



OPERATIONAL TECHNOLOGY (OT)

Ist Ihre OT-Umgebung
vor Angriffen auf die
Cybersicherheit geschützt?

Wir prüfen die Sicherheit Ihrer
OT und beraten Sie zu sinnvollen
Verbesserungen.

Sicherheit von OT-Umgebungen

Angriffe auf die OT und Ausfälle der Systeme können fatale Folgen haben, z. B. für die Fortführung der Produktion, die Logistik von Rohstoffen und Erzeugnissen, die Versorgung mit Energie, Wasser und Betriebsstoffen oder für die Funktionsfähigkeit der eingesetzten Maschinen. Je nach Branche besteht bei einem Vorfall auch Gefahr für Leib und Leben der Mitarbeitenden oder der Bevölkerung.

Die SySS kann Ihnen helfen, die Sicherheit Ihrer OT-Umgebung zu prüfen und zu stärken. Um eine Beeinträchtigung des Betriebs zu vermeiden, sollte im ersten Schritt mit unserem OT-Workshop ein konzeptuelles Review der OT-Umgebung stattfinden, im Zuge dessen auch genau angepasste OT-Penetrationstests geplant werden. Die Pentests werden idealerweise selektiv nur von bestimmten Systemen und über bestimmte Zugriffswege durchgeführt.



SySS Pentest
Expert



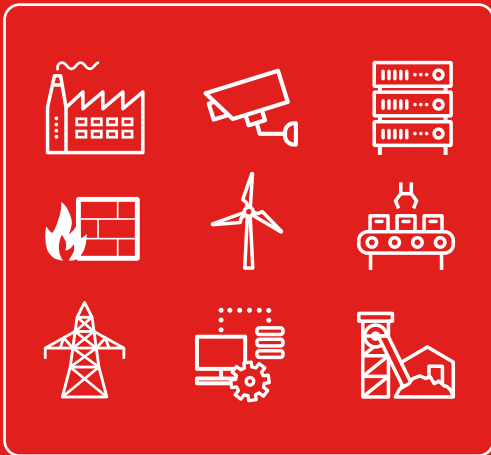
Konzept



OT-Administrator



SySS Pentest Expert



OT-Administrator

OT-Workshop

Unser OT-Workshop stellt als Einstieg das erste Projekt im Zusammenhang mit Ihrer OT-Umgebung dar:

- Der OT-Workshop betrachtet Ihre OT-Umgebung unter allen IT-sicherheitsrelevanten Aspekten.
- Der Workshop findet üblicherweise bei Ihnen vor Ort statt und umfasst zwei Tage plus Doku.
- Die SySS erstellt einen Bericht, der die aktuelle Architektur skizziert, mögliche Schwachstellen und Problemfelder aufzeigt und Angriffsszenarien identifiziert. Der Bericht enthält Empfehlungen zur Verbesserung und Optimierung der Architektur.
- Es ist kein Stillstand der Anlagen notwendig.

Der Workshop behandelt u. a. diese Themen:

- Netzwerkstruktur mit besonderem Fokus auf Separierung und Netzwerkübergänge
- Produktionsleitsystem und dessen Schnittstellen
- Authentifizierung und Identitätsmanagement
- Umgang mit Dienstleistern
- Fernzugriffsmodelle
- Updateprozesse
- Datenhaltung und Backupstrategie
- Physische Sicherheit
- Drahtlose Netzwerke (z. B. Bluetooth, WLAN, LTE)
- Mobile Geräte (z. B. Laptops, Handscanner etc.)
- Umgang mit Virtualisierung
- Logging und Monitoring
- SIEM und Incident Response-Prozesse
- Autarke Funktionsweise von Maschinen

OT-Penetrationstest

Ein OT-Penetrationstest kann u. a. die folgenden Fragestellungen beantworten:

- Welche Möglichkeiten bieten sich einem Angreifer, der in Ihre Steuerungsnetze vorgedrungen ist?
- Welche Angriffswege ergeben sich aus physischem Zugriff auf Netzwerkkomponenten bzw. -anschlüsse?
- Wie ist die Prozessleittechnik abgesichert und welche Kommunikationswege bestehen zur Unternehmens-IT?
- Können Angreifer aus anderen internen Netzwerken (z. B. IT) Zugriff auf die OT-Umgebung erlangen?
- Welche Kommunikationswege existieren nach extern, die sich ggf. für die gezielte Steuerung von Angriffen verwenden lassen?

Wir prüfen die verwendeten Systeme auf Schwachstellen, etwa ausgehend von einer kompromittierten Engineering-Workstation oder mit Netzwerkzugriff in der Leitwarte.

Hardware-Analyse von OT-Komponenten:

Wir testen die von Ihnen eingesetzten OT-Komponenten – Steuerungen, Fernwirkgeräte, industrielle IoT u. v. m. – im SySS-Labor auf ihre Sicherheit.

Das SySS-Labor ist bestens ausgestattet, um die von Ihnen eingesetzte Hardware zu analysieren.

Unser Team für Embedded Security greift dabei auf langjährige Analyseerfahrung von unterschiedlichen Geräten zurück.

SIE WOLLEN IHRE OT STÄRKEN?

Wir unterstützen Sie durch eine umfassende Beratung zum aktuellen Stand Ihrer IT-Sicherheit und helfen Ihnen mit Pentests, Schwachstellen zu beheben.

Unsere Consultants beraten Sie gerne zu passenden Projekten für Ihre OT-Umgebung.

Melden Sie sich bei uns!

SYSS
Operational Technology

ot@syss.de

THE PENTEST EXPERTS

WWW.SYSS.DE

Syss GmbH
Schaffhausenstraße 77 • 72072 Tübingen • Deutschland

+49 (0)7071 - 40 78 56-0
anfrage@syss.de
www.syss.de