Microsoft 365 Security Administration (MS-500)

Microsoft 365 Security Administration (MS-500)

Seminar | Zurzeit keine Termine | Teilnahmebescheinigung

Präsenz / Virtual Classroom | 32 Unterrichtseinheiten

Seminarnummer: 29524 | Herstellernummer: MOC-MS-500

Stand: 06.05.2024. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29524

In diesem Kurs lernen Sie, wie Sie den Benutzerzugriff auf die Ressourcen Ihrer Organisation sichern. Der Kurs behandelt den Schutz von Benutzerkennwörtern, Multi-Faktor Authentifizierung, die Aktivierung von Azure-Identitätsschutz, die Einrichtung und Verwendung von Azure AD Connect. Sie lernen Technologien zum Schutz vor Bedrohungen kennen, die zur Sicherheit Ihrer Microsoft 365 Umgebung beitragen.

Nutzen

Sie erfahren etwas über Secure Score, Exchange Online Schutz, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection und Bedrohungsmanagement. In diesem Kurs erfahren Sie mehr über Informationsschutztechnologien, mit denen Sie Ihre Microsoft 365-Umgebung schützen können. Es werden speziell mit Informationsrechten verwaltete Inhalte, Nachrichtenverschlüsselung sowie Beschriftungen, Richtlinien und Regeln behandelt, die die Verhinderung von Datenverlust und den Schutz von Informationen unterstützen. Abschließend lernen Sie die Archivierung und Aufbewahrung in Microsoft 365 sowie die Datenverwaltung und das Durchführen von Inhaltssuchen und -untersuchungen. In dem 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.

Zielgruppe

Der Microsoft 365 Security Administrator arbeitet mit einem Microsoft 365 Enterprise Administrator, den Geschäftsteilhabern und anderen Workload Administratoren für Planung und Implementierung von Sicherheitsstrategien zur Gewährleistung zusammen, damit die Lösungen mit den Richtlinien und Bestimmungen der Organisation übereinstimmen. Diese Rolle sichert proaktiv Microsoft 365-Unternehmensumgebungen. Zu den Aufgaben gehören das Reagieren auf Bedrohungen, das Implementieren, Verwalten und Überwachen von Sicherheits- und Compliance-Lösungen für die Microsoft 365-Umgebung. Sie reagieren auf Vorfälle, Untersuchungen und die Durchsetzung von Data Governance. Der Microsoft 365 Sicherheitsadministrator ist mit Microsoft 365 Workloads und hybriden Umgebungen

vertraut. Diese Rolle verfügt über starke Fähigkeiten und Erfahrungen mit Identitätsschutz, Informationsschutz, Bedrohungsschutz, Sicherheitsmanagement und Datenverwaltung.

Voraussetzungen

- Grundlegendes konzeptionelles Verständnis von Microsoft Azure, wie sie z.B. im Seminar AZ-900 vermittelt werden.
- Erfahrung mit Windows 10-Geräten.
- Erfahrung mit Office 365.
- Grundlegendes Verständnis von Autorisierung und Authentifizierung.
- Grundlegendes Verständnis von Computernetzwerken.
- Grundkenntnisse in der Verwaltung mobiler Geräte.

Inhalte des Seminars

Modul 1: Benutzer und Gruppenschutz

In diesem Modul wird das Verwalten von Benutzerkonten und Gruppen in Microsoft 365 erläutert. Es führt Sie in das privilegierte Identitätsmanagement in Azure AD sowie in den Identitätsschutz ein. Das Modul legt den Grundstein für den weiteren Verlauf des Kurses.

- Konzepte für die Identitäts- und Zugriffsverwaltung Zero Trust-Sicherheit
- Benutzerkonten in Microsoft 365
- Kompetenz: Verwalten von Administratorrollen und Sicherheitsgruppen in Microsoft 365
- Passwortverwaltung in Microsoft 365
- Azure AD Identitätsschutz

Modul 2: Identitätssynchronisation

In diesem Modul werden Konzepte zur Synchronisierung von Identitäten für Microsoft 365 erläutert. Insbesondere konzentriert es sich auf Azure AD Connect und das Verwalten der Verzeichnissynchronisierung, um sicherzustellen, dass die richtigen Personen eine Verbindung zu Ihrem Microsoft 365-System herstellen.

- Einführung in die Identitätssynchronisierung
- Planen von Azure AD Connect
- Azure AD Connect-Implementieren
- Verwalten synchronisierter Identitäten
- Einführung in Verbundidentitäten

Modul 3: Zugriffsverwaltung

Dieses Modul erläutert die Zugangskontrolle für Microsoft 365 und wie sie zur Kontrolle des Zugriffs auf Ressourcen in Ihrer Organisation verwendet werden kann. Das Modul erklärt auch die rollenbasierte Zugriffskontrolle (RBAC) und Lösungen für den externen Zugriff.

- Zugangskontrolle
- Verwalten des Gerätezugriffs
- Rollenbasierte Zugriffskontrolle (RBAC)
- Entwerfen von Lösungen für den externen Zugriff

Modul 4: Sicherheit bei Microsoft 365

In diesem Modul werden die verschiedenen Cyberangriffsbedrohungen erläutert. Anschließend werden Sie mit den Microsoft-Lösungen vertraut gemacht, die zur Eindämmung dieser Bedrohungen eingesetzt werden. Das Modul endet mit einer Erläuterung von Microsoft Secure Score und der Verwendung dieses Moduls zur Bewertung und Meldung der Sicherheitslage Ihres Unternehmens.

- Bedrohungsvektoren und Datenverletzungen
- Sicherheitsstrategie und -prinzipien
- Sicherheitslösungen in Microsoft 365
- Microsoft Secure Score

Modul 5: Erweiterter Bedrohungsschutz

Dieses Modul erläutert die verschiedenen Technologien und Services zum Schutz vor Bedrohungen, die für Microsoft 365 verfügbar sind. Insbesondere deckt das Modul den Nachrichtenschutz von Exchange Online Protection, Azure Advanced Threat Protection und Windows Defender Advanced Threat Protection ab.

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Verwalten sicherer Anhänge
- Verwalten sicherer Links
- Azure Advanced Threat Protection
- Microsoft Defender Advanced Threat Protection

Modul 6: Bedrohungsmanagement

In diesem Modul wird das Microsoft Threat Management erläutert, das Ihnen die Tools zur Bewertung und Bekämpfung von Cyberbedrohungen und zur Formulierung von Reaktionen bietet. Sie lernen, wie Sie das Sicherheits-Dashboard und den Azure Sentinel für Microsoft 365 verwenden können. Das Modul

erklärt und konfiguriert auch die Microsoft Advanced Threat Analytics.

- Verwendung des Sicherheits-Dashboards
- Microsoft 365 Untersuchung und Reaktion auf Bedrohungen
- Azure Sentinel für Microsoft 365
- Konfigurieren der erweiterten Bedrohungsanalyse

Modul 7: Mobilität

Dieses Modul konzentriert sich auf die Sicherung mobiler Geräte und Anwendungen. Sie erfahren etwas über die Verwaltung mobiler Geräte und wie sie mit Microsoft Intune funktioniert. Sie erfahren auch, wie Intune und Azure AD zur Sicherung mobiler Anwendungen eingesetzt werden können.

- Planung für das Mobile App Management
- Verwaltung mobiler Anwendungen planen
- Mobilgerätemanagement bereitstellen
- Geräte für das Mobilgerätemanagement registrieren

Modul 8: Informationsschutz

Das Modul erklärt, wie Azure Information Protection und Windows Information Protection implementiert werden können.

- Konzepte für den Informationsschutz
- Azure Informationsschutz
- Windows-Informationsschutz

Modul 9: Rechteverwaltung und Verschlüsselung

In diesem Modul wird die Verwaltung von Informationsrechten in Exchange und SharePoint erläutert. Das Modul beschreibt auch Verschlüsselungstechnologien, die zur Sicherung von Nachrichten verwendet werden.

- Informationsrechts-Management
- Einführung in die sichere Mehrzweck-Internet-Mail-Erweiterung
- Office 365-Nachrichtenverschlüsselung

Modul 10: Prävention von Datenverlust

Dieses Modul konzentriert sich auf die Verhinderung von Datenverlusten in Microsoft 365. Sie erfahren, wie Sie Richtlinien erstellen, Regeln bearbeiten und Benutzerbenachrichtigungen zum Schutz Ihrer Daten

anpassen können.

- Erklärung zur Prävention von Datenverlust
- Richtlinien zur Prävention von Datenverlust
- Benutzerdefinierte DLP-Richtlinien
- Erstellen einer DLP-Richtlinie zum Schutz von Dokumenten
- Richtlinientipps

Modul 11: Cloud-Anwendungssicherheit

Dieses Modul konzentriert sich auf die Sicherheit von Cloud-Anwendungen in Microsoft 365. Das Modul erläutert die Cloud-Erkennung, App-Connectors, Richtlinien und Warnungen. Sie werden lernen, wie diese Funktionen funktionieren, um Ihre Cloud-Anwendungen zu sichern.

- Erklärung der Sicherheit von Cloud-Anwendungen
- Verwenden von Sicherheitsinformationen für Cloud-Anwendungen

Modul 12: Konformität in Microsoft 365

Dieses Modul befasst sich mit der Datenverwaltung in Microsoft 365. Das Modul führt Sie in den Compliance-Manager ein und erläutert die globale Datenschutzverordnung (GDPR).

- Plan für die Einhaltung der Anforderungen
- Aufbau ethischer Mauern in Exchange Online
- Aufbewahrung in E-Mails verwalten
- Problembehebung bei Data Governance

Modul 13: Archivierung und Aufbewahrung

In diesem Modul werden Konzepte zur Aufbewahrung und Archivierung von Daten für Microsoft 365 einschließlich Exchange und SharePoint erläutert.

- Archivierung in Microsoft 365
- Aufbewahrung in Microsoft 365
- Aufbewahrungsrichtlinien im Microsoft 365 Compliance Center
- Archivierung und Aufbewahrung im Austausch
- In-Place Dokumentenverwaltung in SharePoint

Modul 14: Inhaltssuche und Untersuchung

Dieses Modul konzentriert sich auf die Suche nach Inhalten und Untersuchungen. Das Modul behandelt die Verwendung von eDiscovery zur Durchführung von erweiterten Untersuchungen von Microsoft 365-Daten. Außerdem werden Audit-Protokolle behandelt und Anfragen von DSGVO-Betroffenen erörtert.

- Audit Log-Untersuchungen

Wichtige Hinweise

jetzt auch online Teilnahme möglich durch unsere Virtual Classroom (VC) Lösung. Wegen Reiseeinschränkungen können Sie nicht zu uns kommen? Wir binden Sie gerne online in das live Seminar ein. Kontaktieren Sie uns direkt damit wir dieses für Sie organisieren.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29524 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.