

# Wie Sie OT-Cyber Risiken minimieren und Ihre Systeme härten

Aus dem Tagebuch eines Pentesters: Wenn das Werkstor früh schon offensteht



Das Werkstor steht offen obwohl noch gar keine Schicht begonnen hat. Ganz klar eine Anomalie die auffällt und zum Handeln zwingt. Bei digitalen Anomalien in Prozessnetzen oder Steuerungseinheiten bleibt dies für lange Zeit oft verborgen und damit ein weit verbreitetes OT-Cyber Risiko. Mit der NIS2-Regulierung hat sich dies geändert und die Cybersicherheit ist endgültig in der Operational Technology (OT) deutscher Unternehmen angekommen. Doch während IT-Abteilungen seit Jahrzehnten auf etablierte Standardprozesse zurückgreifen, stehen OT-Verantwortliche vor einer völlig anderen Realität.

Historisch gewachsene Infrastrukturen, Legacy-Systeme mit Lebenszyklen von über 20 Jahren und der absolute Vorrang der Anlagenverfügbarkeit machen einen blinden „Rundumschlag“ nach klassischem IT-Vorbild unmöglich. Wer versucht, starre IT-Konzepte unüberlegt über die Produktion zu stülpen, riskiert im schlimmsten Fall teure Stillstände.

Wie sieht also eine effektive, praxisnahe OT-Absicherung aus, die reale Budget- und Personalrestriktionen berücksichtigt? Ein guter Ansatz, hier den Blickwinkel zu wechseln und die eigene Infrastruktur mit den Augen eines Angreifers – oder eines Pentesters – zu sehen.

Rhebo GmbH - a Landis+Gyr Company  
www.rhebo.com/de

## Der Blick aus dem Tagebuch eines Pentesters

Dass selbst gut gemeinte, oberflächliche Härtingsmaßnahmen ins Leere laufen können, zeigen zwei reale Fälle aus der Praxis, die unmissverständlich klarmachen: Cybersicherheit beginnt nicht erst in der Firewall, sondern am Werkstor.

### Fallbeispiel 1: In 20 Minuten zur Turbinensteuerung

In einem modernen Kraftwerk hatten die Betreiber bereits vorbildliche Hausaufgaben gemacht: Windows-Updates waren aktuell, Gruppenrichtlinien nach CIS-Benchmarks umgesetzt und starke Passwörter vergeben. Ein Pentest sollte die Wirksamkeit prüfen. Das Ergebnis war ernüchternd: Der Pentester gelangte unbemerkt in einem Fahrzeug auf das Gelände, fand einen offenen Schaltraum vor und steckte sein Notebook an einen zu Wartungszwecken offenen Port einer OT-Firewall. Über einen schlecht konfigurierten OPC-UA-Server der sich als unüberwachter, blinder Fleck herausstellte hatte er innerhalb von nur 20 Minuten uneingeschränkten Lese- und Schreibzugriff auf die sensiblen Turbinensteuerungen des Kraftwerks.

### Fallbeispiel 2: Die Hintertür im Leitsystem

Ein anderer Betreiber legte höchsten Wert auf ein transparentes Zugriffsmanagement und richtete für den Support eines Drittanbieters eine strenge Zwei-Faktor-Authentifizierung (2FA) ein. Als ein Wartungsfall eintrat, erledigte der Techniker den Support jedoch komplett ohne die erforderliche Freigabe. Die Ursache? Der Leitsystemhersteller hatte, ohne Wissen des Kunden, ein 5G-Modem als permanente Hintertür direkt im System verbaut. Ohne VPN, ohne Verschlüsselung und rund um die Uhr geöffnet. Jedes Drittunternehmen hatte so unbemerkt freien Zugang direkt ins innerste OT-Netzwerk.

### Drei Sofort-Maßnahmen für spürbar mehr OT-Sicherheit

Diese Beispiele zeigen: Die größte Gefahr in der OT sind blinde Flecken und mangelnde

Sichtbarkeit. Um Ihre Infrastruktur effektiv und ohne Produktionsrisiken zu härten, sollten Sie folgende drei Schritte priorisieren:

- **Zuständigkeiten und Prozesse schärfen:** Klären Sie eindeutig, wer von IT- und OT-Seite für welche Komponente zuständig ist. Unüberwachte „Schatten-IT“ oder vergessene Systeme (wie der OPC-UA-Server) sind die Einfallstore Nummer eins.
- **Netzwerk segmentieren (Zones & Conduits):** Trennen Sie konsequent die IT- Welt, die OT-Infrastruktur sowie Engineering- und Remote-Zugänge. Nutzen Sie gehärtete Firewalls zwischen den Zonen, um laterale Bewegungen von Angreifern im Keim zu ersticken.
- **Das Restrisiko mittels passivem Monitoring kontrollieren:** Da 100%ige Prävention in der OT (aufgrund von Legacy-Systemen) eine Illusion ist, benötigen Sie ein Frühwarnsystem. Ein netzbasiertes Intrusion Detection System (NIDS) spiegelt die Kommunikation über einen Mirror-Port völlig rückwirkungsfrei. Es erkennt Anomalien, Protokollbrüche und Cyberangriffe in Echtzeit, ohne den industriellen Prozess auch nur im Geringsten zu belasten.

### Bereit für das vollständige Pentester-Playbook?

Die Absicherung Ihrer industriellen Infrastruktur ist kein unbezwingbares Mammutprojekt – man muss nur anfangen. Schritt für Schritt.

In unserem neuen „Playbook für OT-Sicherheit - nach Art eines Pentesters“ gehen wir weit über diese ersten Schritte hinaus. Wir führen Sie detailliert durch die zehn wichtigsten organisatorischen und technischen Härtingsmaßnahmen (von Gruppenrichtlinien über Application Whitelisting bis hin zum Incident Management) und zeigen Ihnen, wie Sie die Anforderungen von IEC 62443, ISO 27001 und NIS2 praxisnah und budgetschonend lösen. Eine Video-Serie, welche Beispiele näher erläutert und bildlich beschreibt ist bereits in Arbeit. ◀

## Link

Laden Sie sich hier das kostenlose Playbook herunter und sichern Sie Ihre OT-Infrastruktur effektiv ab:

[/www.rhebo.com/de/downloads/playbook-fur-ot-sicherheit---nach-art-eines-pentesters?utm\\_campaign=408036546-OT-Sicherheit%20Pentester&utm\\_source=Beam-Verlag\\_IT-Produktion&utm\\_medium=Beam-Verlag\\_IT-Produktion&utm\\_term=IT-Produktion&utm\\_content=OT-Playbook](https://www.rhebo.com/de/downloads/playbook-fur-ot-sicherheit---nach-art-eines-pentesters?utm_campaign=408036546-OT-Sicherheit%20Pentester&utm_source=Beam-Verlag_IT-Produktion&utm_medium=Beam-Verlag_IT-Produktion&utm_term=IT-Produktion&utm_content=OT-Playbook)