

IT-Sicherheit - Sichere Windows-Netzwerke einrichten und überwachen

In unserem IT-Sicherheit Seminar erwerben Sie essentielle Fähigkeiten, um Windows-Netzwerke gegen die ständig wandelnden Bedrohungen des Internets zu schützen. Erlernen Sie die Erkennung und Abwehr verschiedener Angriffsmethoden, sichern Sie Netzwerke durch Basismaßnahmen und verbessern Sie die Sicherheit mit regelmäßigem Patching.

Sie lernen, Administrator-Kennwörter mit Windows-LAPS zu sichern, Multifaktor- und biometrische Authentifizierung einzurichten und die Konfiguration von Authentifizierungsrichtlinien sowie Privilegierte Administrativen Arbeitsstationen (PAW) vorzunehmen. Der Kurs deckt auch Verschlüsselungstechnologien, die Einrichtung von Windows Credential Guard und Defender Application Guard, sowie die Nutzung von TPM-Modulen und Smartcards ab.

Vertiefen Sie Ihr Verständnis von Windows Sicherheitseinstellungen, Gruppenrichtlinien, Security Baselines, und Festplattenverschlüsselung mit Bitlocker. Lernen Sie, wie man Windows Defender, die Windows Firewall, PowerShell-Sicherheit, Just Enough Administration, und Active Directory absichert, Netzwerke mit Schwachstellenscannern überprüft und sich auf Sicherheitsvorfälle vorbereitet.

Dieses Seminar ist ideal, um Ihre Kompetenzen in der Netzwerksicherheit zu erweitern und Windows-Netzwerke vor modernen Bedrohungen zu schützen, indem Sie Ihre IT-Infrastruktur sicher und widerstandsfähig gestalten.

Zielsetzung:

Bei diesem Seminar lernen Sie die entscheidenden Schritte zur Absicherung Ihrer Windows Server Infrastruktur kennen und werden darauf vorbereitet, Ihr Windows-Netzwerk sicher und effektiv zu betreiben.

Angesprochener Teilnehmerkreis:

Der Kurs richtet sich an Administratoren und Sicherheitsbeauftragte, die sich mit der Absicherung von Windows-Netzwerken auseinandersetzen müssen.

Seminar- bzw. Schulungsinhalte

- Aktuelle Bedrohungsszenarien in Windows-Netzwerken
 - Angriffe erkennen und abwehren
 - Wie dringen Angreifer ins Netzwerk ein
- Basismaßnahmen zur Absicherung von Windows-Netzwerken
 - Maßnahmen zur regelmäßigen Aktualisierung/Patching der Software
 - Administrator-Kennwörter mit dem Windows-LAPS-Tool absichern
 - Sichere Kennwortrichtlinien implementieren
 - Multifaktorauthentifizierung einrichten
 - Biometrische Authentifizierung mit Windows Hello
 - Einrichten von Privilegierten Administrativen Arbeitsstationen (PAW)
 - Authentifizierung-Richtlinien und Authentifizierungs-Richtlinien-Silos einrichten

- Verschlüsselung
 - Überblick über Kryptografische Verfahren
 - Einführung in die Symmetrische Verschlüsselung mit AES
 - Einführung in die Asymmetrische Verschlüsselung
 - Signaturen und Zertifikate
 - Funktion und Zweck von TPM-Modulen und Smartcards
- Virtualisierungsbasierte Sicherheit implementieren
 - Einführung in die Funktionsweise von UEFI, Secure Boot und Measured Boot
 - Windows Credential Guard
 - Sichere Browser-Einrichtung mit dem Windows Application Guard
 - Windows Defender Application Guard einrichten
- Windows Sicherheitseinstellungen verwalten
 - Windows mit Gruppenrichtlinien sichern
 - Die Windows Security Baselines einrichten und testen
 - Festplattenverschlüsselung mit Bitlocker einrichten
 - Die Windows Firewall mit Gruppenrichtlinien und Powershell konfigurieren
 - Windows Defender Sicherheitsfunktionen konfigurieren
 - Typische Angriffsszenarien mit Exploitation-Frameworks und Powershell
- Powershell absichern
 - Mit Ausführungsrichtlinien die Ausführung von Skripten verhindern
 - Die Language Modes von Powershell verstehen
 - Die Ausführung von Powershell-Skripten mit Applocker oder Application Control einschränken
 - Skriptblock-Logging aktivieren, um die Ausführung von Skripten zu überwachen
 - Just Enough Administration verstehen und einrichten
 - Weitere Maßnahmen
- Active Directory sichern
 - Einrichten und verwalten von managed Service Accounts
 - Die Protected Users Gruppe verwenden
 - Authentication Silos zur Sicherung von Administrativen Workstations einrichten
 - Implementieren und testen der Microsoft Security Baselines
 - Kerberos verstehen und härten
 - Read Only Domain Controller einrichten
 - Überblick über die Gefahren falsch eingerichteter Zertifikatsdienste
 - Überblick über die Vor- und Nachteile von Enhanced Security Administrative Environments (Red Forest)
- Windows-Überwachungs-Richtlinien einrichten
 - Überwachungsrichtlinien aktivieren
 - Das Sicherheits-Ereignisprotokoll auswerten
 - Das Sicherheits-Ereignisprotokoll zentral sammeln mit Eventlog-Forwarding
 - Einrichten von Security Onion zur Protokollierung von ungewöhnlichen Netzwerkzugriffen
- Weitere Maßnahmen

- Netzwerke mit Schwachstellenscannern überprüfen
- Vorbereitung auf Sicherheits-Vorfälle: Vorgehensweise und Checklisten
- Sichere Backups einrichten

Seminar- bzw. Schulungsvoraussetzungen

Solide Windows-Server und Active-Directory Kenntnisse.

Seminarart

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

Dauer

5 Tage von 09:00 bis 16:00 Uhr

Preise

Teilnahmegebühr: ab 3.490,00 € (4.153,10 € inkl. 19% MwSt.) Preis abhängig vom Standort

Im Preis enthalten sind PC-COLLEGE - Zertifikat, Pausenverpflegung, Getränke und Kursmaterial.

Anmeldung

Bitte **online** anmelden oder per **Fax**.

Termine

Die aktuellen Termine und Standorte für IT-Sicherheit - Sichere Windows-Netzwerke einrichten und überwachen finden Sie **online**.

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 15.09.2024

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