



## DER IDEALE ÜBERBLICK

# ADVANCED LINUX SECURITY

**Die Herausforderung: Auch Linux-Systeme sind von Schwachstellen und Exploits betroffen.** Da Linux-Systeme im IT-Bereich sowie beim Endnutzer breite Verwendung finden, braucht es auch hier eine gezielte Sicherheitsstrategie: gerade im Serverumfeld oder beim Einsatz in Umgebungen. Dieses Seminar befähigt Sie dazu, fortgeschrittene Härtungstechniken für Linux umzusetzen, die es Angreifern stark erschweren, dem System zu schaden. Sichern Sie Ihr Linux System mit individuellen Strategien und Mechanismen.

### Inhalte des Seminars

#### Filesystem Security

- Hands-on: Demonstration und Erklärung eines Exploits
- Integrität des Dateisystems/Verschlüsselung
- Hands-on: Setup besonderer Dateisysteme

#### Virtualisierungstechniken

- Isolierung von Prozessen (Prozessgruppen) und sichere IPC (Interprozesskommunikation) mit Virtualisierungstechniken
- Hands-on: Experimente mit Virtualisierungstechniken

#### Capabilities, Cgroups, Seccomp

- Hands-on: Konfiguration mit Cgroups
- Hands-on: Anwendungen von Seccomp und Capabilities

#### Linux Security Modules (LSM)

- LSM, Implementierungen und Richtlinien
- Hands-on: LSM Setup
- Entwurf von sicheren, virtualisierten Systemen

#### Trusted Computing und Secure Hardware

- HSMs und Secure Elements
- Trusted Computing und (Remote) Attestation für Linux
- Hands-on: IMA/TPM Application und Remote Attestation

#### Hardwareerweiterungen für Virtualisierung und Sicherheit

- Intel-VT- und AMD-V-Virtualisierungstechnologien
- TEEs (ARM TrustZone, Intel TXT/AMD SVM, Intel SGX, AMD SME/SEV)
- Hands-on: Anwendungen von Trusted Hardware


#### Selected Topics and Research


- Kernel Information Leakages
- Coldboot-Angriffe
- Hands-on: Analyse des Arbeitsspeichers/Hauptspeichers
- RAM-Verschlüsselung

### Ihr Nutzen

- » Nach dem Seminar haben Sie ein Verständnis, wie Sicherheitslücken in Linux ausgenutzt werden, und verstehen die Perspektive des Angreifers.
- » Sie lernen, wie Sie Ihr Linux System grundlegend und gezielt härten können.
- » Sie haben ein Verständnis von Virtualisierungen und deren Sicherheitsmechanismen
- » Ausblick zu weiterführenden Angriffsvektoren und möglichen Verteidigungsstrategien


### INFORMATIONEN IM ÜBERBLICK

 Grundprinzipien IT-Sicherheit, Erfahrung mit Linux

 Softwareentwickler\*innen, technische Sicherheitsbeauftragte

 3 Tage Präsenz

 1800,-

 Garching bei München, inhouse

Veranstaltet durch

 **Fraunhofer**  
AISEC

Referent:



Sascha Wessel,  
Abteilungsleiter  
Fraunhofer AISEC



Weitere Infos und aktuelle Termine buchen unter:

[www.cybersicherheit.fraunhofer.de/advanced-linux-security](http://www.cybersicherheit.fraunhofer.de/advanced-linux-security)