| | |
|---|---|
| **Mögliche Trainingslösung:** | SALTZ-Seminar |
| **Seminarsprache:** | Englisch |
| **Dauer** | 4Tage |

## Übersicht

Dieser Kurs vermittelt IT-Sicherheitsexperten die Kenntnisse und Fähigkeiten, die zur Implementierung von Sicherheitskontrollen, zur Aufrechterhaltung der Sicherheitslage eines Unternehmens sowie zur Identifizierung und Behebung von Sicherheitslücken erforderlich sind. Dieser Kurs beinhaltet Sicherheit für Identität und Zugriff, Plattformschutz, Daten und Anwendungen sowie Sicherheitsvorgänge.

## Voraussetzungen

Um das Beste aus diesem Kurs herauszuholen, sollten Sie bewährte Sicherheitsmethoden und Sicherheitsanforderungen der Branche verstehen, z. B. gestaffelte Verteidigung, Zugriff mit geringsten Berechtigungen, rollenbasierte Zugriffskontrolle, Multi-Faktor-Authentifizierung, gemeinsame Verantwortung und Null-Vertrauens-Modell. sich mit Sicherheitsprotokollen wie VPN (Virtual Private Networks), IPSec (Internet Security Protocol), SSL (Secure Socket Layer), Festplatten- und Datenverschlüsselungsmethoden vertraut machen. Erfahrung in der Bereitstellung von Azure-Workloads haben. Dieser Kurs behandelt nicht die Grundlagen der Azure-Verwaltung, sondern der Kursinhalt baut auf diesem Wissen auf und vermittelt weitere sicherheitsspezifische Informationen. Erfahrung mit Windows- und Linux-Betriebssystemen und Skriptsprachen. Kurslabs können PowerShell und die CLI verwenden.

## Zielgruppe

Dieser Kurs richtet sich an Azure Security Engineers, die die zugehörige Zertifizierungsprüfung ablegen möchten oder bei ihrer täglichen Arbeit Sicherheitsaufgaben ausführen. Dieser Kurs ist auch für Ingenieure hilfreich, die sich auf die Bereitstellung von Sicherheit für Azure-basierte digitale Plattformen spezialisieren und eine wichtige Rolle beim Schutz der Daten eines Unternehmens spielen möchten.

## Erworbene Qualifikationen

- Implementieren Sie Governance-Unternehmesstrategien, einschließlich rollenbasierter Zugriffssteuerung, Azure-Richtlinien und Ressourcensperren.
- Implementieren Sie eine Azure AD-Infrastruktur mit Benutzern, Gruppen und Multi-Faktor-Authentifizierung.
- Implementieren Sie den Azure AD-Identitätsschutz, einschließlich Risikorichtlinien, bedingtem Zugriff und Zugriffsüberprüfungen.

## Agenda

**Modul 1: Identität und Zugriff verwalten**

Dieses Modul behandelt Azure Active Directory, Azure Identity Protection, Unternehmensverwaltung, Azure AD PIM und hybride Identität.

**Lektionen**

- Azure Active Directory
- Azure-Identitätsschutz
- Unternehmensführung
- Implementierung von Azure AD Privilegiertes Identitätsmanagement
- Hybride Identität

- **Lab: Rollenbasierte Zugriffskontrolle**

- **Lab: Azure-Richtlinie**
- **Lab: Ressourcenmanagersperren**
- **Lab: MFA, bedingter Zugriff und AAD-Identitätsschutz**
- **Lab: Azure AD Privilegiertes Identitätsmanagement**
- **Lab: Directory Synchronisation implementieren**

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Governance-Unternehmesstrategien, einschließlich rollenbasierter Zugriffssteuerung, Azure-Richtlinien und Ressourcensperren.
- Implementieren Sie eine Azure AD-Infrastruktur mit Benutzern, Gruppen und Multi-Faktor-Authentifizierung.
- Implementieren Sie den Azure AD-Identitätsschutz, einschließlich Risikorichtlinien, bedingtem Zugriff und Zugriffsüberprüfungen.
- Implementieren Sie die Verwaltung privilegierter Azure AD-Identitäten, einschließlich Azure AD-Rollen und Azure-Ressourcen.
- Implementieren Sie Azure AD Connect einschließlich Authentifizierungsmethoden und lokaler Verzeichnissynchronisierung.

**Modul 2: Plattformschutz implementieren**

Dieses Modul behandelt die Perimeter-, Netzwerk-, Host- und Containersicherheit.

**Lektionen**

- Sicherheitsumfang
- Netzwerksicherheit
- Host-Sicherheit
- Container-Sicherheit

- **Lab: Netzwerksicherheitsgruppen und Anwendungssicherheitsgruppen**
- **Lab: Azure Firewall**
- **Lab: Konfigurieren und Sichern von ACR und AKS**

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Perimeter-Sicherheitsstrategien, einschließlich Azure Firewall.
- Implementieren Sie Netzwerksicherheitsstrategien, einschließlich Netzwerksicherheitsgruppen und Anwendungssicherheitsgruppen.
- Implementieren Sie Host-Sicherheitsstrategien, einschließlich Endpunktschutz, RAS-Verwaltung, Update-Verwaltung und Festplattenverschlüsselung.
- Implementieren Sie Containersicherheitsstrategien, einschließlich Azure Container-Instanzen, Azure Container-Register und Azure Kubernetes.

**Modul 3: Daten und Anwendungen sichern**

Dieses Modul behandelt Azure Key Vault, Anwendungssicherheit, Speichersicherheit und SQL-Datenbanksicherheit.

**Lektionen**

- azure-key-vault
- Anwendungssicherheit
- Speichersicherheit
- SQL Datenbank-Sicherheit

- **Lab: Key Vault (Implementieren sicherer Daten durch die Einstellung „immer verschlüsselt")**
- **Lab: Sichern der Azure SQL-Datenbank**

- **Lab: Service-Endpunkte und Speicher sichern**

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Azure Key Vault, einschließlich Zertifikaten, Schlüsseln und Geheimnissen.
- Implementieren Sie Anwendungssicherheitsstrategien, einschließlich App-Registrierung, verwaltete Identitäten und Service-Endpunkte.
- Implementieren Sie Speichersicherheitsstrategien, einschließlich gemeinsam genutzter Zugriffssignaturen, Blob-Aufbewahrungsrichtlinien und Azure Dateien-Authentifizierung.
- Implementieren Sie Datenbanksicherheitsstrategien, einschließlich Authentifizierung, Datenklassifizierung, dynamische Datenmaskierung, und das immer verschlüsselt.

**Modul 4: Sicherheitsvorgänge verwalten**

Dieses Modul behandelt Azure Monitor, Azure Security Center und Azure Sentinel.

**Lektionen**

- Azure-Monitor
- Azure Security Center
- Azure Sentinel

- **Lab: Azure Monitor**
- **Lab: Azure Security Center**
- **Lab: Azure Sentinel**

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Azure Monitor, einschließlich verbundener Quellen, Protokollanalysen und Warnungen.
- Implementieren Sie Azure Security Center. einschließlich Richtlinien, Empfehlungen und Just-in-Time-Zugriff auf virtuelle Maschinen.
- Implementieren Sie Azure Sentinel, einschließlich Arbeitsmappen, Ereignissen und Wiedergabebüchern