

> MITRE ATT&CK

Der Horizont für Angreifer und Verteidiger

> Information Gathering

Finden ihrer besonders exponierten Systeme und Personen durch Google-Hacking

> Initial Access

Initiale Zugriffsvektoren der Angreifer verstehen und reduzieren

> Security Scanning

Vermeiden von Windows- und Linux-Schwachstellen in ihrem Netzwerk

> Credential Access

Authentifizierungsmechanismen verstehen und unerlaubte Zugriffe verhindern

> Exploits

Zugriff auf Rechner durch fehlende Updates

> Ransomware & Trojaner

Wie Hacker mittels Schadsoftware gepatchte Systeme, Firewalls, Virens Scanner und EDR-Systeme umgehen.

> Discovery

Finden von Lowhangig-Fruits und beschützen von Unternehmenswerten.

> Privilege Escalation

Wie sich Mitarbeiter (nicht mehr) zum Administrator hocharbeiten können

> Persistence

Verstehen, wie sich Hacker den Zugriff sichern und wie dies erkannt werden kann

> „Best Practice“-Schutzmaßnahmen

Detektionsverfahren

IT-Security-Prinzipien

Konfigurationsempfehlungen

Patch Management

Monitoring und Logging

Service Hardening und Service Accounts

Effektiver Schutz vor Malware und Hackern

Hardening verbreiteter Firewall und EDR-Produkte



Attack & Defense I

Angriff & Verteidigung für Admins

IT-Spezialisten haben das **größte Potential**, IT-Schwachstellen zu schaffen oder zu verhindern. Viele übernommene Mythen über Netzdesign, Firewalls, Security-Produkten oder Programmieretechniken **öffnen für Angreifer ungewollt Tür und Tor**.

Dieser Workshop zeigt **aktuelle Hacker-Angriffe**, auf Windows- wie Linux-Systeme, in einfacher und verständlicher Form. Sie **verstehen Angriffsvektoren, Schwachstellen, Gegenmaßnahmen** und lernen über Stärken und Schwächen von **Security-Produkten**, indem Sie sie im Lab-Netzwerk, in praxisnahen Übungen, selbst nachstellen.

Abgerundet durch den Austausch mit gleichgesinnten IT-Administratoren und erfahrenen Penetration-Testern, können Sie nach dem Workshop **aktuelle Angriffe selbst erkennen und verhindern**.

Termin: Mi. 19. – Fr. 21. Jänner 2022

Schulungsort: SoHo2 Innsbruck / wahlweise remote

Voraussetzungen: Gute IT-Grundkenntnisse. Der Workshop richtet sich an IT-Leiter, IT-Administratoren, IT-Security-Verantwortliche und IT-Profis.

Seminarpreis: **2.395 EUR** exkl. MwSt. für 3 Tage