



Cyber-Sicherheitsrat
Deutschland e.V.

Werkzeugkasten Cybersicherheit



Zero Trust

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen, unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.

Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.



Hans-Wilhelm Dünn

Präsident

Cyber-Sicherheitsrat Deutschland e.V.

Zero Trust – Was ist das?

Im Kern bedeutet der Zero Trust-Ansatz, dass Unternehmen und Institutionen **keinem Nutzer oder Gerät automatisch vertrauen**, selbst wenn diese innerhalb der eigenen Netzwerkgrenzen agieren. Stattdessen werden Zugangs- und Zugriffsrechte nur auf Basis der **tatsächlichen Notwendigkeit** und nach **sorgfältiger Überprüfung** gewährt. Zero Trust bedeutet also, dass man grundsätzlich davon ausgeht, dass kein Teilnehmer oder Gerät im Netzwerk vollkommen vertrauenswürdig ist und daher jeder Zugriff überwacht, kontrolliert und begrenzt werden muss.



Welche Maßnahmen sind erforderlich?

Um einen Zero Trust-Ansatz zu implementieren, müssen Unternehmen und Institutionen verschiedene Maßnahmen ergreifen. Dazu zählt zunächst die **Identifizierung und Klassifizierung von Informationen und Ressourcen**, um ihre Sensibilität und den Schutzbedarf festzulegen. Anschließend gilt es, eine **granulare Zugriffskontrolle** auf Basis von Rollen und Berechtigungen einzuführen, um sicherzustellen, dass Nutzer und Geräte nur auf diejenigen Ressourcen zugreifen können, die sie tatsächlich im Rahmen ihrer Tätigkeit benötigen. Zugriffe von Geräten können über die Gerätenummer (MAC) gesteuert werden.

Ein weiterer wichtiger Schritt ist die Implementierung einer **Multi-Faktor-Authentifizierung (MFA)**, die die Sicherheit der Authentifizierung erhöht, indem sie die Kombination aus mehreren Verifizierungsmethoden erfordert, etwa Passwörtern, Biometrie oder Hardware-Tokens. Darüber hinaus sollte eine fortlaufende **Überwachung der Netzwerkaktivitäten** erfolgen, um Anomalien und potenzielle Sicherheitsbedrohungen frühzeitig zu erkennen. Hierbei können künstliche Intelligenz und maschinelles Lernen helfen, um den Umfang und die Effizienz der Analyse zu erhöhen. Die Umsetzung der Maßnahmen sollte in enger Zusammenarbeit zwischen IT-Abteilung, Führungskräften und Mitarbeitern erfolgen, um sicherzustellen, dass alle Beteiligten die Notwendigkeiten und die Vorgehensweise verstehen und unterstützen.


Welche Ansätze gibt es?

In der Welt des Zero Trust gibt es verschiedene Teilbereiche, die je nach Organisationsstruktur an Bedeutung gewinnen können und zu einem umfassenden Konzept gehören: Ein wichtiger Ansatz ist der **Zero Trust Network Access (ZTNA)**, der sich auf die Absicherung des Netzwerkzugriffs konzentriert. Dabei werden **Zugriffe auf Anwendungen und Daten kontrolliert und gesteuert**, indem Faktoren wie Nutzeridentität, Gerätezustand und Kontextinformationen berücksichtigt werden.

Ein weiterer Aspekt von Zero Trust ist die Sicherheit der Daten selbst. Der **Zero Trust Data-Ansatz** sorgt dafür, dass Daten geschützt sind, unabhängig von ihrem Speicherort oder ihrer Verwendung. Um dies zu erreichen, werden verschiedene Methoden wie **Verschlüsselung, Datenklassifizierung und Datenverlustprävention** eingesetzt, die gemeinsam einen umfassenden Schutz der wertvollen Informationen einer Organisation gewährleisten.

Schließlich spielt auch die Sicherheit der Geräte, die auf das Netzwerk zugreifen, eine entscheidende Rolle im Zero Trust-Konzept. Beim **Zero Trust Devices-Ansatz** liegt der Fokus darauf, die **Authentifizierung und Überwachung jedes einzelnen Geräts** sicherzustellen. Um dies zu erreichen, kommen beispielsweise Gerätezertifikate zum Einsatz, die einen sicheren Nachweis der Geräteidentität bieten. Regelmäßige Sicherheitsüberprüfungen und der Einsatz von **Endpoint Protection-Lösungen** stellen zudem sicher, dass die Geräte stets auf dem neuesten Stand der Sicherheitstechnik sind und potenzielle Bedrohungen frühzeitig erkannt werden können.

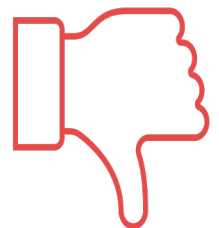
Welche Chancen gibt es?



Der Zero Trust-Ansatz bietet viele Vorteile für Unternehmen und Institutionen. Durch die kontinuierliche Überprüfung von Zugriffsrechten und die granulare Zugriffskontrolle kann das Risiko von Sicherheitsverstößen und **Datenlecks reduziert** werden. Zudem ermöglicht Zero Trust eine **bessere Anpassungsfähigkeit** an sich ändernde Bedrohungslandschaften und neue Technologien. Darüber hinaus kann die Einführung von Zero Trust dazu beitragen, das **Bewusstsein für Cybersicherheit in der Organisation** insgesamt zu erhöhen und die Zusammenarbeit zwischen verschiedenen Abteilungen zu verbessern.

Welche Risiken gibt es?

Trotz der vielen Vorteile gibt es auch einige Risiken und Nachteile, die bei der Einführung eines Zero Trust-Ansatzes berücksichtigt werden müssen. Zum einen kann die Umsetzung von Zero Trust mit hohen Kosten und einem **hohen Ressourcenaufwand** verbunden sein, insbesondere in der Anfangsphase. Des Weiteren kann es zu einer erhöhten **Komplexität der IT-Infrastruktur** und Verwaltung kommen, was wiederum das Potenzial für **menschliche Fehler** und Missverständnisse erhöht. In manchen Fällen kann die Einführung von Zero Trust auch zu einer **Beeinträchtigung der Benutzerfreundlichkeit und Produktivität** führen, wenn die Zugriffskontrollen zu restriktiv oder umständlich sind.



Wem nutzt Zero Trust?

Die Einführung des Zero Trust-Ansatzes betrifft verschiedene Zielgruppen innerhalb von Unternehmen und Institutionen, da er einen ganzheitlichen Ansatz für Cybersicherheit darstellt. Zunächst sind **IT-Abteilungen zuständig für Planung, Implementierung und Wartung** der Sicherheitsmaßnahmen, die im Rahmen von Zero Trust ergriffen werden. Sie stellen sicher, dass die zugrundeliegende Infrastruktur und Systeme sicher und aktuell sind.

Führungskräfte haben eine entscheidende Rolle in der Umsetzung des Zero Trust-Ansatzes, da sie **strategische Entscheidungen** treffen und die Implementierung der Maßnahmen unterstützen müssen. Sie sind dafür verantwortlich, die Vision und die Ziele des Zero Trust-Konzepts im Unternehmen oder der Institution zu verankern und Ressourcen für dessen Umsetzung bereitzustellen.

Mitarbeiter sind ebenfalls direkt von den Zero Trust-Maßnahmen betroffen. Sie müssen sich an die neuen Sicherheitsrichtlinien anpassen und **aktiv dazu beitragen, ein sicheres Arbeitsumfeld aufrechtzuerhalten**. Ihre Sensibilisierung und Schulung sind wichtige Faktoren für den Erfolg von Zero Trust.

Drittanbieter und Geschäftspartner spielen auch eine wichtige Rolle im Zero Trust-Ökosystem. Sie sollten sich ebenfalls an die Zero Trust-Prinzipien halten und angemessene Sicherheitsmaßnahmen ergreifen, um eine durchgehende **Sicherheit entlang der Lieferkette** zu gewährleisten. Dies fördert das Vertrauen und die Zusammenarbeit zwischen Unternehmen und ihren Partnern. Schließlich profitieren **Kunden** von der erhöhten Sicherheit, die der Zero Trust-Ansatz bietet. Ihre Daten und Interaktionen sind besser geschützt, und sie können möglicherweise ein **höheres Vertrauen** in Unternehmen und Institutionen entwickeln, die diesen Ansatz konsequent verfolgen. In der heutigen digitalen Welt ist das Vertrauen in die Sicherheit der eigenen Daten für viele Kunden ein entscheidender Faktor bei der Wahl ihrer Geschäftspartner.

Fazit

Der Zero Trust-Ansatz bietet eine umfassende und flexible **Grundlage** für die Verbesserung der Cybersicherheit in Unternehmen und Institutionen. Durch den konsequenten **Fokus auf Zugriffskontrolle, Überwachung und Anpassungsfähigkeit** trägt er dazu bei, das Risiko von Sicherheitsverstößen und Datenlecks zu reduzieren.

Allerdings ist die Einführung von Zero Trust **kein Selbstläufer** und erfordert eine sorgfältige Planung, Umsetzung und kontinuierliche Überprüfung. Dabei sind die Zusammenarbeit und das **Engagement aller Beteiligten**, von IT-Abteilungen über Führungskräfte bis hin zu Mitarbeitern, unerlässlich. Unternehmen und Institutionen, die bereit sind, in den Zero Trust-Ansatz zu investieren und die damit verbundenen Herausforderungen zu meistern, können jedoch von den zahlreichen Vorteilen profitieren und sich so gegen die wachsenden Cyber Risiken der heutigen digitalen Welt wappnen.

