Sieben Bestandteile einer hochgradig erfolgreichen Zero-Trust-Architektur

Die Zscaler Zero Trust Exchange: Leitfaden für Architekten

Herkömmliche Sicherheitsarchitekturen gewährleisten keinen ausreichenden Schutz mehr

Die bisher gängigen Sicherheitsansätze mit Firewalls und VPNs gewähren den Usern Zugang zum Netzwerk. Damit werden User, Geräte und Workloads anfällig für Angriffe und Infektionen. Zudem können sich Angreifer nach einer Sicherheitsverletzung ungehindert lateral im Netzwerk bewegen und dadurch lukrative Angriffsziele erreichen sowie vertrauliche Daten extrahieren.

Hybride Arbeitsumgebungen lassen sich nur mit Zero-Trust-Ansatz zuverlässig absichern

Innovativ denkende Führungskräfte, die heute und morgen zuverlässigen Schutz für ihre Organisation gewährleisten wollen, setzen auf Zero Trust. Dieser ganzheitliche Sicherheitsansatz basiert auf dem Prinzip der minimalen Rechtevergabe und dem Grundsatz, dass kein User und keine Anwendung automatisch als vertrauenswürdig eingestuft werden darf.

Empfehlungen zur Implementierung einer Zero-Trust-Architektur:

Die **Zscaler Zero Trust Exchange** gewährleistet eine konsequente Umsetzung des Zero-Trust-Konzepts. Die integrierte Cloud-native Plattform verbindet User, Geräte (IoT/Betriebstechnologie) und Workloads direkt mit Anwendungen, ohne ihnen jemals Zugang zum Netzwerk zu gestatten.

Sieben Bestandteile einer Zero-Trust-Architektur

Mit diesem branchenweit einzigartigen Ansatz minimiert Zscaler die Angriffsfläche, verhindert die laterale Ausbreitung von Bedrohungen und schützt das Unternehmen vor Infektionen und Datenverlusten.

1. Wer wird verbunden?

Die angeforderte Verbindung wird beendet und zunächst die Identität des Initiators (User, IoT/Betriebstechnologie, Workload) verifiziert.

2. In welchem Kontext wird der Zugriff angefordert?

Der Kontext des Initiators wird unter Berücksichtigung verschiedener Attribute (Rolle, Aufgabenbereich, Uhrzeit und Umstände der Verbindungsanforderung) validiert.

3. Wohin geht die Verbindung?

Es wird bestätigt, dass das Verbindungsziel bekannt ist, ausreichende Informationen dazu vorliegen und eine kontextbezogene Kategorisierung der Zugriffsanforderung möglich ist. Wenn das Verbindungsziel unbekannt ist, muss die Anfrage zur weiteren Analyse gekennzeichnet werden.

4. Bewertung von Risiken

Mithilfe von KI wird unter Berücksichtigung unterschiedlicher Faktoren (Gerätestatus, Bedrohungslage, Verbindungsziel, Verhalten und Richtlinien) ein dynamischer Risk Score für die angeforderte Verbindung berechnet.

5. Verhindern von Sicherheitsverletzungen

Zur Erkennung und Blockierung schädlicher Inhalte werden Traffic und Inhalte einer Inline-Überprüfung unterzogen.

6. Verhindern von Datenverlusten

Durch Überprüfung des gesamten ausgehenden Traffics werden vertrauliche Daten zuverlässig erkannt und ihre Exfiltration verhindert.

7. Durchsetzen von Richtlinien

Richtlinien werden sitzungsbasiert durchgesetzt, um bedingt über die angeforderte Verbindung zu entscheiden. Wenn die Kriterien für eine Zulassung erfüllt sind, wird eine sichere Verbindung zum Internet bzw. einer SaaS-basierten oder internen Anwendung hergestellt.

Unternehmen, die diese sieben grundlegenden Bestandteile einer Zero-Trust-Architektur konsequent umsetzen, **minimieren ihre Angriffsfläche, verhindern die laterale Ausbreitung von Bedrohungen** und **schützen sich vor Sicherheitsverletzungen und Datenverlusten.**

E-Book lesen

Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA
+1 408 533 0288
www.zscaler.de