>> Windows Server

Security Hardening Workshop

EGOS! the education company

Windows Server ist ein Server-Betriebssystem von Microsoft. Neben Basis-Funktionen wie Datei- und Druckdiensten stellt es die Infrastruktur für alle Microsoft Enterprise Server zur Verfügung.

Ihr Nutzen

Nach dem Seminar können Sie erkannte Schwachstellen in Windows Server Umgebungen beurteilen und Gegenmaßnahmen ergreifen und diese konfigurieren. Das Verständnis von gefundenen Schwachstellen in einem "standardmäßig" installierten Windows Server ist für einen erfolgreichen Betrieb lebensnotwendig.

Voraussetzungen

Gute Administrationskenntnisse inkl. Netzwerk und Active Directory in Windows Server

Preis pro Teilnehmer

EUR 2550,- exklusive der gesetzlichen MwSt.

Hinweise

-

Seminardauer

4 Tag(e)/Day(s)

Version: 2025

Seminarinhalte

1. Tag
* Ist ein Windows Server "secure by default?"
- Review von Security Baselines
- Review von Vulnerability Scans

* Authentication Basics
- NTLM Architektur
- Kerberos Architektur

* Windows Security Architecture
- Access Tokens
- ACL und ACE
- Built-In Identities (System, Network Service, LocalService)
- Special Identities (CREATOROWNER, OWNER RIGHTS)
- User Account Control
- Services und Sessions
- Credential User Interface Settings

2. Tag
* Windows Security Optionen
- User Rights Assignments

* NTFS ACLs und ACEs
- Share-Berechtigungen und NTFS Berechtigungen verstehen
- Alternate Data Streams
- Local SID Filtering, Local Account Filter Policies

* Security Optionen
- SMB Sessions explained
- SMB Versionen verstehen und deaktivieren
- Interactive Logon Options
- Microsoft Network Client/Server Settings
- Domain Member Settings: Signing und Sealing

* Domain Controller Security
- LDAPS Signing
- Kerberos mit Certificates

3. Tag
* Security-Relevants GPOs
- Hardened UNC Paths
- Windows Connection Manager
- Internet Communication Settings
- RPC Policies

* Auditing Settings
- Account/Logon/Logoff Auditing
- File/Object/AD Access Auditing
- Process Auditing
- Advanced Audit Settings
- Eventlog Settings
- Securing Event Logs mit SDDL

* PowerShell Security
- Execution Policies per GPO steuern
- Contrained Language Mode
- PowerShell Transcriptions
- WinRM Security

* Free Add-Ons
- LAPS
- JIT und JEA

4. Tag
* After The Show
- Temp Folders
- Page Files
- Watson Reports und Crash Dumps

* Network Security
- Disable IPv6 or not?
- SSL/TLS Security
- Ciphers deaktivieren
- IISCrypto
- Windows Firewall per GPO konfigurieren
- IPSec und Domain Isolation

* MS Security Baseline
- Security Analyzer
- MS Sec GPOs

* Quick Wins or not?
* Secure Boot and Virtualization Based Security