axians

ZERO TRUST

Wie das Prinzip „Misstrauen“ Ihre Cybersicherheit erhöht

Ein Whitepaper über den datenzentrierten Sicherheitsansatz, bei dem Vertrauen gut, aber Kontrolle besser ist.

VINCI ENERGIES

Dr. W. Edwards Deming

„IN GOD WE TRUST.

All others must bring data.“

authentication

Die erhöhte Cloud-Akzeptanz, immer mehr Remote-Anwender, IoT-Umgebungen, Bring Your Own Device (BYOD), die digitale Transformation und andere Trends schaffen IT-Szenarien, bei denen es ein „innerhalb der Sicherheitsgrenzen“ häufig nicht mehr gibt. Vielmehr befindet sich die neue Sicherheitszone überall. Und bei einer Angriffsfläche, die nie größer und facettenreicher war, ist eine umfassendere Herangehensweise an die Netzwerksicherheit wichtiger denn je.
Mit einer Zero Trust Architektur (ZTA) können Sie auf das „Prinzip Misstrauen“ bauen. Unternehmen, die den Aufwand einer Migration Richtung ZTA investieren, um einen datenzentrierten und identitätsbewussten Sicherheitsansatz zu erreichen, werden mit vielen Vorteilen – wie: größere Transparenz, mehr Netzwerk-Sichtbarkeit, gestärktem Datenschutz und einer besseren Unterstützung bei der Migration in die Cloud belohnt.

In diesem Whitepaper erfahren Sie, was eine Zero Trust Architektur ist, worauf das Konzept basiert, welche Vorteile es bietet und wie Sie es im eigenen Unternehmen umsetzen können.

Photo by Bolun Yan on Unsplash

Inhalt

Einleitung 2

Was ist Zero Trust? 6

6 Aussagen, auf die eine Zero Trust Architektur baut 7

Design-Grundsätze – Zero Trust Architektur Netzwerk 8

Anforderungen einer ZTA 10

Wo liegt der Unterschied zu klassischen Sicherheitsmodellen? 11

Kernelemente einer ZTA 12
- **Adaptive Faktoren 13**
- **Identity Access Management (IAM) 13**
- **Network Access Control (NAC) 13**

7 ZTA-Prinzipien und Best Practices 16
- **Zero Trust Network 16**
- **Zero Trust People 16**
- **Zero Trust Devices 17**
- **Zero Trust Data 17**
- **Zero Trust Workloads 18**
- **Visibility & Analytics 18**
- **Automation & Orchestration 18**

Mehr Sicherheit bei weniger Risiken 19

Migration – Ihr Weg zu einer Zero Trust Architektur 21
- **Vulnerability Scan und Security Health Check 22**
- **Entwicklung und Migration eines Zero Trust-Netzwerks 22**
- **Migration oder Neuaufbau? 23**

Warum Zero Trust und SASE sich perfekt ergänzen 24

Fazit 26

Photo by Juan Davila on Unsplash

Was ist Zero Trust?

Zero Trust ist ein Cyber-Sicherheitsparadigma, das sich auf den Ressourcenschutz konzentriert und von der Prämisse ausgeht, dass Vertrauen niemals implizit gewährt wird, sondern kontinuierlich evaluiert werden muss. Es handelt sich um Leitprinzipien für Workflows und Systemarchitekturen, die die Sicherheitslage verbessern sollen. Viele Organisationen haben bereits Elemente von Zero Trust in ihre Infrastruktur implementiert oder sie sind dabei, Richtlinien und bewährte Verfahren zu migrieren.

Das Zero Trust Konzept war in der Cyber Security schon vorhanden, bevor der Begriff überhaupt geprägt wurde. Die Defense Information Systems Agency (DISA) und das amerikanische Verteidigungsministerium veröffentlichten eine Strategie, die sie als „black core" (BCORE) bezeichneten. Diese beschrieb den Übergang von einem Perimeter basierten Sicherheitsmodell zu einem Modell, das sich auf die Sicherheit einzelner Transaktionen konzentriert. Im Jahr 2004 veröffentlichte das Jericho Forum die Idee der De-Perimeterisierung – also die Begrenzung des impliziten Vertrauens auf Basis des Netzwerkstandorts und auf einzelne Verteidigungsvorrichtungen über ein großes Netzwerksegment hinweg. Das Konzept der De-Perimeterisierung entwickelte sich dann zu der umfassenden Zero Trust Architektur, wie sie von John Kindervag im Jahr 2010 als Vizepräsident und Chefanalyst von Forrester Research geprägt wurde.

Heute handelt es sich um einen ganzheitlichen Ansatz und eine Sicherheitsarchitektur, die auf einem strengen Prozess und ständiger Weiterentwicklung der Identitätsprüfung basiert. Organisationen sollen damit ihre Datenbestände und Geschäftsanwendungen schützen. Und zwar, indem Unsicherheiten bei der Durchsetzung präziser Zugriffsentscheidungen mit den geringsten Privilegien pro Anfrage in Informationssystemen und -diensten angesichts eines als kompromittiert geltenden Netzwerks minimiert werden. Diese Definition konzentriert sich auf das Ziel, unberechtigte Zugriffe auf Daten und Dienste zu verhindern und gleichzeitig die Durchsetzung der Zugriffskontrolle so granular wie möglich zu gestalten.
Und so geht Zero Trust immer und grundsätzlich davon aus, dass Nullkommanull vertrauenswürdig ist.
Kein Nutzer, keine Anfrage, kein Dienst, keine Anwendung, kein Gerät – es sei denn, das Gegenteil wird bewiesen.

Photo by Jamie Street on Unsplash

6 Aussagen, auf die eine Zero Trust Architektur baut:

1. Der Standort allein impliziert noch kein Vertrauen. Interne Zugriffsanfragen müssen die gleichen Sicherheitsanforderungen erfüllen, wie die Anfragen aus fremden Netzwerken.

2. Zugriff auf einzelne Unternehmensressourcen wird pro Sitzung gewährt. Das Vertrauen in den Antragsteller wird bewertet, bevor er Zugang erhält. Es werden auch nur die Privilegien gewährt, die zur Erledigung der Aufgabe erforderlich sind.

3. Zugriff auf Ressourcen wird durch dynamische Richtlinien bestimmt – einschließlich des beobachtbaren Zustands der Identität, Anwendung, des Dienstes und des anfordernden Assets. Dabei stellt eine Richtlinie einen Satz von Zugriffsregeln auf der Grundlage von Attributen dar, die eine Organisation einem Subjekt, einem Datenbestand oder einer Anwendung zuweist – z. B. der Standort des anfordernden Netzwerks, die Zeit, gemeldete aktive Angriffe, usw.

4. Das Unternehmen überwacht und misst die Integrität und Sicherheitslage aller Assets. So sollte im Zuge einer Zero Trust Architektur auch ein System zum Monitoring des Zustands von Geräten und Anwendungen eingerichtet sein (CDM: Continous Diagnostics and Mitigation).

5. Alle Authentifizierungen und Autorisierungen sind dynamisch und werden streng durchgesetzt, bevor der Zugriff gestattet wird. Es handelt sich um einen ständigen Kreislauf aus Zugriffserteilung, scannen und Bewertung von Bedrohungen, Anpassung und ständiger Neubewertung des Vertrauens in die laufende Kommunikation.

6. Das Unternehmen sammelt so viele Informationen wie möglich über den aktuellen Zustand der Assets, der Netzwerkinfrastruktur wie auch der Kommunikation und nutzt sie zur Verbesserung seiner Sicherheitslage.

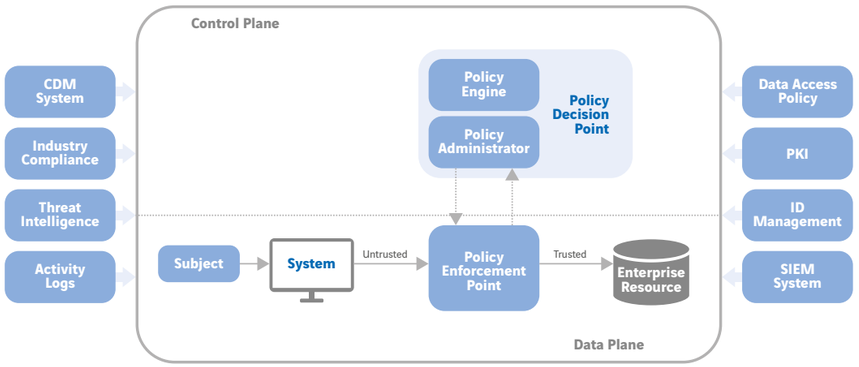
DESIGN-GRUNDSÄTZE

Zero Trust Architektur Netzwerk

Der entscheidende ZTA-Grundsatz lautet, dass das gesamte Unternehmensnetzwerk als nicht-vertrauenswürdige Zone betrachtet wird. Kommunikation darf immer nur auf die sicherste Art und Weise erfolgen. Dazu gehören die Authentifizierung aller Verbindungen und die Verschlüsselung des gesamten Datenverkehrs. Auch können Remote-Objekte und Assets ihrer lokalen Netzwerkverbindung nicht vollständig vertrauen – sie sollen davon ausgehen, dass das nicht unternehmenseigene Netzwerk stets feindlich gesinnt ist.
Alle „Workloads" – hier im Sinne von „Datenströmen" – die sich zwischen der Infrastruktur des Unternehmens und fremder Infrastruktur bewegen, sollten konsistente Sicherheitseigenschaften (verschlüsselt, anonymisiert, pseudonomisiert, etc.) aufweisen. Assets und Workloads sollten ihren Status auch dann beibehalten, wenn sie in die oder aus der unternehmenseigenen Infrastruktur umziehen. Das gilt auch für Geräte, die von Unternehmensnetzwerken in fremde Unternehmensnetzwerke umziehen (d. h. für Remote-Benutzer). Dazu gehören auch Workloads, die von firmeneigenen Rechenzentren in Cloud-Instanzen außerhalb des Unternehmens migriert werden.

- **Die ZTA unterscheidet zwischen der sogenannten Control Plane [Policy Decision Point (PDP)] und Data Plane [Policy Enforcement Point (PEP)]. Die Control Plane steuert welche Kommunikationen erlaubt, bzw. untersagt werden, indem sie die Data Plane entsprechend anweist, bzw. Anfragen von der Data Plane (per session) entscheidet.**

Core Zero Trust Logical Components



Bildbeschreibung: Eine ZTA besteht aus zahlreichen logischen Komponenten, die On-Premises oder Cloud-basiert betrieben werden können. Zur Kommunikation verwenden sie eine separate Management Ebene (Control Plane), während die Anwendungsdaten über die Data Plane kommunizieren.

Neben den Kernkomponenten aus der Control Plane und der Data Plane gibt es eine Reihe von umgebenden (externen und lokalen) Komponenten, die der Control Plane Daten zur Entscheidungsfindung liefern. Zu diesen können u. A. folgende gehören:

- **CDM (Continuous Diagnostics and Mitigation):**
  z. B. via EDR, Network-IPS/NDR (Network Detection and Response)
- **Nutzung von Threat Intelligence Services wie z. B.**
  - Anti Virus
  - Sandboxing
  - URL Filtering
  - DNS Security
  - Anti-Bot
  - Application Control
  - IP Reputation für z. B. E-Mail
  - Geo-Datenbanken
  - Services für Vulnerabilities
- **IAM (Identity Access Management)/PKI (Public Key Infrastructure)**
- **NAC (Network Access Control)**
- **OTP (One Time Password)/MFA (Multi Faktor Authentifizierung)**
- **SIEM (Security Information and Event Management)**
- **User/Group-based Firewalling**
- **Automatisierung**
- **Mikrosegmentierung**
- **Auditing der Security Infrastruktur**
- **Vulnerability Management/Risk Assessment**
- **CASB (Cloud Access Security Broker)**

Photo by Dale Nibbs on Unsplash


Photo by Mitchel Kintz on Unsplash

Anforderungen einer ZTA

- Das Unternehmen kann den gesamten Netzwerkverkehr beobachten. Es zeichnet Pakete auf, die auf der Datenebene gesehen werden, auch wenn es nicht in der Lage ist, eine Inspektion der Anwendungsschicht (d. h. OSI-Schicht 7) für alle Pakete durchzuführen – dazu werden z. B. SIEM/NDR benötigt.

- Unternehmensressourcen sollten ohne Zugriff durch Policy Enforcement Points (PEP) nicht erreichbar sein. Dazu kann z. B. eine WAF (Web Application Firewall) und NGFW (Next Generation Firewall mit Benutzer oder Benutzergruppenbasierten Regeln) verwendet werden.

- Die Datenebene und die Kontrollebene sind logisch getrennt.

- Die Policy Enforcement Points sind die einzigen Komponenten, die als Teil eines Geschäftsablaufs auf den Richtlinienverwalter zugreifen. Jeder PEP im Unternehmens-Netz steht in Verbindung mit der Kontrollebene, um die Kommunikation zwischen Clients und Ressourcen freizugeben.

- Remote-Clients sollten in der Lage sein, auf Unternehmensressourcen (z. B. Cloud Services) zuzugreifen, ohne zuerst die Netzwerkinfrastruktur des Unternehmens durchlaufen zu müssen – daher sollten die Cloud Ressourcen entsprechend abgesichert sein, z. B. via MFA.

- Die Infrastruktur, die zur Unterstützung des ZTA-Zugangsentscheidungsprozesses verwendet wird, sollte skalierbar und ausreichend redundant ausgelegt sein, um Änderungen in der Prozesslast zu berücksichtigen.

- Die Clients könnten aufgrund rechtlicher Vorgaben bestimmte PEPs möglicherweise nicht erreichen. Diese könnten auf dem Standort (Geolokalisierung oder Netzstandort), dem Gerätetyp oder anderen Kriterien beruhen. Es sollte also gesetzliche Regularien beachtet, bzw. Geo Location Threat Intelligence zum Einsatz kommen.

Wo liegt der Unterschied zu klassischen Sicherheitsmodellen?

Angesichts von immer mehr Benutzern, Anwendungen, Geräten und Verbindungen im Netzwerk und der Cloud, ist es auch immer schwieriger, dass jedem und jeder einzelnen Ressource der richtige Zugriff gewährt wird. Traditionelle Sicherheitskonzepte stoßen dabei mehr und mehr an ihre Grenzen.

Denn bisherige Ansätze konzentrieren sich hauptsächlich auf das Scannen nach Bedrohungen im Client-Server-Verkehr, der sich in und aus dem eigenen Sicherheitsperimeter bewegt. Die Strategie von Zero Trust läuft hingegen darauf hinaus, jeden ein- und ausgehenden Datenverkehr zu überprüfen und darüber hinaus den internen Verkehr mit einzubeziehen. **Es wird also auch der Datenfluss als potenzielle Gefahr behandelt, der die Grenzen der eigenen Organisation gar nicht überschreitet.**

Bei traditionellen Modellen wird häufig nur mit starren Sicherheitsgrenzen gearbeitet, bei denen z.B. ein Zugriff von innen per se als vertrauenswürdiger eingestuft wird als einer von außen.

Bei einer Zero Trust Architektur werden hingegen alle Benutzer, Geräte und Ressourcen zunächst als nicht vertrauenswürdig behandelt. Und zwar völlig unabhängig davon, wer oder was sie sind oder von wo sie sich mit dem Unternehmensnetzwerk verbinden.

„Somit verlässt sich Zero Trust weniger auf die Sicherheit eines Netzwerkperimeters, sondern vielmehr auf sichere Prozesse und Technologien, die direkt auf die eigenen Ressourcen angewendet werden können – ganz gleich, wo diese sich befinden und wer von wo darauf zugreifen will.“

[Ben Kröger, Technische Leitung, Axians IT Security GmbH]

Kernelemente einer ZTA

Authentifizierung und Verwaltung von Zugriffen

Die Authentifizierung und Verwaltung von Zugriffen beinhaltet auch die Fähigkeit, unternehmensfremde Geräte zu identifizieren und zu überwachen, die sich in der eigenen Netzwerkinfrastruktur befinden oder auf Unternehmensressourcen zugreifen. Dazu gehören Hardwarekomponenten (z. B. Laptops, Telefone, IoT-Geräte) genauso wie digitale Artefakte (z. B. Benutzerkonten, Anwendungen, digitale Zertifikate). Da eine vollständige Listung aller unternehmenseigenen Assets oft nicht vorhanden ist, sollte die Fähigkeit zur schnellen Identifizierung, Kategorisierung und Bewertung neu entdeckter Assets, die sich in der eigenen Infrastruktur befinden, in Betracht gezogen werden. Das geht über das bloße Katalogisieren und Pflegen einer Datenbank von Unternehmensbeständen hinaus.
Den aktuellen Zustand eines Assets zu beobachten, ist Teil des Prozesses der Bewertung von Zugriffsanfragen. Dazu werden z. B. Monitoring, SIEM und NDR benötigt. Das Unternehmen muss in der Lage sein, virtuelle und physische Ressourcen zu konfigurieren, zu überwachen und zu aktualisieren. Alle Informationen sollten die Management Ebene passieren, wenn Entscheidungen über den Ressourcenzugriff getroffen werden. Auch Unternehmensfremde Assets und eine mögliche Schatten-IT sollten so gut wie möglich katalogisiert werden. Die Schatten-IT stellt ein besonderes Problem dar, da viele Unternehmen keinen Überblick über die Cloud Ressourcen haben, die von Anwendern genutzt werden und so Unternehmensdaten unbemerkt abfließen können. Abhilfe kann z. B. ein CASB schaffen.
Da auch schwache Zugangsdaten ein Hauptgrund für Datenpannen sind, sollen **Single Sign-On (SSO) und die Multi-Faktor-Authentifizierung (MFA)** das Schutzniveau beim Einsatz einer Zero Trust Architektur deutlich erhöhen.

Adaptive Faktoren

Je nach Nutzerrolle und Datensensibilität kommen **zusätzliche adaptive Faktoren** ins Spiel: Nach einer individuellen Risikobewertung (z. B. Standort-ID, das Gerät selbst oder die Anwendung, von der aus der Zugriff erfolgt) werden zusätzliche Authentifizierungsmerkmale wie z. B. biometrische Parameter, verhaltensbezogene Vertrauenspunktzahlen, spezielle Token oder Smart Cards hinzugezogen.

Identity Access Management (IAM)

Ein weiterer unverzichtbarer Baustein, an dem man bei Zero Trust nicht vorbeikommt: Der Aufbau eines **Identity Access Managements** als Basis, um bekannte Identitäten eindeutig zu erkennen. Im ersten Schritt wird festgelegt, wer grundsätzlich worauf zugreifen darf. Im zweiten Schritt folgt das Access Management mit der Definition, ob, wann und wie Passwörter und weitere Faktoren wie z. B. SSO bzw. MFA zum Einsatz kommen.

Network Access Control (NAC)

Einen zusätzlichen Überblick darüber, welche Geräte und Nutzer sich mit dem Netzwerk verbinden und wo sie sich befinden, bietet **NAC.** Durch die Überprüfung und Authentifizierung kann die Netzwerkzugangskontrolle zudem das Einschleusen von Schadsoftware verhindern und die Sicherheitsrichtlinien eines Unternehmens zuverlässig durchsetzen.

Die Einführung von IAM und NAC können zwei von vielen Bausteinen sein, die helfen eine ZTA zu errichten. Dienste, die dann von außerhalb des eigenen Perimeters angesteuert werden, sollten als klassische Einfallstore priorisiert werden: Cloud-Anwendungen, Schnittstellen, Kundenportale u. v. m. Aber auch Anwendungen und Ressourcen, die sensible Informationen nutzen, gilt erhöhte Aufmerksamkeit.

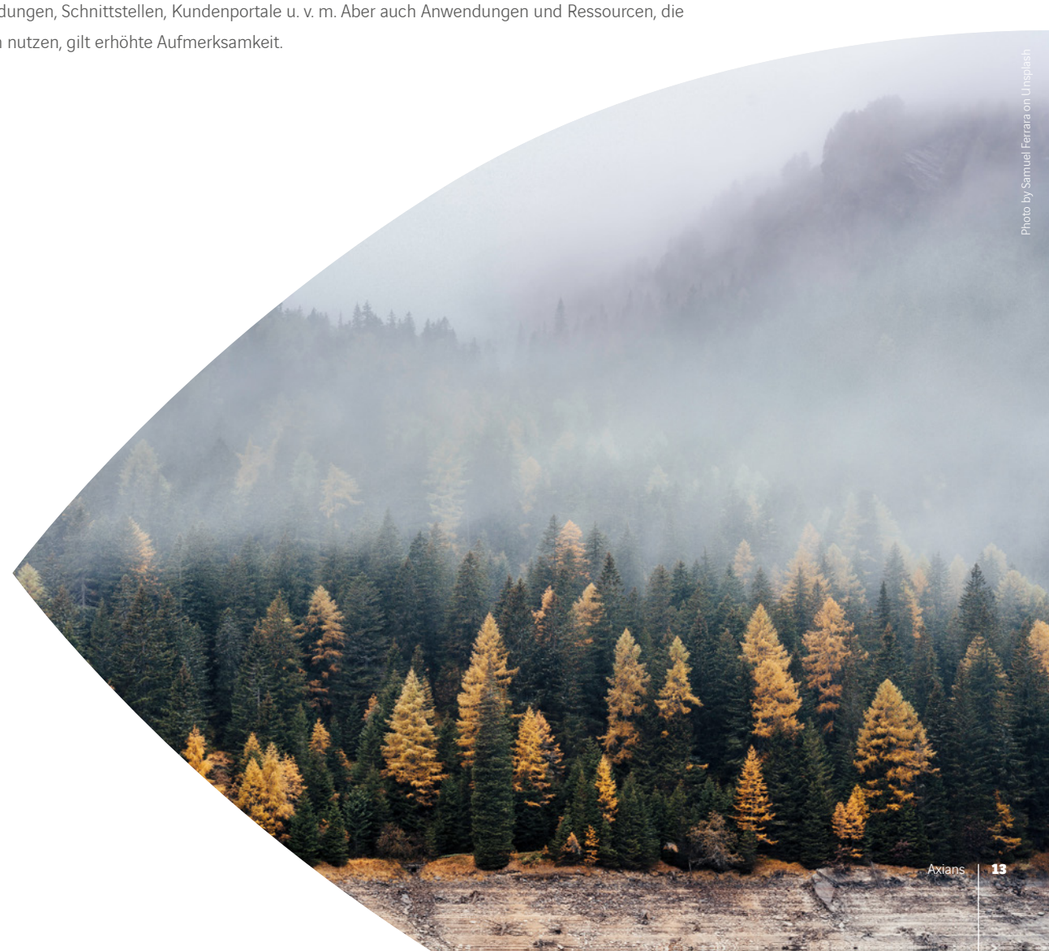


Photo by Samuel Ferrara on Unsplash

STOLPERSTEIN ODER HERAUSFORDERUNG?

Eine Herausforderung besteht darin, dass starke Identitätsmanagement- und Authentifizierungstools ordnungsgemäß konfiguriert und kontinuierlich überprüft werden müssen. Zudem gilt es, sämtliche Benutzerprofile auf dem neuesten Stand zu halten und Vertrauensalgorithmen sorgfältig zu entwickeln, um korrekte Zugriffs- und Nutzungsrechte zu ermöglichen. Auch könnten Benutzer feststellen, dass der Zugriff auf kritische Daten und Systeme einer strengen Prüfung unterzogen wird und möglicherweise zeitaufwendiger ist, als sie es bisher gewohnt waren. Gleichzeitig ist die ständige Kontrolle von verschlüsseltem Datenverkehr rechenintensiv.

7 ZTA-Prinzipien und Best Practices

Die Zero Trust Architektur existiert in verschiedenen Ansätzen und wird fortlaufend weiterentwickelt. Sie basiert auf sieben Schlüsselprinzipien, die die Annahme einer maximal restriktiven Sicherheitshaltung ermöglichen, bei der Systeme gehärtet und isoliert werden, bis das nötige Maß an Vertrauen aufgebaut ist.

ZERO TRUST NETWORK

Böswillige Bewegungen durch granulare Netzwerksegmentierung verhindern

Der Schlüssel, um unbefugten und böswilligen Netzwerkverkehr wie auch die Ausbreitung eines internen Angriffs zu stoppen, ist die Mikrosegmentierung: Da sie Systeme gleicher Schutzklassen in Netzsegmente zusammenfasst, lässt sie nur den absolut minimalen und legitimen Verkehr zwischen einzelnen Segmenten zu, während alles andere automatisch verweigert wird.

Best Practices für das Zero Trust Network:

- Wichtige Daten und Assets identifizieren und nach Sensibilität klassifizieren
- Datenflüsse in alle Richtungen skizzieren (nordwärts, Ost-West, südwärts)
- Assets mit ähnlichen Funktionalitäten und Sensibilitäten in dasselbe Mikrosegment gruppieren
- Einsatz eines Segmentierungs-Gateways, um die Kontrolle über jedes Segment zu erlangen
- Ein „least privilege"-Prinzip für jedes Asset definieren

ZERO TRUST PEOPLE

Kontextsensitive Autorisierung zum Schutz vor Identitäts-Diebstahl verwenden

Viele Datenpannen sind durch gestohlene oder zu schwache Login-Daten bedingt. Da jeder Verbindungsversuch eines Nutzers immer wieder neu bewertet wird, werden diese Schwachstellen durch Zero Trust People überwunden, nachdem der gesamte Zugriffs-Kontext unter der Lupe war.

Best Practices für Zero Trust People:

- Authentifizierung von Identitäten auf Netzwerkebene statt nur auf Anwendungseben
- Vereinfachung des Authentifizierungsprozesses mit Single-Sign-on
- Für bestimmte Fälle eine zusätzliche Multi-Faktor-Authentifizierung nutzen
- Kontextbezogene Sicherheitsrichtlinien anhand mehrerer Bedingungen festlegen
- Verbindungsversuche kontinuierlich verfolgen, um Anomalien aufzuspüren
- Awareness Schulungen, um Phishing E-Mails zu erkennen, bevor sie Schaden anrichten
- Content Security Policy für die Absicherung von E-Mail/Web-Kommunikation
- Dem Nutzer alle Hilfsmittel bieten, um ihn vor Bedrohungen zu schützen

Photo by Ricardo Gomez Angel on Unsplash

ZERO TRUST DEVICES

Alle Geräte schützen und bei Kompromittierung isolieren

Da sich die Anzahl beruflich wie auch privat genutzter mobiler Geräte (BYOD) deutlich erhöht hat, fordert Zero Trust Devices alle Geräte im Netzwerk zu schützen und sie zu isolieren, falls sie kompromittiert werden. Denn oft laufen sie mit nicht gepatchter Software, sind falsch konfiguriert oder kommunizieren über ungesicherte Protokolle.

Best Practices für Zero Trust Devices:

- Verkehr von und zu Geräten sollte durch Netzwerksegmentierung stark eingeschränkt sein
- Geräte in nicht vertrauenswürdigen Netzwerken durch das Erzwingen eines internen Sicherheitsschutzes absichern
- Zugriff infizierter oder anfälliger Geräte auf wichtige Unternehmens-Assets blockieren
- Dies geht über das bloße Katalogisieren und Pflegen einer Datenbank von Unternehmenswerten hinaus

ZERO TRUST DATA

Daten immer und überall klassifizieren, schützen und verschlüsseln

Da Daten ständig zwischen stationären Workstations, mobilen Geräten, Anwendungen, Servern und öffentlichen wie auch privaten Netzwerken getauscht werden, brauchen sie besonderen Schutz – egal, wo auch immer sich diese Daten befinden.

Best Practices für Zero Trust Data:

- Verschlüsselung von Daten immer und überall erzwingen
- Sicheren Zugriff für Remote-Benutzer durch Integration von Zugriffskontrolle, Authentifizierung und Verschlüsselung bereitstellen
- Data Loss Prevention bereitstellen, um sensible Dateien zu klassifizieren und zu schützen

ZERO TRUST WORKLOADS

Workloads durch erweiterte Sichtbarkeit und anpassbare Richtlinien schützen

Besonders in der Public Cloud (z. B. Container oder VMs) ist jeder einzelne Arbeitsauftrag anfällig, der vom beauftragenden System weiterverarbeitet wird oder als Input für einen weiteren Arbeitsauftrag dient. Das Ziel sollte daher sein, vollständige Transparenz über die sich ständig verändernden öffentlichen und privaten Cloud-Ressourcen zu erlangen – wie sich ändernde IP-Adressen, bereitgestellte und wieder beendete Anwendungen, etc.

Best Practices für Zero Trust Workloads:

- Cloud-Ressourcen definieren, für die ein besonderer Schutz vorgesehen ist
- Alle Workloads identifizieren, die sich auf die jeweiligen Ressourcen beziehen und kennzeichnen
- Interne Segmentierung nach „least privilege"-Prinzip definieren
- Kennzeichnung verwenden, um Richtlinien zu konfigurieren und Segmentierung durchzusetzen

VISIBILITY & ANALYTICS

Bedrohungen und Risiken schnell und auf den ersten Blick erkennen

Oft bleiben Sicherheitsverstöße unentdeckt. Da bei Zero Trust jede Aktivität auf den Backend-Servern und deren Applikationen kontinuierlich überwacht und protokolliert wird, lassen sich Bedrohungen und Risiken nicht nur schnell entdecken, sondern auch sehr effektiv eindämmen.

Best Practices für mehr Sichtbarkeit:

- Zentralisiertes Sicherheitsmanagement mit einheitlicher Sichtweise einrichten
- Jede verdächtige und unverdächtige Aktion einschließlich der Endpunkte protokollieren
- Ein Big Data-Analysetool verwenden, um alle Ereignisse festzuhalten und den gesamten Datenverkehr zu protokollieren
- Threat Intelligence Services nutzen, um aktuelle Bedrohungsindikatoren (IoC=Indicator of compromise) bereitzustellen

AUTOMATION & ORCHESTRATION

Sicherheitsaufgaben durch Schnittstellen automatisieren

In dynamischen Umgebungen ist es wegen der hohen Fehleranfälligkeit entscheidend, sicherheitsrelevante Aufgaben automatisiert zu orchestrieren. Eine Zero Trust Architektur sollte sich dabei so in die eigene Infrastruktur integrieren, dass eine voll- oder teilautomatisierte Abwehr möglich ist.

Best Practices für Automation & Orchestration:

- Den Arbeitsaufwand für Sicherheitsadministratoren durch automatisch gesteuerte Workflows reduzieren
- Beispielsweise ein SIEM-System integrieren, um die Erkennung und Behebung von Vorfällen zu automatisieren
- APIs von Sicherheitslösungen zur Integration mit Systemen wie SIEM, Netzwerkmanagement, Sicherheitsbewertung, Identitätsbewusstsein, etc. nutzen
- Updates von Software, Betriebssystemen, AV Pattern, IPS Pattern, etc. automatisieren und protokollieren

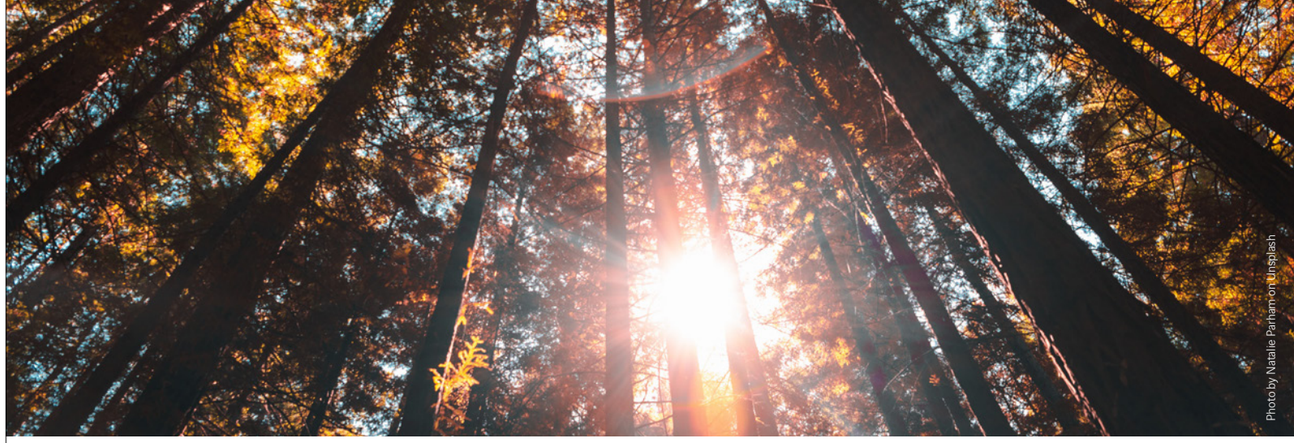


Photo by Natalie Parham on Unsplash

Mehr Sicherheit bei weniger Risiken

Ob es darum geht, Identifizierungs- und Zugriffsrichtlinien zu stärken oder Netzwerke zu segmentieren sowie Daten besser zu schützen – durch Hinzufügen effektiver Zugangsbarrieren und durch Ermöglichung des Zugangs bei Bedarf kann Zero Trust helfen, die Cyber Security deutlich zu stärken und die Angriffsfläche zu begrenzen.
So profitieren Unternehmen mit Zero Trust vor allem von mehr Sicherheit bei weniger Risiken. Denn eine ZTA führt mit seinen Prinzipien und Best Practices vor allem auch dazu, dass sich Unternehmen mit einem ganzheitlichen Sicherheitsansatz beschäftigen müssen.

ZENTRALE VORTEILE AUF EINEN BLICK

- Eine ZTA sorgt für eine weitaus sicherere Umgebung
- Der Zugriff auf sensible Daten ist in aller Regel besser geschützt
- Etablierung einer allgemein gültigen Logik zum sicheren Zugriff auf Assets ohne Bindung an Infrastrukturmerkmalen
- Die immer größere Angriffsfläche, die durch mehr Benutzer, Geräte und Anwendungen entstanden ist, kann besser abgesichert werden
- Indem immer nur der unbedingt notwendige Zugriff auf die zentralen Services gewährt wird, ist eine Mikrosegmentierung im Backend mitsamt zentraler Server, Applikationen und Datenbanken möglich
- Eine ZTA erhöht die Transparenz von Zugriffen, da Zugriffsanfragen und Richtlinienänderungen kontinuierlich überwacht und protokolliert werden
- Mikrosegmentierung des Netzwerks wie auch die Tatsache, dass die Berechtigung auf Applikationsebene erfolgt und die Zugriffe per PEP im Netzwerk gezielt freigeschaltet werden, begrenzen die Auswirkungen bei Sicherheitsverstößen
- Durch besser integrierte Tools, einfachere IT-Betriebsmodelle und die Vermeidung von Datenverlusten lassen sich Kosten einsparen
- Schutz von künftigen Investitionen in Anwendungen und Releases (bereits in der Beschaffung), welche „zero trust ready" sein müssen
- Durch Awareness Trainings einen Angriffspunkt in einen Sicherheitsgewinn drehen

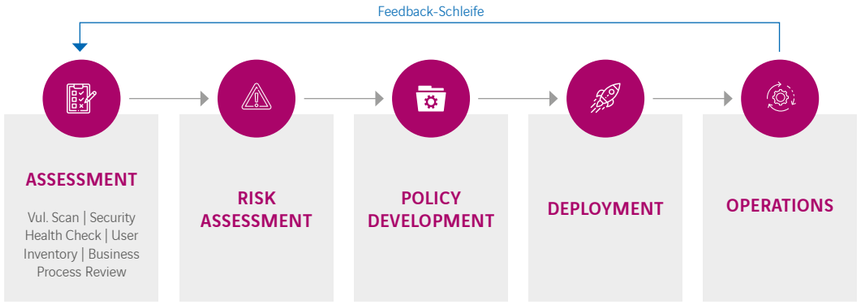
MIGRATION

Ihr Weg zu einer Zero Trust Architektur

Jede Unternehmensumgebung kann nach den Zero Trust Prinzipien gestaltet werden. Allerdings ist es unwahrscheinlich, eine ZTA in einem einzigen Technologie-Aktualisierungszyklus zu migrieren. Es wird also einen unbestimmten Zeitraum geben, in dem ZTA-Workflows mit anderen Abläufen koexistieren. Auch sollte die Migration zu einer ZTA über einen Geschäftsprozess nach dem anderen erfolgen. Dabei muss sichergestellt sein, dass die gemeinsamen Elemente (z. B. ID-Management, Gerätemanagement, Ereignisprotokollierung) flexibel genug sind, um in einer ZTA- und Perimeter-basierten hybriden Sicherheitsarchitektur zu genügen.

Die Migration setzt zudem voraus, dass ein Unternehmen detaillierte Kenntnisse über seine Assets, also Systeme (physisch und virtuell), Objekte (einschließlich Benutzerrechte) und Geschäftsprozesse hat. Auf dieses Wissen greift die Control Plane bei der Auswertung von Ressourcenanfragen zu. Ein vollständiges Bild des Geschäftsprozesses ist notwendig, um diesen innerhalb einer ZTA korrekt abzubilden, damit die ZTA entscheiden kann, ob Workloads zugelassen oder untersagt werden müssen. Dies ist besonders dann ein Problem, wenn in einer Organisation eine Schatten-IT vorhanden ist.

Die Einführung einer Zero Trust Architektur erfordert zuerst eine klare Sicht auf die Funktionen innerhalb der Abteilungen des Unternehmens, die Software, Anwendungen, Zugriffsebenen und Geräte, die aktuell und in Zukunft eingesetzt werden. Die wichtigsten Meilensteine beinhalten in der Regel folgende Punkte, bei denen Axians Sie umfänglich unterstützen und begleiten kann.



Vulnerability Scan und Security Health Check

Axians empfiehlt den Start mit einem **Security Health Check** als umfangreichen Cyber Security Audit. Er klärt, welche Schwachstellen im Unternehmen ausgenutzt werden könnten, ob es bereits Sicherheitsvorfälle gab und ob sensible Daten unerwünscht das eigene Netzwerk verlassen. Das schafft Transparenz und Klarheit als Basis, um finanzielle Risiken zu vermeiden und um optimale Handlungsempfehlungen für die ideale Strategie zu geben.

Entwicklung und Migration eines Zero Trust-Netzwerks

Die Art und Weise, wie im Netzwerk auf schützenswerte Daten zugegriffen wird, bestimmt, wie diese geschützt werden sollten. Die folgende und aufeinander aufbauende Vorgehensweise entspricht unserer Empfehlung für den schrittweisen Rollout eines Zero Trust Networks.

Entwicklung einer umfassenden Sicherheitsarchitektur mitsamt Zero Trust Richtlinien wie „lines of defenses" und „lines of trust" wie auch den dazugehörigen Zugangsmandaten als übergeordnete Logik zur Anwendung auf On-Premises- und Cloud-Infrastrukturen.

Beispiele für Teilprojekte bei der Einführung einer ZTA durch die Axians:

- **On-Premises:** Aufbau eines Hochleistung-NG-Firewall Cluster zur „physikalischen" Abbildung der zuvor entworfenen Sicherheitsarchitektur und als Segmentierungs-Gateway
- **Cloud:** Etablierung einer Virtual Private Cloud mit einer „virtuellen" Abbildung der zuvor entworfenen Sicherheitsarchitektur
- **Kopplung der Cloud und On-Premises-Infrastruktur** zwecks Diensteverteilung, Lastverteilung und Synchronisation
- **Klassifizierung und Verteilung der Dienste** entsprechend dem jeweiligen Schutzbedarf hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität über Cloud und On-Premises
- **Netzwerk:** Redundate Anbindungen an die Netzwerk Infrastruktur, ggf. mit dynamischem Routing.
- **Server:** In Virtualisierungs-Plattformen (VMWare NSX)
- **Shared Service:** Verzeichnisdienste (IAM mit Microsoft AD)
- **Ausbau von Threat Intelligence,** die z. B. für das IPS, DNS, GEO, Anti-Spam, Sandboxing und Bewertungen im SIEM aktuelle Bedrohungsindikatoren liefern kann
- **Etablierung einer User-ID basierten Filterung** anstelle von IP-Adressen sowie einer Vereinfachung der Filterlogik
- **Etablierung einer Control und Data Plane** inklusive konsequenter Trennung sowie Migration der Dienste in eine interne Sicherheitszone bezogen auf den Schutzbedarf der Datenbestände
- **Auflösung der transparenten Client-Server Kommunikation** durch Aufgabe des alleinigen Zugriffs über IP-Adressen und der Einführung zentraler Gruppen- und Rollenrichtlinien, um den Zugriff auf Assets zentral zu prüfen und zu steuern
- **Unterbindung von „hidden" Tunnelmechanismen** durch SSL Inspection und Methodenvalidierung sowie Inhaltskontrolle (Content Security) und DNS Security
- **Etablierung von Infrastruktur zur Aufzeichnung des gesamten Netzwerkverkehrs**
- **Aufbau von SIEM Lösungen**
- **Betrieb von SIEM Lösungen (SOC)**
- **Awareness**

Migration oder Neuaufbau?

Oft ist es einfacher, die Basis zu schaffen und Zero Trust fähige Dienste nach und nach im Betrieb zu migrieren, als einen kompletten Neuaufbau zu wagen. So bleibt die bestehende Infrastruktur während der Übergangszeit funktionsfähig und wichtige Funktionen können bei Bedarf allen BYOD (Bring Your Own Device)- und externen Clients bereitgestellt werden.

In beiden Szenarien sollten Unternehmen, IT- und Sicherheitsteams gemeinsam mit erfahrenen Axians Experten ein Konzept erarbeiten, das die ideale endgültige Infrastruktur und eine Schritt-für-Schritt-Strategie für den Weg dorthin beinhaltet.

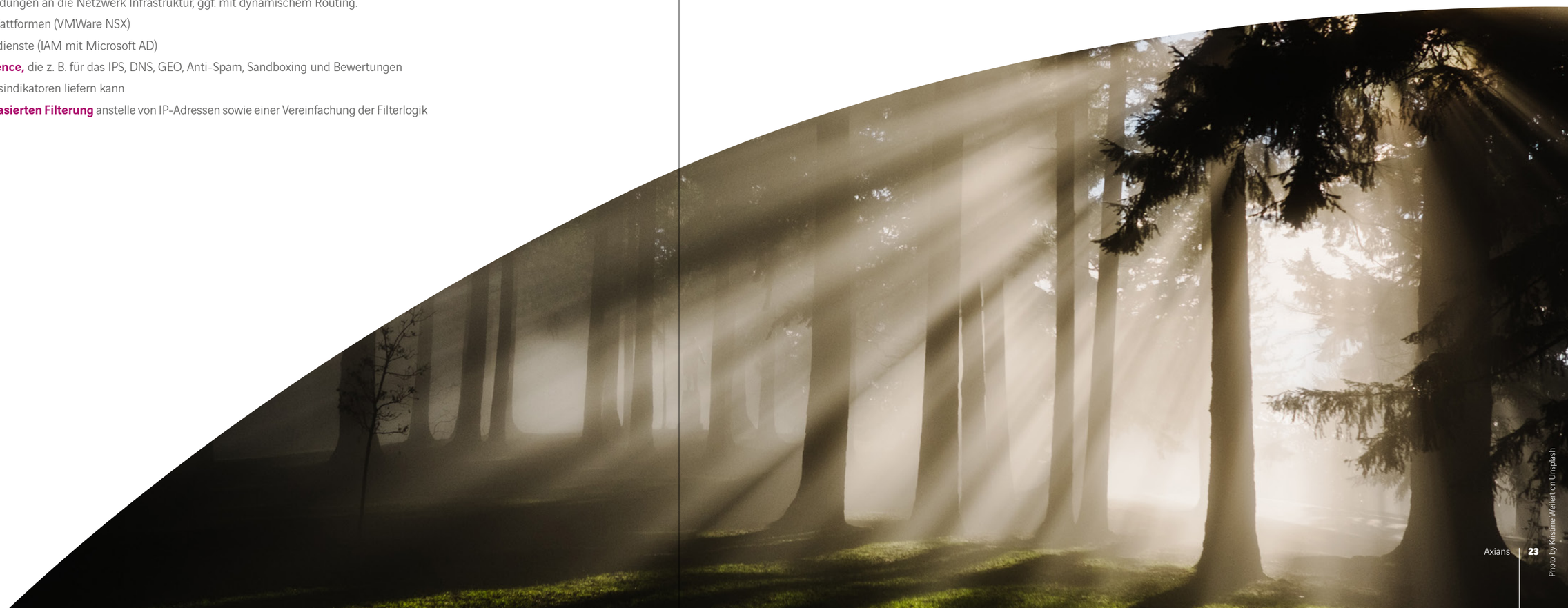


Photo by Kristine Weilert on Unsplash

Warum Zero Trust und SASE sich perfekt ergänzen

SASE ist ein vom Forschungsunternehmen Gartner definiertes Cyber Security Modell, das eine sichere Cloud-Nutzung ermöglichen und mit verschiedenen Technologien (SD-WAN, CASB, Zero Trust Network Access, etc.) dazu beitragen soll, dass sowohl Benutzer als auch Geräte überall und jederzeit sicheren Cloud-Zugriff auf Anwendungen, Daten und Dienste haben.
So wird der Netzwerkperimeter bei SASE nicht mehr als Standort, sondern als eine Reihe dynamischer Edge-Funktionen verstanden, die bei Bedarf als Service aus der Cloud bereitgestellt werden. Das noch relativ junge Konzept zielt – ähnlich wie Zero Trust – darauf ab, den gestiegenen Sicherheitsanforderungen einer agilen, stark vernetzten und von Remote-Arbeit geprägten Unternehmenswelt gerecht zu werden. So sollte eine Zero-Trust-Architektur immer auch die Möglichkeiten berücksichtigen, die SASE bieten kann.

Diese Architektur ermöglicht auch die Sichtbarkeit der Benutzeraktionen, was eine zwingende Voraussetzung für die Erkennung sowie für Forensik und Compliance ist.

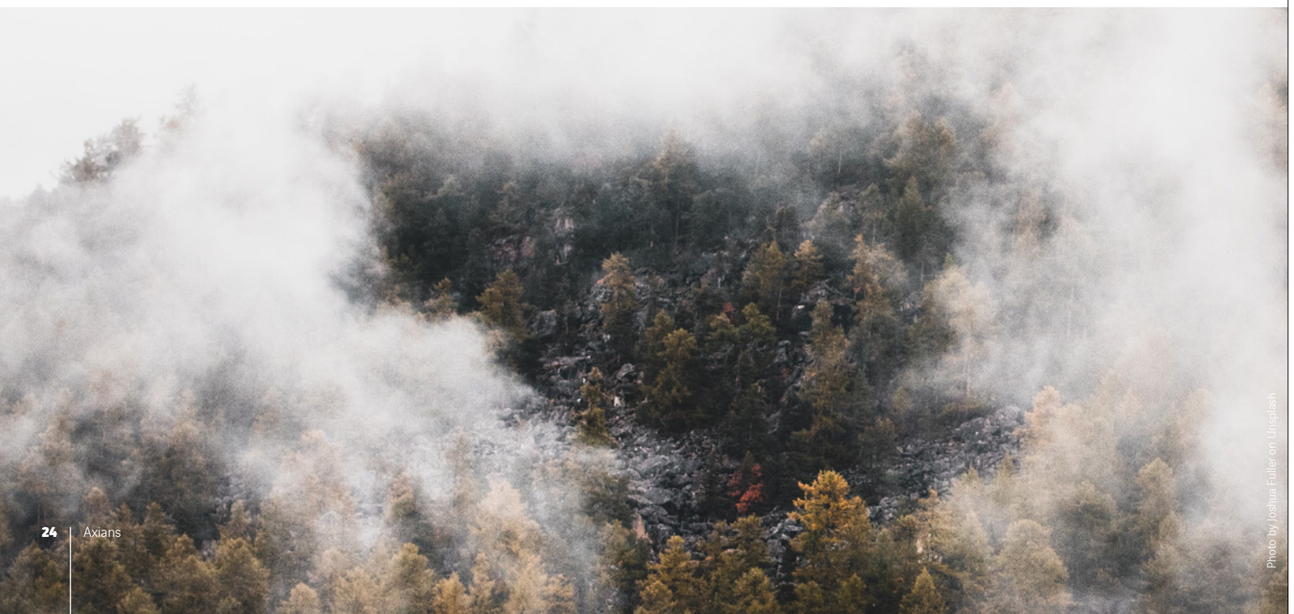
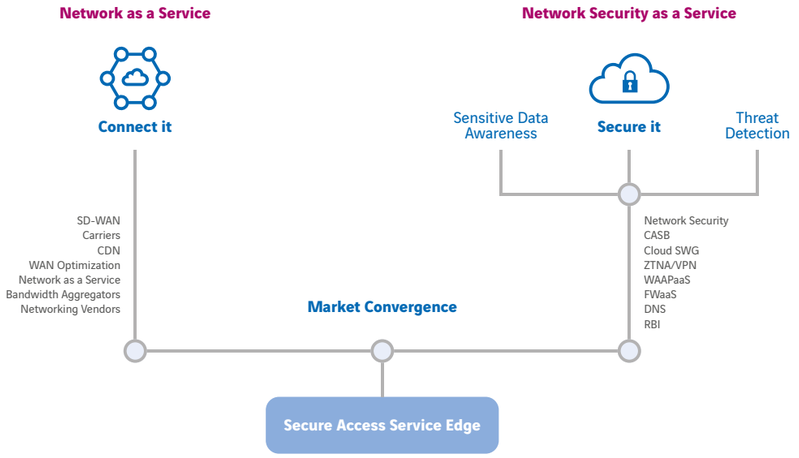


Photo by Joshua Fuller on Unsplash

SASE Convergence



Bildbeschreibung: Die Sicherheits- und Netzwerkinfrastruktur in der Cloud muss neu gestaltet werden, damit Cyber-Security-Teams Sichtbarkeit und Kontrolle über die Infrastruktur in der Cloud haben. Es reicht nicht allein die herkömmlichen Netzwerk- und Sicherheitssysteme zu bündeln und in der Cloud anzubieten. Aus Sicht von SASE und ZTA ist es angeraten, einen direkten Weg zu den Anwendungen für die Benutzer zu schaffen – also ein „Direct-to-App"-Ansatz, mit dem eine bessere Leistung und ein besseres Benutzererlebnis erreicht wird. Lösungsanbieter müssen konvergente Sicherheit bieten und die Cloud für hohe Leistung und Verfügbarkeit optimieren. Nur dann kann sie für eine globale Skalierbarkeit leicht verteilt werden.

SASE und Zero Trust

Durch die Kombination von SASE und den Zero Trust Prinzipien können Unternehmen Zero Trust Network Access erreichen, um Sicherheitsrichtlinien im gesamten Netzwerk konsistent anzuwenden und durchzusetzen. Dabei profitieren sie von der Verwendung einer zentralen Cloud-Anwendung für alle Sicherheits- und Konnektivitätsanforderungen. Statt also Zero Trust und SASE jeweils als eigenständiges Konzept zu sehen, werden sich die beiden Sicherheitskonzepte in Zukunft gegenseitig ergänzen und dafür sorgen, dass eine einzige, holistische Ansicht auf das gesamte Netzwerk möglich ist.

SASE erhöht die Netzwerksicherheit erheblich und kann bei richtiger Implementierung mit minimalen Auswirkungen auf die Endbenutzer eingeführt werden. Die SASE-Optionen bieten IT-Mitarbeitern eine vollständige Verwaltung und Transparenz, die über die Netzwerke und Zwecke des Unternehmens mehr als nur den Zugriff jedes einzelnen Benutzers ermöglicht. Die integrierte und fortlaufende Inspektion und Bewertung des Datenverkehrs in Verbindung mit der dynamischen Durchsetzung von Sicherheitsplänen macht SASE zu einem die Erholung verändernden Mittel für digitale Transformationsinitiativen.

FAZIT

IN ZERO TRUST WE TRUST?

Klar ist, dass Anwendungen und Prozesse heute netzwerkübergreifend kommunizieren müssen. Die entsprechende Öffnung von IT-Umgebungen hat aus Cyber-Security-Sicht jedoch zu einer deutlichen Zunahme von Angriffsflächen geführt. In Summe gilt es einerseits, die Workflows nicht auszubremsen, andererseits müssen sowohl externe als auch interne Gefahren gebannt werden. Zero Trust ist hier nicht das Allheilmittel. Vielmehr können die einzelnen Bausteine einer Zero Trust Architektur in umfassenden Cyber-Security-Konzepten eingesetzt werden um die Sicherheit des Unternehmens zu verbessern. Vor allem sind die ZTA Bausteine auch in der Lage, das gesamte Sicherheitsbewusstsein einer Organisation nachhaltig zu schärfen.

Sie möchten mehr über die Ausgestaltung individueller Zero Trust Architekturen erfahren? Dann nehmen Sie gerne Kontakt mit uns auf!

E-Mail: info-itsecurity@axians.de

06/2022

Axians IT Security GmbH · Christoph-Probst-Weg 27 · 20251 Hamburg
Tel.: +49 40 271661-0 · Fax: +49 40 271661-44
E-Mail: info-itsecurity@axians.de · www.axians.de