Die OT-Cyber-Resilienz-Checkliste

Wie resilient ist Ihre pharmazeutische OT-Umgebung?

In der pharmazeutischen Produktion hat Sicherheit oberste Priorität. Vom externen Angreifer bis zur veralteten internen Infrastruktur – der Schutz von Systemen und Shopfloors ist geschäftskritisch. OT-Cybersicherheit schützt nicht nur Anlagen – sie sichert Produktintegrität, regulatorische Konformität und das Vertrauen der Gesellschaft.

Die entscheidende Frage lautet: **Wie gut sind Sie vorbereitet?**

Diese Checkliste hilft OT- und Security-Verantwortlichen dabei, den Reifegrad ihrer aktuellen Sicherheitsstrategie in fünf Schlüsselbereichen zu bewerten. Identifizieren Sie Stärken und Verbesserungsbedarf – und setzen Sie gezielt Ihre nächsten Prioritäten.

So funktioniert's

Lesen Sie jede Aussage und bewerten Sie Ihre derzeitige Umsetzung auf einer Skala von 0–3:

- **0** Nicht vorhanden
- **1** In Planung
- **2** Teilweise umgesetzt
- **3** Vollständig umgesetzt

Am Ende jedes Abschnitts summieren Sie Ihre Punktzahl und überprüfen Sie Ihr Resilienz-Niveau.

Betriebsunterbrechungen & OT-Resilienz

Warum das wichtig ist: Unerwartete OT-Ausfälle können Chargenproduktionen stoppen, teure Revalidierungen auslösen und Patientenzugänge verzögern. Dieser Abschnitt prüft, wie gut Ihre Organisation Störungen minimieren und schnell reagieren kann.

Aussage	Bewertung (0–3)
Wir haben unsere OT-Systeme kartiert und kritische Assets identifiziert.	
Wir haben Echtzeit-Transparenz in OT-Betrieb und Systemleistung.	
Wir verfügen über spezifische OT-Incident-Response-Playbooks.	
Wir testen regelmäßig unsere Wiederherstellungsprozesse bei Ausfällen.	

Zwischensumme: ___/12

Resilienzstufe:

- **0–4** Reaktiv
- **5–8** In Entwicklend
- **9–12** Betrieblichsrelisierent

Legacy-Risiken in der OT minimieren

Warum das wichtig ist: Legacy-Systeme lassen sich nicht immer ersetzen – und mit den richtigen Schutzmaßnahmen ist das auch nicht nötig. Sicherheit ohne Beeinträchtigung validierter Prozesse ist entscheidend für Compliance und Betriebszeit.

Aussage	Bewertung (0–3)
Wir führen ein vollständiges Inventar veralteter Systeme (z. B. Windows 10).	
Wir haben kompensierende Schutzmaßnahmen für anfällige Endpunkte.	
Wir isolieren Legacy-Systeme so weit wie möglich vom übrigen Netzwerk.	
Wir bewerten regelmäßig das Risikoprofil dieser Systeme.	

Zwischensumme: ___/12

Resilienzstufe: 0–4 Gefährdet | 5–8 Auf dem Weg | 9–12 Geschützt & zukunftsfähig

Regulatorik & Compliance-Bereitschaft

Warum das wichtig ist: NIS2, GMP Annex 11 & Co. erhöhen die Anforderungen an OT-Sicherheit. Proaktive Compliance ist nicht mehr optional – sondern Voraussetzung für den Betrieb..

Aussage	Bewertung (0–3)
Unsere OT/IT-Systeme erfüllen NIS2 und GMP Annex 11.	
Validierte und nicht-validierte Systeme sind klar getrennt.	
Wir führen interne Audits durch und sind auf externe Prüfungen vorbereitet.	
Wir können Zugriffs- und Änderungsprotokolle vorlegen.	

Zwischensumme: ___/12

Resilienzstufe: 0–4 Offenliegend | 5–8 Compliance-bewusst | 9–12 Audit-sicher

Produktsicherheit & Patientenschutz

Warum das wichtig ist: Verfälschte Dosierungen, falsche Etikettierung oder kontaminierte Chargen gefährden Leben – sowohl von Mitarbeitenden als auch Patient:innen. Cyber-Resilienz muss Produktionsqualität und Patientensicherheit unterstützen.

Aussage	Bewertung (0–3)
Wir verstehen die Auswirkungen kompromittierter OT-Systeme auf Qualität und Sicherheit.	
Wir erkennen und verhindern Datenmanipulationen in der Produktion.	
Wir nutzen End-to-End-Integritätsprüfungen bei Chargen.	
Unsere Teams sind für Cyberrisiken im Hinblick auf Patientensicherheit geschult.	

Zwischensumme: ___/12

Resilienzstufe: **0–4** Verwundbar **5–8** Sensibilisiert **9–12** **Vertrauenswürdig & transparent**

Security-Architektur & Endpunktschutz

Warum das wichtig ist: Starke OT-Security erfordert Sichtbarkeit, Segmentierung und abgestimmte Kontrollen bis an den Netzwerk-Rand. Dieser Abschnitt bewertet Ihre technischen Kernfähigkeiten.

Aussage	Bewertung (0–3)
Wir setzen OT-native Security-Tools für Industrieumgebungen ein.	
Unsere Security-Architektur basiert auf Zero Trust (IT & OT).	
Remote-Zugänge und Anbindungen Dritter e sind abgesichert.	
Unsere Endpunktschutzlösungen enthalten HIPS ohne Betriebsstörungen.	

Zwischensumme: Score ___/12

Resilienzstufe: **0–4** Fragmentiert **5–8** **Grundlegend gesichert** **9–12** **Proaktiv gesteuert**

Ihre Gesamtauswertung:	___/60

0–15	Kritisches Risiko – Sofortiger Handlngsbedarf	Ihre OT-Umgebung ist stark gefährdet. Grundlagen fehlen, Ausfälle oder Compliance-Verletzungen sind wahrscheinlich. Handlungsbedarf: sofort.
16–30	In Entwicklung	Einige Fortschritte sind erkennbar – doch große Lücken bleiben, v. a. bei Legacy, Sichtbarkeit und Regulierung. Es braucht einen strukturierten Verbesserungsplan.
31–45	Basis-Schutz	Kernmaßnahmen sind vorhanden, erste Risikosenkung erkennbar. Doch die Resilienz ist uneinheitlich – Bedrohungen oder Audits könnten sie untergraben.
46–55	Betriebsresilient	Gut geschützt, weitgehend compliant. Systeme werden proaktiv verwaltet – mit wenigen verbleibenden Schwachstellen. Weiter optimieren und vertiefen.
56–60	Branchen-Benchmark	Ihre OT-Security ist vorbildlich: proaktiv, auditfähig, integriert über Mensch, Technik & Prozesse hinweg. Ein Vorbild für sichere Pharma-Produktionen.

Möchten Sie tiefer? einsteigen?

Laden Sie unser eBook **„Cyber-Resilienz für die Pharmaindustrie“** herunter oder sprechen Sie mit einem TXOne-Experten, um Ihre nächsten Schritte zur OT-Readiness zu planen.

Direkt Kontakt aufnehmen