Who Contains the Containers? - Container Security auf Linux

Der Vortrag erklärt die Linux-Container-Technologie anhand des Fallbeispiels Docker Community Edition; es erfolgt eine Abgrenzung zur Virtualisierung und es wird auf Implementationsunterschiede zu anderen Container Engines (z.B. Podman) hingewiesen. Die Basistechnologie „Linux Namespaces“, die Linux-Containern zugrunde liegt, wird erklärt und gezeigt. Es werden Angriffsvektoren genannt, und mindestens zwei werden konkret demonstriert. Das Spektrum verfügbarer Gegenmaßnahmen wird erklärt und mindestens zwei werden konkret gezeigt. Es wird versucht, „Best Practises“ beim Aufbau von Container-Images zu benennen, allerdings ohne Anspruch auf Vollständigkeit.

Die praktische Vorführung umfasst:

- Linux Namespaces
- Benutzerrechte auf der Docker Engine
- Benutzer- und Dateisystemrechte auf Volumes
- Netzwerkfilter mit iptables, Docker CE und firewalld
- Linux Security Modules (LSM) am Beispiel AppArmor-Policies
- Security-Filter mit seccomp
- Open Policy Agent (OPA)