Risikoklassen | Aufbau der Regelwerke

Nachfolgend eine exemplarische Übersicht, wie die Regelwerke pro Risikoklasse strukturell aufgebaut sind:

1. Grundlegende Regeln

GPOs – Group Policy Objects

- Festlegung von PAM als zentrale Zugriffsverwaltung
- Festlegung erlaubter Zugriffswege und Clients
- Festlegung erlaubter Protokolle

2. Organisatorische Maßnahmen

Access Policies

- Festlegung von Systemen gemäß Risikoeinstufung
- Festlegung von Benutzerprofilen und -rollen
- Festlegung von orts- und zeitabhängigen Sicherheitsprofilen

3. Sitzungskontrolle (Zero Trust) nach BSI und ISO

Authentication Policies

- Festlegung des Authentifizierungsverfahrens
- Festlegung von Genehmigungsprozessen

Session Policies

- Festlegung des Detailgrades der Sitzungsaufzeichnung
- Festlegung der Zugriffsbereiche (z.B. nur einzelne Apps oder das ganze System?)
- Festlegung von Benutzer-Privilegien pro Applikation („Principle of least privilege“)
- Festlegung von Connection Policies (z.B. Kein User Mapping, keine interaktive Authentifizierung möglich)
- Festlegung weiterer Einschränkungen (z.B. File-Transfer erlaubt? Zwischenablage aktiviert? Systemdienste vollständig oder teilweise gesperrt? Remote-Verbindungen möglich?)

Password Policies

- Festlegung des Passwortstärke und -komplexität des Zielsystems
- Festlegung des Rotationsintervalls
- Notfallmaßnahmen (z.B. Break-Glass)

Das nachfolgende Beispiel beschreibt die Zuordnung der einzelnen Parameter pro Risikoklasse für eine „Password Policy“ in der Risikoklasse 0 und 2.:

Risikoklasse 0 (höchste Priorität) – Linux/SSH Passwort-Richtlinie:

```
Passwortwechselintervall: 60 Minuten
Passwortlänge: mindestens 16 Zeichen
Zeichenaufteilung: mindestens 4 Zeichen jedes Typus
Besonderheiten: keine deutschen Umlaute

Passwortlänge (festgelegt): 16 Zeichen
Sonderzeichen: 4
Kleinbuchstaben: 4
Großbuchstaben: 4
Zahlen: 4

Ausgeschlossene Zeichen: Ä Ö Ü ä ö ü ß

SSH Key Typus: "RSA"
Schlüssellänge: 4096
```

Risikoklasse 2 (mittlere Priorität) – Linux/SSH Passwort-Richtlinie:

```
Passwortwechselintervall: Monatlich (Erster Tag des Monats)
Passwortlänge: mindestens 10 Zeichen
Zeichenaufteilung: mindestens 1 Zeichen von Großbuchstaben und
Sonderzeichen
Limitierung: keine Limitierungen für Anzahl Groß- und Kleinbuchstaben
Besonderheiten: keine deutschen Umlaute

Passwortlänge (festgelegt): 10 Zeichen
Sonderzeichen: 1
Kleinbuchstaben: 0
Großbuchstaben: 1
Zahlen: 0

Ausgeschlossene Zeichen: Ä Ö Ü ä ö ü ß

SSH Key Typus: "RSA"
Schlüssellänge: 2048
```

WALLIX
CYBERSECURITY SIMPLIFIED