Ausbildungsleitfaden: Linux-Shell-Projekte

Infrastruktur & Compliance im Versicherungswesen

André Creutz

4. Februar 2026

Einleitung

In einem regulierten Umfeld (BaFin, DORA, NIS2) ist die Beherrschung der Linux-Shell essenziell für Sicherheit und Compliance. Die folgenden Kleinstprojekte führen in die Grundlagen von RHEL8 ein.

—

1 Projekt 1: Der "Hardening-Auditor"(System-Sicherheit)

Kontext: Gemäß DORA Art. 24 müssen wir die Sicherheit unserer IKT-Systeme gewährleisten. Dieses Projekt lehrt die Prüfung des Sicherheitsstatus.

- **Lerninhalte:** Dateiberechtigungen (Oktalwerte), Dienste-Status, Text-Parsing mit `awk`.
- **Aufgabe:**
  1. Recherche: Was ist SELinux und warum ist der Modus *Enforcing* Pflicht?
  2. Analyse der Datei `/etc/shadow` (Passwort-Hashes und Zugriffsschutz).
  3. Entwicklung eines Scripts zur Prüfung der Berechtigungen (000/400).
- **Lernziel:** Unterschied zwischen Standard-User und Root sowie Informationsfilterung.

2 Projekt 2: Log-Wächter & Storage-Management

Kontext: Sicherstellung der Verfügbarkeit gemäß NIS2 Art. 21 durch Überwachung kritischer Verzeichnisse wie `/var/log`.

- **Lerninhalte:** Verzeichnisstrukturen, Sortieralgorithmen, Variablen.
- **Aufgabe:**
  1. Größenanalyse mittels `du -sh /var/log`.
  2. Identifikation großer Dateien mit `find -size +50M`.
  3. Automatisierung einer Warnmeldung bei Schwellenwertüberschreitung.
- **Lernziel:** Proaktive Systemüberwachung.

3 Projekt 3: ICIS-Infrastruktur-Check (Oracle & Java)

Kontext: Prüfung der Betriebsbereitschaft der Kern-Applikation ICIS auf Basis von Oracle 19c.

- **Lerninhalte:** Prozessliste (`ps`), Netzwerk-Sockets (`ss`), Pipes.
- **Aufgabe:**
  1. Monitoring des Oracle-Prozesses `pmon`.
  2. Prüfung des Listeners (Port 1521) mittels `ss -tulpen`.
  3. Zusammenfassung in einem Status-Script.
- **Lernziel:** Verständnis von Client-Server-Architekturen.

4 Projekt 4: User-Compliance-Audit (DSGVO-Fokus)

Kontext: Umsetzung von Art. 5 DSGVO (Integrität und Vertraulichkeit) durch Verwaltung von Benutzerkonten.

- **Lerninhalte:** Benutzerverwaltung, Datumsformate, CSV-Export.
- **Aufgabe:**
  1. Nutzung von `chage` zur Ablaufprüfung von Passwörtern.
  2. Erstellung einer Benutzerliste aus `/etc/passwd`.
  3. Export der Audit-Daten in eine `audit_users.csv`.
- **Lernziel:** Revisionssichere Berichterstattung für BaFin-Auditoren.

5 Projekt 5: Konfigurations-Backup & Hashing

Kontext: Sicherung des Ist-Zustands vor Ansible-Rollouts gemäß VAIT Kap. 8.2.

- **Lerninhalte:** Archivierung (`tar`), Kompression (`gzip`), Prüfsummen (`sha256sum`).
- **Beispiel-Implementierung:**

```
## Autor: ARC
## Version: 1.0
## Datum: 04.02.2026
## Beschreibung: Backup von System-Configs mit SHA256-Pruefung

TIMESTAMP=$(date +%Y%m%d_%H%M)
BACKUP_FILE="/tmp/config_backup_${TIMESTAMP}.tar.gz"
SOURCE_PATHS="/etc/ssh /etc/fstab /etc/resolv.conf"

echo "Starte Sicherung der Konfigurationsdateien..."

# 1. Archiv erstellen
tar -czf "$BACKUP_FILE" $SOURCE_PATHS 2>/dev/null

if [ $? -eq 0 ]; then
    echo "Backup erfolgreich erstellt: $BACKUP_FILE"

    # 2. SHA256 erzeugen (Compliance: BaFin/DORA)
    sha256sum "$BACKUP_FILE" > "${BACKUP_FILE}.sha256"
    echo "Integritaetscheck-Datei erstellt."
else
    echo "FEHLER: Backup fehlgeschlagen."
    exit 1
fi

echo "Backup-Vorgang abgeschlossen."
## Ende
```

Implementierungshilfe für Neulinge

Rechte: Nutze `sudo` für privilegierte Lesezugriffe in `/etc/`.

Editoren: Verwende `vi` – der Standard auf allen RHEL-Systemen.

Debugging: Starte Scripte mit `bash -x scriptname.sh` zur Fehlersuche.