderungen und Ansätze für die Datensicherung und -wiederherstellung.

Sicherung und Wiederherstellung wurden von Unternehmen bisher als Zuständigkeit der IT betrachtet, doch die zunehmende Verbreitung von Ransomware und die fast vollständige Digitalisierung der Geschäftsbetriebe machen es erforderlich, dass Sicherheitsverantwortliche ihren Blick erweitern, um diesen Bereich ebenfalls einzubeziehen.

In diesem Whitepaper haben wir das Konzept der Zero-Trust-Datenresilienz mit einer Reihe von Grundprinzipien, einer Referenzarchitektur und Erweiterungen des Zero-Trust-Reifegradmodells vorgestellt. Wir sind davon überzeugt, dass Unternehmen mit diesem Zero-Trust-Konzept einen klaren und konkreten Weg zu stärkeren Abwehrmaßnahmen, effizienteren Abläufen und schnelleren Wiederherstellungen erhalten. Unternehmensdaten sind zu wichtig, um Best Practices für die Sicherheit zu ignorieren, und Zero Trust ist die effektivste Methode, dies zu vermeiden.

Über Veeam Software

Veeam®, der Weltmarktführer im Bereich Datenresilienz, ist der Ansicht, dass jedes Unternehmen in der Lage sein sollte, nach einer Unterbrechung des Geschäftsbetriebs mit der Gewissheit und Kontrolle über alle seine Daten weiterzumachen, wann und wo immer es diese benötigt. Veeam nennt dies maximale Ausfallsicherheit und wir arbeiten kontinuierlich daran, innovative Lösungen zu entwickeln, mit denen unsere Kunden diese Zielvorgabe erreichen. Veeam-Lösungen wurden speziell für die Datenresilienz entwickelt, indem sie Daten-Backup, Datenwiederherstellung, Datenfreiheit, Datensicherheit und Datenintelligenz bereitstellen. Mit Veeam können Verantwortliche im IT- und Sicherheitsbereich darauf vertrauen, dass ihre Anwendungen und Daten in allen Umgebungen in der Cloud, in virtuellen, physischen, SaaS und Kubernetes sicher und jederzeit verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 550.000 Kunden, darunter 74 % der Global 2000-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam. Erfahren Sie mehr unter www.veeam.com, oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.

Weitere Informationen:
veeam.com/de