CTW-100 IT-Sicherheit in Windows Server 2016/2019/2022 OnPremise

Die Lage der IT-Sicherheit ist im Wandel. Waren es früher einfache, gestreute Angriffe, die auf eine bestimmte Lücke im System zielten so sind es heute vollautomatisierte Malware-Suiten im professionellen Design und mit kommerziellen Strukturen. Aber auch die Hersteller von Betriebssystemen und Applikationen haben den Trend erkannt und stellen immer mehr Schutzkomponenten zur Verfügung. In unserem praxisorientierter Workshop lernen Sie die Schwachstellen einer Windows Infrastruktur kennen und lernen anhand aktuell verfügbarer Schutzkomponenten Angriffe erfolgreich abzuwehren bzw. einzugrenzen.

Listenpreis

2.100,00 € exkl. MwSt

2.499,00 € inkl. MwSt

Dauer

3 Tage

Leistungen Präsenz

- Schulung im Trainingscenter
- Verpflegung
- Teilnahmebestätigung / Zertifikat

Leistungen bei VCL Training

- Technischer Support
- Online Zugang
- Teilnahmebestätigung / Zertifikat

Ihre Ansprechpartnerin

Gabriela Bücherl
Geschäftsführung
Vertrieb

Kontakt/Fragen:
g.buecherl@cbt-training.de
Telefon: +49 (0)89-4576918-16

Inhalte

- **Einstieg**
  - Rechtliches
  - aktuelle Bedrohungsszenarien
  - Begriffe und Definitionen
  - Hacking Cycle (Anatomie eines Hacks)
  - Standard-Schutzkomponenten (AntiVirus, Firewall, UAC, Applocker, Windows Updates)
- **Erkennen und Reagieren**
  - Angriffe erkennen
  - auf Angriffsszenarien reagieren
- **Physikalische Sicherheit**
  - Angriffsvektoren
  - Bitlocker
  - UEFI SecureBoot
- **Authentifizierung**
  - Grundlagen
  - Angriffsszenarien
    - Credential Storage (CredMan, SAM, LSASS, LSA, NTDS)
    - Authentication Packages (WDIGEST, NTLM, Kerberos)
    - Credential Validation (Keylogger, Clipboardmonitor)
  - Schutzmaßnahmen
    - PasswordPolicies
    - LockoutPolicies
    - AD-Konten absichern
    - Umgang mit lokalen Credentials & LAPS
    - Umgang mit CredMan
    - Secure Desktop und UserSwitching
    - Protected Users
    - WDigest Hardening
    - Deaktivierung von NTLM

  - LSA Protection
  - Device Guard & Credential Guard
  - SmartCard
  - MFA
  - Umgang mit ServiceAccounts (Group Managed Service Accounts)
  - LDAPS
- **Active Directory**
  - aktuelle Empfehlungen
  - Security Compliance Toolkit (SCT)
  - Least Privilege (Tier Management, Security Scopes
  - Privileged Access Management
  - ESAE - Administrative Forest im Überblick
  - KRBTGT
- **Netzwerk**
  - Absicherung der Namensauflösung
  - Man in The Middle (MiTM, ARP-Poisoning, Hardware)
  - Absicherung von WLAN
  - Sicherheitsfeatures von SMB
  - Härtung von TLS
  - Netzwerksegmentierung, Privileged Access Workstation (PAW), Jumpserver
  - Intrusion Detection/Prevention Systems (IDS, IPS) im Überblick
- **PowerShell**
  - PowerShell als Angriffswerkzeug
  - Execution Policy
  - Script Block Logging
  - Transcription
  - Anti Malware Scan Interface (AMSI)
  - Constrained Language Mode

Ziele

Lernen Sie in diesem modularen Workshop eine moderne LAB-Infrastruktur (Windows Server 2016/2019/2022 und Windows Client) aus der Perspektive eines Angreifers kennen.

Sie bekommen einen grundlegenden Einblick in die aktuellen Komponenten einer Windows Infrastruktur und lernen deren Schwachstellen kennen. Danach werden etliche Gegenmaßnahmen besprochen und praxisnah im LAB implementiert. Werden diese einem weiteren Angriff standhalten? Nur wer die Werkzeuge und Methoden der Angreifer kennt und die aktuellen Schutzkomponenten versteht kann aktuelle Angriffe erfolgreich abwehren bzw. eingrenzen!

Der Workshop ist modular aufgebaut. Die thematische Breite und die Intensität wird in der praxisnahen Gestaltung individuell vom Dozenten mit den Teilnehmern bestimmt.

Bei Inhouse- und Firmenschulungen werden explizite Themenwünsche gerne vorab besprochen.

Zielgruppe

IT-Professionals, die Ihre Windows Server Infrastruktur mit den zur Verfügung stehenden Werkzeugen und Methoden absichern möchten.

Voraussetzungen

Sie benötigen gute Kenntnisse in der Administration und dem Design von Windows Server Infrastrukturen (Active Directory, DNS, FileServices, DHCP).
Grundlegende Schutzmaßnahmen (Antivirus, Windows Firewall, Benutzersteuerung, Windows Updates) sind Ihnen keine Fremdworte.
Aber auch Grundlagen im Netzwerkbereich (OSI, IPv4, optional IPv6) sind von Vorteil.
