Empfohlene Sicherheitseinstellungen für SEH-Deviceserver

Optimale Konfiguration für maximale Sicherheit und Compliance

Moderne Unternehmensnetzwerke stellen hohe Anforderungen an die Sicherheit – insbesondere bei eingebetteten Geräten wie USB-Deviceservern. Die SEH Deviceserver-Familie (utnserver Pro, utnserver ProMAX, dongleserver Pro, dongleserver ProMAX, INU-100 und INU-50) bietet umfangreiche Sicherheitsfunktionen. Durch gezielte Konfiguration lassen sich diese Geräte zuverlässig in bestehende Sicherheitsrichtlinien integrieren – und bestehen auch Sicherheits- und Schwachstellenscans ohne Fehlalarme.

1. Webinterface absichern

Der Schutz des Webinterfaces ist zentral, da es die zentrale Verwaltungsschnittstelle für das Gerät darstellt.

- **Starke Passwörter setzen:** Für alle Benutzerkonten (Admin, USB-Manager, Lesezugriff-Benutzer) sollten individuelle, sichere Passwörter verwendet werden.
- **Nur HTTPS zulassen:** HTTP-Zugriff deaktivieren und HTTPS als Standard setzen.
- **Gültige Zertifikate nutzen:** Selbstsignierte Zertifikate sollten durch signierte ersetzt werden (z. B. via Firmen-CA), um Authentizität und Vertrauenswürdigkeit sicherzustellen.
- **Zugriff einschränken:** Webinterface-Zugriff nur über vertrauenswürdige Management-Netze erlauben oder gezielt deaktivieren, wenn nicht benötigt.

2. USB-Kommunikation verschlüsseln

Die Kommunikation zwischen Deviceserver und SEH UTN Manager sollte grundsätzlich verschlüsselt erfolgen.

- **TLS-Verschlüsselung aktivieren:** Diese Option aktivieren, damit alle USB-Datenströme geschützt übertragen werden.

3. SNMP absichern oder deaktivieren

SNMP wird häufig für Monitoring-Zwecke verwendet, kann aber in veralteten Versionen ein Sicherheitsrisiko darstellen.

- **SNMPv1 deaktivieren:** Überträgt Daten unverschlüsselt und ist für heutige Umgebungen ungeeignet.
- **SNMPv3 nutzen:** Nur wenn SNMP zwingend notwendig ist, sollte SNMPv3 mit Authentifizierung und Verschlüsselung verwendet werden.
- **SNMP ganz deaktivieren**, wenn kein Monitoring via SNMP stattfindet.

4. Bonjour (mDNS) deaktivieren

Bonjour (mDNS) erlaubt die automatische Geräteerkennung, gibt aber auch Informationen über das Gerät preis.

- **Deaktivieren**, wenn die Funktion nicht zwingend erforderlich ist – insbesondere in sicherheitskritischen Netzwerken.

5. TLS-Konfiguration optimieren

Die Verschlüsselung der Management- und Gerätedaten sollte den aktuellen Standards entsprechen.

- **TLS 1.3 bevorzugen:** Aktivieren Sie TLS 1.3, um modernste Verschlüsselung und Performance zu nutzen.
- **TLS 1.2 nur als Fallback zulassen**, falls ältere Clients im Einsatz sind.

6. Netzwerkzugang und Segmentierung

Zusätzliche Sicherheit bieten Maßnahmen zur Kontrolle des Netzwerkzugriffs.

- **802.1X-Authentifizierung verwenden:** Schützt das Netzwerk vor unautorisierten Geräten (z. B. via RADIUS).
- **VLANs nutzen:** Durch Segmentierung lassen sich Gerätegruppen logisch und sicher voneinander trennen.

7. USB-Port- und Geräteverwaltung (optional, aber empfohlen)

- **Nicht genutzte USB-Ports deaktivieren**
- **Gerätebindung:** USB-Geräte via PID/VID fest bestimmten Ports zuweisen
- **Zugriffsschlüssel und Zeitsteuerung:** Steuerung, wann und durch wen Ports nutzbar sind
- **Gerätetypen-Filter:** Beispielsweise HID-Geräte (Tastaturen/Mäuse) blockieren

8. Monitoring, Logging und Benachrichtigungen aktivieren

Aktives Monitoring hilft, ungewollte Aktivitäten frühzeitig zu erkennen.

- **Integrierte Überwachungsfunktionen nutzen**, um sicherheitsrelevante Ereignisse wie unautorisierte Zugriffe oder Konfigurationsänderungen zu erkennen.
- **Logging aktivieren**, um alle relevanten System- und Zugriffsvorgänge mitprotokollieren zu lassen.
- **Benachrichtigungsfunktionen wie E-Mail oder SNMP-Traps einrichten**, um bei sicherheitsrelevanten Ereignissen sofort informiert zu werden.

9. Minimierung der Angriffsfläche

Nach dem Prinzip „Weniger ist mehr“:

- **Alle nicht benötigten Protokolle und Dienste deaktivieren** (SNMP, Bonjour, ungenutzte USB-Ports etc.).
- **Nur Funktionen aktivieren, die im Einsatz sind** – so wird die potenzielle Angriffsfläche reduziert.

Zusammenfassung – Empfehlungen auf einen Blick

Maßnahme	Empfehlung
Webinterface	Starke Passwörter verwenden, HTTPS aktivieren, Zugriff begrenzen
SNMP	SNMP v1 deaktivieren, SNMP v3 nutzen oder SNMP vollständig deaktivieren (bei Bedarf)
Bonjour (mDNS)	deaktivieren (nur aktivieren, wenn zwingend notwendig)
USB-Kommunikation	TLS-Verschlüsselung der USB-Kommunikation aktivieren
Verschlüsselung allgemein	TLS 1.3 als Standard nutzen
Authentifizierung	802.1X verwenden (optional, empfohlen)
Netzwerksegmentierung	VLANs zur Zuweisung von USB-Geräten in getrennte Teilnetze
USB-Portverwaltung	Nicht benötigte Ports abschalten
Monitoring	Logging & Benachrichtigungen aktivieren
Protokoll-/Dienstverwaltung	Nur notwendige Dienste aktiv halten

Fazit

SEH Deviceserver bieten eine Vielzahl an Sicherheitsfunktionen, die sich flexibel an die Anforderungen moderner IT-Umgebungen anpassen lassen. Durch eine konsequente Konfiguration – wie in diesem Artikel beschrieben – lassen sich Geräte effektiv absichern, Angriffsflächen minimieren und Sicherheitsprüfungen bestehen.

Diese Empfehlungen stellen sicher, dass Ihre Geräte sowohl in klassischen Unternehmensnetzwerken als auch in sensiblen Umgebungen zuverlässig und sicher betrieben werden können.