HowTo – lokale Sicherheitsrichtlinien (secpol.msc)

Kategorie	Windows Administration
Autor	Lugstein Markus
Datum	15.03.2026
Version	1.0

Inhalt

1. Ziel der Anleitung

> Ziel dieser Anleitung ist die Konfiguration von lokalen Sicherheitsrichtlinien auf einem Windows-System.
>
> Dabei werden wichtige Sicherheitsmaßnahmen eingerichtet, um den Zugriff auf das System zu kontrollieren und sicherheitsrelevante Ereignisse zu protokollieren.

Folgende Richtlinien werden konfiguriert:

- Kontosperrungsrichtlinien
- Überwachungsrichtlinien (Audit)
- Sicherheitsoptionen für Anmeldung und Benutzerkonten

Diese Einstellungen erhöhen die Sicherheit des Systems und ermöglichen eine bessere Nachverfolgung von sicherheitsrelevanten Ereignissen.

2. Voraussetzungen

Für die Durchführung der Aufgabe werden folgende Voraussetzungen benötigt:

- Windows Betriebssystem (z. B. Windows 10 / Windows 11 Pro oder Enterprise)
- Administratorrechte
- Zugriff auf die lokalen Sicherheitsrichtlinien

Das Tool kann über folgenden Befehl geöffnet werden:

```
secpol.msc
```

3. Warnhinweise

⚠️ Änderungen an Sicherheitsrichtlinien können Auswirkungen auf Benutzerkonten und Systemzugriff haben.

Daher sollte beachtet werden:

- Richtlinien nur mit Administratorrechten ändern
- falsche Einstellungen können Benutzerkonten sperren
- Änderungen sollten dokumentiert werden

4. Übersicht der Aufgabe

Die Aufgabe umfasst drei Hauptbereiche:

Bereich	*Konfiguration*
Kontosperrung	Fehlversuche begrenzen
Überwachung (Audit)	Sicherheitsereignisse protokollieren
Sicherheitsoptionen	Anmeldung und Konten sichern

5. Schritt-für-Schritt Anleitung

5.1 Schritt 1 – Kontosperrungsrichtlinie konfigurieren

1. Öffnen Sie die lokalen Sicherheitsrichtlinien:

```
secpol.msc
```

2. Navigieren Sie zu:

```
Kontorichtlinien
 → Kontosperrungsrichtlinie
```

3. Konfigurieren Sie folgende Einstellungen:

Kontosperrungsschwellenwert

```
5 Fehlversuche
```

Sperrdauer

```
30 Minuten
```

Zurücksetzen des Kontosperrungszählers nach

```
15 Minuten
```

Diese Einstellungen verhindern Brute-Force-Angriffe auf Benutzerkonten.

5.2 Schritt 2 – Überwachungsrichtlinien (Audit) konfigurieren

Navigieren Sie zu:

```
Lokale Richtlinien
 → Überwachungsrichtlinie
```

Aktivieren Sie folgende Einstellungen:

Anmeldeereignisse überwachen

```
Erfolg und Fehler
```

Objektzugriff überwachen

```
Erfolg und Fehler
```

Richtlinienänderungen überwachen

```
Erfolg und Fehler
```

> Diese Richtlinien sorgen dafür, dass wichtige Sicherheitsereignisse im Windows Ereignisprotokoll gespeichert werden.

5.3 Schritt 3 – Sicherheitsoptionen konfigurieren

Navigieren Sie zu:

```
Lokale Richtlinien
 → Sicherheitsoptionen
```

Konfigurieren Sie folgende Einstellungen:

5.3.1 Letzten Benutzernamen nicht anzeigen

```
Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen → Aktiviert
```

Dadurch wird verhindert, dass der zuletzt angemeldete Benutzer angezeigt wird.

5.3.2 Gastkonto deaktivieren

```
Konten: Gastkonto Status → Deaktiviert
```

Damit wird das Gastkonto vollständig deaktiviert.

5.3.3 Meldungstext bei Anmeldung

Öffnen Sie die Richtlinie:

```
Interaktive Anmeldung: Meldungstext für Benutzer bei der Anmeldung
```

Tragen Sie folgenden Text ein:

```
Nur für autorisierte Mitarbeiter der Vision GmbH
```

Optional kann auch ein Titel gesetzt werden, z. B.:

```
Sicherheitshinweis
```

Diese Meldung erscheint vor jeder Anmeldung am System.

6. Ergebnis / Kontrolle

Nach erfolgreicher Konfiguration gelten folgende Sicherheitsregeln:

- Benutzerkonten werden nach 5 falschen Anmeldeversuchen gesperrt
- Sperre dauert 30 Minuten
- Sicherheitsereignisse werden protokolliert
- letzter Benutzername wird nicht angezeigt
- Gastkonto ist deaktiviert
- Anmeldemeldung erscheint vor der Anmeldung

Die Ereignisse können im Ereignisprotokoll überprüft werden:

```
eventvwr.msc
```

7. Dokumentation / Abgabe

Für die Abgabe müssen folgende Nachweise erstellt werden:

- ✓ Screenshots der konfigurierten Sicherheitsrichtlinien
- ✓ Screenshot der Audit-Einstellungen
- ✓ Screenshot der Anmeldemeldung

Zusätzlich muss eine Exportdatei erstellt werden mit:

```
secedit /export /cfg C:\Scripts\security-policy.inf
```

Diese Datei enthält alle lokalen Sicherheitsrichtlinien.

8. Anhang (optional)

Optional können ergänzt werden:

- Screenshot der Ereignisanzeige
- Test eines falschen Anmeldeversuchs
- Screenshot der Kontosperrung
- Inhalt der exportierten .inf Datei