

SECURITY NIGHTMARE 2026

AGENDA - 30.10.2026

13:30 **Anmeldung und Begrüßung**

14:00 **Einführung**

- Aufbau typischer Angriffe und Motivation für Angriffsmodelle
- Vorstellung der Cyber Kill Chain und ihrer Phasen
- Einordnung gängiger Angriffstechniken nach MITRE ATT&CK
- Storytelling-Intro: Szenariobeschreibung für das Training

14:30 **Phase 1: Reconnaissance**

- Zielsystem verstehen und erste Informationen sammeln
- Überblick: Open Source Intelligence (OSINT) Methoden
- Praktischer Teil: Erkennen von Angriffsflächen und Auffinden sensibler Informationen

15:00 **Phase 2–5: Weaponization & Delivery**

- Überblick zu gängigen Ansätzen für Weaponization und Delivery
- Beispielhafte Wege zur Ausnutzung von Schwachstellen
- Praktischer Teil: Aufbau und Einschleusen eines manipulierten Artefakts in eine Zielumgebung

16:30 **Pause**

16:45 **Phase 6: Installation / Exploitation**

- Ausweitung des initialen Zugriffs: Persistence, Privilege Escalation, Exploitation
- Praktischer Teil: Durchführung vorbereiteter Exploits und Etablierung eines verdeckten Zugangs

18:15 **Pause – Abendessen (Pizza)**

19:00 **Phase 7: Actions on Objectives**

- Zielorientierte Angriffe: Datendiebstahl, Manipulation, Cluster-Kontrolle
- Praktischer Teil: Umsetzung eines finalen Angriffsschritts zur Demonstration der möglichen Auswirkungen

20:45 **Abschluss & Recap**

- Rückblick auf die Phasen und zentrale Erkenntnisse
- Diskussion: Welche Schwachstellen haben den Angriff ermöglicht?
- Transfer in die eigene Praxis: Was lässt sich daraus für den Alltag ableiten?