Zero Trust mit Microsoft Entra

Workshop – Identität, Zugriff und Risiko in einem Modell zusammenführen

2 Tage	Fortgeschritten	Deutsch
Kursdauer (16 UE)	Niveau	Sprache

Inhalts-Kurzbeschreibung

Zero Trust ist kein Produkt, sondern ein Entscheidungsmodell für Zugriffe: „Never trust, always verify“. Dieser Workshop baut auf bewährten Entra-ID-Grundlagen auf, fokussiert aber konsequent auf die Zero-Trust-Prinzipien: Conditional Access als Policy-Engine, Identity Protection zur Risikobewertung, Continuous Access Evaluation zur Echtzeit-Durchsetzung sowie Zugriffskontrolle für Geräte und Apps. Praxisnah statt theoretisch – am Ende steht ein konkreter Rollout-Fahrplan für den eigenen Tenant.

Zielgruppe

IT-Verantwortliche, Security-Architekten sowie Identity- und Cloud-Administratoren, die Zero Trust nicht nur als Folie, sondern als konkrete Tenant-Konfiguration umsetzen wollen.

Voraussetzungen

Grundkenntnisse Microsoft Entra ID (z. B. AZ-104- oder MS-100-Niveau) · Basiswissen Conditional Access von Vorteil, aber nicht zwingend.

Kurz-Agenda (Modul-Übersicht)

Modul	Schwerpunkt	Kerninhalte (Auszug)
M1	**Zero-Trust-Prinzipien**	Never trust always verify · Vertrauensmodell · Angriffsfläche · Bezug zur Microsoft-Referenzarchitektur
M2	**Identität als Kontrollpunkt**	Conditional-Access-Policy-Design · Authentication Strength · Named Locations · Sign-in Frequency
M3	**Risikobasierte Zugriffssteuerung**	Identity Protection · User-/Sign-in-Risk-Policies · Continuous Access Evaluation
M4	**Geräte und Apps**	Compliance-Policies · App-Schutzrichtlinien · Managed- vs. Unmanaged-Geräte-Zugriff
M5	**Monitoring & Nachweis**	Access Reviews · Sign-in-Logs · Secure Score als Zero-Trust-Reifegradmesser

Lernziele – nach diesem Kurs können Teilnehmer …

- eine Conditional-Access-Strategie nach Zero-Trust-Prinzipien entwerfen.
- Risikosignale aus Identity Protection in Zugriffsentscheidungen einbinden.
- Geräte- und App-Konformität als Zugriffsvoraussetzung konfigurieren.
- den Zero-Trust-Reifegrad des eigenen Tenants mit Secure Score einschätzen.

Format & Methodik

2 Tage à 8 Unterrichtseinheiten · Live-Demos im Entra-Tenant des Trainers und/oder Kunden-Sandbox · Teilnehmer erhalten PDF-Folien sowie eine Checkliste „Zero-Trust-Rollout in 5 Schritten“. Inhouse, Online-Live (Microsoft Teams) oder Hybrid buchbar.

Trainer & Buchung

Thomas Drilling – IT-Trainer & Berater, Microsoft Certified Trainer (MCT) und Fachautor mit über 25 Jahren Erfahrung in IT-Infrastruktur, Cloud Computing und Identity-Themen. Autor zahlreicher Fachbeiträge, u.a. bei iX, c't und Heise sowie regelmäßiger Gastautor bei WindowsPro. Schulungs-Schwerpunkte: Microsoft Azure, Microsoft Entra ID, Microsoft 365, Cloud-Architektur, Security.

Kontakt & Buchung: info@drilling-it.de · www.cloudtrain.de
Formate: Inhouse vor Ort · Online-Live-Training via Microsoft Teams · Hybrid