

AZ500 Microsoft Azure Security Technologies

Kurzbeschreibung:

Im Seminar **AZ500 Microsoft Azure Security Technologies (AZ-500)** erwerben Sie fundiertes Wissen in den Bereichen Azure-Datenschutzmechanismen, -Datenverschlüsselungsmethoden, Azure-Sicherheitsdiensten und -funktionen. Nach dem Workshop können Sie Identitäten und Zugriffe verwalten sowie Daten, Anwendungen und Netzwerke schützen. Sie erkennen und beheben Schwachstellen, implementieren den Schutz vor Bedrohungen und reagieren auf Eskalationen bei Sicherheitsvorfällen. Der Kurs beinhaltet zudem die Themen Automatisierung, Virtualisierung und Cloud N-Tier-Architektur.

Zielgruppe:

Das Training richtet sich vor allem an:

- erfahrene Sicherheitsingenieure die das AZ-500 Examen zum Azure Security Engineer Associate anstreben
- Administratoren und Architekten, die für die Planung und Umsetzung von Azure Cloud Infrastrukturen und Lösungen verantwortlich sind
- Cloud Consultants

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo im Workshop **AZ500 Microsoft Azure Security Technologies (AZ-500)** gut folgen zu können, sind Vorkenntnisse aus folgenden Bereichen von Vorteil:

- Erfahrungen mit der Bereitstellung und Sicherung von Azure-Workloads
- Vertrautheit mit Sicherheitsprotokollen wie VPN (Virtual Private Networks), IPsec (Internet Security Protocol), SSL (Secure Socket Layer), Datenträger- und Datenverschlüsselungsmethoden
- Erfahrungen mit Windows- und Linux-Betriebssystemen und Skriptsprachen

Wir empfehlen vorab den Besuch des Kurses [AZ104 MS Azure Administration](#)

Sonstiges:

Dauer: 4 Tage

Preis: 2490 Euro plus Mwst.

Ziele:

In diesem Workshop erwerben die Teilnehmer fundiertes Wissen in folgenden Bereichen:

- Konfiguration Microsoft Azure Active Directory für Workloads
- Implementierung des Schutzes der Azure Datenplattform und der Netzwerksicherheit
- Verwaltung von Azure Sicherheitsvorgängen
- Beschreibung von spezialisierten Datenklassifizierungen in Azure
- Identifizieren von Azure-Datenschutzmechanismen



Inhalte/Agenda:

- **◆ Modul 1: Identity and Access**
 - ◆ ◇ Konfigurieren von Azure Active Directory für Azure-Workloads und -Abonnements
 - ◆ ◇ Konfigurieren von Azure AD Privileged Identity Management
 - ◆ ◇ Sicherheitskonfiguration für ein Azure-Abonnement

- **◆ Modul 2: Azure Plattformschutz**
 - ◆ ◇ Netzwerkaufbau und -absicherung
 - ◆ ◇ Implementieren der Host-Sicherheit
 - ◆ ◇ Implementieren der Plattformsicherheit
 - ◆ ◇ Implementieren der Abonnementsicherheit

- **◆ Modul 3: Sicherheitsmaßnahmen**
 - ◆ ◇ Konfigurieren von Sicherheitsdiensten
 - ◆ ◇ Konfigurieren von Sicherheitsrichtlinien mithilfe des Azure Security Centers
 - ◆ ◇ Verwalten von Sicherheitswarnungen
 - ◆ ◇ Reagieren auf und Beheben von Sicherheitsproblemen
 - ◆ ◇ Erstellen von Sicherheits-Baselines

- **◆ Modul 4: Daten und Anwendungen**
 - ◆ ◇ Konfigurieren von Sicherheitsrichtlinien zum Verwalten von Daten
 - ◆ ◇ Konfigurieren der Sicherheit für die Dateninfrastruktur
 - ◆ ◇ Konfigurieren der Verschlüsselung für ruhende Daten
 - ◆ ◇ Sichere Anwendungen
 - ◆ ◇ Konfigurieren und Verwalten von Azure Key Vault