

Linux härten

LinkedIn Learning Kurs

Grundlagen der Härtung

nicht härtbare System müsten in ein separates Netzwerk verschoben werden.

Hardware und Firmware härten

- Rechnergehäuse abschließen
- BIOS durch Passwörter schützen
- Harddisk-Verschlüsselung über Controller (FDE)
- Systemverschlüsselung über Hardware-Sicherheitsmodul (HSM)
- Richtlinien für den Umgang mit externen Schnittstellen implementieren
- nicht benötigte Laufwerke entfernen/deaktivieren

Arbeitsumgebung härten

- nicht benötigte Software entfernen
- nicht benötigte Funktionalitäten entfernen/deaktivieren
- Datenverarbeitung mittels Software oder HSM verschlüsseln
- alle Anwendungen aktuell halten
- Passwortrichtlinien, Least-Privilege-Zugriffe für Daten und Anwendungen

Angriffspunkte

Startvorgang

Boot-CD

Über Boot-CD in Troubleshooting wechseln > Continuu.

Danach ist man als root angemeldet

mit `df -h` Laufwerke anzeigen lassen.

Unter `/dev/mapper/centos-root` kann man schauen wo das System gemountet ist. `/mnt/sysimage`

```
nano /lib/systemd/system/rescue.service
```

```
# Datei anpassen
```

```
ExecStart= sulogin in sushell ändern
```

Schon kann man sich in das System ohne Passwort einloggen.

```
# Bootprozess unterbrechen und mit e editieren
```

```
# in der Zeile mit linux16... zu swap rhgb quiet navigieren und dort rhgb durch rescue ersetzen
```

Single-User-Mode

```
# Die Shadowdatei: /etc/shadow
```

```
# Startprozesse bei Ubuntu Startvorgang mit esc unterbrechen
```

Mit e anpassen

unter Linux ro durch rescue aufrufen

Verhindern

```
cd /etc/grub.d
```

```
vim 40_custom
```

```
# Hinzufügen
```

```
set superusers="admin"
```

```
password admin password # Setzt das password auf password
```

Das password wird nicht verschlüsselt abgespeichert

Konfigurationsdatei anpassen

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Dadurch muss man zum editieren der Startdatei ein Passwort eingegeben werden.

```
# Entfernen des Passworts
```

Mit Boot-CD kann man das entfernen

Benutzer

Revision #3

Created 14 July 2023 10:19:32 by Hermann

Updated 17 October 2023 13:28:29 by Hermann