MOC 20744 Securing Windows Server 2016

Seminardauer: 5 Tage, 09:00 Uhr bis 17:00 Uhr
Schulungsunterlagen: nach Absprache

In diesem Kurs lernen die Teilnehmer, wie sie die Sicherheit Ihrer IT-Infrastruktur durch verschiedene Methoden und Tools verbessern können.

Zielgruppe

IT professionals
Windows Server 2016 Administratoren

Kurs Voraussetzungen

Besuch der Kurse MOC 20740 Installation, Storage and Compute with Windows Server 2016, MOC 20741 Networking with Windows Server 2016 und MOC 20742 Identity with Windows Server 2016oder äquivalent
Mindestens zwei Jahre Erfahrung im IT Umfeld
Praktisches Verständnis für TCP/IP, User Datagram Protocol (UDP), Domain Name System (DNS), Active Directory Domain Services (AD DS), Hyper-V Virtualisierung und Windows Server Security

Agenda

Attacks, Breach Detection, und Sysinternals tools

- Angriffe verstehen
- Erkennen von Sicherheitsverletzungen
- Überprüfung der Aktivitäten mit den Tools von Sysinternals

Anmeldedaten schützen und bevorrechtigter Zugang

- Benutzerrechte verstehen
- Computer- und Servicekonten
- Schützen von Anmeldeinformationen
- Privilegierter Zugriff auf Workstations und Jump-Server
- Lokale Administrator-Passwort-Lösung

Beschränkte Administratorenrechte mit Just Enough Administration

- JEA verstehen
- Verifizierung und Bereitstellung von JEA

Bevorrechtigtes Zugriffs-Management und Administrative Forests

- ESAE Forests
- Überblick über Microsoft Identity Manager
- Überblick über JIT-Administration und PAM

Abwehr von Malware und Bedrohungen

- Konfigurieren und Verwalten von Windows Defender
- Einschränkung der Software
- Konfigurieren und Verwenden der Device Guard-Funktion

Aktivitätsanalyse mit erweiterten Audits und Protokollanalysen

- Überblick über die Auditierung
- Erweiterte Auditierung
- Windows PowerShell-Auditierung und -Protokollierung

Bereitstellung und Konfiguration von Advanced Threat Analytics und Microsoft Operations Management Suite

- Bereitstellen und Konfigurieren von ATA
- Bereitstellen und Konfigurieren der Microsoft Operations Management Suite
- Bereitstellen und Konfigurieren von Azure Security Center

Sichere Virtualisierungsinfrastruktur

- Geschütztes Gewebe
- Abgeschirmte und von Verschlüsselung unterstützte virtuelle Maschinen

Sicherung der Anwendungsentwicklung und der Server-Workload-Infrastruktur

- Verwendung von SCT
- Container verstehen

Planung und Schutz von Daten

- Planung und Implementierung von Verschlüsselung
- Planung und Implementierung von BitLocker
- Schutz von Daten durch den Einsatz von Azure Information Protection

Optimierung und Sicherung von Dateidiensten

- Dateiserver-Ressourcen-Manager
- Implementierung von Klassifizierungs- und Dateiverwaltungsaufgaben
- Dynamische Zugriffskontrolle

Sicherung des Netzwerkverkehrs mit Firewalls und Verschlüsselung

- Verständnis für netzwerkbezogene Sicherheitsbedrohungen
- Windows-Firewall mit erweiterter Sicherheit verstehen
- Konfigurieren von IPsec
- Firewall im Rechenzentrum

Sicherung des Netzwerkverkehrs

- Konfigurieren von erweiterten DNS-Einstellungen
- Untersuchung des Netzwerkverkehrs mit dem Message Analyzer
- Sicherung und Analyse des SMB-Verkehrs