

L I N U X C H E C K L I S T E

- SELinux aktivieren
- UEFI mit Passwort schützen
- SSH deaktivieren
- Updates durchführen
- Sudo Benachrichtigungen
- Logs prüfen
- Runterfahren statt sperren
- Backups anlegen

L I N U X C H E C K L I S T E

SELinux aktivieren

Security Enhanced Linux ist in vielen Linux Distributionen enthalten und dient der Zugangskontrolle auf Kernel Level.

UEFI mit Passwort schützen

Veränderungen am UEFI durch nicht autorisierte User müssen unterbunden werden. Deshalb sollte ein starkes Passwort gesetzt werden.

SSH deaktivieren

Als normaler User muss man in der Regel nicht per SSH auf den PC zugreifen und sollte SSH deshalb deaktivieren.

Updates durchführen

Mit `apt-get update` && `apt-get upgrade` kann man das Betriebssystem schnell auf den neusten Stand bringen.

Sudo Benachrichtigungen

Optional kann jedes Mal wenn ein User Sudo verwendet eine Mail an den Admin versendet werden.

Logs prüfen

Mit `logwatch` kann man sich Reports über alle Aktivitäten im System erstellen lassen.

Runterfahren statt sperren

Über eine Cold Boot Attacke können bestimmte Daten aus dem Speicher gelesen werden solange das System nicht heruntergefahren wurde.

Backups anlegen

Vor und nach größeren Systemveränderungen sollten Backups angelegt werden. Diese Backups müssen regelmäßig getestet werden.