0800 5777333
kostenlose Beratung
training@pc-college.de

PC·COLLEGE®
Seminare, die begeistern!

Microsoft 365 - MS-500T00 - Microsoft 365 Security Administration

ACHTUNG:
- Dieser Kurs wurde von Microsoft zum 30.06.2023 abgekündigt und kann deshalb nicht mehr mit den Original Unterlagen und Schulungssetup angeboten werden. Gerne können wie Ihnen eine Schulung mit ähnlichen oder speziell für Sie angepassten Inhalten als Einzel- oder Firmenschulung bzw. Workshop anbieten.
- Eventuell kommt für Sie auch alternativ die Schulung Azure - AZ-500T00 - Microsoft Azure Security Technologies in Frage.

Kursinformationen:
In dem Kurs "MS-500T00 - Microsoft 365 Security Administration" 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 und führt Sie in die Zugangskontrolle in Microsoft 365 ein.

Sie lernen Technologien zum Schutz vor Bedrohungen kennen, die zum Schutz Ihrer Microsoft 365 Umgebung beitragen. Insbesondere werden Sie über die Bedrohungsvektoren und die Sicherheitslösungen von Microsoft zur Eindämmung von Bedrohungen lernen. Sie erfahren etwas über Secure Score, Exchange Online Schutz, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection und Bedrohungsmanagement.

In diesem Seminar 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, in diesem Kurs lernen Sie die Archivierung und Aufbewahrung in Microsoft 365 sowie die Datenverwaltung und das Durchführen von Inhaltssuchen und -untersuchungen. 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.

Dieses Seminar enthält folgende Schwerpunkte:
- Verwalten der Benutzer und Gruppenzugriff in Microsoft 365.
- Erläutern und Verwalten von Azure Identity Protection
- Planen und Implementieren von Azure AD Connect.
- Verwalten synchronisierter Identitäten.
- Erläutern und Verwenden des bedingten Zugriffs.
- Beschreiben der Bedrohungsvektoren für Cyberangriffe.
- Erläutern von Sicherheitslösungen für Microsoft 365.
- Bewerten und Verbessern Ihrer Sicherheitslage mit Microsoft Secure Score.
- Verschiedene erweiterte Bedrohungsschutzdienste für Microsoft 365.
- Planen und Bereitstellen sicherer mobiler Geräte.
- 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.
- Anfragen von GDPR-Datensubjekten verwalten.
- Erläutern und Verwenden von Vertraulichkeitsbezeichnungen.

Angesprochener Teilnehmerkreis:
- Administratoren
- Microsoft 365 Security Administratoren

Hinweis:
Der Kurs wird in deutscher Sprache gehalten, die MOC Unterlagen sind nur in englischer Sprache verfügbar.

Seminar- bzw. Schulungsinhalte

- Modul 1: Benutzer- und Gruppenverwaltung
  - Konzepte für Identitäts- und Zugriffsverwaltung
  - Das Zero Trust-Modell
  - Planen Ihrer Identitäts- und Authentifizierungslösung
  - Benutzerkonten und -rollen
  - Kennwortverwaltung

- Modul 2: Identitätssynchronisierung und -schutz
  - Planen der Verzeichnissynchronisierung
  - Konfigurieren und Verwalten synchronisierter Identitäten
  - Azure AD Identity Protection

- Modul 3: Identitäts- und Zugriffsverwaltung
  - Anwendungsverwaltung
  - Identity Governance
  - Verwalten des Gerätezugriffs
  - Rollenbasierte Zugriffssteuerung
  - Lösungen für externen Zugriff
  - Privileged Identity Management

- Modul 4: Sicherheit in Microsoft 365
  - Bedrohungsvektoren und Sicherheitsverletzungen
  - Sicherheitsstrategie und -prinzipien
  - Microsoft-Sicherheitslösungen
  - Sicherheitsbewertung

- Modul 5: Threat Protection
  - Exchange Online Protection (EOP)
  - Microsoft Defender für Office 365
  - Verwalten sicherer Anlagen

  - Verwalten sicherer Links
  - Microsoft Defender for Identity
  - Microsoft Defender für den Endpunkt

- Modul 6: Threat Management
  - Sicherheits Dashboard
  - Untersuchung von und Reaktion auf Bedrohungen
  - Azure Sentinel
  - Advanced Threat Analytics

- Modul 7: Mobilität
  - Verwaltung mobiler Anwendungen
  - Mobile Geräteverwaltung (MDM)
  - Bereitstellen von Diensten für mobile Geräte
  - Registrieren von Geräten für die Verwaltung mobiler Geräte

- Modul 8: Information Protection und Governance
  - Konzepte für Informationsschutz
  - Governance und Datensatzverwaltung
  - Vertraulichkeitsbezeichnungen
  - Archivierung in Microsoft 365
  - Aufbewahrung in Microsoft 365
  - Aufbewahrungsrichtlinien im Microsoft 365 Compliance Center
  - Archivierung und Aufbewahrung in Exchange
  - Direkte Datensatzverwaltung in SharePoint

- Modul 9: Rights Management und Verschlüsselung
  - Information Rights Management (IRM)
  - S-MIME (Secure Multipurpose Internet Mail Extension)
  - Office 365-Nachrichtenverschlüsselung

- Modul 10: Verhinderung von Datenverlust
  - Grundlagen zur Verhinderung von Datenverlust
  - Erstellen einer DLP-Richtlinie
  - Anpassen einer DLP-Richtlinie
  - Erstellen einer DLP-Richtlinie zum Schutz von Dokumenten
  - Richtlinientipps

- Modul 11: Complianceverwaltung
  - Compliance Center

- Modul 12: Management von Insiderrisiken
  - Insiderrisiko
  - Privilegierter Zugriff
  - Informationsbarrieren
  - Aufbauen ethischer Mauern in Exchange Online

- Modul 13: Suchen und Reagieren

- Inhaltssuche
- Überwachungsprotokolluntersuchungen
- Advanced eDiscovery

Seminar- bzw. Schulungsvoraussetzungen

- 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.

Seminarart

Dieses Seminar können Sie als Präsenzseminar oder als Live-Online-Training (virtuelles Präsenzseminar) buchen.

Dauer

4 Tage von 09:00 bis 16:00 Uhr

Anmeldung

Bitte online anmelden oder per Fax.

Weitere Seminare

Alle Seminare finden Sie in unserer Seminarübersicht.

Gerne unterbreiten wir Ihnen auch ein individuelles Angebot entsprechend Ihrer Wünsche und Vorstellungen. Senden Sie hierfür Ihre Anfrage einfach an training@pc-college.de.

Erstellt am 23.03.2025

Viele Partner für ein Ziel: Beste Leistung und Rundum-Service

Live-Online-Training
Berlin
Bremen
Dortmund
Dresden
Düsseldorf
Erfurt
Essen
Frankfurt
Freiburg
Hamburg
Hannover
Jena
Karlsruhe
Kassel
Koblenz
Köln
Krefeld
Leipzig
Mannheim
München
Münster
Nürnberg
Paderborn
Regensburg
Saarbrücken
Siegen
Stuttgart
A-Wien
CH-Basel
CH-Bern
CH-Zürich

PC-COLLEGE Zentrale Berlin

Stresemannstraße 78 (Nähe Potsdamer Platz) | D-10963 Berlin
Telefon: 0800 5777 333 / +49 (0)30 235 0000 | Fax: +49 30 2142988 | E-Mail: training@pc-college.de
Ansprechpartner*in: Stefanie Wendt und Kollegen*innen

Alle Informationen und Aktionsangebote finden Sie unter www.pc-college.de