Microsoft Azure Security Technologies – Intensive Training («AZ500»)

Dieses AZ-500 Training findet im intensiven Format statt, bei dem Sie ganztägige Sessions mit unseren MCT-Experten haben.

Dauer: 4 Tage
Preis: 2'550.– zzgl. 8.1% MWST
Kursdokumente: Offizielle Microsoft-Unterlagen und Microsoft Learn
Herstellercode: AZ-500

Inhalt

Der Inhalt dieses Intensive Trainings leitet sich aus der Prüfung «AZ-500: Microsoft Azure Security Technologies» ab. Beginnen Sie schon jetzt auf Microsoft Learn mit der Vorbereitung auf den Kurs und nutzen Sie den Learning Support, wenn Sie Fragen haben. Während den intensiven Trainingstagen mit unseren Trainern arbeiten Sie mit den offiziellen Microsoft-Kursunterlagen (mehr Informationen unter «Methodik & Didaktik»).

Modul 1: Identität und Zugang verwalten
Vorbei sind die Zeiten, in denen sich die Sicherheit auf eine starke Perimeter-Verteidigung konzentrierte, um böswillige Hacker fernzuhalten. Alles, was sich ausserhalb des Perimeters befand, wurde als feindlich behandelt, während man innerhalb der Mauer den Systemen einer Organisation vertraute. Die heutige Sicherheitshaltung besteht darin, einen Bruch anzunehmen und das Zero-Trust-Modell anzuwenden. Sicherheitsexperten konzentrieren sich nicht mehr auf die Verteidigung des Perimeters. Moderne Organisationen müssen den Zugang zu Daten und Diensten sowohl innerhalb als auch ausserhalb der Unternehmensfirewall gleichmässig unterstützen. Dieses Modul wird Ihnen als Fahrplan dienen, wenn Sie damit beginnen, mehr Sicherheit in Ihre Azure-Lösungen einzubauen.

Lektionen:

- Azure AD PIM konfigurieren
- Konfigurieren und Verwalten von Azure Key Vault
- Konfigurieren von Azure AD für Azure-Arbeitslasten
- Sicherheit für ein Azure-Abonnement

Modul 2: Implementieren von Plattformschutz
Sicherheit in der Cloud ist Aufgabe Nr. 1 ist und es ist wichtig, dass Sie genaue und aktuelle Informationen über Azure-Sicherheit finden. Einer der besten Gründe, Azure für Ihre Anwendungen und Dienste zu verwenden, ist die Nutzung des breiten Spektrums an Sicherheitstools und -fähigkeiten von Azure. Diese Tools und Fähigkeiten ermöglichen es, sichere Lösungen auf der sicheren Azure-Plattform zu erstellen.

Lektionen:

- Cloud-Sicherheit verstehen
- Azure-Networking
- Sichern des Netzwerks
- Implementieren der Host-Sicherheit
- Implementieren der Plattform-Sicherheit
- Implementieren der Subscription-Sicherheit

Modul 3: Daten und Anwendungen sichern
Azure-Sicherheit für Daten und Anwendungen bietet eine umfassende Lösung, die Unternehmen dabei

unterstützt, die Vorteile von Cloud-Anwendungen voll auszuschöpfen und gleichzeitig die Kontrolle mit verbesserter Transparenz der Aktivitäten zu behalten. Darüber hinaus erhöht sie den Schutz kritischer Daten in Cloud-Anwendungen. Mit Tools, die dabei helfen, die Schatten-IT aufzudecken, Risiken zu bewerten, Richtlinien durchzusetzen, Aktivitäten zu untersuchen und Bedrohungen zu stoppen, können Unternehmen sicher in die Cloud wechseln und gleichzeitig die Kontrolle über kritische Daten behalten.

Lektionen:

- Konfigurieren von Sicherheitsrichtlinien zur Datenverwaltung
- Konfigurieren der Sicherheit für die Dateninfrastruktur
- Konfigurieren der Verschlüsselung für Daten im Ruhezustand
- Anwendungssicherheit verstehen
- Sicherheit für den Lebenszyklus von Anwendungen implementieren
- Sichere Anwendungen

Modul 4: Security Operations verwalten
Azure bietet Sicherheitsmechanismen zur Unterstützung von Administratoren, die Azure-Cloud-Dienste und virtuelle Maschinen verwalten. Diese Mechanismen umfassen: Authentifizierung und rollenbasierte Zugriffskontrolle, Überwachung, Protokollierung und Auditierung, Zertifikate und verschlüsselte Kommunikation sowie ein Web-Verwaltungsportal.

Lektionen:

- Konfigurieren von Sicherheitsdiensten
- Konfigurieren von Sicherheitsrichtlinien mit Azure Security Center
- Sicherheitswarnungen verwalten
- Reagieren auf eine Behebung von Sicherheitsproblemen
- Erstellen von Sicherheitsgrundlinien

Bitte beachten Sie, dass am Ende dieses Kurses keine Prüfung abgelegt wird.

Key Learnings

- Beschreibung von spezialisierten Datenklassifikationen auf Azure
- Identifizierung von Azure-Datenschutzmechanismen
- Implementierung von Azure-Datenverschlüsselungsverfahren
- Sicherung von Internet-Protokollen und deren Implementierung auf Azure
- Beschreibung der Sicherheitsdienste und -merkmale von Azure

Zielpublikum

Teilnehmer mit mindestens einem Jahr praktischer Erfahrung in der Sicherung von Azure-Workloads und Erfahrung mit Sicherheitskontrollen für Workloads auf Azure, die ihr Wissen über die Sicherheitsfunktionen und -möglichkeiten von Azure erweitern möchten.

Anforderungen

- 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.

- Microsoft Azure Fundamentals (Hands-on) – Intensive Training («A900IC»)
- Microsoft Azure Fundamentals – Flexible Training («AZ900V»)

Zertifizierung

Dieses Intensive Training bereitet Sie vor auf:

- **Prüfung:** «AZ-500: Microsoft Azure Security Technologies» für die
- **Zertifizierung:** «Microsoft Certified: Azure Security Engineer Associate»

Zusatzinfo

Die beiden Workshops SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel und SC-5002: Secure Azure Services and Workloads with Microsoft Defender for Cloud Regulatory Compliance Controls werden in diesen Kurs integriert.

Weiterführende Kurse

- Microsoft Cybersecurity Architect – Intensive Training («SC100»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-azure/microsoft-certified-azure-security-engineer-associate/kurs-microsoft-azure-security-technologies-intensive-training-az-500