Secure cloud resources with Microsoft security technologies (AZ-500T00)

ID AZ-500T00 **Preis** 2.590,– € (exkl. MwSt.) **Dauer** 4 Tage

Kursüberblick

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.

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.

Empfohlenes Training für die Zertifizierung zum

Microsoft Certified: Azure Security Engineer Associate (MCASEA)

Voraussetzungen

Erfolgreiche Teilnehmer verfügen über Vorkenntnisse und Verständnis für:

- Verständnis bewährter Sicherheitsmethoden und Branchensicherheitsanforderungen, z. B. tiefgehende Verteidigung (Defense in Depth), Zugriff mit geringstmöglichen Berechtigungen, rollenbasierte Zugriffssteuerung, mehrstufige Authentifizierung, gemeinsame Verantwortung und Zero Trust-Modell
- Vertrautheit mit Sicherheitsprotokollen wie VPN (Virtual Private Networks), IPsec (Internet Security Protocol), SSL (Secure Socket Layer), Datenträger- und Datenverschlüsselungsmethoden
- Erfahrungen mit der Bereitstellung von Azure-Workloads. 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.

Die vorherige Teilnahme am Kurs Microsoft Azure Administrator (AZ-104T00) wird empfohlen.

Kursziele

- 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.
- 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.
- 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.
- 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.

Kursinhalt

Modul 1: Verwalten von Identität und Zugriff

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

Lektionen

- Azure Active Directory
- Azure Identity Protection
- Governance in Unternehmen
- Azure AD Privileged Identity Management
- Hybrididentität
- Lab: Rollenbasierte Zugriffssteuerung
- Lab: Azure Policy
- Lab: Resource Manager-Sperren
- Lab: MFA, bedingter Zugriff und AAD-Identitätsschutz
- Lab: Azure AD Privileged Identity Management
- Lab: Implementieren der Verzeichnissynchronisierung

Nach Abschluss dieses Moduls können die Schüler:

- Implementieren Sie Governance-Unternehmensstrategien, 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: Implementieren des Plattformschutzes

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

Lektionen

- Umgebungssicherheit
- Netzwerksicherheit
- Hostsicherheit
- Containersicherheit
- Lab: Netzwerksicherheitsgruppen und Anwendungssicherheitsgruppen
- Lab: Azure Firewall
- Lab: Konfigurieren und Schützen 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: Schützen von Daten und Anwendungen

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

Lektionen

- Azure-Schlüsseltresor
- Anwendungssicherheit
- Speichersicherheit
- SQL-Datenbank-Sicherheit
- Lab: Key Vault (Implementieren sicherer Daten durch Einrichten von „Always Encrypted“)
- Lab: Schützen von Azure SQL-Datenbank
- Lab: Dienstendpunkte und Schützen von Speicher

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: Verwalten von Sicherheitsvorgängen

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.

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch