Checkliste für die sichere Konfiguration eines Linux-basierten Root-Servers

- [ ] SSH Login absichern
- [ ] TCP-Wrapper verwenden
- [ ] Fail2ban einsetzen
- [ ] Automatische Updates aktivieren
- [ ] Benutzer-Accounts mit Zwei-Faktor-Authentifizierung absichern
- [ ] Regelmäßige Backups
- [ ] Empfohlene Sicherheitstools verwenden (Auswahl)
    - [ ] rdiff-backup oder rsnapshot für Backups
    - [ ] nmap für Port-Scans
    - [ ] debsums für Überprüfung von Files
    - [ ] etckeeper als Versionierungsmöglichkeit
    - [ ] rkhunter und chkrootkit
    - [ ] logcheck für Durchsuchung von Logfiles
    - [ ] Lynis für automatisierte Sicherheitsevaluierungen
- [ ] Remote Management Interface absichern
    - [ ] IMPI-Firmware aktualisieren
    - [ ] IPMI im separaten LAN und dedizierte NIC verwenden
    - [ ] Ausschließlich verwendete Dienste aktivieren
    - [ ] Sichere Benutzernamen und Passwörter verwenden
    - [ ] Monitoring nur mittels IPMI-User-Rechten
    - [ ] IPMI-Firewall aktivieren
    - [ ] EOL: IPMI Firmware flashen / Mainboard zerstören

THOMAS KRENN®