UEFI Secure Boot

Inhaltsverzeichnis

UEFI Secure Boot stellt sicher, dass beim Start nur signierte Bootloader und Kernels geladen werden. Manipulationen an der Bootkette werden blockiert oder erkennbar verhindert.

1 Funktionsweise

Firmware prüft digitale Signaturen gegen hinterlegte Keys. Nur vertrauenswürdige Komponenten dürfen die Boot-Kette fortsetzen.

- **DB/PK/KEK:** Key-Hierarchie der Firmware
- **Signed Boot Path:** Bootloader/Kernel
- **Enrollment:** eigene Keys in Enterprise-Szenarien

2 Typische Einsatzbereiche

- Schutz vor Bootkits auf Clients und Servern
- Compliance- und Hardening-Baselines
- Kombination mit Disk Encryption und TPM

3 Wichtige Hinweise

- Eigene Kernel/Module brauchen Signatur-Prozesse.
- Falsche Key-Zustände können Systeme unbootbar machen.
- Firmware-Passwörter und physischen Zugriff mitdenken.

4 Fazit

Secure Boot härtet den Systemstart gegen unsignierten Code – wirksam als Teil einer durchgängigen Device-Trust-Kette.