Was ist echtes Zero Trust?

Immer mehr Unternehmen stellen zur Beschleunigung ihrer sicheren digitalen Transformation auf Zero-Trust-Architekturen um.
Es ist aber nicht immer einfach, sich bei den „Zero Trust"-Lösungen zurechtzufinden.
Wer bei dem Angebot an echten und vermeintlichen Zero-Trust-Lösungen den Überblick behalten will, muss wissen, woran man den Unterschied erkennt.

Echtes Zero Trust

SO NICHT

Die Lösung setzt perimeterbasierte Firewalls und VPNs ein, um ein flaches Netzwerk auf Remote-User auszuweiten, und vergrößert dadurch die Angriffsfläche des Unternehmens.

Implizites Vertrauen

Bekannte User, Anwendungen und Geräte werden als vertrauenswürdig eingestuft

Zugang der User zum Netzwerk

Der Traffic von Usern und Anwendungen wird über ein routingfähiges Netzwerk mit lateraler Bewegungsfreiheit geleitet

Passthrough Traffic erlaubt

Verschlüsselter Traffic wird nicht auf Bedrohungen und vertrauliche Daten überprüft

SO GEHT'S

Die Lösung stuft prinzipiell alles als bösartig oder kompromittiert ein und genehmigt Zugriff nur aufgrund stringenter Sicherheitsmaßnahmen:

Verifizierung von Identität und Kontext

Die Verbindung wird getrennt, damit zunächst Identität und Kontext der Anfrage (Wer, was und wo) verifiziert werden können

Kontrolle von Inhalten und Zugriff

Die mit der Anforderung verbundenen Risiken werden bewertet und **der Traffic auf** Cyberbedrohungen und vertrauliche Daten überprüft

Sitzungsspezifische Entscheidung und Durchsetzung von Richtlinien

Richtlinien werden durchgesetzt, bevor Verbindungen zu internen oder externen Anwendungen hergestellt werden

So funktioniert One True Zero Trust:
Die Zscaler Zero Trust Exchange

Zero Trust ohne Kompromisse: Vertrauen Sie auf eine nahtlose, sichere und kosteneffiziente Zero-Trust-Architektur, damit Ihr Unternehmen die digitale Transformation zügig und souverän bewältigt.

Zum Whitepaper

Experience your world, secured.™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
USA
+1 408 533 0288
www.zscaler.de