# Server-Hardening

## Inhaltsverzeichnis



Server-Hardening bezeichnet Maßnahmen, die ein System gegen Angriffe härten: unnötige Dienste entfernen, Zugriffe einschränken, Updates pflegen und Sicherheitsfunktionen konsequent aktivieren.

## 1 Funktionsweise

Ziel ist, die Angriffsfläche zu verkleinern und verbleibende Zugänge streng zu kontrollieren. Hardening ist kein einmaliger Schritt, sondern ein wiederkehrender Prozess aus Konfiguration, Kontrolle und Aktualisierung.

- **Minimize:** nur benötigte Pakete und Dienste betreiben.
- **Restrict:** Firewall, SSH-Keys, Least Privilege, MFA wo möglich.
- **Monitor:** Logs, Intrusion Detection und Update-Status im Blick behalten.

## 2 Typische Maßnahmen

- SSH absichern (Key-Auth, Root-Login deaktivieren, Fail2ban)
- Firewall-Regeln und Netzwerksegmentierung
- Automatische Sicherheitsupdates und Patch-Management
- Dateirechte, SELinux/AppArmor, getrennte Dienstkonten

## 3 Wichtige Hinweise

- Vor produktiven Änderungen Backups und Rollback-Plan vorsehen.
- Zu strikte Regeln können Dienste ungewollt blockieren – schrittweise härten und testen.
- Dokumentation der Baseline erleichtert Audits und Wiederherstellung.

## 4 Fazit

Server-Hardening macht Systeme robuster gegen typische Angriffe und Fehlkonfigurationen. In Kombination mit Monitoring und Updates ist es ein zentraler Baustein sicherer Infrastrukturen.