Risikoanalyse

Dieses Beispiel zeigt eine vereinfachte, praxisnahe Risikoanalyse für eine typische OT-Umgebung.

1. Systembeschreibung

Anlage: Produktionslinie (z. B. Fertigung)

Komponenten:

☐ PLC (SPS) zur Steuerung

☐ SCADA-System zur Überwachung

☐ Engineering Workstation

☐ Fernwartungszugang

☐ Verbindung zur IT

2. Asset-Bewertung

Asset	Kritikalität	Begründung
PLC	Hoch	Steuerung der Produktion
SCADA	Hoch	Visualisierung und Kontrolle
Engineering Station	Mittel	Konfiguration, selten genutzt
Remote Access	Hoch	Eintrittspunkt für Angriffe

3. Bedrohungsszenario

Szenario:

☐ Angreifer kompromittiert Remote-Zugang

Möglicher Ablauf:

☐ Zugriff über schwache Authentifizierung

☐ Bewegung im Netzwerk (lateral movement)

4. Schwachstellen

☐ Kein Multi-Faktor-Login für Fernzugriff

☐ Flaches Netzwerk ohne Segmentierung

☐ Unzureichendes Monitoring

☐ Veraltete Systeme (keine Updates möglich)

5. Risikobewertung

Kriterium	Bewertung
Eintrittswahrscheinlichkeit	Mittel
Auswirkung	Hoch
Gesamtrisiko	Hoch

6. Maßnahmen

Technische Maßnahmen:

☐ Netzwerksegmentierung einführen

☐ Jump Host für Fernzugriff einsetzen

☐ Monitoring (IDS/IPS) implementieren

Organisatorische Maßnahmen:

☐ Zugriffskonzepte definieren

☐ Incident-Response-Prozess etablieren

☐ Schulungen durchführen

Kompensierende Maßnahmen:

☐ Virtual Patching einsetzen

☐ Einschränkung von Kommunikationspfaden

7. Restrisiko

☐ Risiko reduziert, aber nicht eliminiert

☐ Regelmäßige Überprüfung erforderlich

8. Ergebnis

Die Analyse zeigt, dass insbesondere Fernzugriffe und fehlende Segmentierung kritische Risiken darstellen. Durch gezielte Maßnahmen kann das Risiko signifikant reduziert werden, ohne den Betrieb zu beeinträchtigen.

Mehr zum Thema OT-Sicherheit

Der vollständige Leitfaden „OT-Sicherheit in der Praxis - Wenn das schwächste Glied entscheidet“