

CHECKLISTE

FERNWARTUNG IM INDUSTRIELLEN UMFELD

Anforderungen an Fernwartungslösungen

Prüfen Sie, ob Ihre Lösung diese 22 Punkte erfüllt:

1. Architektur

- Eine **einheitliche Lösung** verringert die Anzahl der Angriffsvektoren, sowie die Komplexität.
- Fernwartungskomponenten sollten immer in der **DMZ** installiert werden und nicht direkt im Produktionsnetz. Firewall-Regeln verwenden um erlaubte IP-Adressbereiche festzulegen.
- Der Fernwartungszugriff sollte **feingranular pro IP und Port geregelt** werden. Keine pauschale Freigabe der (Sub)Netze.
- Verbindungsaufbau** immer von innen nach außen. Alternativ: Temporäre Aktivierung und Deaktivierung durch Mitarbeitende.
- Verwendung von **dezidierten Systemen** ausschließlich für die Fernwartung.

2. Sichere Kommunikation

- Einsatz von **sicheren Protokollen** wie IPsec, SSH oder SSL/TLS.
- Benutzung von sicheren Verfahren zur Verschlüsselung z.B. AES.

3. Authentisierungsmechanismen

- Starke Authentisierungsmechanismen** wie Zwei-Faktor-Authentisierung mit Versand von Einmal-Token-Codes.
- Unterstützung und ggf. Forcierung einer Passwort-Policy für erhöhte **Passwortsicherheit**.
- Mechanismen zur **Angriffserkennung** und Vorkehrungen gegen das wiederholte Durchprobieren.

4. Organisatorische Anforderungen

- Durchführung einer **Risikoanalyse** vor der Integration der Lösung.
- Nur unbedingt erforderliche Fernzugriffsmöglichkeiten implementieren (**Minimalitätsprinzip**)
- Etablierung von **Prozessen** zur Freigabe von Verbindungen, Sperrungen, Notfallprozeduren und regelmäßiger Wechsel von Authentisierungsdaten.
- Freigabe von Remote-Zugängen nur bei Bedarf oder in einem definierten **Zeitfenster**.


- Regelmäßige **Funktionsprüfung** der Fernwartung.
- Fernwartende müssen bestimmte **Vorgaben** erfüllen in Bezug auf die verwendete IT und Schutzmechanismen der Remote-Clients.
- Ein definierter **Patch-Prozess** sollte Aktualisierungen in Fernwartungskomponenten regelmäßig einspielen um die Sicherheit der Industriekomponenten zu gewährleisten
- Verbindungsdaten und fehlgeschlagene Anmeldeversuche sollten **protokolliert** werden. **Logdaten** sollten automatisiert ausgewertet werden und es sollte ggf. eine **Alarmierung** erfolgen.

5. Sonstiges

- Skalierbare Systeme** senken Kosten für Betrieb, Wartung und Pflege durch ein zentrales Management, Bulk-Rollout, Bulk-Configuration oder Bulk-Actions, wie das Ausführen von Skripten.
- Damit Systeme auch zukünftige Anforderungen erfüllen, sollten sie erweiterbar und nachhaltig sein im Sinne des **Investitionsschutzes**.
- Die **Hochverfügbarkeit** der Komponenten sollte gewährleistet sein z.B. durch redundante Verwendung mehrere Mobilfunknetze.

Erfüllt Ihre Fernwartungslösung diese Anforderungen? Benötigen Sie Unterstützung bei der Planung, Implementierung oder dem Betrieb?

Wir helfen Ihnen gerne weiter!

 info@hwi-it.de  +49 7644 92662-0 www.hwi-it.de/