Sicherheitscheckliste für LXC-Container

System- und Softwareaktualisierung

[ ] `apt update && apt upgrade -y && apt autoremove -y` ausführen

[ ] Automatische Updates per Cron eingerichtet

Benutzer und Berechtigungen

[ ] Kein Root-Login via SSH erlaubt

[ ] Eigener Admin-Nutzer mit `sudo` vorhanden

[ ] `.ssh/authorized_keys` mit passenden Rechten

Netzwerksicherheit

[ ] UFW-Firewall aktiv und korrekt konfiguriert

[ ] SSH-Zugriff nur auf bekannte IPs (optional)

[ ] DDoS-Regeln in `iptables` aktiv

[ ] Spoofing-Schutz per `sysctl` aktiv

[ ] Offene Ports regelmäßig geprüft (nmap, ss)

Zugriffsschutz

[ ] Fail2ban aktiv und korrekt konfiguriert

[ ] Zwei-Faktor-Authentifizierung eingerichtet (optional)

[ ] CrowdSec aktiv und Firewall-Integration funktioniert

Härtung und Monitoring

[ ] AppArmor oder SELinux aktiv

[ ] `auditd`, `aide`, `lynis` installiert und verwendet

[ ] `logwatch`, `rkhunter` aktiv

[ ] Zentralisiertes Monitoring aktiv (optional)

Backups

[ ] Regelmäßige Backups mit `restic`/`borg` eingerichtet

[ ] Backup-Integrität regelmäßig überprüft

Protokolle und Dienste

[ ] Nur sichere Protokolle aktiv (kein Telnet, FTP)

[ ] HTTPS mit gültigem Zertifikat eingerichtet

[ ] Warnbanner bei SSH-Login gesetzt