OT CYBER SECURITY PENTESTING

Unsere Erfahrung in der Arbeit mit OT-Umgebungen ermöglicht es uns, erfolgreiche OT-Penetrationstests für Ihre Industrieanlagen durchzuführen.

Moderne Informations- und Kommunikationstechniken vernetzen die Industriewelt. Operational Technology (OT) wie Produktionsanlagen, Leitsysteme etc. sind für Cyberkriminelle höchst interessant. Denn die zunehmende Automatisierung der Industrieprozesse erfordert eine Vernetzung der OT- und IT-Technologien und verändert somit die Bedrohungs- und Risikolandschaft. Wo stehen Sie bei der Digitalisierung und Automatisierung, sind ihre Business-Prozesse in den Schutzzielen der Vertraulichkeit, Verfügbarkeit und Integrität abgesichert? Um zu überprüfen ob auch Ihre OT-Infrastrukturen geschäftskritisch sind, ist ein Cyber-Security-Audit die Lösung.

Täglich sind Sie als Unternehmen von einer Vielzahl an vertraulichen Informationen und sensiblen Daten umgeben, die es aufgrund ansteigender Cyber-Angriffe und Datendiebstähle zu schützen gilt. Die Aspekte Vertraulichkeit, Verfügbarkeit und Integrität gewinnen in dem Zusammenhang immer mehr an Bedeutung, um ihre Produktion zu schützen.

Wir testen OT-Systeme durch realistische Hacking-Simulationen und Cyber-Angriffe

DIE VORTEILE EINES AUDITS

VERTRAUEN

Die Bestätigung einen unabhängigen Audit stellt sicher, dass anhand einer OT Prüfung die besondere Sicherheit geprüft wurde und die Tätigkeit einer ständigen Überwachung unterliegt, schafft Vertrauen bei den Kunden.

KONKURRENZ-VORTEIL

Mit dem Cyber Security OT Audit einer unabhängigen Stelle gewinnen die Sachverständigen Wettbewerbsvorteile gegenüber der Konkurrenz.

WERBEMITTEL

Hinweise auf ein Cyber Security OT Audit können in Kommunikationsmedien eingebaut werden. Für die Sachverständigen ist eine Zertifizierung ein Zeugnis für Professionalität und die Verpflichtung zur Verfügbarkeit ihrer Produktionsumgebung.

Businesskritikalitätseinstufung

Eine Businesskritikalitätseinstufung bewertet die Schadenspotenziale der Anlage bzw. der Maschinen-Infrastruktur. Darauf aufbauend wird eine Schadenseingliederung zu potentiellen materiellen und immateriellen Schäden erstellt.

Risikoanalyse

Die Risikoanalyse umfasst das Identifizieren und Bewerten von Risiken der Maschienen und der Infrastruktur, sie umfasst die technische Datenanalyse in der bewertet wird, welche Sicherheitsprobleme auftreten können.

Penetration Testing

Ein Penetrationstest, auch als Pen-Test bekannt, ist ein gezielter simulierter Cyberangriff auf die Anlage und Infrastruktur, um ausnutzbaren Schwachstellen zu finden und darauf aufbauend die Sicherheitslücken zu schließen.

OT CYBER SECURITY TEST MODULE

01

ANGRIFFSVEKTOR-ANALYSE

Abbildung aller Angriffsvektoren, die gegen die Infrastruktur und Geräte ausgeführt werden können.

Folgendes wird festgestellt:

- Etwaige Schwachstellen, z. B. in der Netzarchitektur, dem Entwurf, Konfiguration und Firewalls
- Wie Angreifer diese Schwachstellen als Angriffswege in Netzwerke oder Geräte nutzen können

02

SCHWACHSTELLEN-SCANNING

Suchen Sie nach Schwachstellen, um Unterbrechungen zu vermeiden.

Folgendes wird festgestellt:

- Ein Überblick über Schwachstellen auf Geräte-, Netz- und Kommunikationsebene sowie deren Komplexität und Ausnutzbarkeit
- Wie die gefundenen Schwachstellen getestet und dokumentiert werden

03

OT PENETRATION TEST

(Live system hacking) Testen aller Zugangspunkte von externen zu internen Netzwerken

Folgendes wird festgestellt:

- Ausnutzbarkeit des Systems, der Geräte, der Frequenzen und ihre Auswirkungen auf die Systemsicherheit
- Wie man alle gefundenen Schwachstellen schließt

04

PROZESS-BEWERTUNG FÜR OT-SECURITY-OPERATIONEN

Bewertung der Situation Ihrer Cybersicherheit

Folgendes wird festgestellt:

- Fehlende Prozesse, Lücken auf Basis von Standards
- Fragen zu Sicherheitspraktiken und Strategien
- Detaillierte Informationen über Schwachstellen bei der Umsetzung, den Leitlinien und den Verfahren
- Beherrschung, um Probleme im Betrieb zu vermeiden

05

OT DEVICE LEVEL TESTING

Eingehende Prüfung von Geräten: Testen aller Schwachstellen und Verwundbarkeiten und Möglichkeiten zur Ausnutzung der Geräte

Folgendes wird festgestellt:

- Ausnutzbarkeit der Geräte und die Auswirkungen auf die Systemsicherheit