Zero Trust-Architektur

Bei der traditionellen Netzwerksicherheit unterscheidet man zwischen zwei Arten von Netzwerken: Das Netzwerk, dem ich vertraue und das Netzwerk, dem ich nicht vertraue.

Der Begriff Netzwerk bezeichnet dabei zum einen ein lokales LAN und zum anderen das Internet. Dazwischen befindet sich der Großteil der Sicherheitskomponenten. Sie bilden eine möglichst große Mauer, die Angriffe verhindern soll. Dieses Modell verliert jedoch an Wirkung, sobald der Netzwerkaufbau komplizierter wird. In Zeiten von Internet-of-Things und Cloud Computing verschwimmt die Grenze zwischen externen und internen Netzwerken.

Mobile Mitarbeiterinnen und Mitarbeiter müssen außerhalb des lokalen LANs mit Hilfe anderer Ressourcen auf das Netzwerk zugreifen. IT-Dienstleister brauchen ebenfalls Remotezugriff, aber beschränkt auf wenige Services. Für Angreifer öffnen sich dadurch viele neue Türen, über die der initiale Eintritt stattfinden kann. Angreifern, die in das interne Netzwerk eindringen können, wird automatisch vertraut. Dieses Perimeter-Sicherheitsmodell, das für die Sicherheit am Übergang zwischen dem Unternehmensnetz und dem öffentlichen Netz sorgt, hat somit Schwachstellen.

Zahlreiche IT-Konzerne arbeiten an einem Ansatz, bei dem jeder User gleich behandelt und nur auf Basis von Anmeldeinformationen und Zugriffsregeln als vertrauenswürdig klassifiziert wird: Zero Trust.

Zero Trust setzt direkt bei den Ressourcen an. Keinem Gerät, Netzwerk oder User wird ohne Weiteres vertraut. Dieser Ansatz unterscheidet nicht mehr zwischen intern oder extern. Jede Anfrage wird evaluiert. Entscheidend bei der Evaluierung ist vor allem der Kontext der Anfrage.

Zero Trust macht an der Netzwerkgrenze keinen Halt. Auch Cloud-Applikationen und Third-Party-Dienste können nach demselben Schema behandelt werden. Zugriffe von außen, wie sie bei externen Mitarbeiterinnen und Mitarbeitern oder im Homeoffice auftreten, müssen nicht mehr gesondert behandelt werden.

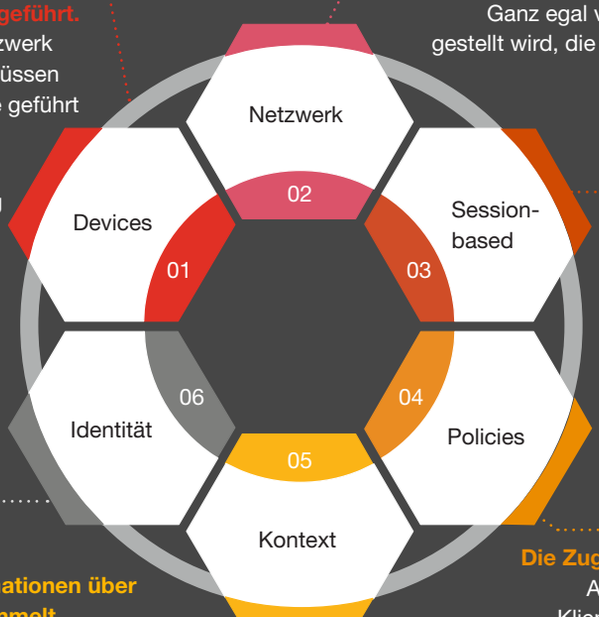
Ist Zero Trust auch etwas für Sie? In diesem Dokument wollen wir Ihnen die Grundsätze und Funktionalitäten von Zero Trust erstmals etwas näherbringen. Im Anschluss bieten wir gern unsere Unterstützung bei der Umsetzung an.

Grundsätze von Zero Trust

Alle Geräte, die einen Fußabdruck hinterlassen, werden als Ressource geführt.
Um Zugriffe auf das Unternehmensnetzwerk kontrollieren und steuern zu können, müssen alle Geräte vollumfassend in einer Liste geführt werden.

Schematische Neu-Authentifizierung und Neu-Autorisierung während einer aufrechten Kommunikation.
Eine neue Evaluierung der User-Identität kann mehrere Gründe als Ursache haben (z. B.: Zeitablauf der Session, Änderung der Ressource). Bei sensiblen Daten kann es notwendig sein, weitere Faktoren zur Authentifizierung miteinzubeziehen.

Es werden sämtliche Kontext-Informationen über Geräte und Kommunikationen gesammelt.
Mit den Daten werden Informationen über die Sicherheit-slage, den Netzwerkstatus und vieles mehr generiert. Sie helfen, das Netzwerk zu optimieren.



Jede Kommunikation im Netzwerk ist gleichwertig.
Ganz egal von wo eine Anfrage an eine Ressource gestellt wird, die Zugriffsregeln gelten für jede Anfrage – unabhängig von deren Herkunft.

Genehmigte Zugriffe betreffen ausschließlich eine Session.
Zugriffe werden auf Basis von Sessions vergeben. Ein Zugriff auf eine benachbarte Ressource erfordert eine neuerliche Genehmigung.

Die Zugriffsregeln gestalten sich dynamisch
Aktuelle Statusinformationen von Usern, Klienten, Applikationen und der Ressource, auf die zuge¬griffen wird, beeinflussen die Zugriffsregeln. Dazu kommen Verhaltensmuster und Umgebungseigenschaften.

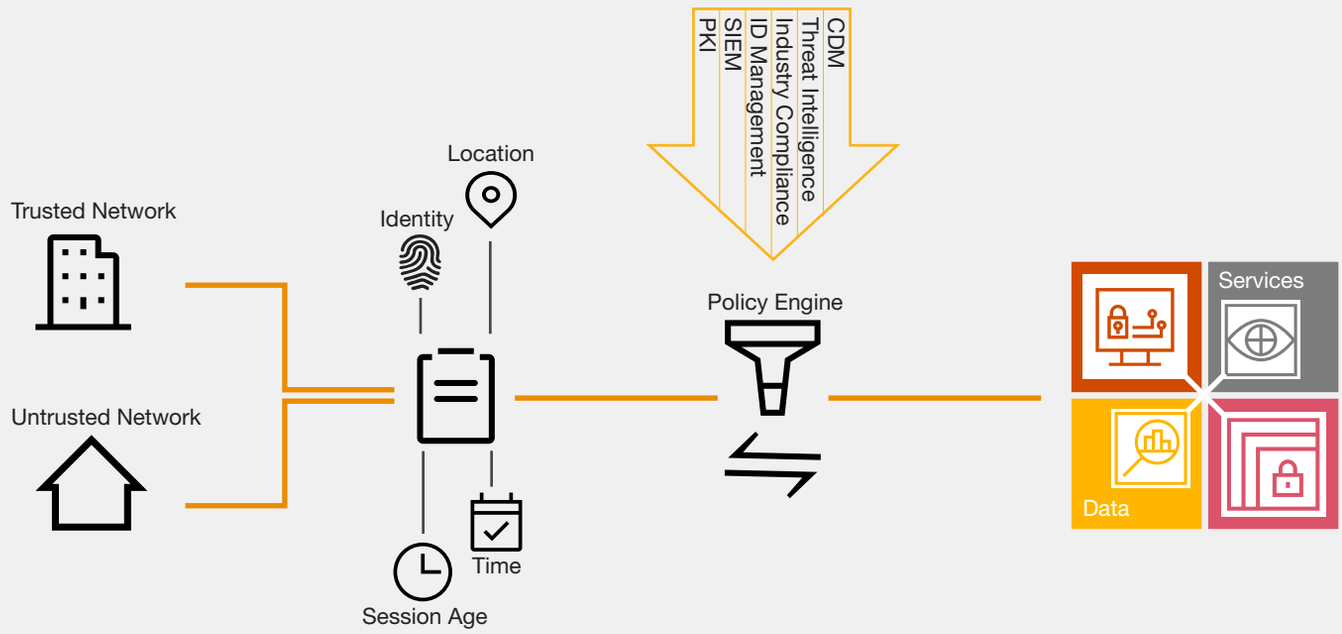
Central Policy Engine

Alle Anfragen kommen an einem zentralen Punkt zusammen, von wo aus sie evaluiert werden. Für den User macht es keinen Unterschied, ob er sich im internen oder in einem öffentlichen Netzwerk befindet. Der Anmeldevorgang ist für ihn vollkommen transparent und überall gleich.

Zusätzlich zu den Informationen, wer worauf zugreifen will, werden der Anfrage Kontextinformationen (z. B. Standort, Zugriffszeit, Session) hinzugefügt. Diese Informationen werden später bei der Entscheidungsfindung benötigt und sind maßgeblich für den Erfolg der Anfrage.

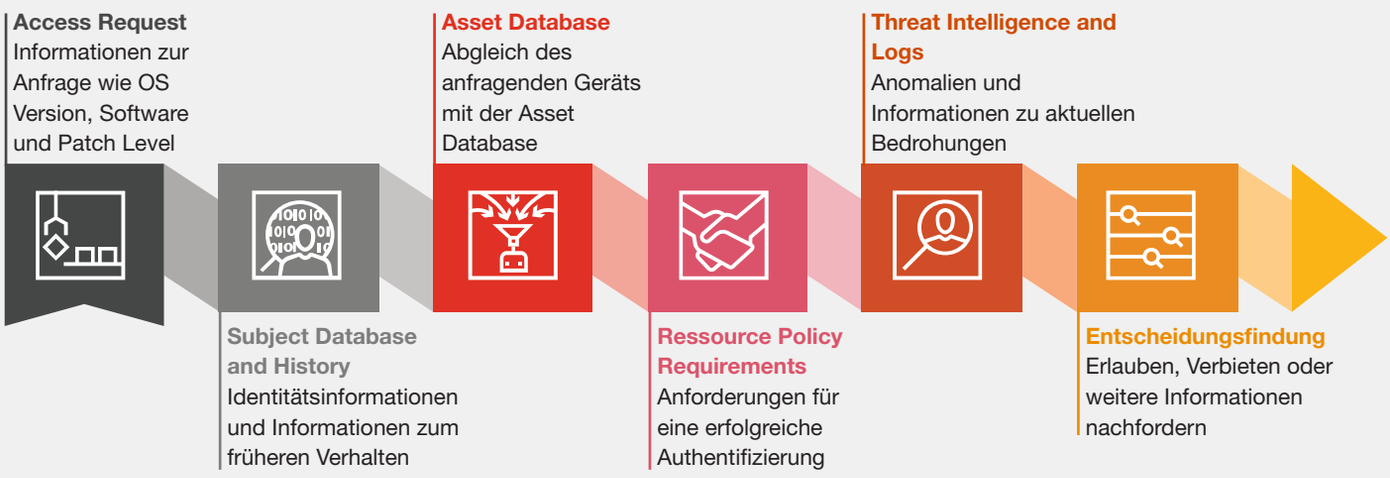
Die zentrale Access Control Einheit übernimmt die Anfrage anschließend. Ihr hinterlegt sind verschiedene Policies, die den Zugriff regeln. Sie sind dynamisch und von vielen Einflussfaktoren abhängig. Der gesamte Prozess läuft im Hintergrund. Benutzerinnen und Benutzern wird nur das Ergebnis präsentiert: Zugriff gewährt, Zugriff verweigert oder die anfragende Identität wird aufgefordert, sich weiter zu authentifizieren.

Nach erfolgreicher Authentifizierung und Autorisierung kann man auf die Ressource zugreifen. Im Falle eines Session-Timeouts oder dem Wechsel der Ressource wiederholt sich der Prozess. Das reduziert die Wahrscheinlichkeit, dass sich Angreifer unbemerkt im Netzwerk bewegen können.



Der Zero Trust-Algorithmus (ZTA)

Für ein Unternehmen mit ZTA-Einsatz kann man sich die Policy Engine als Gehirn vorstellen. Der Trust-Algorithmus der Policy Engine ist in diesem Beispiel der primäre Denkprozess. Der Trust-Algorithmus ist jener Prozess, den die Policy Engine verwendet, um den Zugang zu einer Ressource zu gewähren oder zu verweigern. Die Policy Engine nimmt Eingaben aus mehreren Quellen entgegen. Dazu zählen die Policy Datenbank mit beobachtbaren Informationen über das zugreifende Objekt, über Objektattribute und Rollen, historische Verhaltensmuster des Objekts, Quellen für Bedrohungsinformationen und andere Metadatenquellen. Die Einflussfaktoren lassen sich folgendermaßen gruppieren:



Der Weg zu Zero Trust

Viele Unternehmen zögern, den ZTA zu implementieren. Sie fürchten es koste viel Zeit und Geld, die klassische Netzwerkarchitektur in den Zero-Trust-Ansatz zu überführen. Allerdings müssen Sie die alte Infrastruktur bei der Implementierung nicht ersetzen. Sie können Zero Trust parallel zum bestehenden Netzwerk aufbauen. Letzteres bildet dabei die Basis des neuen Zero-Trust-Konzepts. Schritt für Schritt bauen Sie neue Netzwerksegmente ein, für die Sie eigene Zugriffsregeln erstellen. Anschließend verlagern Sie das gewünschte Asset in das neue Segment und planen die nächste Ressource. So wird der Einsatz von Zero-Trust-Netzwerken verwaltbar, kostengünstig und unterbrechungsfrei. Die Überführung des Unternehmensnetzwerkes lässt sich in fünf Schritten zusammenfassen.

1

Define Your Project Surface
Bei der Definition der schützenswerten Assets müssen alle kritischen Daten, Anwendungen, Assets oder Services (DAAS) identifiziert und klassifiziert werden.

2

Map the Transaction Flows
Das Scannen und Abbilden der Datenströme im Netzwerk ist essenziell um zu verstehen, wie verschiedene DAAS-Komponenten mit anderen Ressourcen im Netzwerk interagieren.

3

Architect a Zero Trust Network
Die zu schützende Oberfläche und die ermittelten Kommunikationswege geben bereits ein genaues Bild ab. Nun muss das Netzwerk entsprechend der ermittelten Informationen segmentiert werden.

4

Create the Zero Trust Policy
Als nächstes müssen die Zugriffs-Policies erstellt werden. Zu definieren ist dabei: Wer? Auf was für ein Gerät? Wann? Worauf wird zugegriffen? Warum darf zugegriffen werden? Wie darf zugegriffen werden?

5

Monitor and Maintain the Network
Der letzte Schritt ist die Überwachung und Wartung des Netzwerks im Hinblick auf operative Aspekte von Zero Trust. Dabei werden alle internen und externen Protokolle kontinuierlich betrachtet.

Wir von PwC helfen Ihnen

Sie sind unsicher, ob Zero Trust die geeignete Architektur für Sie ist? Gern analysieren wir Ihre persönliche Ausgangslage. Gemeinsam passen wir den Weg zu einem Zero-Trust-Netzwerk individuell auf Ihr Unternehmen an und begleiten Sie in jeder Phase der Umsetzung.

Sobald der erste Schritt in Richtung Zero-Trust-Architektur gesetzt ist, beginnen wir mit der Auswertung und arbeiten daran, das Konzept kontinuierlich zu verbessern. So profitieren Sie bestmöglich von Zero Trust.

Weitere Leistungen

1 Hilfe beim Identifizieren und Analysieren von kritischen und sensiblen Unternehmenswerten.

2 Definieren und Klassifizieren von Daten

3 Guidelines für die Einführung einer Zero-Trust-Architektur im Unternehmen

4 Compliance-Monitoring-as-a-Service oder Hilfestellungen für das Unternehmen beim Überwachen

Ihre Ansprechpartner

Georg Beham
Partner
Cybersecurity & Privacy
Tel.: +43 732 611 750 19
georg.beham@pwc.com

Markus Sojer
Senior Manager
Cybersecurity & Privacy
Mobil +43 676 8337 79824
markus.sojer@pwc.com

Florian Brunner
Senior Manager
Cybersecurity & Privacy
Tel.: +43 676 8337 75455
florian.brunner@pwc.com

PwC Österreich
Donau-City-Str. 7
1220 Wien

www.pwc.at