Microsoft 365 Security Administrator (MOC MS-500)

Überblick

In diesem Kurs lernen die Teilnehmer den Benutzerzugriff auf Ressourcen einer Organisation zu sichern.
Der Kurs behandelt den Schutz von Benutzerkennwörtern, Multi-Faktor Authentifizierung, die Aktivierung von Azure-Identitätsschutz, die Einrichtung und Verwendung von Azure AD Connect und führt die Teilnehmer in die Zugangskontrolle in Microsoft 365 ein.
Des Weiteren erfahren die Teilnehmer die Technologien zum Schutz vor Bedrohungen kennen, die zum Schutz der Microsoft 365 Umgebung beitragen, insbesondere werden die Bedrohungsvektoren und die Sicherheitslösungen von Microsoft zur Eindämmung von Bedrohungen behandelt.
Auch lernen die Teilnehmer mehr über die Themen Secure Score, Exchange Online Schutz, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection und Bedrohungsmanagement kennen sowie Informationsschutztechnologien, mit denen eine Microsoft 365-Umgebung geschützt werden kann.
Im Speziellen werden in diesem Kurs mit Informationsrechten verwaltete Inhalte, Nachrichtenverschlüsselung sowie Beschriftungen, Richtlinien und Regeln behandelt, die die Verhinderung von Datenverlust und den Schutz von Informationen unterstützen.
Abschließend erfahren die Teilnehmer die Archivierung und Aufbewahrung in Microsoft 365 sowie die Datenverwaltung und das Durchführen von Inhaltssuchen und -untersuchungen kennen.
In diesem Kurs werden insbesondere die Richtlinien und Tags für die Datenaufbewahrung, die direkte Datensatzverwaltung für SharePoint, die E-Mail-Aufbewahrung und die Durchführung von Inhaltssuchen behandelt, die eDiscovery-Untersuchungen unterstützen.

Die Zertifizierungsprüfung MS-500 wurden zum 30.06.2023 abgekündigt. Die Kursinhalte gehen in die Kurse SC-200, SC-300 und AZ-500 auf.

Dauer:
4 Tage

Preis:
2.150,00 € (2.558,50 € inkl. MwSt.)

Kursinhalt

User and Group Management

- Identity and Access Management concepts
- The Zero Trust model
- Plan your identity and authentication solution
- User accounts and roles
- Password Management

Identity Synchronization and Protection

- Plan directory synchronization
- Configure and manage synchronized identities
- Azure AD Identity Protection

Identity and Access Management

- Application Management
- Identity Governance
- Manage device access
- Role Based Access Control (RBAC)
- Solutions for external access
- Privileged Identity Management

Security in Microsoft 365

- Threat vectors and data breaches
- Security strategy and principles
- Microsoft security solutions
- Secure Score

Threat Protection

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Threat Management

- Security dashboard
- Threat investigation and response
- Azure Sentinel
- Advanced Threat Analytics

Microsoft Cloud Application Security

- Deploy Cloud Application Security
- Use cloud application security information

Mobility

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Deploy mobile device services
- Enroll devices to Mobile Device Management

Information Protection and Governance

- Information protection concepts
- Governance and Records Management
- Sensitivity labels
- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention policies in the Microsoft 365 Compliance Center
- Archiving and retention in Exchange
- In-place records management in SharePoint

Rights Management and Encryption

- Information Rights Management (IRM)
- Secure Multipurpose Internet Mail Extension (S-MIME)
- Office 365 Message Encryption

Data Loss Prevention

- Data loss prevention fundamentals
- Create a DLP policy
- Customize a DLP policy
- Create a DLP policy to protect documents
- Policy tips

Compliance Management

- Compliance center

Insider Risk Management

- Insider Risk
- Privileged Access
- Information barriers
- Building ethical walls in Exchange Online

Discover and Respond

- Content Search
- Audit Log Investigations
- Advanced eDiscovery

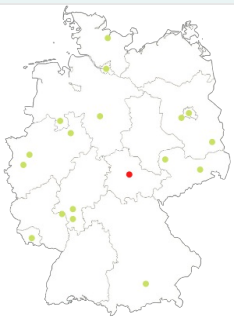
Voraussetzungen

- Grundlegendes konzeptionelles Verständnis von Microsoft Azure
- Erfahrung mit Windows 10-Geräten
- Erfahrung mit Office 365
- Grundlegendes Verständnis von Autorisierung und Authentifizierung
- Grundkenntnisse der Computernetzwerke
- Grundkenntnisse in der Verwaltung mobiler Geräte

Zielgruppe

Dieser Kurs richtet sich an Sicherheitsexperten und Netzwerkadministratoren, die eine Microsoft 365-Unternehmensumgebung proaktiv sichern möchten.

Ihr Weg zu uns



dama.go GmbH Erfurt

Anger 66 - 73
99084 Erfurt
Phone: 0361 64433-95
Email: steve.liebing@damago.de