ICS Audit - Leitsystem / OT-Security

Angenehme, professionelle Zusammenarbeit in einem offenen und ehrlichen Zusammenarbeitsverhältnis.
SH POWER

Wir waren mit dem Audit und dem Auditor sehr zufrieden. Kompetente, unkomplizierte und angenehme Zusammenarbeit.
St. Gallisch Appenzellische Kraftwerke AG

Zielgruppe

:: Betreiber von Versorgungsleitsystemen
:: Betreiber von Kraftwerkleitsystemen
:: Betreiber von Industrieleitsystemen

Einleitung

Wo früher noch klassische ICS Protokolle anzutreffen waren, sind heute klassische Netzwerkprotokolle wie TCP/IP im Einsatz. Leitsysteme müssen über das Internet erreichbar und steuerbar sein. Die Sicherheit von Leitsystemen ist eine Anforderung, die aufgrund dieser Entwicklung plötzlich im Fokus steht. Gleichzeitig können klassische Sicherheitsmassnahmen nicht immer 1:1 übernommen werden.

Durch die zunehmende Vernetzung und dem Zusammenspiel der IT und OT Welt wirken neue Gefahren auf die ICS Infrastruktur. Diese gilt es zu identifizieren und auf ein akzeptables Niveau zu reduzieren.

Inhalte

Die Prüfobjekte hängen von Ihrer Infrastruktur ab. Damit ein optimales Ergebnis erreicht werden kann, startet das Audit nach der Vorbesprechung mit einem Workshop. Dort werden Ihre Bedürfnisse festgehalten. Zusätzlich ermöglicht es unseren Experten, Ihre Infrastruktur besser zu verstehen und aus externer Sicht lohnende Objekte zu identifizieren. Wir sind überzeugt, dass die Synergie von internem Systemverständnis und externem Security Knowhow zum massgeblichen Erfolg führt.

Folgende Elemente werden kontrolliert:
:: Aufbau des Leitsystems (Konzeptionierung)
:: vorhandene Dokumentation
:: Konfiguration von Servern
:: Kommunikation PLC/SPS
:: Sicherheitsbewertung Kontrollraum
:: Sicherheitsbewertung Netzwerk
:: Manipulationsmöglichkeiten HMI
:: Analyse / Manipulation Protokolle
:: Verfügbarkeit und Backup

Nutzen

Mit den Resultaten aus dem ICS Audit können Sie allfällige Schwachstellen in Ihrer ICS-Infrastruktur systematisch beheben. Durch den detaillierten Bericht erhalten Sie auch Hintergrundinformationen, weshalb unsere Experten eine Massnahme vorschlagen und bekommen Lösungswege aufgezeigt. Mit dem ergänzenden Massnahmenkatalog erfahren Sie die Bewertung der Schwachstellen aus unserer Sicht. Er hilft Ihnen bei der abschliessenden Definition der umzusetzenden Massnahmen sowie bei der Umsetzungskontrolle. Der Massnahmenkatalog ist so aufgebaut, dass Sie die notwendigen Schritte selbstständig oder mit Ihrem vertrauten Dienstleistungspartner umsetzen können.

Somit können Sie sicher sein, Ihre Kontrollfunktion gewissenhaft wahrgenommen zu haben und reduzieren die Gefahr von vermeidbaren Ausfällen und Störungen in Ihrer ICS-Infrastruktur.

Vorgehen

Bedürfnisaufnahme
In einem vorgängigen Gespräch werden Ihre Anforderungen und Anliegen aufgenommen und beschrieben. Dieses Gespräch bildet die Basis für das ICS-Audit und legt fest, welche Systeme und Netzwerke angeschaut werden.

Vorbereitungen
Der Ihnen zugewiesene Auditor setzt sich mit der uns ausgehändigten Dokumentation auseinander, überprüft deren Umfang.

Bedürfnisfestigung
Am Tag des Audits findet ein ausführliches Kick Off statt. Idealerweise sind alle Beteiligten (inkl. Externe) dabei. Der Fokus und der Ablauf des ICS-Audits werden nun gefestigt.

Audit
Die definierten Elemente werden unter Ihrer Aufsicht geprüft. Die enge Zusammenarbeit mit Ihnen ist uns wichtig. Wichtige Feststellungen erfahren Sie jeweils direkt. Je nach Umfang und Komplexität dauert das ICS Audit bei Ihnen vor Ort zwischen 3 und 10 Tagen.

Erstellung des Berichts
Die Auditoren erstellen anschliessend an das Audit den umfassenden Bericht.

Präsentation der Resultate
Die Präsentation findet bei Ihnen statt. Sie definieren, welche Personen an der Präsentation teilnehmen. Sämtliche Dokumentationen werden Ihnen an diesem Termin übergeben.

Lieferobjekte (digital)

:: Zusammenfassung
:: Ausführlicher Bericht
:: Massnahmenliste mit Priorisierung
:: Präsentation und Besprechung der Resultate

Aufwand

Je nach Umfang der zu prüfenden Elemente, liegt der Aufwand zwischen 5 und 20 Tagen. Darin eingeschlossen sind alle beschriebenen Tätigkeiten. Gerne erstellen wir Ihnen nach der Bedürfnisaufnahme eine persönliche Offerte.

Kontakt

goSecurity AG
Sandro Müller
Schulstrasse 11
8542 Wiesendangen
052 511 37 37
info@goSecurity.ch
www.goSecurity.ch

Referenzen

Werden auf Anfrage inkl. Kontaktperson zur Verfügung gestellt.