# Vertrauen ist gut, kein Vertrauen ist besser?!

## Entwicklung und Implementierungen von „Zero Trust"

**Zero-Trust-Modelle verabschieden sich von der klassischen Unterscheidung vertrauenswürdiger Netze, Geräte oder Benutzer und hinterfragen mehr oder minder jeden einzelnen Zugriff. Unser Autor erläutert, in welchen Systemen und Lösungen dieser Ansatz heute zu finden ist.**

*Von Stefan Strobel, Heilbronn*

Vertrauen ist eine wichtige Grundlage für die Zusammenarbeit in Unternehmen und auch in der Informationssicherheit ist man es gewohnt, Personen, Systemen, Daten oder Netzwerken zu vertrauen. Beim aktuellen Trend „Zero Trust" soll es aber zumindest kein implizites Vertrauen mehr geben. Um diese Tendenz einordnen zu können, lohnt es, sich die Entwicklungen der letzten Jahre oder sogar Jahrzehnte vor Augen zu führen.

Vor nicht allzu langer Zeit war es üblich, dass eine Internet-Firewall das „gefährliche" Internet vom „vertrauenswürdigen" internen Netz einer Organisation trennt. Im internen Netz waren alle Server und Arbeitsplätze miteinander verbunden, ohne dass die Kommunikation in jedem Fall authentifiziert oder verschlüsselt wurde. Zahlreiche Serverdienste waren für alle Mitarbeiter frei verfügbar. Mitarbeiter, die sich einmal angemeldet hatten, konnten auf alle für sie freigegebenen Ressourcen zugreifen, ohne dass dies bei jedem Zugriff infrage gestellt wurde.

Für manche Organisationen mag dies immer noch so gelten – für viele hat sich aber einiges geändert: Einzelne Dienste, zum Beispiel der E-Mail-Service, werden inzwischen immer häufiger von einem Dienstleister oder Cloudprovider bereitgestellt. Ganze Server sind aus dem eigenen Rechenzentrum in Cloudstrukturen umgezogen und befinden sich damit nicht mehr im eigenen Netzwerk. Aber auch die Arbeitsplätze sind oft nicht mehr im Firmennetz: Schon vor Covid19 war mobiles Arbeiten ein starker Trend, aber seit der Pandemie ist Arbeiten aus dem Homeoffice in vielen Bereichen die Regel geworden. Wenn dabei immer noch ein vom Unternehmen verwaltetes „vertrauenswürdiges" Notebook verwendet wird, ist „nur" das Heim-Netz nicht vertrauenswürdig. Wenn die Heimarbeit aber sogar auf dem privaten PC eines Mitarbeiters erfolgt, dann fällt auch das vertrauenswürdige Gerät weg.

Man muss sich letztlich fragen, welche Teil der IT sich überhaupt noch „innerhalb" einer Organisation befinden und wo eigentlich der Perimeter, also die bisher so wichtige Grenze zwischen dem vertrauenswürdigen Netz und dem Rest der Welt, verläuft.

Selbst das Vertrauen in die Identität der Mitarbeiter schwindet im Kontext moderner Cloud-Strukturen: Immer häufiger werden Azure-AD-Konten, Apple-IDs oder Google-Accounts von Angreifern übernommen. Microsoft selbst sprach 2019 schon von täglich 300 Millionen illegalen Login-Versuchen auf ihre Services. Ein Hersteller von Erkennungslösungen veröffentlichte 2021 eine Studie, wonach bei 71 % aller Office-365-Kunden nicht nur einmal ein Account übernommen wurde, sondern im Durchschnitt siebenmal im vergangenen Jahr (www.mspalert.com/cybersecurity-research/office-365-account-takeovers-surge-research-finds/). Die IT-Welt hat sich also geändert und die klassische Perimeter-Sicherheit reicht schon eine Weile nicht mehr aus.

### Anfänge von Zero Trust

Die Zero-Trust-Idee an sich ist auch gar nicht so neu. 2003 haben David Lacey von Royal Mail und andere CISOs das Jericho Forum gegründet. Sie waren schon damals davon überzeugt, dass es nicht auf Dauer funktionieren kann, sich hinter einer Internet-Firewall zu verstecken und darauf zu hoffen, dass im internen Netzwerk keine


 

Gefahren lauern. Im Jericho Forum wollten sie daher die Abschaffung der Perimeter vorantreiben und alternative Sicherheitsansätze diskutieren.

Diese Gemeinschaft war ihrer Zeit offenbar voraus und erst als John Kindervag von Forrester 2009 den Begriff „Zero Trust" geprägt hat, bekam das Thema weiteren Auftrieb: Seiner Ansicht nach konnte das perimeterbasierte Sicherheitsmodell nicht funktionieren, da Angriffe schließlich auch aus dem internen Netz kommen. Vermutlich in jeder größeren Firma gibt es verärgerte Mitarbeiter, Accounts, die von externen Angreifern kompromittiert wurden, oder Geschäftspartner mit Zugang zum internen Netz. Kindervag forderte, dass jeder Zugriff auf Ressourcen unabhängig von seiner Herkunft gesichert erfolgen muss, Rechte minimiert, strenge Zugriffskontrollen durchgeführt und jegliche Netzwerkkommunikation überwacht werden soll.

2014 veröffentlichte Google sein BeyondCorp-Konzept mit ähnlichen Ideen [1]. Eine zentrale Rolle spielen dabei ein Proxy beziehungsweise Sicherheits-Gateways: Dort erlauben oder verbieten Policies den Zugriff auf interne Applikationen nicht mehr anhand des Netzwerks, aus dem ein Zugriff erfolgt, sondern anhand von Informationen über das zugreifende Gerät, seinen Status und den zugehörigen Benutzer. Das interne Netzwerk ist dabei genauso wenig „trusted" wie externe Netzwerke.

2018 veröffentlichte Forrester ein neues Zero-Trust-Modell mit dem Namen „Zero Trust eXtended", in dem verschiedenste Lösungen von Herstellern einsortiert werden können, die einzelne oder mehrere Aspekte von Zero Trust unterstützen. Ein solches Modell passt natürlich gut zum Geschäftsmodell der Analysten, die ja davon leben, möglichst viele Hersteller in Analysen und Berichten zu positionieren.

Den letztlichen Ritterschlag hat der Begriff 2020 bekommen, als die US-amerikanische Standardisierungsbehörde NIST ihr Paper SP 800-207 zu Zero Trust veröffentlicht hat [2]. Darin definiert NIST die Begriffe „Zero Trust" und „Zero-Trust-Architektur" und beschreibt, wie eine Organisation ihre Sicherheit damit verbessern kann. Im Februar 2021 hat auch die NSA eine Empfehlung für Zero Trust veröffentlicht [3] und die Vorteile einer solchen Architektur zum Schutz interner Daten angepriesen.

## Heutige Sicht

„Zero Trust" ist kein Produkt, das man kaufen und in kurzer Zeit einführen kann. Vielmehr ist es eine Menge von Konzepten zum Schutz von Daten, Diensten oder allgemein Ressourcen, bei denen es kein implizites Vertrauen mehr gibt – weder in ein internes Netz noch in Firmengeräte oder Benutzer. Stattdessen wird für jeden einzelnen Zugriff erneut überprüft, ob er zulässig ist – alle Aktivitäten werden überwacht und fließen ebenso in diese Entscheidung ein wie die Benutzeridentität oder der Sicherheitsstatus des Geräts, von dem aus der Zugriff erfolgen soll.

Bei Zero Trust gelten die Grundsätze „Never trust, always verify!" und „Assume breach!". Man geht also davon aus, dass das interne Netzwerk bereits kompromittiert ist und versucht durch möglichst feingranulare Zugriffskontrolle Missbrauch oder Datenabfluss zu verhindern.

## Systematik von Lösungen

Am Markt findet man derzeit hauptsächlich vier Kategorien von Produkten, die mit Zero Trust assoziiert werden:

- Lösungen mit Fokus auf dynamische, risikobasierte Authentifizierung
- Mikrosegmentierungsprodukte
- Zero-Trust-Network-Access (ZTNA)
- Lösungen zur Erkennung von Kompromittierungen, vor allem Endpoint-Detection and -Response (EDR) und dessen Erweiterung Extended Detection and Response (XDR)

### Dynamische und risikobasierte Authentifizierung

Dynamische und risikobasierte Authentifizierung ist eine natürliche Weiterentwicklung der Techniken im Bereich der starken Authentifizierung. Begonnen hat dieser Markt mit Lösungen für Zwei-Faktor-Authentifizierung (2FA) – meist waren das kleine Token beziehungsweise Geräte, deren Besitz der Anwender für die Authentifizierung beweisen musste, zusammen mit einem Server, der das Ganze verwaltet. Über die Jahre kamen dazu andere Formfaktoren mit USB-Steckern, Funk-Kommunikation oder andere Verfahren, bei denen man einen Freigabecode per SMS an Telefone schickt oder die Freigabe über eine Smartphone-App erteilt wird.

Um die Art der Authentifizierung nicht für jede Anwendung gleich aufwendig und sicher (oder aber unsicher) festlegen zu müssen, kamen danach dynamische Systeme auf den Markt, bei denen ein gemeinsames Verwaltungssystem die Art der Authentifizierung von den Sicherheitsanforderungen der Ziel-Applikation abhängig gemacht hat. Für manche Zugriffe reichte ein Passwort aus, für andere Zugriffe wurde zusätzlich noch der Besitz eines Tokens gefordert.

Diese Idee hat sich weiterentwickelt, sodass auch die Quelle des Zugriffs und der Sicherheitsstatus des Geräts, von dem aus der Zugriff erfolgen soll, mit in die Authen-

tifizierungs-Entscheidung einfließen. Gleichzeitig wird das Login-Verhalten überwacht und analysiert, sodass ein kompromittierter Account beispielsweise erkannt werden kann, weil „derselbe Mitarbeiter" sich innerhalb kurzer Zeit von geografisch weit entfernten Orten aus anmeldet. Für die Erkennung dieses sogenannten Impossible-Travel-Szenarios, musste man früher alle Anmelde-Events an ein SIEM schicken, das dann diese Zugriffe/Events über Geolocation-Datenbanken korrelieren konnte – moderne Authentifizierungssysteme haben solche und ähnliche Mechanismen allerdings bereits eingebaut.

### Mikrosegmentierung

Beim zweiten Zero-Trust-Segment handelt es sich, wie bereits erwähnt, um Lösungen für Mikrosegmentierung: Hier war Zero Trust nicht der Treiber für die Entwicklung der Produkte. Es hat sich aber gezeigt, dass solche Techniken gut zu dessen Paradigmen passen und die Hersteller haben den neuen Hype gerne aufgegriffen und vermarkten ihre Produkte nun entsprechend.

Bei der Mikrosegmentierung versucht man ein internes Netzwerk so fein wie möglich zu segmentieren und die Kommunikation mit Regeln zu begrenzen, um schon auf der Kommunikationsschicht einem Angreifer so wenig Zugriffsrechte wie möglich zu geben. Statt mit klassischen Netzwerk-Firewalls setzt man dabei jedoch eher auf vorhandene Komponenten: Entweder sind das vorhandene Router und Switches oder sogar die Endgeräte selbst, auf denen Endpoint-Firewalls (aka Desktop- oder Client-Firewalls) so konfiguriert werden, dass nur noch die tatsächlich benötigte Kommunikation erlaubt ist.

Diese Idee ist ebenfalls nicht neu, allerdings liegt die Problematik in der sinnvollen Erstellung von Firewall-Regeln und dem damit verbundenen Betriebsaufwand. Moderne Mikrosegmentierungslösungen verwenden hier künstliche Intelligenz (KI) und ein automatisiertes Einlernen der tatsächlich benötigten Kommunikation, die dem Administrator dann in einer aufbereiteten grafischen Darstellung als Grundlage angezeigt wird.

### Zero-Trust-Network-Access (ZTNA)

Dieser Bereich von Zero-Trust-Network-Access (ZTNA, vgl. [5]) wird vor allem als Alternative zu bisherigen Remote-Access-VPNs positioniert. Statt wie bei klassischen Virtual Private Networks (VPNs) nach einer erfolgreichen Authentifizierung den kompletten vorgesehenen Zugriff freizuschalten, wird hier jeder Applikationszugriff einzeln betrachtet, bei Bedarf stärker authentifiziert und über ein Gateway selektiv freigegeben. Das Gateway wird dabei ZTNA-Broker genannt und stellt die Zugriffe her. Bei vielen Anbietern wird der ZTNA-Broker als Cloud-Service vom Hersteller angeboten.

Bei den technischen Details gibt es auch hier verschiedene Varianten: Manche Hersteller benötigen einen weiteren Agenten, der dann verschiedene Protokolle über den Broker leiten kann sowie auch den lokalen Sicherheitsstatus des Endgeräts erfasst und an den Broker übermittelt. Andere Hersteller verzichten auf Agenten und beschränken sich dann typischerweise auf Applikationen, die auf dem Endgerät in einem Browser dargestellt werden können.

Der ZTNA-Broker greift bei manchen Herstellern direkt auf die eigentlichen Server beziehungsweise Dienste zu. Andere Hersteller setzen noch ein weiteres Gateway in der Infrastruktur des Kunden ein, das dann die Vermittlung zwischen dem Broker und den eigentlichen Applikationen herstellt und seinerseits eine ausgehende Verbindung zum Broker aufbaut. Dadurch wird zusätzlich verhindert, dass Dienste nach außen für Unbefugte überhaupt sichtbar werden: Erst wenn der ZTNA-Broker in der Cloud einen legitimen Zugriff erkennt, wird die Applikation für den authentifizierten Anwender sichtbar.

Dadurch, dass ein ZTNA-Broker bevorzugt als Cloud-Dienst angeboten wird, passt er gut zu Anbietern anderer Cloud-Sicherheits-Gateways wie externen Web-Proxies oder Mail-Gateways. Perspektivisch bündeln die Anbieter das dann und nennen es *„Secure Access Service Edge" (SASE)* (vgl. [6]). Dieses neue Buzzword steht für einen kompletten Perimeter in der Cloud – inklusive WAN-Vernetzung für die Standorte des Kunden, die ihrerseits nur noch ein VPN zum nächstgelegenen Rechenzentrum des SASE-Anbieters aufbauen.

### Endpoint-Detection and -Response (EDR) / Extended Detection and Response (XDR)

Die kontinuierliche Überwachung aller Aktivitäten zur dynamischen Bewertung des Risikos spielt eine wichtige Rolle bei Zero Trust. So ist es nicht verwunderlich, dass sich auch die Anbieter von EDR/XDR in diesem Kontext positionieren und Partnerschaften mit den Anbietern von Mikrosegmentierung oder ZTNA-Lösungen eingehen. EDR-Lösungen überwachen alle technischen Aktivitäten der Prozesse auf Endgeräten, korrelieren sie und versuchen mit modernen Machine-Learning-Verfahren bösartiges Verhalten zu erkennen.

Die Anbieter von EDR-Lösungen waren – wie so oft in der Security-Branche – zunächst kleine Start-ups, die dynamisch und innovativ neue technische Ideen implementiert haben und teilweise von größeren Anbietern aufgekauft wurden. Oft haben diese im nächsten Schritt versucht, die zugekaufte EDR-Lösung mit bestehenden Produkten zu integrieren, sodass beispielsweise ein Alarm aus einer bestehenden Netzwerk-Anomalie-Erkennung automatisch von der EDR-Lösung verifiziert wird. Neben

dem Endgerät bieten sich dabei ein Netzwerk-Sensor oder auch Sensoren für Aktivitäten in Cloud-Umgebungen und Containern an. Um die eigenen, derart integrierten Produkte von denen der Marktbegleiter abzugrenzen, entstand dabei die Bezeichnung „Extended Detection and Response" (XDR) – es handelt sich also um eine nahe liegende Weiterentwicklung von EDR.

Bisher gibt es fast keine Lösungen, die XDR über die Produkte verschiedener anderer Hersteller ermöglichen – vielmehr geht es eigentlich immer um die Integration der Lösungen eines einzelnen Herstellers. Das ist durchaus verständlich, denn die nötige Integration ist weitaus komplexer als nur das Zusammenfassen einzelner Events: Um wirklichen Mehrwert zu erzeugen, müssen die Einzelteile einer XDR-Lösung eng verzahnt sein, Informationen mit Kontext austauschen und aktiv zusammenarbeiten.

XDR übernimmt – ebenso wie moderne Authentifizierungssysteme mit eingebauter risikobasierter Bewertung des Login-Verhaltens – die Erkennungsfunktionen, die früher in einem Security-Information- and -Event-Management (SIEM) angesiedelt waren. Das SIEM wird dabei mehr und mehr zu einer zentralen Konsole, während die Erkennungsintelligenz in spezialisierten Lösungen liegt, die näher am Geschehen sind, mehr Kontext-Informationen haben und dadurch eine bessere Erkennungsqualität liefern können als ein klassisches SIEM, das Events ohne Kontextdaten korrelieren musste, um daraus erst einen Kontext zu rekonstruieren.

Die zentrale Intelligenz und Verwaltung einer XDR-Lösung ist fast immer in der Cloud des Herstellers angesiedelt. Dies unterstreicht die Intention, den erforderlichen Aufwand weitgehend beim Anbieter zu belassen und den Betrieb von XDR für den Kunden so einfach wie möglich zu machen.

XDR als „Out-of-the-box"-Lösung aus der Hand eines einzelnen Herstellers, bei der die verschiedenen Sensoren aufeinander abgestimmt sind und automatisch zusammenarbeiten, ist auf der einen Seite eine interessante Perspektive. Auf der anderen Seite macht man sich durch die Einführung einer solchen Lösung stark von einem einzelnen Anbieter abhängig. Das mag noch harmlos sein, wenn XDR nur aus einer Endpoint-Software und zusätzlichen Netzwerk-Sensoren besteht. Wenn aber XDR voraussetzt, dass auch die Firewall sowie das Web- und E-Mail-Gateway vom gleichen Hersteller kommen oder sogar das Betriebssystem der Endgeräte, dann ergibt sich eine Abhängigkeit und Monokultur, die man durchaus kritisch bewerten kann.

## Fazit

„Zero Trust" ist kein Produkt, das man einfach so kaufen und einführen kann – auch wenn viele Hersteller damit werben. Vielmehr steht Zero Trust für eine Menge von Ideen beziehungsweise Paradigmen, die von der klassischen netzwerk- und perimeterbasierten Sicherheit abweichen.

Viele dieser Ideen sind offensichtlich sinnvolle Weiterentwicklungen bisheriger Techniken und erfordern somit keine radikale Erneuerung der Sicherheitsinfrastruktur in Organisationen: Man kann sich in mehreren Bereichen schrittweise in Richtung Zero Trust weiterentwickeln – egal ob man mit EDR für die bessere Erkennung von Kompromittierungen, mit einer dynamischen risikobasierten Authentifizierung oder mit einer stärkeren Segmentierung oder sogar Mikrosegmentierung beginnt. ■

*Stefan Strobel ist Geschäftsführer der cirosec GmbH.*

## Literatur

[1] Rory Ward, Betsy Beyer, BeyondCorp – A New Approach to Enterprise Security, ;login: Vol. 39 No. 6, S. 6, Dezember 2014, https://www.usenix.org/publications/login/dec14/ward

[2] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, Zero Trust Architecture, National Institute of Standards and Technology (NIST) Special Publication 800-207, https://doi.org/10.6028/NIST.SP.800-207 https://csrc.nist.gov/publications/detail/sp/800-207/final

[3] National Security Agency (NSA), Embracing a Zero Trust Security Model, Februar 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[4] Evren Eren, Der Weg zum Zero-Trust-Networking, <kes> 2020#6, S. 52 und <kes> 2021#1, S. 50

[5] Laurence Pitt, Am Rand kommt alles zusammen, Wie Netzwerkmanagement und Security mit SASE in der Cloud zusammenwachsen, <kes> 2020#6, S. 60