

Active Directory Security Attacks & Defenses

Trainings-ID: ADSAD

Zum Seminar →

Das nehmen Sie mit

Zentrale Identity & Access Management Systeme (wie Microsofts Active Directory) stellen aufgrund ihrer Komplexität und meist fehlenden Härtung der Systeme und Protokolle ein verhältnismäßig hohes Risiko dar gegenüber externen Angreifern dar. Aus diesem Grund zielen Angreifer mittlerweile fast ausschließlich auf die Ausweitung Ihrer Rechte durch verschiedene Schwachstellen der Active Directory & Kerberos-Protokollfamilie ab. In über 90% aller erfolgten Angriffsfälle wird das zentrale Benutzer und Rechtemanagement-System infiltriert. Öffentlich verfügbare Angriffstools wie „Mimikatz“ stellen daher ein enormes Bedrohungspotential dar, zudem diese mittlerweile auch in so genannten „File-less“-Varianten für Angreifer verfügbar sind, welche lediglich im flüchtigen Arbeitsspeicher laufen, sodass übliche Anti-Viren-Scanner gar keine Chance zur Identifikation der Malware bzw. der Systeminfiltration bekommen.

Das Training richtet sich primär an IT-Sicherheitsverantwortliche, System & Sicherheitsarchitekten sowie Systemadministratoren.

Mit dem Wissen über aktuelle Angriffe und Sicherheitskonzepten bewaffnet, können Sie Sicherheitsmaßnahmen in die oberste Planungs- und Steuerungsebene Ihrer Organisation integrieren und Ihr zentrales IAM-System entsprechend absichern. So können finanzielle Kosten durch Reputations- und Opportunitätsverluste sowie Aufwände für die nachträgliche Aufklärung und Behandlung von erfolgten Angriffen minimiert werden.

Lernen Sie in diesem Kompakt-Training worauf es im Kontext Active Directory Security ankommt und wie Sie Ihr Unternehmen effizient schützen können.

Das Training führt die Teilnehmer in 4 Bausteinen schnell, kompakt und umfassend in die aktuellen Risiken, Angriffe, Sicherheitsstrategien sowie Methoden und Tools zur Wirksamkeitsprüfung von Sicherheitsmaßnahmen für Active Directory Systeme ein.

Sie haben Fragen?  +43 1 533 1777-0  info@etc.at  Modecenterstraße 22, 1030 Wien

Dabei wird auf die zugrunde liegenden Bedrohungsszenarien und die Vorgehensweisen von Angreifern eingegangen und allgemeine Anforderungen an die Steuerung der IT anhand des SANS Top 20 CSC Modells erläutert, anhand dessen ein Beispiel zur Umsetzung von Standard-Sicherheitsmaßnahmen dargestellt wird.

Im Angriffs-Teil werden die wichtigsten bzw. verbreitetsten Angriffe auf Active Directory/Kerberos-Umgebungen anhand von Mimikatz dargestellt. Zudem wird gezeigt, wie Angreifer Mimikatz-Varianten so manipulieren, dass bestehende Anti-Viren-Systeme diese nicht erkennen können.

In weiterer Folge werden die verfügbaren Sicherheitskonzepte und empfohlenen Konfigurationshärtungen mit Ihren Vor- und Nachteilen dargestellt sowie Anleitungen zur Durchführung von technischen und organisatorischen Self-Assessments und Wirksamkeitsprüfungen vermittelt.

Zielgruppen

- IT-Sicherheitsverantwortliche
- System & Sicherheits-Architekt*innen
- IT-Verantwortliche
- Informationssicherheitsbeauftragte
- IT-Risikomanager*innen
- Incident Manager*innen
- Datenschutzbeauftragte und -koordinatoren

Termine & Optionen

Datum	Dauer	Ort	Angebot	Preis
02.07.2024	1 Tag	Wien	Preis (Präsenz)	€ 1.050,-
02.07.2024	1 Tag	Wien	Preis (Online)	€ 1.050,-
24.09.2024	1 Tag	Wien	Preis (Präsenz)	€ 1.050,-
24.09.2024	1 Tag	Wien	Preis (Online)	€ 1.050,-

Sie haben Fragen?  +43 1 533 1777-0  info@etc.at  Modecenterstraße 22, 1030 Wien