OT-Security-Checkliste für Unternehmen

Diese Checkliste dient als praktische Arbeitsgrundlage für die Einführung, Bewertung und Verbesserung der OT-Sicherheit in Unternehmen. Sie orientiert sich an gängigen OT-Sicherheitspraktiken, an IEC 62443 für industrielle Automatisierungs- und Steuerungssysteme sowie an NIS-2-bezogenen Anforderungen für industrielle Netzwerke.

Governance und Organisation

- Zuständigkeiten für OT-Sicherheit sind klar definiert, etwa für Management, OT-Verantwortliche, Instandhaltung, IT-Sicherheit und externe Dienstleister.
- Eine verbindliche OT-Sicherheitsrichtlinie ist dokumentiert und mit vorhandenen ISMS- oder Sicherheitsrichtlinien abgestimmt.
- OT-Sicherheit ist in Risiko-, Change-, Incident- und Notfallmanagement eingebunden.
- Sicherheitsziele für Verfügbarkeit, Integrität und sichere Betriebsführung sind dokumentiert und vom Management freigegeben.
- Ein Verbesserungsprogramm mit Maßnahmen, Prioritäten, Budget und Verantwortlichen ist vorhanden.

Asset Management

- Ein vollständiges Inventar aller OT-Assets liegt vor, einschließlich PLCs, HMIs, SCADA-Systemen, Engineering-Stationen, Netzwerkkomponenten, Remote-Zugängen und IIoT-Gateways.
- Kritische Assets und Prozesse sind identifiziert und nach Auswirkung auf Produktion, Sicherheit, Umwelt und Qualität bewertet.
- Kommunikationsbeziehungen zwischen Systemen, Zonen und externen Anbindungen sind dokumentiert.
- End-of-Life- und End-of-Support-Systeme sind gekennzeichnet und gesondert behandelt.

Netzwerk und Segmentierung

- IT- und OT-Netze sind technisch getrennt und nicht als flaches Gesamtnetz betrieben.
- Eine DMZ zwischen IT und OT ist eingerichtet, etwa für Historian, Update-Server oder Fernwartungszugänge.

- Zonen und Conduits sind definiert und nach Kritikalität segmentiert.
- Es sind nur ausdrücklich benötigte Verbindungen, Ports und Protokolle freigegeben.
- Direkter Internetzugang aus OT-Systemen ist unterbunden.

Hardening und Zugriffsschutz

- Nicht benötigte Dienste, Komponenten und Schnittstellen auf OT-Systemen sind deaktiviert oder entfernt.
- Standardkennwörter und Default-Konten wurden auf allen relevanten Geräten geändert.
- Für typische OT-Systeme existieren Hardening-Vorgaben.
- Rollenbasierte Berechtigungen sind eingeführt und regelmäßig überprüft.
- Kritische Zugänge und Fernzugriffe sind mit starker Authentisierung abgesichert.
- Physische Zugänge zu Leitwarte, Schalträumen und Netzwerkschränken sind kontrolliert.

Fernzugriff

- Alle Fernzugänge sind inventarisiert und dokumentiert.
- Externe Zugriffe erfolgen ausschließlich über freigegebene, abgesicherte Zugangswege wie VPN, Jump Host oder Remote-Access-Gateway.
- Remote-Sitzungen sind freigabepflichtig, zeitlich begrenzt und nachvollziehbar protokolliert.
- Dauerhaft offene Fernwartungsverbindungen ohne konkreten Bedarf sind deaktiviert.

Patch- und Schwachstellenmanagement

- Es gibt einen OT-spezifischen Patch-Prozess mit Test, Freigabe, Wartungsfenster und Rollback-Regelung.
- Herstellerhinweise, CERT-Meldungen und bekannte Schwachstellen werden regelmäßig ausgewertet.
- Patches werden risikobasiert priorisiert, unter Berücksichtigung von Verfügbarkeit und Safety.
- Wenn Patchen nicht möglich ist, werden dokumentierte kompensierende Maßnahmen umgesetzt, etwa Segmentierung oder zusätzliches Monitoring.

Monitoring und Reaktion

- Relevante Protokolle und Ereignisse aus OT-Servern, Netzwerkkomponenten und Sicherheitskomponenten werden zentral erfasst.
- OT-spezifische Überwachungsmechanismen wie IDS, Anomalieerkennung oder Protokollanalyse sind etabliert.
- Es gibt definierte Use Cases für sicherheitsrelevante OT-Ereignisse, etwa neue Geräte im Netz oder Änderungen an Steuerungen.
- Ein OT-spezifischer Incident-Response-Plan mit Eskalationswegen und Wiederanlaufmaßnahmen ist dokumentiert.
- Backups kritischer Konfigurationen und Systeme sind vorhanden, getestet und gegen Manipulation geschützt.

Schulung und Lieferkette

- Mitarbeitende in Betrieb, Instandhaltung und Engineering erhalten OT-spezifische Security-Schulungen.
- Der Umgang mit USB-Medien, Service-Laptops und mobilen Datenträgern ist geregelt.
- Externe Dienstleister unterliegen vertraglich geregelten OT-Sicherheitsanforderungen.
- Sicherheitsanforderungen an Hersteller, Integratoren und neue Anlagen werden bereits bei Beschaffung, FAT und SAT berücksichtigt.

Prüfübersicht

Bereich	Prüffrage
Governance	Sind Rollen, Richtlinien und Management-Freigaben für OT-Sicherheit definiert?]
Assets	Existiert ein vollständiges und gepflegtes OT-Inventar?
Netzwerk	Sind IT und OT getrennt und in Zonen segmentiert?
Zugriffe	Sind Berechtigungen, MFA und Fernzugriffe kontrolliert?
Patching	Gibt es einen getesteten OT-Patch- und Ausnahmeprozess?
Monitoring	Werden OT-Ereignisse erkannt, protokolliert und bearbeitet?
Reaktion	Gibt es Playbooks, Backups und Wiederanlaufpläne?
Lieferkette	Sind Sicherheitsanforderungen an Externe und Hersteller festgelegt?

Verwendung der Checkliste

Die Checkliste eignet sich als Grundlage für interne Standortbewertungen, Lieferantenaudits, GAP-Analysen oder zur Vorbereitung auf formalisierte Sicherheitsprogramme im OT-Umfeld.

Haben Sie weitere Fragen?

Sie erreichen uns unter:

CONSUVATION GmbH
Tilsiter Str. 6
71065 Sindelfingen
www.consuvation.com

Telefon: +49 7031 4181-860
E-Mail: contact@consuvation.com