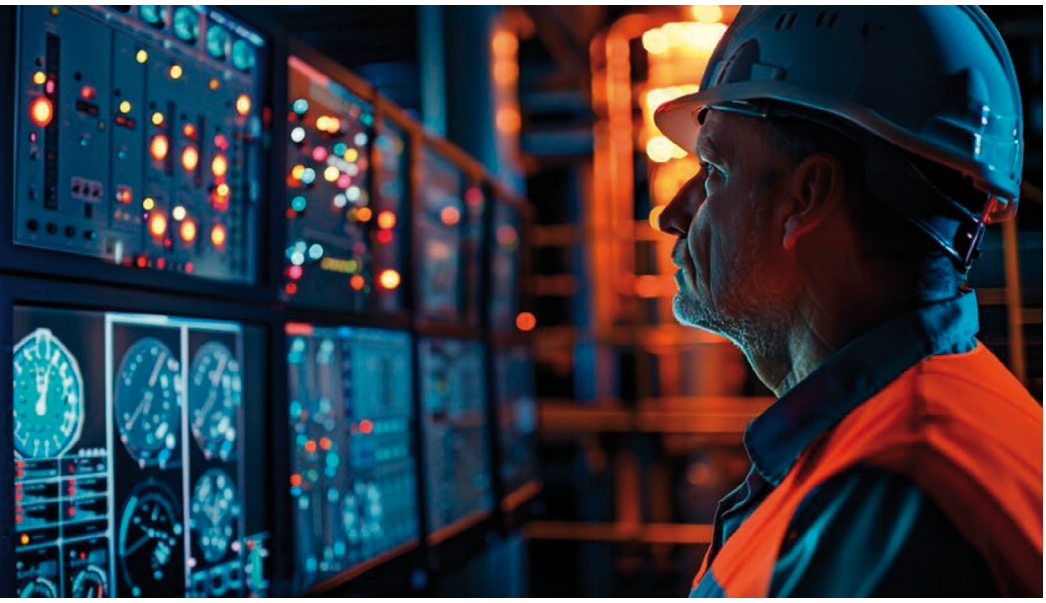
## Nachholbedarf bei OT-Sicherheit

# Wie Unternehmen IT und OT ganzheitlich absichern können



*OT-Security in der Industrie ist in vielen Unternehmen ein blinder Fleck. © Obrela/Shutterstock*

*Autoren:*

*Stefan Bange*
*Managing Director Germany*
*Obrela*
*www.obrela.com*

*Peter Thiel*
*Team Leader IT/OT-Security*
*PLT networks*
*www.plt-networks.de*

Während IT-Systeme seit Jahren im Zentrum der Sicherheitsstrategien stehen, bleibt die Operational Technology (OT) vieler Unternehmen ein blinder Fleck. Dabei kann OT von der IT lernen – durch die Konvergenz beider Welten. Etablierte Schutzmechanismen und Security as a Service helfen, Risiken sichtbar zu machen und Angriffe frühzeitig abzuwehren.

### Steigende Bedrohung

Ransomware-Angriffe und Zero-Day-Exploits stellen in industriellen Steuerungssystemen mittlerweile eine ernsthafte Bedrohung dar. Sie führen zu weitreichenden Störungen wie dem Stillstand von Fertigungsstraßen sowie daraus resultierenden Unterbrechungen in der Lieferkette.

Laut dem IBM X-Force Threat Intelligence Index 2025 [1] ist die Fertigungsindustrie der am häufigsten angegriffene Sektor. Besonders kritisch ist der direkte Zugriff über öffentlich erreichbare Anwendungen. In 29 Prozent der Fälle nutzen Angreifer diesen Weg als primären Einstiegspunkt.

### OT-Umgebungen

Für OT-Umgebungen ist das kritisch: Über Webportale, VPN/Remote-Zugänge, Plattformen zum Datenaustausch oder Cloud-Schnittstellen gelangen Angreifer von der IT in die Produktion und können so direkt auf Steuerungssysteme zugreifen. Das Problem: Viele Unternehmen betrachten IT- und OT-Sicherheit isoliert voneinander und konzentrieren sich oft nur auf die „klassische“ IT-Sicherheit.

### Typische Hürden bei der Integration von IT und OT

Die gute Nachricht zuerst: Eine engere Verzahnung von IT- und OT-Security schafft Transparenz und ermöglicht schnellere Reaktionen auf Angriffe. Gleichzeitig zeigt die Praxis: Wer seine IT-Sicherheitsstrategie auf OT-Systeme überträgt, trifft auf typische Hürden – technisch, organisatorisch, kulturell und regulatorisch.

### Technik

In vielen OT-Anlagen treffen jahrzehntealte Maschinen und System ohne aktuelle Sicherheitsstandards auf moderne Schnittstellen, digitale Transformation und das IIoT. Diese Kombination aus veralteten Steuerungen und neuen Plattformen – etwa für präventive Überwachung, Datenanalyse oder Cloud – macht einheitliche Sicherheitskonzepte schwierig. Schon ein einziges falsch gesetztes Update oder eine unbedachte Regel kann zu erheblichen Betriebsstörungen führen.

### Organisation

IT und OT arbeiten traditionell in getrennten Strukturen. Im Ernstfall ist oft unklar, wer die Verantwortung trägt – der CISO oder der Produktionsleiter. In der Praxis bedeutet das: Während die IT sofort Systeme isolieren will, besteht die OT auf der Aufrechterhaltung der Produktion. Häufig fehlen zudem etablierte Prozesse und spezifisches Know-how, um beide Ziele miteinander zu verbinden und im Ernstfall schnell Entscheidungen zu treffen.

### Mindset

In der IT gilt Anpassung als Stärke – Updates, neue Tools, schnelle Zyklen. In der OT dagegen zählt Stabilität. Ein Beispiel: Viele Steuerungen laufen seit über 20 Jahren zuverlässig, können aber keine Sicherheits-Patches mehr aufnehmen. Sie erfüllen in vielen Fällen keinerlei heutige Sicherheitsstandards und lassen sich auch nicht entsprechend nachrüsten.

### Regulierung

Vorschriften wie NIS2 oder die KRITIS-Verordnung adressieren die speziellen OT-Herausforderungen, verschärfen jedoch zugleich den Handlungsdruck. Für OT-Spezialisten bedeutet das, neue Dokumentationspflichten zu erfüllen und Audits zu bestehen – oft parallel zum laufenden 24/7-Betrieb der Anlagen.

## Health Check: Schwachstellen systematisch erkennen

Im Alleingang lassen sich solche Hürden für viele Unternehmen nur schwer überwinden. Denn während die IT häufig über eigene Führungskräfte wie einen CIO verfügt, bleibt die OT häufig ohne dedizierte Verantwortung. Denn während in der IT klare Rollen und Verantwortlichkeiten etabliert sind, fehlt in der OT häufig eine vergleichbare Struktur. Besonders im Mittelstand, aber auch in großen Unternehmen, gibt es selten spezialisierte Teams, die Sicherheit systematisch angehen. Es fehlt an Ressourcen, Fachwissen und praktischer Erfahrung. Das führt dann dazu, dass bekannte Risiken oft unadressiert bleiben. Unbekannte Risiken wiederum werden mangels strukturierten Risikomanagement gar nicht erst erkannt.

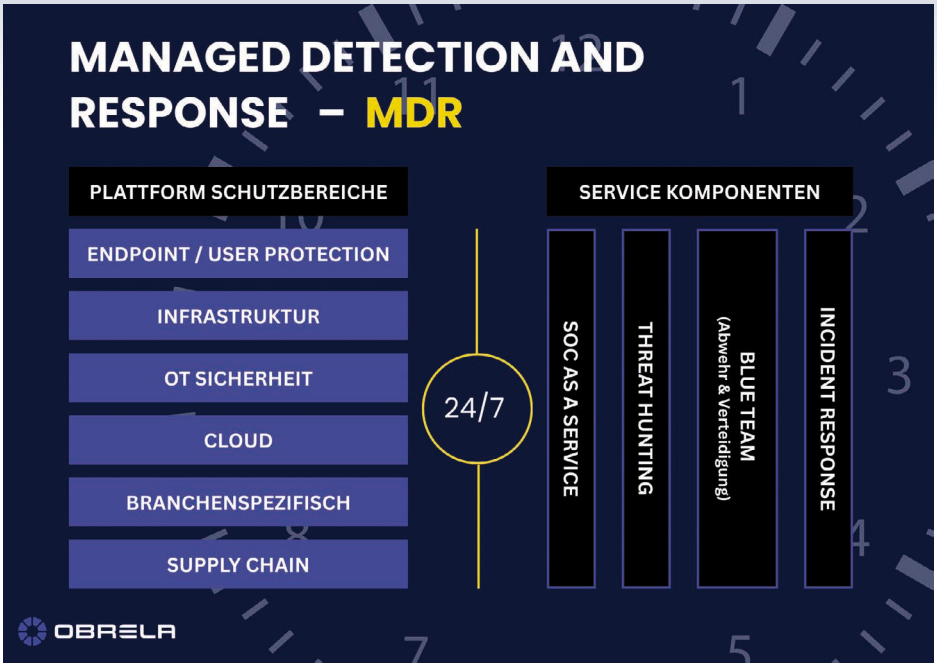
## Handlungsempfehlung

Eine konkrete Handlungsempfehlung zu Beginn ist die Inventarisierung aller OT/IT-Assets. Ein Health Check liefert Unternehmen eine umfassende Einschätzung ihrer OT-Sicherheitslage, die die größten Schwachstellen aufdeckt und Gegenmaßnahmen priorisiert. Die Überprüfung sollte auf Best Practices basieren und sich an bekannten Sicherheits-Frameworks (z. B. SANS „Five Critical Controls for ICS“ [2]) orientieren. Der tiefe Einblick in die eigene Sicherheitsarchitektur hilft Unternehmen, ihre Security-Roadmap anzupassen und ihre Cyber-Resilienz gezielt zu erhöhen.

## 4-Stufen-Modell

Der Health Check folgt einem strukturierten 4-Stufen-Modell:

1. **Ist-Zustand erfassen:** Zu Beginn steht die systematische Aufnahme aller bestehenden Prozesse, Technologien und Verantwortlichkeiten. Dazu gehören Workshops mit OT-, Engineering- und Security-Teams sowie eine erste Schwachstellenanalyse der wichtigsten OT-Assets. Ziel ist ein realistisches Bild der aktuellen Sicherheitslage, ohne den laufenden Betrieb zu stören.




*Wichtig für MDR: Eine zentrale Plattform für Rund-um-die Uhr Schutz*

2. **Zielbild definieren:** Auf Basis dieser Bestandsaufnahme wird gemeinsam ein Soll-Zustand für die OT-Sicherheit entwickelt. Dabei geht es um klare Zielvorstellungen für Incident Response, sichere Architektur, Netzwerk-Monitoring, Remote Access und Schwachstellenmanagement. Das Ergebnis ist ein abgestimmtes Zielbild, das sich an den Geschäftsanforderungen und Risiken des Unternehmens orientiert.

3. **Gap-Analyse:** Anschließend werden Ist- und Soll-Zustand gegenübergestellt und mit einem Reifegradmodell bewertet. Dieses Modell macht sichtbar, wo die größten Lücken bestehen und in welchen Bereichen Handlungsbedarf besonders dringend ist. Ein Dashboard zeigt die Ergebnisse auf einen Blick und erleichtert die Priorisierung.

4. **Maßnahmenplan entwickeln:** Zum Abschluss wird ein strategischer Handlungsplan erarbeitet, der alle Ergebnisse des OT Health Check zusammenführt. Er zeigt priorisierte Quick Wins ebenso wie mittel- und langfristige Maßnahmen, die direkt an den größten Lücken ansetzen. Das Strategiedokument enthält eine Executive Summary, den Maturity Score, die Gap-Analyse sowie klare Handlungsempfehlungen für die nächsten 12 bis 24 Monate.

## Security-as-a-Service

Nur wer seine IT- und OT-Umgebungen ganzheitlich betrachtet, versteht, wo die größten Risiken liegen. Unternehmen setzen häufig auf einzelne Sicherheitslösungen wie Patch-Management, Multi-Faktor-Authentifizierung oder die Segmentierung von Remote-Zugängen. Das ist wichtig, reicht aber nicht aus. Für die Praxistauglichkeit von OT- und IT-Sicherheit ist zudem ein eigenes Security Operations Center (SOC) im 24/7-Betrieb kombiniert mit realer OT-Security Expertise entscheidend. Doch genau dafür fehlt es in vielen Unternehmen an Ressourcen.

Ein hybrider Ansatz, der internes Fachwissen für Prozesse und Abläufe mit externer Expertise für Monitoring, Forensik und Compliance kombiniert, stellt hier Reaktionsfähigkeit sicher und erfüllt regulatorische Vorgaben.

## Wer schreibt:

Stefan Bange ist Geschäftsführer Deutschland beim Cybersecurity-Experten Obrela.

Peter Thiel leitet das Team IT/OT-Security bei der deutschen PLT networks GmbH. Gemeinsam entwickeln die Partner ganzheitliche Lösungen zur Absicherung der OT, darunter den OT Health Check Service. Damit unterstützen sie Unternehmen, eine umfassende Einschätzung ihrer OT-Sicherheitslage zu gewinnen und Sicherheitsrisiken zu minimieren. ◄

*Statt ein Security Operations Center (SOC) selbst zu betreiben, gibt es auch SOC-as-a-Service.*

## Quellenangaben

[1] IBM X-Force Threat Intelligence Index 2025, www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

[2] SANS „Five Critical Controls for ICS“ https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls