Mögliche Trainingslösung:	SALTZ-Seminar
Seminarsprache:	Englisch
Dauer	4 Tage

Übersicht

In diesem Kurs lernen Sie, wie Sie den Benutzerzugriff auf Ressourcen Ihrer Organisation sichern. Der Kurs behandelt den Schutz von Benutzerkennwörtern, die Multi-Faktor-Authentifizierung, das Aktivieren von Azure Identitätsschutz, das Einrichten und Verwenden von Azure AD Connect, sowie eine Einführung in den bedingten Zugriff in Microsoft 365. In diesem Kurs erfahren Sie mehr über Informationsschutztechnologien, mit denen Sie Ihre Microsoft 365-Umgebung schützen können. Insbesondere lernen Sie Bedrohungsvektoren und die Sicherheitslösungen von Microsoft kennen, um Bedrohungen zu mindern. Sie erhalten Informationen zu Secure Score, Exchange Online-Schutz, Azure Advanced Threat Protection und Windows Defender Advanced Threat Protection, sowie zur Verwendung von Threat Management. In diesem Kurs erfahren Sie mehr über Informationsschutztechnologien, mit denen Sie Ihre Microsoft 365-Umgebung schützen können. In diesem Kurs werden speziell mit Informationsrechten verwaltete Inhalte, Nachrichtenverschlüsselung sowie Beschriftungen, Richtlinien und Regeln behandelt, die die Verhinderung von Datenverlust und den Schutz von Informationen unterstützen. In diesem Kurs lernen Sie die Archivierung und Aufbewahrung in Microsoft 365, sowie die Datenverwaltung und das Durchführen von Inhaltssuchen und -untersuchungen. Dieser Kurs behandelt Richtlinien und Tags zur Vorratsdatenspeicherung, die direkte Verwaltung von Datensätzen für SharePoint, die Aufbewahrung von E-Mails und die Durchführung von Inhaltssuchen, die eDiscovery-Untersuchungen unterstützen.

Voraussetzungen

Die Lernenden sollten diesen Kurs bereits mit den folgenden Fähigkeiten beginnen:

- Grundlegendes konzeptionelles Verständnis von Microsoft Azure.
- 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.

Zielgruppe

Der Microsoft 365 Security Administrator arbeitet mit einem Microsoft 365 Enterprise Administrator, Wirtschaftsakteuren und anderen Workload Administratoren für die Planung und das Implementieren von Sicherheitsstrategien zusammen und gewährleistet, dass die Lösungen mit den Richtlinien und Bestimmungen des Unternehmens 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 Hybridumgebungen vertraut. Diese Rolle verfügt über umfassende Fähigkeiten und Erfahrungen in den Bereichen Identitätsschutz, Informationsschutz, Bedrohungsschutz, Sicherheitsmanagement und Datenverwaltung.

Erworbene Qualifikationen

- Verwalten der Benutzer und Gruppenzugriff in Microsoft 365.
- Erläutern und Verwalten des Azure-Identitätsschutzes.
- Planen und Implementieren von Azure AD Connect.
- Verwalten synchronisierter Benutzeridentitäten.
- Bedingten Zugriff erklären und verwenden.

- Beschreiben der Bedrohungsvektoren für Cyberangriffe.
- Erläutern von Sicherheitslösungen für Microsoft 365.
- Verwenden von Microsoft Secure Score, um Ihre Sicherheitslage zu bewerten und zu verbessern.
- Verschiedene erweiterte Bedrohungsschutzdienste für Microsoft 365.
- Planen und Bereitstellen sicherer mobiler Geräte.
- Planung und Bereitstellung von sicheren mobilen Geräten.
- Implementieren Informationsrechts- Management.
- Nachrichten in Office 365 sichern.
- Datenverlust-Präventionsrichtlinien konfigurieren.
- Bereitstellen und Verwalten der Cloud-App-Sicherheit.
- Implementieren von Windows-Informationsschutz für Geräte.
- Planen und Bereitstellen eines Datenarchivierungs- und Aufbewahrungssystems.
- Erstellen und verwalten einer eDiscovery-Untersuchung.
- Erklären und verwenden von Empfindlichkeitsetiketten.

Agenda

Modul 1: Benutzer- und Gruppenverwaltung

In diesem Modul wird erläutert, wie Sie Benutzerkonten und Gruppen in Microsoft 365 verwalten. Es führt Sie in das Zero Trust-Konzept sowie in die Authentifizierung ein. Das Modul legt den Grundstein für den weiteren Verlauf des Kurses.

Lektionen

- Identitäts- und Zugriffsmanagementkonzepte
- Das Zero Trust-Modell
- Planen Sie Ihre Identitäts- und Authentifizierungslösung
- Benutzerkonten und Rollen
- Azure AD Identitätsschutz

- **Labor : Initialisieren Sie Ihren Mandanten - Benutzer und Gruppen**
- Richten Sie Ihren Microsoft 365 Probanden ein
- Verwalten Sie Benutzer und Gruppen

- **Labor : Passwortverwaltung**
- Konfigurieren Sie das Zurücksetzen des Self-Service-Kennworts (SSPR) für Benutzerkonten in Azure AD
- Stellen Sie Azure AD Smart Lockout bereit

Nach Abschluss dieses Moduls können die Teilnehmer:

- Erstellen und Verwalten von Benutzerkonten.
- Beschreiben und Verwenden von Microsoft 365-Administratorrollen.
- Kennwortrichtlinien und Authentifizierung planen.
- Beschreiben der Konzepte der Zero Trust-Sicherheit.
- Erläutern Sie das Zero Trust-Modell.

Modul 2: Identitätssynchronisation und -schutz

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.

Lektionen

- Planen der Verzeichnissynchronisierung
- Konfigurieren und verwalten von synchronisierten Identitäten

- Azure AD-Identitätsschutz

- **Labor : Implementieren der Identitätssynchronisierung**
- Einrichten Ihrer Organisation für die Identitätssynchronisierung

Nach Abschluss dieses Moduls können die Teilnehmer:

- Beschreiben der Authentifizierungsoptionen für Microsoft 365.
- Die Verzeichnissynchronisierung erläutern.
- Die Verzeichnissynchronisierung planen.
- Beschreiben von Azure AD Connect und seine Verwendung.
- Voraussetzungen für Azure AD Connect konfigurieren.
- Verwalten der Benutzer und Gruppen mit der Verzeichnissynchronisierung.
- Beschreiben des Active Directory-Verbunds.
- Aktivieren des Azure-Identitätsschutzes

Modul 3: Identitäts- und Zugriffsverwaltung

Wir diskutieren Identity Governance als Konzept und seine Komponenten.

Lektionen

- Bewerbungsmanagement
- Identity Governance
- Verwalten des Gerätezugriffs
- Rollenbasierte Zugriffskontrolle (RBAC)
- Entwerfen von Lösungen für den externen Zugriff
- Privilegierte Identitätsverwaltung

- **Labor : Bedingten Zugriff verwenden, um MFA zu aktivieren**
- MFA Authentifizierungs Pilot (MFA für bestimmte Anwendungen erforderlich)
- Bedingter MFA Zugang (Abschluss einer MFA Einführung)

- **Labor : Konfigurieren Sie die Verwaltung privilegierter Identitäten**
- Verwalten von Azure-Ressourcen
- Verweisen von Verzeichnisrollen
- Aktivieren und deaktivieren von PIM-Rollen
- Verzeichnisrollen
- PIM-Ressourcen-Workflows
- Anzeigen des Überwachungsverlaufs für Azure AD-Rollen in PIM

Nach Abschluss dieses Moduls können die Teilnehmer:

- Beschreiben Sie das Konzept des bedingten Zugriffs.
- Beschreiben und verwenden Sie Richtlinien zur Zugangskontrolle.
- Planen der Gerätekonformität.
- Bedingte Benutzer und Gruppen konfigurieren.
- Konfigurieren Sie eine rollenbasierte Zugriffskontrolle.
- Beschreiben von Konzepten der Identitäts-Governance
- Konfigurieren und verwenden von Privileged Identity Management

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.

Lektionen

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

- **Labor : Microsoft Secure Score verwenden**
- Verbessern Sie Ihre sichere Punktzahl im Microsoft 365 Security Center

Nach Abschluss dieses Moduls können die Teilnehmer:

- Beschreiben Sie verschiedene Techniken, die Angreifer verwenden, um Benutzerkonten per E-Mail zu manipulieren.
- Beschreiben Sie die Techniken, die Angreifer verwenden, um die Kontrolle über die Ressourcen zu erlangen.
- Listen Sie die Arten von Bedrohungen auf, die mit EOP und Microsoft Defender für Office 365 vermieden werden können.
- Die Vorteile von Secure Score beschreiben und welche Arten von Diensten analysiert werden können.
- Beschreiben Sie, wie Sie Secure Score verwenden, um Lücken in Ihrer aktuellen Microsoft 365 Sicherheitsposition zu identifizieren.

Modul 5: Erweiterter Bedrohungsschutz

Dieses Modul erläutert die verschiedenen Technologien und Services zum Schutz vor Bedrohungen, die für Microsoft 365 verfügbar sind. Das Modul umfasst den Nachrichtenschutz durch Exchange Online-Schutz, Microsoft Defender für Identität und Microsoft Defender für Endpoint.

Lektionen

- Exchange Online Protection (EOP)
- Microsoft Defender für Office 365
- Verwalten sicherer Anhänge
- Verwalten sicherer Links
- Microsoft Defender für Identität
- Microsoft Defender für Endpoint

- **Labor : Microsoft 365 Security Services verwalten**
- Implementieren Sie Microsoft Defender-Richtlinien

Nach Abschluss dieses Moduls können die Teilnehmer:

- Die Anti-Malware-Pipeline beschreiben, während E-Mails von Exchange Online Protection analysiert werden.
- Beschreiben, wie sichere Anhänge verwendet werden, um Zero-Day-Malware in E-Mail-Anhängen und Dokumenten zu blockieren.
- Beschreiben Sie, wie sichere Links Benutzer vor böswilligen URLs schützen, die in E-Mails und Dokumenten eingebettet sind und auf die verwiesen wird.
- Konfigurieren Sie Microsoft Defender für die Identität.
- Konfigurieren Sie Microsoft Defender für Endpoint.

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.

Lektionen

- Sicherheits-Dashboards

- Bedrohungsuntersuchung und Reaktion
- Azure Sentinel
- Advanced Threat Analytics

- **Labor : Benutzung des Angriffssimulators**
- Durchführung einer simulierten Spear Phishing Attacke
- Simulierte Passwortangriffe durchführen

Nach Abschluss dieses Moduls können die Teilnehmer:

- Beschreiben, wie man mit dem Threat Explorer Bedrohungen untersuchen und Ihren Mandanten schützen können.
- Beschreiben Sie, wie das Security Dashboard Führungskräften auf C-Level einen Einblick in die wichtigsten Risiken und Trends gibt.
- Beschreiben, was die erweiterte Bedrohungsanalyse (ATA) ist und welche Anforderungen für die -Bereitstellung erforderlich sind.
- Konfigurieren fortgeschrittener Bedrohungsanalysen.
- Verwenden Sie den Angriffssimulator in Microsoft 365.
- Beschreiben Sie, wie Azure Sentinel für Microsoft 365 verwendet werden kann.

Modul 7: Microsoft 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 erfahren, wie diese Funktionen Ihre Cloud-Anwendungen schützen.

Lektionen

- Bereitstellen der Cloud-Anwendungssicherheit
- Verwenden Sie Sicherheitsinformationen für Cloud-Anwendungen

Nach Abschluss dieses Moduls können die Teilnehmer:

- Die Cloud App-Sicherheit zu beschreiben.
- Erläutern, wie die Cloud-App-Sicherheit bereitgestellt wird.
- Kontrollieren Ihrer Cloud-Apps mit Richtlinien.
- Verwenden des Cloud-App-Katalogs.
- Verwenden des Cloud-Discovery-Dashboards.
- Verwalten von Cloud-App-Berechtigungen.

Modul 8: Mobilität

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

Lektionen

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Bereitstellen von Services für mobile Geräte
- Registrieren von Geräten für die Verwaltung mobiler Geräte

- **Labor : Geräteverwaltung**
- Enable Device Management
- Configure Azure AD for Intune
- Erstellen der Richtlinien für Compliance und bedingten Zugriff

Nach Abschluss dieses Moduls können die Teilnehmer:

- Konfigurieren von Kennzeichnungen und Richtlinien für den Azure Informationsschutz.
- Konfigurieren erweiterter AIP-Diensteinstellungen für Rechtsmanagementdienst (RMS) -Vorlagen.
- Planen einer Bereitstellung von Windows-Richtlinien für den Informationsschutz.

Modul 9: Informationsschutz und Governance

Dieses Modul konzentriert sich auf die Verhinderung von Datenverlust in Microsoft 365. Sie erfahren, wie Sie Richtlinien erstellen, Regeln bearbeiten und Benutzerbenachrichtigungen anpassen, um Ihre Daten zu schützen.

Lektionen

- Informationsschutzkonzepte
- Governance und Records Management
- Empfindlichkeitsetiketten
- Archivierung in Microsoft 365
- Aufbewahrung in Microsoft 365
- Aufbewahrungsrichtlinien im Microsoft 365 Compliance Center
- Archivierung und Aufbewahrung in Exchange
- In-Place-Datensatzverwaltung in SharePoint

- **Labor: Archivierung und Aufbewahrung**
- Initialisieren Sie die Konformität
- Konfigurieren Sie Aufbewahrungs-Tags und -Richtlinien

Nach Abschluss dieses Moduls können die Teilnehmer:

- Konfigurieren Sie Empfindlichkeitsbezeichnungen.
- Konfigurieren Sie die Archivierung und Aufbewahrung in Microsoft 365.
- Planen und konfigurieren Sie die Datensatzverwaltung

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.

Lektionen

- Information Rights Management (IRM)
- Sichere Mehrzweck-Internet-Mail-Erweiterung (S-MIME)
- Office 365 Message Encryption

- **Labor : Richtlinien zur Verhinderung von Datenverlusten implementieren**
- DLP-Richtlinien verwalten
- Testen Sie die MRM- und DLP-Richtlinien

Nach Abschluss dieses Moduls können die Teilnehmer:

- Prävention von Datenverlust (DLP) beschreiben.
- Verwenden von Richtlinienvorlagen, um DLP-Richtlinien für häufig verwendete Informationen zu implementieren.
- Konfigurieren von korrekten Regeln zum Schutz von Inhalten.
- Beschreiben, wie vorhandene Regeln von DLP-Richtlinien geändert werden.
- Konfigurieren einer Option zur Benutzerübersteuerung für eine DLP-Regel.
- Erläutern, wie SharePoint Online gecrawlte Eigenschaften aus Dokumenten erstellt.

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.

Lektionen

- Grundlagen zur Verhinderung von Datenverlust
- Erstellen einer DLP-Richtlinie
- Passen einer DLP-Richtlinie an
- Erstellen Sie eine DLP-Richtlinie zum Schutz von Dokumenten
- Richtlinien-Tipps

Nach Abschluss dieses Moduls können die Teilnehmer:

- Beschreiben der Cloud-App-Sicherheit.
- Erläutern, wie die Cloud-App-Sicherheit bereitgestellt wird.
- Kontrollieren Ihrer Cloud-Apps mit Richtlinien.
- Verwenden des Cloud-App-Katalogs.
- Verwenden des Cloud-Discovery-Dashboards.
- Verwalten von Cloud-App-Berechtigungen.

Modul 12: Compliance Management

In diesem Modul wird das Compliance Center in Microsoft 365 erläutert. Es werden die Komponenten des Compliance-Scores erläutert.

Lektionen

- Compliance center

Nach Abschluss dieses Moduls können die Teilnehmer:

- Beschreiben, wie der Compliance-Score verwendet wird, um organisatorische Entscheidungen zu treffen.
- Beschreiben Sie, wie Bewertungen zur Bestimmung des Compliance-Scores verwendet werden.

Modul 13: Insider-Risikomanagement

Dieses Modul konzentriert sich auf Insider-Risikofunktionen in Microsoft 365. Es umfasst nicht nur das Insider-Risikomanagement im Compliance-Center, sondern auch Informationsbarrieren und das privilegierte Zugriffsmanagement.

Lektionen

- Insider-Risiko
- Privilegierter Zugriff
- Informationsbarrieren
- Aufbau ethischer Mauern in Exchange Online

- **Labor : Privilegierte Zugriffsverwaltung**
- Einrichten der privilegierten Zugriffsverwaltung und verarbeiten der Anforderung

Nach Abschluss dieses Moduls können die Teilnehmer:

- Insider-Risiko-Management in Microsoft 365 erklären und konfigurieren.
- Konfigurieren und genehmigen Sie privilegierte Zugriffsanforderungen für globale Administratoren.
- Konfigurieren und verwenden Sie Informationsbarrieren, um den organisatorischen Vorschriften zu entsprechen.
- Ethische Mauern in Exchange Online bauen

- Kunden-Lockbox konfigurieren

Modul 14: Entdecken und antworten

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.

Lektionen

- Inhaltssuche
- Audit Log-Untersuchungen
- Erweitertes eDiscovery

- **Labor : Suche und Untersuchungen verwalten**
- Untersuchen Ihrer Microsoft 365-Daten
- Eine Anfrage an das Datensubjekt durchführen

Nach Abschluss dieses Moduls können die Teilnehmer:

- Inhaltssuchen in Microsoft 365 durchführen.
- Protokolluntersuchung durchführen und prüfen.
- Konfigurieren Sie Microsoft 365 für die Überwachungsprotokollierung.
- Erweitertes eDiscovery nutzen