Zero Trust:
Die Grundlage für sicheres Business Enablement

In einem neuen Report stellen IDC-Analysten Erkenntnisse zur weiteren Entwicklung von Zero Trust vor und erläutern die Konsequenzen für die Cybersicherheit von Unternehmen.

Die Bedrohungslage verschärft sich rapide.

80 % mehr Ransomware-Angriffe im vergangenen Jahr[1]

314 % mehr Angriffe über verschlüsselte Kanäle[2]

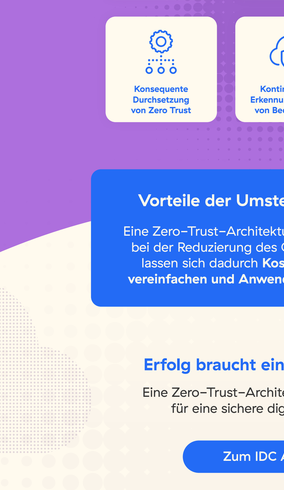
436 % mehr Phishing-Angriffe auf die Einzel- und Großhandelsbranche[3]

Perimeterbasierte Sicherheitsarchitekturen sind nicht mehr zeitgemäß.

Perimeterbasierte Sicherheitsarchitekturen wurden zum Schutz von Mitarbeitern entwickelt, die hauptsächlich am Standort der Organisation arbeiteten und auf Ressourcen im Rechenzentrum zugriffen.[4]

Hybride Arbeitskonzepte sind komplex und unübersichtlich.

Die User arbeiten an wechselnden Standorten und greifen mit unterschiedlichen Geräten auf Daten und Anwendungen in SaaS-Umgebungen, Rechenzentren und öffentlichen Clouds zu.



Die bisher gängigen Schutzmechanismen reichen nicht mehr aus.

Firewalls, virtuelle Firewalls, VPNs und andere perimeterbasierte Schutzmaßnahmen sind mit der Abwehr von dynamischen Bedrohungen und Advanced Persistent Threats überfordert.[4]

Unter heutigen Vorzeichen ist ein neuer Ansatz erforderlich.

Zur Bewältigung dieser Herausforderungen steigen immer mehr Unternehmen auf Zero Trust um. Im Unterschied zu perimeterbasierten Sicherheitsansätzen beruht das Zero-Trust-Konzept auf dem Prinzip der minimalen Rechtevergabe und dem Grundsatz, dass kein User und keine Anwendung automatisch als vertrauenswürdig eingestuft werden darf.

Zero Trust — die Grundlagen

Zero Trust ist keine Einzeltechnologie, sondern eine Strategie, auf der das gesamte Sicherheitsökosystem einer Organisation aufbauen sollte. IDC definiert sechs Kernelemente des Zero-Trust-Konzepts[4]:

- **Granulare Berechtigungen**
- **Robuste Identitätskontrolle und Authentifizierung**
- **Kontextbasierte Richtlinien**
- **Konsequente Durchsetzung von Zero Trust**
- **Kontinuierliche Erkennung/Abwehr von Bedrohungen**
- **Zugriff ausschließlich gemäß Erforderlichkeitsprinzip**

Vorteile der Umstellung auf Zero Trust

Eine Zero-Trust-Architektur unterstützt Organisationen bei der Reduzierung des Geschäftsrisikos. Außerdem lassen sich dadurch **Kosten senken, IT-Aufgaben vereinfachen und Anwendererfahrungen optimieren.**

Erfolg braucht ein solides Fundament

Eine Zero-Trust-Architektur bildet die Grundlage für eine sichere digitale Transformation.

Zum IDC Analyst Brief

[1] Zscaler, ThreatLabz-Report zu Ransomware-Angriffen für 2022.
[2] Zscaler, ThreatLabz-Report zu Angriffen im verschlüsselten Traffic für 2021.
[3] Zscaler, ThreatLabz-Report zu Phishing-Angriffen für 2022.
[4] IDC Analyst Brief from Zscaler in Auftrag gegeben, „Implementing Zero Trust as a Foundation for Secure Business Enablement," Dokument # US49043922, April 2022.

© 2022 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™, Zero Trust Exchange™ sowie weitere unter zscaler.de/legal/ trademarks aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Markenzeichen sind Eigentum ihrer jeweiligen Inhaber.

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