INDUSTRIE RISIKO MANAGEMENT AUTOMATISIERUNG

CYBEResilienz IT · OT · OK

Resilienz-Bestimmung für Industrie-IT

Die Herausforderung

Die Verbesserung Ihrer Sicherheit ist unser gemeinsames Ziel! Wir haben ein Konzept für den Einstieg in die Operational Technologie (OT) Sicherheit entwickelt, damit Sie sich diesem Ziel nähern, Erfahrungen sammeln und die Widerstandsfähigkeit Ihrer Produktion / Anlage besser bewerten können. Weg von der gefühlten Sicherheit – hin zu den Fakten, dem Ist-Zustand.

Die effiziente Absicherung der gewachsenen Informationstechnik von Produktionsanlagen gegen aktuelle Bedrohungen wie Cyberangriffe, interne Manipulationen oder fehlerhafte Konfigurationen ist eine zunehmend komplexere Anforderung – an Mensch und Technik. Denn aus diesen Bedrohungen können Systemausfälle bis hin zum Stillstand der kompletten Produktion resultieren.

Bei welchen Vorhaben ist diese objektive Evaluierung besonders sinnvoll?

- Sie wollen sich gegen Cyberrisiken **versichern**
- Sie (oder ein Unternehmen aus Ihrer Branche) hatten einen konkreten **Vorfall** oder haben **ältere Automatisierungsgeräte** im Einsatz
- Sie benötigen eine objektive Entscheidungshilfe für weitere **Investitionen** / Erneuerungen
- Sie wollen in eine Zertifizierung oder müssen die **regulatorische Anforderungen** erfüllen
- ... oder effizient die **Risiken** auf Basis der aktuellen Übersicht aller Geräte und System **bewerten**

Zwei Module für mehr Sicherheit in der Anlage

1. Im ersten Schritt erfolgt die **Evaluierung** durch den Einsatz der IRMA ® Security Appliance zur selbstständigen Aufnahme und Analyse der Assets sowie deren Datenverbindungen. Auf Basis dieser aktuellen Informationen evaluieren unsere Netzwerk- und OT-Security-Spezialisten mit ihnen mögliche Bedrohungen und Risiken.
2. Anhand dieser konkret vorliegenden Informationen wird im zweiten Arbeitsschritt eine **Angriffs-Simulation** zur Bestimmung des aktuellen Infrastruktur-Resilienz-Wertes mit Hilfe von securiCAD durchgeführt.

Ihre Vorteile

- Sofortige Verfügbarkeit der Analyseergebnisse
- Planung der weitergehenden, prioren Sicherheitsmaßnahmen auf Basis der übersichtlichen Analyseergebnisse
- Zugriff auf OT-Security Spezialisten, die Sie aktiv in jedem Schritt der Evaluierung unterstützen

INDUSTRIE RISIKO MANAGEMENT AUTOMATISIERUNG

CYBEResilienz IT · OT · OK

Der Fahrplan – Vorgehen und Details

Ergebnisse in Modul 1: IRMA ® OT-Evaluierung

- Unmittelbare Übersicht und Transparenz ihrer IT-/ OT-Geräte
- Sichtbarkeit von Anomalien im Evaluierungszeitraum
- Ergebnisliste und empfohlene Maßnahmen
- Nachweis des begonnenen Sicherheitsprozesses
- Risikoanalyse der hoch kritischen Erkenntnisse

Modul 1 mit 30-tägiger Nutzung der IRMA® Security Appliance vor Ort:

IRMA ® OT-Evaluierung

VORBEREITUNG UND BETREUTE INSTALLATION der IRMA® Security Appliance	Vorab wird telefonisch der optimale Messort in der Anlage identifiziert und die Schritte zur Installation vor Ort besprochen. Versand der vorinstallierten IRMA® per Post.
TRANSPARENZ UND EINSICHT	Umgehend sichtbare Daten der Geräte und Systeme mit detaillierter Darstellung der Kommunikationen und genutzten Protokolle werden direkt nach der Installation gemeinsam in Augenschein genommen.
MONITORING UND ALARMIERUNG	Die kontinuierliche Aufzeichnung erfolgt durch die kognitive Analyse der Kommunikationen. Es werden sofort Auffälligkeiten erkannt und Alarmierungen ausgelöst.
ERSTE STATUSBESTIMMUNG	In gemeinsamer Analyse mit einem OT-Security- und Netzwerkspezialisten werden die gesammelten Daten analysiert, welche Auffälligkeiten bestehen und welche Maßnahmen sich daraus ableiten.
ERGEBNISPRÄSENTATION	Abschließend zum Messzeitraum von 30 Tagen werden die gesammelten Ergebnisse der Analyse und Maßnahmenempfehlungen präsentiert.
BERICHT	Elektronischer Report über die gefundenen Geräte und Kommunikationen sowie das Ergebnis der ersten Risikobetrachtung.

Ab 1580,- Euro

INDUSTRIE RISIKO MANAGEMENT AUTOMATISIERUNG

CYBEResilienz IT · OT · OK

Ergebnisse in Modul 2: securiCAD® Resilienz-Bestimmung

securiCAD® liefert als Ergebnis der Angriffs-Simulation den Resilienz-Wert *time to compromise*. Dieser gibt an, wie lange ein potenzieller Angreifer statistisch gesehen benötigt, um die Produktions-Anlage zu kompromittieren.

Die Simulation leitet die aktuellen Infrastruktur-Schwachstellen ab und priorisiert diese. Über die Simulation lassen sich die wahrscheinlichsten Angriffs-Wege in die Infrastruktur betrachten, um die wertvollsten Schutzmaßnahmen abzuleiten.

Modul 2 mit securiCAD® Resilienz-Bestimmung:

securiCAD ® Resilienz-Bestimmung	VORBEREITUNG	Die gesammelten Daten werden im Zuge der Aufbereitung gemeinsam mit dem Kunden gesichtet und nachqualifiziert, um ein bestmögliches Mess-Ergebnis zu gewährleisten.
	RESILIENZ-BESTIMMUNG DER ANLAGE	Die aufbereiteten Daten werden an die Modellierungs-Komponente securiCAD® weitergegeben. Mit Hilfe quantitativer Stochastik wird eine Resilienz-Analyse der identifizierten Infrastruktur durchgeführt.
	RESILIENZ-BERICHT	Das Ergebnis der Resilienz-Analyse wird in einem Ergebnis-Bericht festgehalten, in welchem die Widerstandsfähigkeit der identifizierten Kronjuwelen, sowie der wahrscheinlichste Angriffspfad beschrieben werden. Die identifizierten Schwachstellen werden priorisiert zusammengefasst und mit einer Handlungsempfehlung versehen.

Ab 1260,- Euro

Die Vorteile im Bundle

Es ist der Start für den Security Management Prozess. Das passive Monitoring ermöglicht schnell und rückwirkungsfrei die Aufnahme der Daten. Sämtliche Informationen stehen für die Resilienz-Bestimmung mit wenig Aufwand zur Verfügung. Nach der Angriffs-Simulation können unmittelbar Verbesserungen der Cybersicherheit in der Anlage erfolgen.

- Bewertung zum Status der OT-Sicherheit innerhalb von 30 Tagen
- Unterstützung durch erfahrene OT-Security-Speziallisten für 8 Stunden je Modul
- Nutzung der IRMA® Security Appliance vor Ort und Ergebnisbericht der Resilienz-Analyse durch securiCAD® mit identifizierten Schwachstellen

Bundle-Preis ab 2840,- Euro

Weitere Informationen, Kontakt und Bestellung gleich hier:

kontakt@acht-werk.de oder **helmut.oppitz@cyberesilienz.de**