Stefan Strobel

Zero Trust

Technische Möglichkeiten und Grenzen

„Buzzwords" sind aus der IT-Sicherheit nicht wegzudenken. So wie seit einiger Zeit jeder von künstlicher Intelligenz spricht und auf einmal überraschend viele Hersteller die vermeintlichen KI-Techniken in ihren Produkten bewerben, sieht man dies auch mit Begriffen wie „Extended Detection and Response (XDR)" und eben „Zero Trust".

Kaum ein großer Hersteller von Sicherheitsprodukten wirbt nicht damit, dass sein Produkt Zero Trust umsetzt, was auch immer im Einzelfall dahintersteckt.

Dabei sind die Ideen hinter Zero Trust alles andere als neu. Sie gehen teilweise auf das Jericho Forum[1] zurück, das 2003 von David Lacey und anderen CISO großer Organisationen ins Leben gerufen wurde. Die Idee damals war, dass man sich nicht auf ein schützendes Netzwerk-Perimeter verlassen sollte, sondern für die Zukunft andere Sicherheitskonzepte benötigt.

Auch der Begriff Zero Trust selbst wurde schon im Jahr 2009 durch John Kindervag bei Forrester[2] geprägt, aber erst seit im Jahr 2020 die amerikanische Standardisierungsbehörde NIST einen „Leitfaden"[3] zu Zero Trust veröffentlicht hat, begann der Siegeszug dieses neuen Schlagworts.

1 Grundidee von Zero Trust

Im Kern geht es bei Zero Trust darum, das implizite Vertrauen in ein sicheres internes Netzwerk, ein sicheres Endgerät oder einen sicheren Account abzuschaffen und stattdessen davon auszugehen, dass alles schon kompromittiert sein könnte. „*Assume breach.*" wird dabei oft als ein Grundprinzip zitiert, meist ergänzt wird „*Always verify.*" oder auch „*Use least privilege access.*"[4].

Die vielen öffentlich diskutierten Sicherheitsvorfälle der letzten Jahre untermauern den Sinn einer solchen Betrachtungsweise. Insbesondere Angriffe über die Lieferkette wie am Beispiel der sogenannten Sunburst-Angriffe[5] über kompromittierte Updates der Produkte von der Softwarefirma Solarwinds zeigen, dass man sich auch mit umfassenden Sicherheitsmaßnahmen kaum davor schützen kann, Opfer eines Angriffs zu werden.

Daraus ergeben sich für Unternehmen bspw. die folgenden Herausforderungen:

- Eingekaufte Softwareprodukte könnten bereits Schadcode enthalten, der mit bisherigen Malwareschutzmaßnahmen nicht entdeckt werden kann.
- Die Wartungszugänge für externe Dienstleister könnten für Angriffe missbraucht werden, wenn der Dienstleister unbemerkt unterwandert wurde.
- Selbst entwickelte Software könnte Bibliotheken einbetten, die zwar als sicher und vertrauenswürdig gelten, aber längst Hintertüren enthalten.

Es bleibt den Unternehmen daher nichts anderes übrig, als sich von der Idee eines sicheren und vertrauenswürdigen internen Netzwerks, eines vertrauenswürdigen Geräts oder Accounts zu verabschieden.

2 Grundlegende Anforderungen

In der Konsequenz werden Sicherheitsmechanismen gefordert, die für jeden Zugriff auf eine Ressource den Kontext und das Risiko neu bewerten, um dann zu entscheiden, ob der Zugriff erlaubt wird oder nicht. Ressourcen sind dabei keine Netzwerksegmente, sondern individuelle Geräte, Applikationen oder Daten. Es wird eine feingranulare Zugriffskontrolle auf allen Ebenen angestrebt.

1 Weitere Infos zum Jericho Forum, das mittlerweile in der Open Group aufgegangen ist bspw. unter https://blog.opengroup.org/tag/jericho-forum/ (zuletzt abgerufen am 30. Juni 2023).

2 Einen historischen Rückblick zu Zero Trust findet man bspw. online unter https://www.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/ (zuletzt abgerufen am 30. Juni 2023).

3 Die NIST SP-800-207 „Zero Trust Architecture" ist online verfügbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (zuletzt abgerufen am 30. Juni 2023).

4 So bspw. Microsoft im Artikel „What is Zero Trust?", online verfügbar unter https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview (zuletzt abgerufen am 30. Juni 2023).

5 Umfassende Informationen zu diesem Angriff finden sich bspw. im Blogeintrag „New sophisticated email-based attack from NOBELIUM", online verfügbar unter https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/ (zuletzt abgerufen am 30. Juni 2023).

Stefan Strobel

ist Geschäftsführer der cirosec GmbH. Er verfügt über langjährige Erfahrungen in der Beratung großer Firmen mit sehr hohem Sicherheitsbedarf und in der Erstellung von Konzepten und Policies. Neben seiner Tätigkeit hält er regelmäßig Vorträge an Hochschulen und auf Sicherheitskonferenzen und ist Autor verschiedener Fachbücher, die in mehreren Sprachen erschienen sind.
E-Mail: stefan.strobel@cirosec.de

Für die Bewertung des Kontexts und des Risikos wird eine deutlich bessere Sichtbarkeit auf die Vorgänge und das Verhalten nötig. Das gilt sowohl im Kontext von Benutzeraccounts, Endgeräten, aber auch im Netzwerk und in Applikationen. Gerade, wenn man davon ausgeht, dass alles bereits kompromittiert sein könnte, ist es essenziell, Einbrüche oder Anomalien frühzeitig zu erkennen und dies bei allen Zugriffsentscheidungen zu berücksichtigen.

Ebenso naheliegend ist es, auch im internen Netz alle Datenübertragungen zu verschlüsseln. Wenn heute Daten über das öffentliche Internet übertragen werden, dann ist es fast selbstverständlich, dass dabei TLS-Verschlüsselung verwendet wird oder die Daten über einen verschlüsselten VPN-Tunnel übertragen werden. Im internen Netzwerk unterstützen zwar die meisten modernen Softwareprodukte eine Übertragung mit TLS-Verschlüsselung, in der Regel ist dafür jedoch eine Verteilung beziehungsweise Konfiguration von Zertifikaten nötig. Genau das findet oft nicht statt.

Zero Trust ist also nichts, was man einfach kaufen kann, sondern eine Menge von Paradigmen, die man bei der Erstellung oder Weiterentwicklung von Konzepten und Architekturen sowie bei der konkreten Konfiguration berücksichtigt. Entsprechend gibt es auch viele Bereiche und Ebenen, in denen Zero-Trust-Ideen einfließen können.

3 „Produkte" zur Umsetzung von Zero Trust

Die Produkte, die in der Praxis am häufigsten im Kontext Zero Trust zum Einsatz kommen, sind meist auch keine Neuentwicklungen, die zur Umsetzung von Zero Trust entwickelt wurden, sondern eher naheliegende Weiterentwicklungen in ihrem jeweiligen Bereich.

3.1 Absicherung des Netzwerks

Die Idee, interne Netzwerke insbesondere durch eine sinnvolle Segmentierung stärker abzusichern, ist so alt wie die Einführung interner IP-Netze. Auch die Idee, dies durch kleinste Mikro-Segmente umzusetzen, in denen im Extremfall nur je ein Endgerät angeschlossen ist, ist schon mindestens seit zehn Jahren ein Thema.

Anbieter, die damals begonnen haben, sich auf Mikrosegmentierung zu spezialisieren, haben diesen Ansatz nicht als Technik für Zero Trust, sondern als Weiterentwicklung von Segmentierungstechniken positioniert. Aus heutiger Sicht positionieren die Analysten genau diese Hersteller und Produkte als Marktführer für Zero Trust, wenngleich sie nur einen kleinen Anwendungsbereich der Zero-Trust-Ideen abdecken.

Ein Angreifer, der die Kontrolle über ein Endgerät oder einen Server übernehmen konnte, kann bei einer optimal konfigurierten Mikrosegmentierung nur noch die anderen Systeme und Services erreichen, die im Normalbetrieb von dem Ausgangssystem auch erreichbar sein müssen.

Mikrosegmentierung ist damit auf Netzwerkebene das Gegenteil eines offenen und flachen Netzwerks und passt so sehr gut zu der Idee, von einem als generell vertrauenswürdig eingestuften internen Netzwerk wegzukommen und von einer bereits erfolgten Kompromittierung auszugehen. Allerdings haben Produkte für Mikrosegmentierung in der Regel keinen Einblick in die tatsächlichen Vorgänge auf den Endgeräten, den Sicherheitsstatus der Endgeräte oder das Verhalten der Anwender innerhalb von Applikationen.

3.2 Absicherung der Endgeräte

Auf den Endgeräten liegt die Stärke eines anderen Produktbereichs, der sogenannten Endpoint Detection and Response (EDR) -Lösungen. Im Kern von EDR stehen Softwareagenten auf den Endgeräten, die das technische Verhalten jedes Programms bzw. Prozesses überwachen und mit Kontext an eine zentrale Managementstation übermitteln, die dann anhand des Gesamtbildes das Verhalten bewerten und darauf reagieren kann.

So wird bspw. ein Programm, das über einen Webbrowser heruntergeladen wurde und danach von sich aus Code aus Russland nachlädt, welcher danach sicherheitsrelevante Einstellungen in der Registry ändert, i. d. R. zu einem Alarm führen. Die EDR-Management-Komponente würde das Verhalten im Gesamtbild grafisch darstellen und den Sicherheitsexperten damit auf „intuitive" Art und Weise erlauben, Alarme zu verifizieren oder geeignete Reaktionen zu starten.

Auch EDR-Lösungen wurden nicht für Zero Trust entwickelt und werden auch heute nicht immer in diesem Kontext positioniert. Sie sind vielmehr als natürliche Weiterentwicklung von Sicherheitsmechanismen auf Endgeräten entstanden. Aber auch sie passen gut zu den Grundideen und Zielen von Zero Trust – der kontinuierlichen Überwachung und Erkennung möglicherweise gefährlicher Aktivitäten. EDR-Produkte sind ein deutlicher Fortschritt bezogen auf die Sicherheit und insbesondere die Erkennung von Kompromittierungen auf einem Arbeitsplatz-PC. Die Vorgänge innerhalb von Applikationen, oder auch nur das Anmeldeverhalte von Benutzern sind aber wiederum ganz andere Themen.

3.3 Auswertung des Nutzerverhaltens

Gerade dieses Anmeldeverhalten ist ein sehr wertvoller Indikator für den Missbrauch von Identitäten und in der Vergangenheit haben viele Unternehmen versucht, hier mit SIEM-Systemen und Korrelation der Authentisierungs-Logs zu erkennen, ob ein Angreifer versucht, das Passwort eines Kontos zu erraten oder ob er erfolgreich ein Konto übernommen hat und dieses nun von einer ungewöhnlichen Quelladresse beziehungsweise aus einem ungewöhnlichen Land zu verwenden.

Wenn ein Mitarbeiter sich gerade eben aus München an einer Unternehmensfirewall angemeldet hat und derselbe Mitarbeiter fünf Minuten später versucht sich aus Singapur anzumelden, dann ist offensichtlich, dass dies nicht sein kann.[6] Eine Reise von München nach Singapur dauert länger und entsprechend spricht man von einem „*impossible travel*".[7] Vermutlich wurden die Zugangsdaten dieses Mitarbeiters gestohlen und nun versucht ein Angreifer diese zu missbrauchen.

6 Von besonderen Situationen wie bspw. der absichtlichen, intensiven Verwendung von sich ändernden VPN-Verbindungen mit weltweit unterschiedlichen Exit-Servern sehen wir hier aus Vereinfachungsgründen ab.

7 Zu weiteren Erläuterungen siehe bspw. den Blogeintrag „Detecting and Remediating Impossible Travel", online verfügbar unter https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/detecting-and-remediating-impossible-travel/ba-p/3366017 (zuletzt abgerufen am 30. Juni 2023).

Moderne Authentisierungssysteme vieler Hersteller enthalten bereits die entsprechende Erkennungslogik. SIEM-Systeme sind für diesen Anwendungsfall nicht mehr notwendig. Man spricht dann von dynamischer und risikobasierter Authentisierung. Auch hier waren nicht die Ideen von Zero Trust der Treiber – vielmehr haben die Hersteller von Authentisierungssystemen einfach nur ihre Produkte konsequent weiterentwickelt.

3.4 Nutzung von „Zero Trust Network Access"

Auch beim Zugriff auf eine bestehende Applikation müsste der Zugriff nicht nur verschlüsselt erfolgen. Vielmehr müsste auch die Authentisierung mit einem der modernen Identity-Provider erfolgen, der auffälliges Anmeldeverhalten wie beispielsweise den oben beschriebenen „*impossible travel*" erkennt und die Anmeldung verhindert.

Ebenso müsste das Anmeldesystem den Sicherheitsstatus des IT-Systems, von dem der Zugriff erfolgt, in die Zugriffsentscheidung einbeziehen. Dafür wäre eine Integration mit dem dort verwendeten EDR-System wünschenswert. Solche Integrationen sind bisher jedoch eher selten zu finden. Etablierte Standards fehlen bisher und nur wenn einzelne Hersteller zusammenarbeiten, gibt es einzelne „Brücken", die aber keine vollständige Lösung darstellen.

Eine Produktkategorie versucht nun genau in diesem Umfeld zu punkten: die so genannten „Zero Trust Network Access (ZTNA)"-Produkte. Dabei handelt es sich um Gateways, über die der Zugriff auf alle Applikationen erfolgen soll. Das ZTNA-Produkt soll dabei den Anwender authentisieren, den Sicherheitsstatus des Endgeräts und den vollständigen Kontext berücksichtigen und so risikobasiert entscheiden, ob der Zugriff erfolgen darf. Da es in gewachsenen IT-Infrastrukturen kaum vermittelbar ist, alle Applikationszugriffe über neu anzuschaffende Gateways umzuleiten, vermarkten die Hersteller ihre Produkte oft als Ersatz für klassische VPN-Produkte, die Zugriffe aus dem Internet beziehungsweise aus dem Homeoffice sicherer ermöglichen sollen als dies bisher mit VPN-Gateways umgesetzt wurde.

Ein wesentliches Argument ist dabei, dass die Zugriffe nur applikationsbezogen freigeschaltet werden und nicht wie bei vielen VPN-Konfigurationen alle internen Systeme über den VPN-Tunnel erreichbar sind. Ein Mitarbeiter, der beispielsweise nur auf eine interne Web-Applikation und den Fileserver zugreifen darf, würde das ZTNA-Produkt als Gateway verwenden und bekäme dort die beiden Systeme meist über eine Web-Oberfläche angeboten. Andere interne Systeme wären für ihn nicht sichtbar. Für die Web-Applikation arbeitet das Gateway dann wie ein Reverse-Proxy.

Wirklich neu ist diese Idee nicht, denn auch SSL-VPN-Produkte vor 15 Jahren haben bereits diesen Ansatz verfolgt. Auch Konzepte auf Basis von Terminalservern, die je Benutzer nur die jeweils benötigten Applikationen anzeigen, erreichen ein ähnliches Ergebnis. Aus diesem Grund sollte man gut überlegen, ob man etablierte VPN-Lösungen tatsächlich ablösen möchte, denn auch ZTNA-Produkte sind allenfalls Puzzleteile, die ihrerseits mit anderen Teilen integriert werden müssen.

Für eine dynamische und risikobasierte Authentisierung muss beispielsweise ein entsprechendes Authentisierungssystem angebunden werden. Die ZTNA-Produkte selbst enthalten solche Funktionen in der Regel nicht.

Ebenso ist die Sichtbarkeit auf den Sicherheitsstatus des Endgeräts begrenzt. Einige ZTNA-Produkte bringen zwar einen Software-Agenten mit, den man auf den Endgeräten installieren kann und der dann Informationen über den Sicherheitszustand an das Gateway übermitteln soll, aber die Informationen, die von den heutigen Produkten abgefragt werden, sind doch recht oberflächlich und nicht mit den Details eines EDR-Produktes vergleichbar. Eine Schnittstelle zwischen dem ZTNA-System und einer EDR-Lösung wäre wünschenswert, in der Praxis haben jedoch allenfalls einzelne Produkte Schnittstellen zueinander. Oft sind darüber hinaus die Hersteller von ZTNA-Lösungen noch recht junge Startups und die Produkte entsprechend noch wenig ausgereift.

4 Der Weg ist das Ziel

Einzelne Puzzlestücke, die bei der Umsetzung von Zero Trust hilfreich sind, gibt es in vielen etablierten Bereichen. Für eine deutliche Verbesserung des Sicherheitsniveaus müssten diese Puzzlestücke aber ineinandergreifen und mit der bestehenden IT-Infrastruktur integriert werden.

4.1 Integration mittels SOAR

Manche Unternehmen versuchen die Integration der verschiedenen Puzzleteile selbst über Orchestrierungs- und Automatisierungs-Werkzeuge (sog. SOAR-Lösungen) umzusetzen. Diese werden vor allem in Security Operations Centern (SOC) als Ebene über einem Security Information and Event Management (SIEM) verwendet.

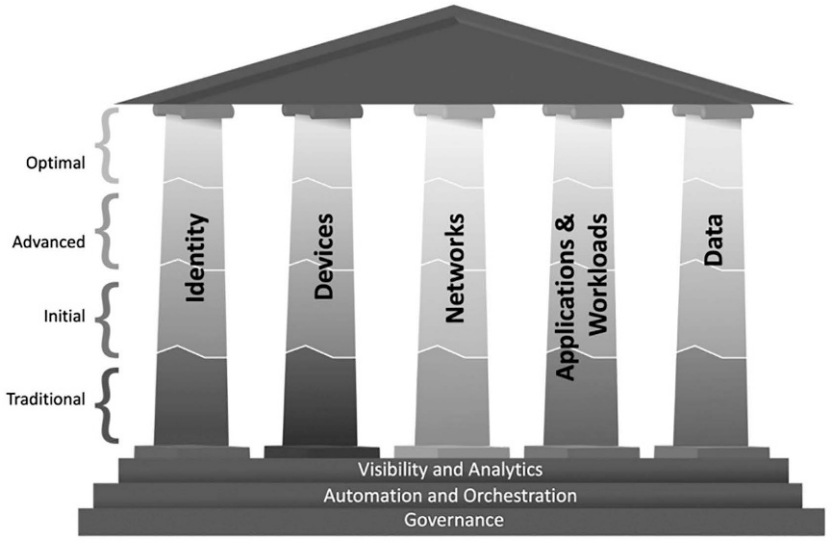
In den Projekten zur Einführung eines SOAR-Werkzeugs geht es meist vorrangig darum, Analysten im SOC zu entlasten und möglichst viele Routine-Tätigkeiten zu automatisieren. Neben der automatischen Anreicherung von Informationen zu gemeldeten Alarmen sind dabei auch automatische Reaktionen wie das Sperren von Accounts oder Zugriffsprivilegien als Folge einer erkannten Kompromittierung denkbar, wenngleich man hier auch mögliche Probleme und Seiteneffekte bedenken muss.

4.2 Praxisprobleme

Die Integration von verschiedenen Bausteinen einer Zero-Trust-Architektur über eine SOAR-Lösung mag zwar prinzipiell machbar sein, aber in der Praxis bedeutet dies doch, dass ein erheblicher Aufwand und viele individuelle Konfigurationen geschaffen werden. Die dadurch entstehende Komplexität ist der Sicherheit auch nicht unbedingt zuträglich.

Es ist realistisch betrachtet nicht möglich, die Ideen von Zero Trust in kurzer Zeit in allen Bereichen vollumfänglich umzusetzen. Eine vollständige Integration ist weit entfernt. Auch wird kaum eine Organisation ihre bisherige IT-Landschaft einfach über Bord werfen und auf Basis von Zero-Trust-Ideen neu aufbauen. Die einschlägigen Veröffentlichungen zu Zero Trust sind sich in diesem Punkt einig und sprechen von einer kontinuierlichen Weiterentwicklung und Verbesserung der bestehenden IT-Sicherheits-Architekturen in Richtung Zero Trust, bei der viele vorhandene Maßnahmen ihren Platz in einer Zero-Trust-Architektur haben können.

Abbildung 1: Die fünf Säulen des ZTMM der CISA[9]



4.3 Reifegradmodelle

Man kann sich dabei an mehreren Reifegradmodellen für Zero Trust orientieren. Meist definieren diese mehrere Säulen oder Kernbereiche wie Identitäten, Netzwerk, Endgeräte, Daten, Applikationen oder Workloads. Für jede Säule kann man dann die bestehenden Maßnahmen betrachten und einordnen, wie weit sie schon Zero Trust Ideen berücksichtigen.

Ein beliebtes Beispiel ist das „Zero Trust Maturity Model (ZTMM)" der amerikanischen „Cybersecurity and Infrastructure Security Agency (CISA)".[8]

Für die fünf Säulen „Identity", „Devices", „Networks", „Applications & Workloads" und „Data" werden dabei jeweils vier Ebenen beziehungsweise Reifegrade von „Traditional" über „Initial", „Advanced" bis „Optimal" unterschieden.

Beispielsweise würde ein flaches Netzwerk mit wenig Segmentierung im unteren Bereich (also als „Traditional") einsortiert, während eine feingranulare Mikrosegmentierung unter Berücksichtigung der Risikoprofile einzelner Applikationen im oberen Bereich landet.

5 Fazit

Zero Trust ist ein aktuelles Buzzword in der IT-Sicherheit und wie bei allen neuen Buzzwords in der IT versuchen Hersteller von Produkten solche Begriffe für den Verkauf ihrer Produkte zu nutzen und weisen beispielsweise darauf hin, dass ihr Produkt Zero Trust implementiert

Zero Trust ist jedoch kein Produkt, das man einkaufen kann. Vielmehr handelt es sich um eine Menge von Paradigmen beziehungsweise Ideen, die man bei der Weiterentwicklung von Sicherheitsarchitekturen berücksichtigen sollte. Einzelne Trends in Teilbereichen der IT-Sicherheit wie dynamische risikobasierte Authentisierung oder auch Mikrosegmentierung können hilfreiche Puzzlebausteine für die Umsetzung von Zero Trust sein. Man sollte sich aber auf keinen Fall von den Werbeversprechungen der Hersteller treiben lassen, sondern ein individuelles Konzept erstellen, bei dem die vorhandene Infrastruktur ebenso wie die individuellen Sicherheitsbedürfnisse und Ziele berücksichtigt sind.

8 Exemplarisch sei hier das „Zero Trust Maturity Model" genannt, online verfügbar unter https://www.cisa.gov/zero-trust-maturity-model (zuletzt abgerufen am 30. Juni 2023).

9 Die Abbildung wurde der Publikation „Zero Trust Maturity Model", online verfügbar unter https://www.cisa.gov/zero-trust-maturity-model (zuletzt abgerufen am 30. Juni 2023), entnommen.