Zero Trust Journey

Die zunehmende Verlagerung von Assets und Identitäten ausserhalb des Unternehmensnetzwerks erfordert strengere Überprüfungen. Traditionelle Sicherheitsstrategien wie das «Trusted Network» sind nicht mehr ausreichend, um fortgeschrittenen Angriffsmethoden entgegenzuwirken.

Warum brauchen Unternehmen Zero Trust?
Assets und Identitäten verlassen zunehmend das Unternehmensnetzwerk (BYOD, Homeoffice, Mobile & Cloud) und immer mehr interne und externe Benutzer haben Zugang zu den Unternehmensressourcen. Das erfordert Weisungen, Methoden und Applikationen für eine stringente, auditierbare Benutzer- und Berechtigungsprüfung. Zudem ermöglichen fortgeschrittene Angriffsmethoden Identitätsdiebstahl wie Phishing und Diebstahl von Zugangsdaten. Die «Trusted Network» Sicherheitsstrategie reicht somit nicht mehr aus, um das Unternehmensnetzwerk umfangreich zu schützen. Zero Trust bietet eine Sammlung von Konzepten und Ideen, um die Unsicherheit bei der Durchsetzung präziser Zugriffsentscheidungen mit den geringsten Rechten pro Anfrage in Informationssystemen und -diensten zu minimieren. Ziel ist es, durch Sicherheitsvorfälle verursachte Kosten zu senken und mögliche Reputationsschäden zu verhindern. Unser Security Consulting Team berät Ihr Unternehmen zur Führung und Umsetzung von Zero-Trust-Konzepten, um Ihre Infrastruktur und Ihr Business noch umfassender zu schützen. Mit unserer standardisierten Vorgehensweise zur Einführung einer Zero-Trust-Architektur führen wir Sie in Ihrem Tempo zur erforderlichen Maturität.

Ihr Nutzen einer Zero-Trust-Beratung

Erstellung der Roadmap und des Migrationsplans

Eine Roadmap und ein Migrationsplan mit strategischen Zero-Trust-Projekten werden von unseren Expert*innen erarbeitet. ✓

Höhere Sicherheit – Erhöhung der Resilienz

Bei konsequenter Umsetzung von Zero-Trust-Konzepten werden Angriffe abgewehrt, eingegrenzt oder früher erkannt. ✓

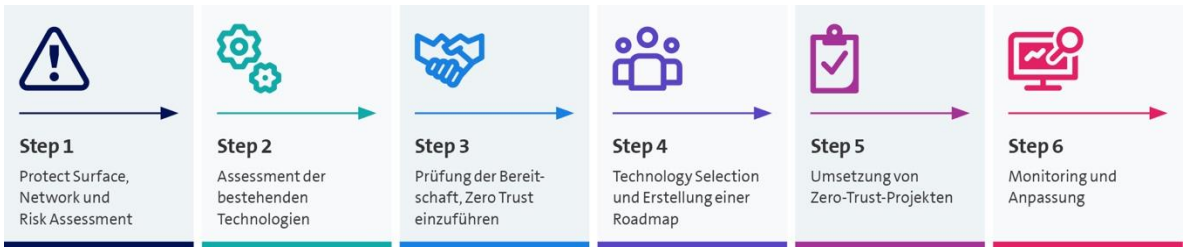
Awareness für Compliance und regulatorische Anforderungen

Unterstützung bei der Weiterentwicklung der Governance zur Führung von Zero-Trust-Projekten. ✓

Maturitätsassessments

Die kulturelle und technische Maturität Ihres Unternehmens wird erhoben und der notwendige Maturitätsgrad bestimmt. ✓

Beratungsansatz zur Einführung einer Zero-Trust-Architektur



swisscom

Facts & Figures

Assessment & Workshops

- Kundenworkshops – Bestimmung des notwendigen Maturitätsgrads
- Maturitäts- und Technische Assessments
  - Identifizierung der wichtigsten und wertvollsten Daten, Assets, Apps und Services
  - Identifizierung der wichtigsten Risiken und des regulatorischen Geltungsbereichs
  - Identifizierung von Identitäts- und Netzwerklösungen für Endbenutzer und DC
- Roadmap mit strategischen Zero-Trust-Projekten
- Erarbeitung einer Roadmap mit strategischen Zero-Trust-Projekten
- Migrationsplan hin zur Zero-Trust-Referenzarchitektur

Awareness

- Cultural Awareness: Auswirkungen von Zero Trust auf die bestehende Unternehmenskultur
  - Bereitschaft zur Einführung eines ZT-Sicherheitsframeworks auf Basis kritischer Ressourcen, Schlüsselrisiken, vorhandener Technologien und kultureller Aspekte
- Konzeption/Implementierung von Sensibilisierungskampagnen im Bereich Informationssicherheit:
  - Durchführung von Security-Awareness-Schulungen
  - Planung & Implementation von Phishing-Kampagnen

Projektbezogene und organisatorische Unterstützung

- Unterstützung bei der Weiterentwicklung der Governance zur Führung von Zero-Trust-Projekten und der ganzen Zero Trust Adoption (Zero Trust Journey)
- Weiterentwicklung der Security-Organisation anhand der Geschäftsbedürfnisse

Mehr Informationen und den Kontakt zu unseren Experten finden Sie auf swisscom.ch/security-consulting

Swisscom (Schweiz) AG Enterprise Customers, Postfach, CH-3050 Bern, Tel. 0800 800 900, www.swisscom.ch/enterprise