SICHERHEIT IN IT UND OT:
ZWEI WELTEN, EIN ANSATZ

Industrial Cyber Security Workshop

Die Vernetzung von Produktionssystemen ermöglicht es Ihnen, ein nie dagewesenes Maß an Effizienz und Flexibilität für Ihr Unternehmen zu erzielen. Doch wo Licht ist, ist auch Schatten: Je höher der Vernetzungsgrad, je höher die Digitalisierung, desto größer die Anfälligkeit für Attacken.
Denn auch hier sind Spionage und Sabotage ein Mittel, sich Wettbewerbsvorteile zu verschaffen oder einfach nur Schaden anzurichten. Und wenn das Know-how zu Hacks und Angriffen fehlen sollte: Für skrupellose „Dienstleister" und Malware nach Maß gibt es heute einen wachsenden Markt.

Mit diesem Workshop möchten wir die gefährlichen Lücken zwischen allgemeinem und technischem Sicherheitsdenken schließen, die sich derzeit noch im industriellen Milieu auftun. Denn diese Trennung existiert nicht mehr. Egal ob Objekte in der Produktion vernetzt werden oder einfach nur Daten in der Produktion gesammelt sowie analysiert werden und die Verbesserungen über eigenes Personal oder einen Wartungsdienstleister zurück in die Produktionsanlage gespeist werden. Gerade auch bei der Einbindung von IIoT (Industrial Internet of Things) in die Produktion steigt das Risiko von erfolgreichen Attacken extrem stark an, da Sensoren selten direkt abgesichert werden können. Wo auf PCs noch eine Software installiert werden kann, muss ein Sensor häufig so verwendet werden, wie er aus der Verpackung kommt.

Erfahren Sie in unserem Workshop die Vorteile von Cyber Security und im Besonderen die Sicherheitsvorteile einer gelebten IT-/OT-Konvergenz.
Wir analysieren gemeinsam mit Ihnen den Ist-Zustand Ihres Unternehmens und erarbeiten einen Soll-Zustand – damit Sie sich um die Sicherheit Ihres Unternehmens keine Gedanken machen müssen.

IHR ANSPRECHPARTNER

Timmi Hopf (Business Development Manager)
E-Mail: info-itsecurity@axians.de

„Jeder Produktionsprozess, egal auf welcher Anlage dieser stattfindet, kann abgesichert werden. Dabei spielt es keine grundlegende Rolle, ob die Anlage groß, klein, alt oder neu ist."

Timmi Hopf, Axians

GEMEINSAM MIT AXIANS

Vom Ist- zum sicheren Soll-Zustand

Schritt 1: Ist-Analyse Ihrer Produktion

In einem Zeitraum von 1–2 Wochen werden Informationen über Netzwerkgeräte, Netzwerktopologie, Geräte in der DMZ, sowie Gerätschaften im Level 0–3 des Purdue Modells (z. B. Fertigungssysteme, PLCs, IIoT- Geräte) mit 100% passive Sensoren gesammelt. Diese Informationen bieten Ihnen einen umfänglichen Überblick über verwendete Gerätschaften inkl. Firmware-/Hardware-Version, mögliche Einschübe, Standort, bekannte Schwachstellen und Bedrohungen, ein- und ausgehende Kommunikation des jeweiligen Assets, etc.

Datenschutz: Die Appliance ist zum Test von Systemparametern entwickelt worden, persönliche Daten werden im Rahmen der eigentlichen Informationssammlung nicht erhoben.

Schritt 2: Analyse der auffälligen Informationen

Axians Cyber Security Experten analysieren die gesamten Informationen, die während der 1–2-wöchigen Laufzeit gesammelt wurden.

Schritt 3: Ergebnis und Handlungsempfehlung

Basierend auf der Analyse der Informationen erstellen wir gemeinsamen mit Ihnen den Soll-Zustand Ihres Cyber Security Modells.

- Klärung Ihrer Fragen
- Übersicht der risikoreichsten Bedrohungen
- Darstellung der Kommunikationswege
- Tipps für den Ausbau Ihrer abgesicherten Infrastruktur
- Empfehlungen zur Risikoentschärfung

OPTIONAL

KOSTENFREIER REPORT

- pcap-File Auswertung Ihres gewünschten Unternehmensbereiches
- Ergebnis in Form eines pcap-Files:
  - Informationen über erkannte Assets
  - Erkennung relevanter Schwachstellen der erkannten Assets
  - Kommunikationsbeziehungen zwischen den erkannten Assets

axians

Axians IT Security GmbH · Arndtstraße 25 · 22085 Hamburg
Tel.: +49 40 271661-0 · Fax: +49 40 271661-44 · E-Mail: info-itsecurity@axians.de · www.axians.de