



Holger Reibold

Zero Trust Roadmap

Wie Sie implizites Vertrauen
eliminieren und jeden
Zugriff verifizieren

BRAIN-MEDIA.DE

12-Monats-Roadmap

Eine 12-Monats-Roadmap dient als pragmatischer Einstieg in Zero Trust. Ziel ist es, innerhalb eines Jahres messbare Sicherheitsverbesserungen zu erzielen, gleichzeitig eine tragfähige Grundlage für die weitere Transformation zu schaffen. Der Fokus liegt auf klar abgegrenzten Maßnahmen mit hoher Wirkung und überschaubarer Komplexität.

Monat 0–3: Transparenz und Fundament schaffen. In der initialen Phase steht die Analyse und Konsolidierung im Vordergrund.

- Durchführung einer Reifegradanalyse
- Identifikation kritischer Anwendungen und Zugriffe
- Konsolidierung von Identitäten und Verzeichnissen
- Einführung oder Erweiterung von Multi-Faktor-Authentifizierung
- Definition erster zentraler Sicherheitsrichtlinien

Ziel dieser Phase ist es, Transparenz zu schaffen und eine zentrale Steuerungsbasis aufzubauen.

Monat 3–6: Erste Use Cases umsetzen. Es folgt die Umsetzung konkreter Pilotprojekte.

- Einführung von ZTNA für ausgewählte Anwendungen
- Absicherung externer Zugriffe (Ablösung erster VPN-Szenarien)
- Schutz privilegierter Konten (z. B. Just-in-Time-Zugriffe)
- Erste Integration von Endpoint-Signalen (z. B. Gerätezustand)

Diese Phase liefert sichtbare Ergebnisse und erhöht die Akzeptanz im Unternehmen.

Monat 6–9: Integration und Skalierung starten. Die erfolgreich getesteten Ansätze werden erweitert.

- Ausweitung von ZTNA auf weitere Anwendungen
- Integration von Identity, Endpoint und Zugriffskontrolle
- Aufbau zentraler Telemetrie (Logs, Events, Monitoring)
- Erste Schritte in Richtung Mikrosegmentierung

Ziel ist es, isolierte Maßnahmen zu verbinden und erste architektonische Konsistenz zu erreichen.

Monat 9–12: Standardisierung und Governance festigen. In der letzten Phase des ersten Jahres wird die Grundlage stabilisiert.

- Etablierung zentraler Policy- und Entscheidungslogik
- Standardisierung von Zugriffsmodellen
- Integration von Telemetrie in Entscheidungsprozesse
- Aufbau von Governance-Strukturen und Reporting
- Definition der nächsten Transformationsphase (12–24 Monate)

Am Ende dieser Phase existiert ein belastbares Fundament für eine skalierbare Zero-Trust-Architektur.

Meilensteine und Abhängigkeiten

Eine erfolgreiche Roadmap hängt nicht nur von einzelnen Maßnahmen ab, sondern von deren richtiger Reihenfolge und Verzahnung. Bestimmte Fähigkeiten sind Voraussetzungen für nachgelagerte Schritte. Die zentralen Meilensteine sind.

- Zentrale Identitätsbasis etabliert
- Erste Anwendungen über ZTNA abgesichert
- Endpoint-Signale integriert
- Zentrale Telemetrie verfügbar
- Policy-Framework definiert und umgesetzt

Kritische Abhängigkeiten

- Identity vor Zugriff: Ohne zentrale Identitätsverwaltung sind konsistente Zugriffskontrollen nicht möglich. IAM ist die Grundlage für ZTNA, Mikrosegmentierung und datenbasierte Policies.
- Telemetrie vor Intelligenz: Ohne ausreichende Datenbasis können keine belastbaren Entscheidungen getroffen werden. AI und Signal-Intelligenz setzen qualitativ hochwertige Telemetrie voraus.
- Integration vor Automatisierung: Automatisierte Entscheidungen erfordern integrierte Systeme. Isolierte Tools verhindern konsistente Steuerung.
- Governance vor Skalierung: Ohne klare Richtlinien und Verantwortlichkeiten führt Skalierung zu Inkonsistenz und erhöhtem Risiko.

- Einordnung. Die 12-Monats-Roadmap ist bewusst pragmatisch angelegt. Sie priorisiert schnelle Erfolge, ohne die langfristige Zielarchitektur aus den Augen zu verlieren. Entscheidend ist nicht die vollständige Umsetzung von Zero Trust, sondern die Etablierung eines stabilen Fundaments.

Organisationen, die diese Phase erfolgreich abschließen, verfügen über einen zentrale Steuerungsmechanismen, erste integrierte Sicherheitskomponenten, messbare Fortschritte und eine klare Basis für die weitere Transformation. Damit wird Zero Trust von einer Vision zu einem operativ steuerbaren Programm.

Mehr zum Thema: die Zero Trust Roadmap

 [Jetzt bei Amazon bestellen](#)