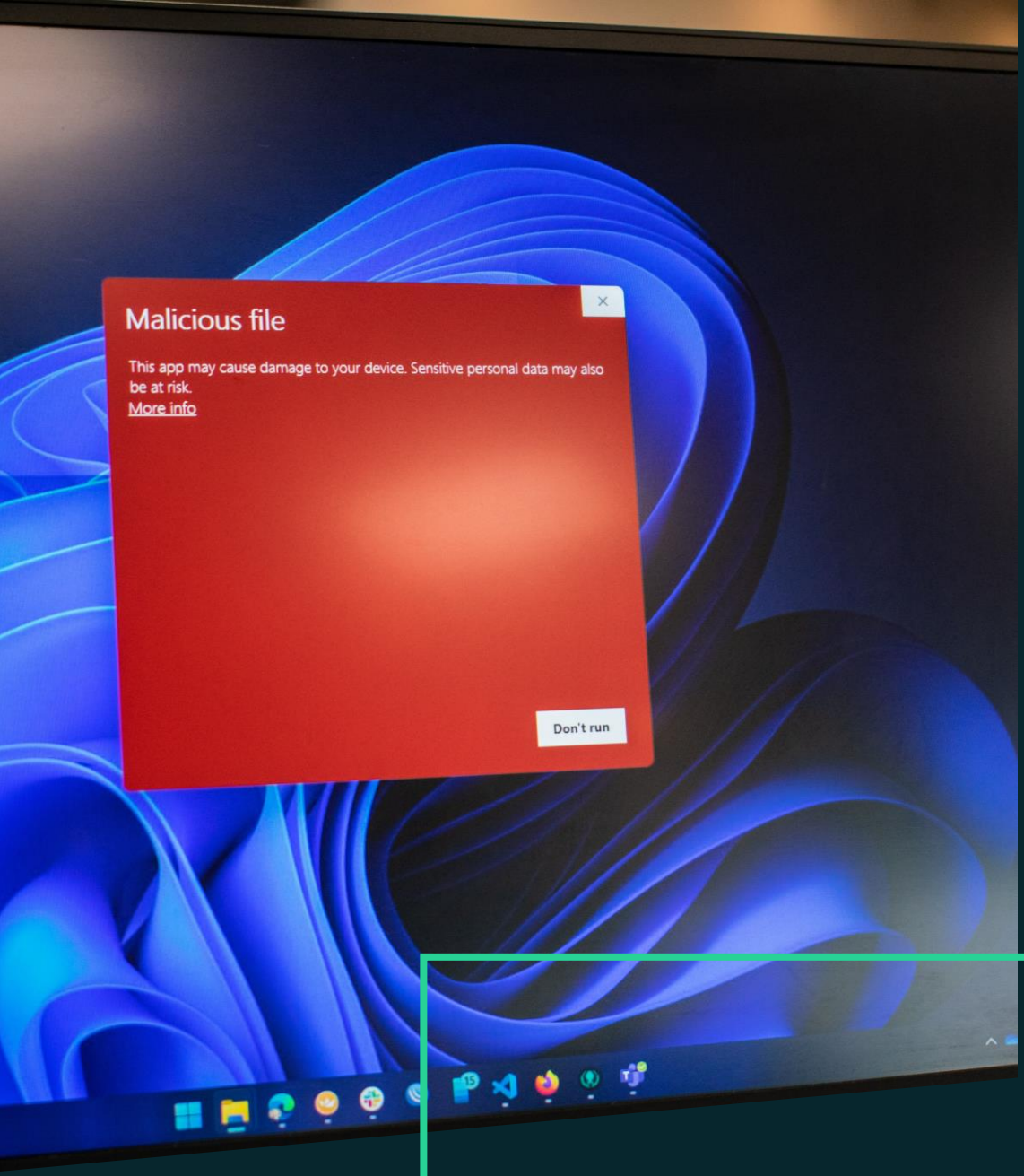
bitkom
akademie



Windows Security Expert

Wie Sie die Active Directory schützen und Sicherheitslücken schließen

Windows Security Expert

Wie Sie die Active Directory schützen und Sicherheitslücken schließen

Kurzbeschreibung

Ein Cyberangriff ist keine Frage des “Ob” – sondern bloß eine Frage des “Wann”. So kommt es regelmäßig in Unternehmen vor, dass Mitarbeitende einen (Verschlüsselungs-)trojaner auf dem System ausführen. Wie weit sich ein Angreifer in so einem Fall dann in Ihrem Unternehmensnetzwerk ausbreiten kann und wie schlimm die Konsequenzen für Sie sind, hängt maßgeblich von der Sicherheit Ihrer Active-Directory-Infrastruktur ab. Bereits kleine Konfigurationsfehler können die vollständige Kompromittierung Ihrer Windows-Domäne bedeuten.

In diesem **Zertifikatslehrgang** erwerben Sie höchstrelevante IT-Security-Kenntnisse, um die on-premise Microsoft Windows-Infrastruktur (Active Directory) in Ihrem Unternehmen vor Angriffen zu sichern. Sie lernen dabei anhand von praktischen Übungen in einem virtuellen Labor, in dem eine realitätsnahe Windows-Infrastruktur nachgebaut ist.

Inhalt

- Typische Angriffspfade auf Windows-Infrastruktur
- Funktionsweise Windows-spezifischer Protokolle und Dienste
- Werkzeuge, die Hacker nutzen und warum sie funktionieren
- Sicherheitskritische Konfigurationsoptionen
- Härtung von Active-Directory-Infrastrukturen

Was lernen Sie in diesem Zertifikatslehrgang?

Sie lernen die technischen Grundlagen, Funktionsweisen und Sicherheitsimplikationen von Windows-spezifischen Protokollen, Diensten und Konfigurationsoptionen kennen und erfahren, wie leicht Hacker Konfigurationsfehler ausnutzen können, um ihre Infrastruktur vollständig zu kompromittieren. Unsere Referenten erklären und veranschaulichen Ihnen, wie Sie Ihre Active-Directory-Installation gegen Angriffe härten können. Nach Abschluss dieses Seminars sind Sie selbst in der Lage Sicherheitsprobleme in Ihrer Windows-Infrastruktur (on-premise) aufzudecken und zu beseitigen.

bitkom akademie

Windows Security Expert

Wie Sie die Active Directory schützen und Sicherheitslücken schließen

Zielgruppe

Dieser Zertifikatslehrgang richtet sich an Administratoren von IT-Infrastrukturen und an alle Mitarbeitenden, die mit Aufgaben im Bereich der IT-Sicherheit betraut sind. Grundkenntnisse im Umgang mit der Active Directory (AD) von Windows werden vorausgesetzt.

Didaktischer Aufbau

Der Lehrgang ist **sehr praxisorientiert** gestaltet: Sie wenden das Gelernte in einem **virtuellen Labor** selbst. Durch das Nachvollziehen von typischen Angriffswegen lernen Sie aktiv, wie Systeme gegen Sicherheitslücken gehärtet werden können. Am ersten Schulungstag werden zunächst wichtige technische Grundlagen aus dem Bereich der Windows-Infrastruktur und deren Sicherheitsimplikationen behandelt sowie die grundlegenden Vorgehensweisen von Angreifern, die ein Windows-Netzwerk infiltrieren wollen. Der zweite Schulungstag behandelt **fortgeschrittenere Mechanismen und Fehlkonfigurationen**. Alle Themengebiete werden anhand von praktischen Beispielen erläutert.

Zertifikatsprüfung

Diese Schulung beinhaltet eine Zertifikatsprüfung, bei der Sie Ihr erworbenes Wissen in einem virtuellen Labor praxisnah unter Beweis stellen müssen. Nach Bestehen der Prüfung erhalten Sie ein Zertifikat, das auf einem Qualitätsstandard basiert, den sich die Bitkom Akademie und ihre Partner als Qualitätssiegel für ihre Ausbildungslehrgänge gesetzt haben.

Zusatzinformationen

- Das Seminar findet im kleinen Kreis mit einer Maximalteilnehmerzahl von **15 Personen** statt. Die Mindestteilnehmerzahl beträgt 5.
- **Systemvoraussetzungen:** Für die Teilnahme benötigen Sie eine Software für das Ausführen von virtuellen Maschinen (s. Spezifikation auf Website).
- Der Online-Lehrgang wird mit Zoom durchgeführt. Systemvoraussetzungen und unterstützte Betriebssysteme können Sie hier einsehen. Für die Einwahl in Zoom über die verschiedenen Anwendungen (Desktop Client, App oder Web-Client) bietet Ihnen diese Tabelle einen zusätzlichen Vergleich zu den Eigenschaften.
- Die Bitkom Akademie ist anerkannter Bildungsträger in Baden-Württemberg und Nordrhein-Westfalen. Teilnehmende haben im Rahmen des Bildungszeitgesetzes die Möglichkeit, Bildungsurlaub bzw. eine Bildungsfreistellung zu beantragen. Auf Anfrage erstellen wir auch Anträge auf Anerkennung unserer Veranstaltungen in anderen Bundesländern.
- Wir erklären ausdrücklich, dass beim Bitkom – Unterzeichner der Charta der Vielfalt – jede Person, unabhängig von Geschlecht, Nationalität, ethnischer Herkunft, Religion oder Weltanschauung, Behinderung, Alter, sexueller Orientierung und Identität willkommen ist.

bitkom akademie

Seminarprogramm

Windows Security Expert

Tag 1

Tag 1

Basiswissen: Auffrischung
- (Windows-)Netzwerke
- Wichtige Server und Dienste
- Angriffsmodelle und Angriffsvektoren

Protokolle und Mechanismen im Windows-Umfeld kennen und Sicherheitsimplikationen verstehen
- Kerberos
- SMB
- NTLM-Authentifizierung
- RDP
- Lokale Administratoren

Enumeration von Windows-Netzwerken
- Bloodhound
- smbmap, enum4linux
- PowerView

Passwörter, Relaying und Pass-the-Hash-Angriffe
- crackmapexec
- mimikatz
- Service Accounts

Tag 2

Tag 2

SMB-Fehlkonfigurationen
- SMB 1
- Signatur von SMB-Nachrichten
- RPC

Exploit-Chains über Veraltete Software und Software-Fehlkonfigurationen
- Vom Jenkins-User zum Domänenadministrator

(Unconstraint) Delegation, ACLs
- Rubeus

Kerberos
- Kerberoast
- Golden Tickets

bitkom akademie

Seminarprogramm

Windows Security Expert

Tag 3

Tag 3

Wiederholung der wichtigsten Konzepte und Werkzeuge

- Enumeration
- Pass-the-Hash
- SMB
- Wichtige Werkzeuge

Zertifikatsprüfung

- Lösen von Aufgaben in einem virtuellen Prüfungslabor

bitkom akademie

Ihre Referenten

Dr. Jochen Rill

Head of Cyber Security
Alter Solutions Deutschland GmbH

Dr. Jochen Rill hat im Bereich Kryptographie promoviert und leitet seit Anfang 2022 den Cyber-Security-Bereich bei Alter Solutions Deutschland. Als Offensive-Security-Experte hat er alle typischen Sicherheitsfehlern bei Windows-Infrastruktur schon einmal gesehen.

Julian Herr

Team Lead Security Testing
Alter Solutions Deutschland GmbH

Julian Herr verfügt über langjährige Expertise in den Bereichen IT-Sicherheit und Kryptographie. Im Rahmen verschiedener Projekte beteiligte er sich an Sicherheitsaudits verschiedener Anwendungen im Gesundheitsbereich und anderer kritischer Infrastrukturen. Seit 2022 unterstützt er die Alter Solutions Deutschland GmbH bei verschiedenen Pentests von (Web-) Anwendungen, Netzwerken sowie der sicheren Softwareentwicklung im IoT-Bereich.

Shortfacts

Termine, Veranstaltungsort und Preise

Die aktuellen Informationen entnehmen Sie bitte der ↗ Website der Bitkom Akademie.

Kontaktieren Sie uns – wir beraten Sie gern.

Bitkom Akademie | Albrechtstraße 10 | 10117 Berlin
T 030 27576-540 | info@bitkom-akademie.de
Weitere Seminare finden Sie unter **www.bitkom-akademie.de**

bitkom akademie