Zero Trust Security

Durch Misstrauen eine vertrauenswürdige Kommunikation garantieren

Bisher entschied die Grenze des Unternehmensnetzwerks über die Vertrauenswürdigkeit eines Zugriffs. Allerdings wandern Anwendungen zunehmend in die Cloud und Anwender setzen vermehrt eigene Geräte ein. Zero Trust Security verspricht einen sicheren, validierten Zugriff auf sämtliche Anwendungen und Ressourcen.

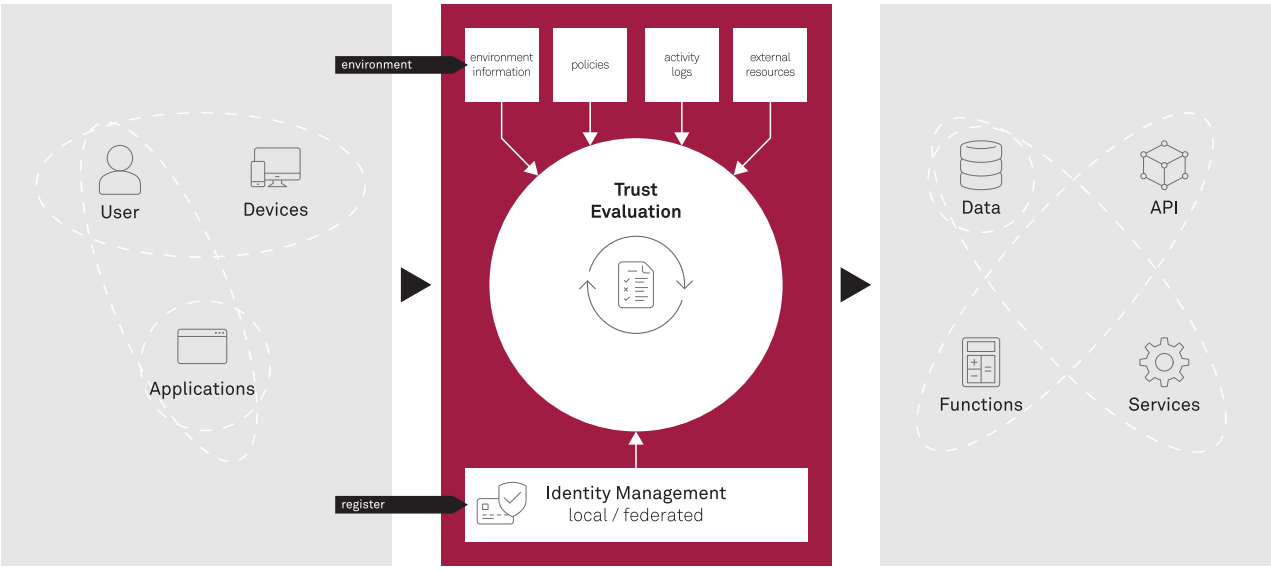
Definition

Zero Trust Security folgt dem Ansatz "newer trust - always verify". Der Ansatz legt fest, dass es Subjects und Assets gibt, die auf beliebige Unternehmensressourcen zugreifen wollen. Subjects sind Personen oder Personengruppen, Assets sind Anwendungen oder Geräte - aber auch Kombinationen aus diesen. Unternehmensressourcen können Daten, Anwendungen, APIs oder Funktionen sein. Der Zugriff der Subjects und Assets erfolgt nie direkt, sondern stets über einen Trust Broker. Dieser prüft, ob das Subject oder Asset berechtigt ist, die definierten Sicherheitsanforderungen erfüllt sind, und entscheidet über die Zulässigkeit des Zugriffs. Der als Trust-Evaluation-Prozess ist dynamisch und wird mit jeder neuen Anfrage erneut durchlaufen.

Die Trust Evaluation zieht verschiedene Informationsquellen heran. Klassische Policies beschreiben in statischer Weise die Zugriffsberechtigungen von Subjects und Assets auf Unternehmensressourcen. Segmentierung teilt Subjects, Assets, Unternehmensressourcen, Anwendungsklassen, Netzwerksegmente und Datencluster in mitunter sehr feingranulare und hochvariable Gruppen auf. Basierend auf diesen Segmenten lassen sich wiederum Policies definieren.

Weitere Quellen für die Trust Evaluation sind Activity Logs, die Daten über Häufigkeiten, Zeitpunkte und transferierte Informationen sammeln. Verhaltensbasierte Modelle können dann untypische Zugriffe identifizieren. Auch Datenbanken mit bekannten Schwachstellen bezieht Trust-Evaluation-Prozess mit ein. Schlussendlich geben auch noch Environment Information Auskunft darüber, wo sich Subjects und Assets während des Aufrufs befinden, welche anderen Programme auf dem Asset laufen oder ob bestimmte Nutzungsrichtlinien eingehalten werden.

Voraussetzung dafür ist eine zuverlässige Identifikation und Authentifizierung von Assets und Subjects. Als Identitäten gelten Anwender, Geräte und Anwendungen. Das Identity Management ist somit eine zentrale Säule.



Subject / Asset | Trust Broker | Enterprise Resource

Risiken im Cloud-Stack

- Anwendungen laufen in der Cloud
- externer Anbieter kontrolliert Cloud-Umgebung
- Zugriff erfolgt über das Internet

Geräte-Identitäten und Lifecycle

- suspekte Geräte
- mobiles Internet
- große Anzahl neuer, unbekannter Geräte

ZTR

Heterogene Benutzer-Identitäten

- externe Verwaltung von Benutzer-Identitäten, etwa "Login with ..."
- Identitätsnachweis durch MFA

Verhaltensbasierte Maßnahmen

- Sammeln von Verhaltens- und Umgebungsdaten
- Datenbanken mit bekannten Angriffsvektoren

Referenzszenario

Einige der Anwendungen eines Unternehmens sind in die Cloud gewandert, weitere könnten folgen. Mitarbeiter dürfen bereits ihre eigenen Geräte einsetzen - und autonome Clients sollen Zugriff auf Unternehmensressourcen erhalten. Ferner greifen Anwender mitunter von außerhalb auf die abgesicherte Unternehmensumgebung zu.

Das Unternehmen kann die Zugriffe nicht mehr auf Basis allgemeinen Vertrauens regeln und muss per se von Missbrauch ausgehen. Auf Basis von Zero Trust Security validiert das Unternehmen nun jedes einzelnen Zugriffs und verwaltet sämtliche Identitäten zentral.

Potenzial

Die Sicherheit der eigenen Ressourcen stellt für jedes Unternehmen ein existenzielles Risiko dar. An Zero Trust Security führt deshalb kein Weg mehr vorbei.

Zugleich birgt der Einsatz einer Zero-Trust-Infrastruktur auch das Potenzial, anderen Unternehmen die eigenen Unternehmensressourcen als abgesicherte Services bereitzustellen, somit neue Märkte zu erschließen, Geschäftsbeziehungen aufzubauen und Chancen zu ergreifen.

Reifegrad

Längst haben sich verschiedene Zero-Trust-Lösungen am Markt etabliert. Die größte Herausforderung für Unternehmen ist es, diese Lösungen anzuwenden, weil sie tief in die Infrastruktur integriert werden müssen. Analysten empfehlen, auf eine einzelne fertige Lösung zu setzen und diese konsequent unternehmensweit einzuführen.

Marktübersicht

Der Markt identifiziert zwei Klassen von Zero-Trust-Lösungen. Zero-Trust-as-a-Service stellt die zentralen Komponenten wie Trust Evaluation in der Cloud bereit. Dem gegenüber finden sich Stand-alone-Lösungen, die ein Unternehmen selbst betreiben kann.

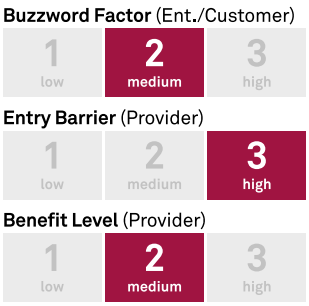
Die Anbieter solcher Lösungen stammen vor allem aus dem Bereich der Netzwerkdomäne, etwa Cisco und Akamai, aber auch Okta als Anbieter einer Identity-Management-Lösung. Dazu gesellen sich die großen Cloud-Anbieter wie Microsoft, Google und Amazon.

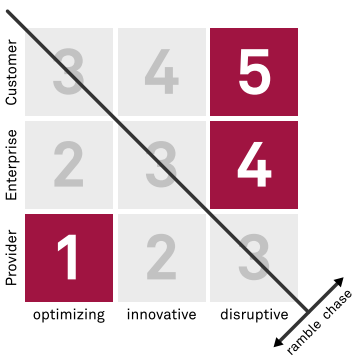
Alternativen

Netzwerksegmentierungen in Form von Demilitarized Zones (DMZ), der Einsatz von auf Reverse Proxys basierenden Firewalls, die Ausweitung des Perimeters mittels VPN, aber auch Absicherungstechniken wie API-Gateways oder Content-Delivery-Netzwerke sind Einzelmaßnahmen, die sich ebenso im Zero-Trust-Ansatz wiederfinden.

Fazit

- \+ Benutzer-, Geräte- und ortsunabhängige Sicherheit
- \+ temporäre, minimale Berechtigung
- \+ dynamische Berechtigungsprüfung
- \+ einheitliche technologieübergreifende Berechtigungsprüfung
- \- Trust Broker ist Ausfallpunkt
- \- Trust Broker ist Angriffsziel
- \- komplexe Administration
- \- für Anwender und Betrieb potenziell intransparente Berechtigungen





https://msg.direct/techrefresh

Stand: Dezember 2021

msg systems ag

Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113 | www.msg.group | info@msg.group