

Container Security Fundamentals

In Kooperation mit dem SBA

Referenten:

Andreas Boll & Mathias Tausig (SBA Research)

Dauer: 1 Tag

Reduzierung von IT-Risiken innerhalb der eigenen Organisation durch die Erlangung der Fähigkeit Container sicher zu Erstellen und zu Betreiben.

- Container sicher betreiben
- Supply Chain Probleme verhindern
- Ressourcen sparen durch schlanke Images
- Sinnvoll für Docker, Podman und Kubernetes

Die Containerisierung von Applikationen hat sich zu einer Standardtechnik im IT-Betrieb entwickelt. Im Vergleich mit einer traditionellen Laufzeitumgebung entsteht dadurch ein relevanter Sicherheitsgewinn. Aber, wie bei jeder Technologie, müssen auch hier die Vorteile mit dadurch entstehenden neuen Risiken abgewogen werden. Weiters ist für eine vollständige Ausnutzung der potentiellen Sicherheitsvorteile von Containern ein tiefes Verständnis der verwendeten Technologie notwendig.

Dieser Kurs erläutert und demonstriert zahlreiche Techniken, die über den gesamten Lebenszyklus einer containerbasierten Applikation angewandt werden können mit dem Ziel eines signifikanten Sicherheitsgewinns bei der Erstellung und beim Betrieb der Container. Die besprochenen Themen beinhalten:

- *Supply-Chain*-Angriffe mittels Container Images
- Reduktion der Angriffsfläche durch die Erstellung minimaler Images
- Umgang mit externen Abhängigkeiten
- Reduktion der Berechtigungen innerhalb eines Containers
- Isolierungstechnologien des Linux Kernels (Namespaces, CGroups)
- Einsatz von *Capabilities* zur Begrenzung der Berechtigungen eines Containers
- Absicherung von Container Netzwerken
- Sicherheit im Betrieb: Docker vs. Podman
- Härtung der Laufzeitumgebung
- Verwaltung von Geheimnissen

Auch wenn dieser Kurs Orchestrierungstools wie Kubernetes nicht direkt behandelt, lassen sich die meisten der besprochenen Aktivitäten auf fast alle *Container Runtimes* übertragen, um einen soliden Grundschutz zu erreichen.

Praktische *Hands-on*-Übungen ergänzen die theoretischen Inhalte des Vortrags, um ein tieferes Verständnis und eine leichte Umsetzbarkeit in der Praxis bei allen Teilnehmer:innen sicherzustellen.

Kursziele

Erreichung einer Reduktion von IT-Risiken innerhalb der eigenen Organisation durch die Erlangung der Fähigkeit Container sicher zu Erstellen und zu Betreiben.

- Systemadmins
- SoftwareentwicklerInnen
- DevOps

In der Kursgebühr sind die Kursmaterialien sowie die volle Verpflegung enthalten.

TeilnehmerInnenanzahl: 15 Personen

Sprachen: Deutsch, Englisch

Referenten

Andreas Boll is senior information security consultant at SBA Research.

Consulting Area: Andreas' consulting activities are focused on the technical aspects of information security.

He frequently conducts penetration tests on a wide range of computer systems, including:

- Web application security
- Mobile app security
- Infrastructure security
- Source Code Audits
- Architecture Review



Mathias Tausig is information security consultant at SBA Research.

Consulting Area: Mathias' consulting activities are focusing on web application penetration testing, threat modeling and teaching activities, mainly in the areas of Application Security and Secure Software Development. He is a regular speaker at security- and Open Source focused conferences (e.g. sec4dev, Linuxwochen, RIOT-OS Summit, CCC Easterhegg, Heise DevSec).

