# Was ist Zero Trust?

*Zero Trust ist eine Philosophie. die das moderne Sicherheitsmodell vorantreibt.*
*Andreas Riepen*

Die rasche Einführung von Cloud-Diensten und das Arbeiten von zu Hause demonstrieren eindrücklich, wie das traditionelle Unternehmensnetzwerk schnell an Bedeutung verliert. Der Perimeter verschwindet und es gibt keine vertrauenswürdigen Zonen mehr. Alle Ressourcen müssen von überall her erreicht werden können. In diesem Zusammenhang hört man oft den Begriff „Zero Trust". Aber was genau ist Zero Trust? Ist es eine Referenzarchitektur, die es zu implementieren gilt? Ist es nur eine Geisteshaltung? Ist es ein Stück Technologie, das erworben und implementiert werden muss? Oder handelt es sich wirklich nur um ein Schlagwort, das von einer Marketingabteilung in die Welt gesetzt wurde?

An all diesen Definitionen ist etwas Wahres dran, und deshalb ist es so wichtig, sich über dieses Thema zu informieren. Vor allem in der heutigen Zeit, in der das moderne Unternehmen eine Neuausrichtung erfährt. Und obwohl Zero Trust im Allgemeinen einige Technologielösungen gegenüber anderen bevorzugt, geht es um mehr als nur ein technisches „Stack" im engeren Sinne.

In seiner ursprünglichen Konzeption war Zero Trust ein Prinzip, das für die Anwendung in traditionellen Unternehmensnetzwerken konzipiert war. Google übernahm das Prinzip, nachdem es in der Operation Aurora erfolgreich kompromittiert worden war, und dokumentierte seine Umsetzung der Prinzipien unter dem Namen BeyondCorp.

Die heutige Welt, in der sich die Daten eines Unternehmens in einem privaten Rechenzentrum, einer öffentlichen Cloud oder einer SaaS-Anwendung befinden können, ist jedoch weit entfernt von einem traditionellen Unternehmensnetzwerk aus dem Jahr 2010. Die Diskussion über den Wegfall der Netzwerkgrenzen (Perimeter) begann mit dem Jericho Forum, das 2004 von einer Gruppe interessierter CISOs aus Unternehmen gegründet wurde, um sich die Sicherheitsimplikationen einer Welt vorzustellen, in der eine Netzwerkgrenze nur schwer (oder gar nicht) zu identifizieren ist. Die heutige Konzeption von Zero Trust ist eine Verschmelzung dieser beiden Prinzipien.

***Andreas Riepen (✉)***
*Andreas Riepen ist als Mitglied der Geschäftsführung für die Region Central Europe (Deutschland, Österreich, Schweiz, Liechtenstein sowie Osteuropa) bei Vectra AI zuständig und verfügt über 25 Jahre Erfahrung in der IT, im Enterprise- sowie SMB-Bereich. Vor Vectra AI war Herr Riepen langjährig bei Riverbed, F5 Networks, Ruckus Networks, Alcatel Lucent Enterprise, Juniper Networks, Logicalis, Netsize sowie Cisco tätig und kennt die Branche quer durch die verschiedensten Lösungsfacetten.*
*ariepen@vectra.ai*

*[1]Head of Central and Eastern Europe, Vectra AI, San Jose, United States of America*

Die Zero-Trust(ZT)-Leitlinien des U.S. National Institute of Standards and Technology (NIST[1]) definieren Zero Trust (ZT) als „ein Paradigma der Cybersicherheit, das sich auf den Schutz von Ressourcen und die Prämisse konzentriert, dass

1 https://www.vectra.ai/blogpost/why-the-nist-zero-trust-architecture-no-longer-requires-decryption.

Wirtschaftsinformatik & Management 2022 • 14 (1): 29–31
https://doi.org/10.1365/s35764-021-00381-4
Angenommen: 16. Dezember 2021
Online publiziert: 31. Januar 2022

Vertrauen niemals stillschweigend gewährt wird, sondern kontinuierlich bewertet werden muss". Die veröffentlichten Leitlinien des US-Verteidigungsministeriums (DoD) und der National Security Agency (NSA) beschreiben Zero Trust als ein „Sicherheitsmodell[, das] neu überlegt, wie der Sicherheitszugriff auf Ressourcen zu implementieren ist, und das durch dynamische Richtlinien bestimmt wird – einschließlich des beobachtbaren Zustands der Client-Identität, der Anwendung/des Dienstes und des anfragenden Assets – und auch andere Verhaltens- und Umgebungsattribute umfassen kann".

Aus den obigen Ausführungen wird deutlich, dass es bei der Verinnerlichung und Einführung von Zero Trust um mehr als nur um Technologie geht – es erfordert ein ganzheitliches Überdenken einiger Grundpfeiler der bestehenden Technologiearchitektur. Glücklicherweise kann es hilfreich sein, sich den Weg zu Zero Trust in den Dimensionen Mensch, Prozess und Technologie vorzustellen.

## Menschen: Verinnerlichung der Philosophie von Zero Trust

Der erste Schritt auf dem Weg zu Zero Trust ist eine Neuausrichtung des persönlichen Verständnisses und der Philosophie, die Entscheidungsträger im Bereich Sicherheit und Technologie vornehmen müssen. Dies lässt sich in ein paar kurzen Faustregeln zusammenfassen:

1. *Explizite Verifizierung*: Alle Entitäten müssen explizit validiert, authentifiziert und autorisiert werden. Wird eine solche Prüfung nicht durchgeführt, muss die Standard-Zugriffsrichtlinie den Zugriff verweigern, und der Zugriff darf nicht über das festgelegte Maß an Vertrauen hinaus gewährt werden.
2. *Kompromittierung voraussetzen*[2]: Wenn Zeit, Ressourcen und Motivation vorhanden sind, wird ein Angreifer einen Weg finden, einen Vermögenswert innerhalb des Netzwerks und der Service-Enklaven eines Unternehmens zu kompromittieren. Der Zugang muss so gestaltet werden, dass diese Unvermeidlichkeit erwartet wird.
3. *Kontinuierliche Überwachung und Neubewertung*: Vertrauen ist kein statisches Attribut, sondern muss ständig überprüft werden, um festzustellen, ob oder wann eine Anlage, ein Benutzer oder ein Dienst abtrünnig geworden ist.

2 https://event.on24.com/wcc/r/3439803/3F9505FA8746F8EFAB24664BE96BC7EC.

## Prozess: Zugang, Vertrauen und risikobasierter Fortschritt

Der Weg zu Zero Trust führt nicht von heute auf morgen – und das ist auch gut so. Das Verständnis und die Verinnerlichung der Philosophie helfen dabei, die Erwartungen für den bevorstehenden Prozess festzulegen. In den meisten Fällen kann dies schrittweise über einen längeren Zeitraum hinweg geschehen, wobei sichergestellt wird, dass Zugang, Vertrauen und Risiko angemessen berücksichtigt werden. Ein guter Anfang ist die Erstellung eines nützlichen Inventars von Vermögenswerten, Ressourcen, Diensten und Daten mit Blick auf die folgenden Themen:

**Zugang:** Durch die Kombination von Remote-Mitarbeitern mit der Cloud-Infrastruktur und -Einführung müssen sich Unternehmen einen klaren Überblick darüber verschaffen, wer Zugang hat und benötigt. Braucht jeder Zugang zu allen Cloud-Anwendungen? Wie wird darauf zugegriffen? Wie greifen die Mitarbeiter auf das Unternehmensnetzwerk zu, und ist dieser Zugang definiert? Welcher Prozess wird die laufenden und sich entwickelnden Anforderungen in diesem Bereich verwalten? Das Verständnis dieser Fragen öffnet die Tür für eine effektive Verwaltung und Segmentierung.

**Vertrauen:** Dies mag in Anbetracht des vorliegenden Themas offensichtlich erscheinen, doch die Einrichtung eines effektiven Prozesses zur Authentifizierung, Autorisierung und kontinuierlichen Validierung von Benutzern ist nicht nur eine gute Praxis, sondern auch entscheidend für das Funktionieren einer Zero-Trust-Architektur. Und zwar in beide Richtungen: Welches Maß an Vertrauen ist für den Zugriff auf bestimmte Dienste und Daten erforderlich, und welches Maß an Vertrauen kann von den Entitäten, die authentifiziert und für den Zugriff autorisiert werden, vernünftigerweise aufgebaut werden?

**Risikobasierter Fortschritt:** Rom wurde nicht an einem Tag erbaut, und eine Zero-Trust-Architektur ist nicht so einfach wie das Umlegen eines Lichtschalters. Deshalb müssen Unternehmen einen internen Prozess entwickeln, um die Teile ihres Portfolios zu priorisieren, die am störanfälligsten sind, und sich auf die Maßnahmen konzentrieren, die das Risiko in diesen Bereichen maximal reduzieren. Dies ist eine fortlaufende, unvollkommene Aufgabe – das ist in Ordnung, denn es geht darum, schrittweise und in ausreichendem Tempo Fortschritte zu erzielen.

## Technologie: Kontrollen und kontinuierliche Überwachung

Nachdem Sie die Änderung der Philosophie verinnerlicht und die Bestandsaufnahme und Planung durchgeführt ha-

ben, ist es sinnvoll, sich mit der Technologie zu befassen. Grob gesagt, können die folgenden Kategorien nützlich sein:

**Mobilität und Vertrauen:** Welche technischen Kontrollen sind in der Lage, Vertrauen für eine mobile Belegschaft zu schaffen? Gerätemanagement und Multi-Faktor-Authentifizierung (MFA) sind häufig gewählte Tools zum Aufbau von Vertrauen, wobei cloudnative Endpunkterkennung und -reaktion (EDR) in der Lage sind, ein gewisses Maß an Sicherheit für eine Anlage zu bieten, unabhängig davon, in welchem Netzwerk sie auftaucht.

**Identitäts- und Netzwerkanalyse:** Wie können Sie feststellen, ob eine Identität kompromittiert wurde oder eine Anlage oder ein Dienst abtrünnig geworden ist? Network Detection and Response (NDR) und Cloud Detection and Response (CDR) Tools sind die Antwort auf diese Frage. Sie geben Netzwerkverteidigern die Sicherheit, Angreifer zu identifizieren, zu verfolgen und zu vertreiben, die von kompromittierten mobilen Ressourcen auf kritische Dienste und Infrastrukturen übergehen.

**Zugang und Segmentierung:** Herkömmliche VPNs können einen vollständigen Fernzugriff auf ein Netzwerk gewähren, während Zero-Trust-Network-Access(ZTNA)-Technologien einen sicheren Fernzugriff und Dienste auf der Grundlage definierter Zugriffskontrollrichtlinien bieten. Der Wechsel von einem VPN zu einer ZTNA-Lösung kann eine zusätzliche Schutzebene für Anwendungen und Dienste bieten, indem sie strikt auf diejenigen beschränkt werden, die einen direkten Zugriff benötigen. Darüber hinaus kann Zero Trust auch dabei helfen, eine Methodik für die Segmentierung einzurichten, indem die Frage beantwortet wird, „warum" und „wie" ein Unternehmen segmentieren sollte.

## Nach Hause bringen

Unabhängig davon, in welchem Stadium sich ihr Wissen oder ihre Erfahrung im Bereich Zero Trust befindet, haben die meisten Praktiker zu diesem Zeitpunkt eine Vorstellung davon, was es für ihre Organisation bedeuten könnte – und es ist eindeutig mehr als nur ein Marketingbegriff. Wie bei jeder neuen Philosophie kann das Verständnis des ganzheitlichen Charakters von großem Nutzen sein. Jede Organisation, die sich in Richtung Zero Trust[3] bewegt, wird ihre eigenen Überlegungen zu den beteiligten Personen, Prozessen und Technologien anstellen.

Eine übergreifende Sicht auf die einzelnen Bereiche wird auch in Zukunft von Nutzen sein. Je mehr Unternehmen die Cloud nutzen und je mehr sich die Mitarbeiter daran gewöhnen, aus der Ferne zu arbeiten, desto mehr kann Zero Trust für Angreifer ein erhebliches Hindernis darstellen. Wir haben zu viele Beispiele gesehen, in denen Bedrohungsakteure über gestohlene Anmeldeinformationen oder unter Umgehung von Sicherheitsvorkehrungen Zugang erlangt haben. Zu wissen, wer auf was Zugriff hat, und nur denjenigen den Zugang zu Diensten zu gestatten, die ihn benötigen, trägt wesentlich dazu bei, Unternehmen sicherer zu machen, während es für Angreifer schwerer wird.



3 https://content.vectra.ai/rs/748-MCE-447/images/SolutionOverview_ZeroTrust.pdf.