Erwerben Sie die spezifischen Kenntnisse des ICS Security Manager für die Planung und Etablierung eines Informationssicherheitsmanagementsystems (ISMS) für industrielle Automatisierungssysteme gemäß IEC 62443, ISO 27001 und BSI IT-Grundschutz

Die **Haupttätigkeit** des "ICS (Industrial Control System) Security Manager" besteht darin, die Leitung der Organisation in der Wahrnehmung ihrer Pflichten zur Sicherstellung eines angemessenen **Informationssicherheitsniveaus**, bei dem Betrieb von industriellen Automatisierungssystemen (IACS) , zu unterstützen, sowie die angemessenen **Security Level** und **Protection Level** zu bestimmen.

Die stark zunehmende Vernetzung von Prozesssteuerungssystemen mit IT Netzen führt zu zusätzlichen, spezifischen Risiko- und Bedrohungsszenarien, insbesondere für die Betreiber von IACS. Bei der Entwicklung, der Integration sowie dem Betrieb von IACS müssen insbesondere geltende Normen und Rechtsvorschriften beachtet werden, um eine **risikoadäquate** Entwicklung der organisationsspezifischen **Sicherheitsstrategie** sowie die Umsetzung eines angemessenen **ganzheitlichen Sicherheitskonzeptes** sicherzustellen.

Bedrohungen wie Sabotage, Spionage oder gezielte Angriffe auf Daten und Systeme sowie geistiges Eigentum und Know-how fordern ein proaktives Sicherheitsdenken der verantwortlichen Personen sowie einen bewussten Umgang mit dem Thema Betriebs- und Informationssicherheit. Die zu berücksichtigenden Sicherheitsfunktionen, beim Design der Hard- und Softwarekomponenten von ICS und IACS, auf Betriebsplattformen und in den hochgradig vernetzten Infrastrukturen, erfordern oftmals ein komplexes internes Prozessmanagement, sichere Systemarchitekturen sowie anlagenspezifische Schutzmaßnahmen.

ZIEL DER AUSBILDUNG

Der Schwerpunkt der Ausbildung liegt auf der Vermittlung von Fachbegriffen und Methoden zur Planung und Umsetzung der Informationssicherheit in IT-gestützten Steuerungs- und Automatisierungsanlagen.

Die Teilnehmer können nach Abschluss der Ausbildung das Zusammenwirken von IT Sicherheit und Anlagensicherheit, für einen sicheren Betrieb von ICS-Umgebungen, erkennen und bewerten. Unter Einbeziehung der Anforderungen an ein ISMS sowie durch die Einbindung des Business Continuity Managements können die Teilnehmer die angemessenen Maßnahmen zur Etablierung des geforderten Sicherheitsniveaus planen und zur Umsetzung bringen.

Die Ausbildung entspricht inhaltlich den **„Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld" des Bundesamtes für Sicherheit in der Informationstechnik (BSI).**

INHALT

- Die IEC 62443-Normenreihe für industrielle Kommunikationsnetze
- Anforderungen an Hersteller, Betreiber und Integratoren
- Die „Defense in Depth"-Strategie beim Betrieb von ICS und IACS
- Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
- Anforderungen an die Fähigkeiten des Integrators
- Anforderungen an Sicherheitsmaßnahmen bei der Erbringung von Dienstleistungen an IACS
- Die ISO 270xx-Normenreihe für ISMS
- Die VDI/VDE-Richtlinie 2182
- Vorgehensbeschreibung der VDI/VDE 2182
- IT-Sicherheit in industriellen Anlagen
- Das IT-Sicherheitsgesetz und KRITIS
- Sicherheitskataloge der BNetzA für Energie und ITK
- Informationssicherheit und IT Sicherheitskonzepte für ICS-Umgebungen
- IT-Sicherheitsmaßnahmen beim Betrieb von IACS
- Die Schutzzieldefinitionen in der industriellen IT
- Security Level und Protection Level
- Cyber Security und ICS
- Der IT-Grundschutz des BSI
- Bausteine und Umsetzungshinweise für ICS
- IT-Sicherheit vs. Betriebssicherheit
- Security by Design / Security by Default
- Bestimmung von Security Levels in der Automation
- Die ISO 22301 für Business Continuity Management Systeme (BCMS)
- Aufbau eines ISMS und BCMS
- Risikomanagement beim Betrieb von ICS-Systemen
- Zonen, Conduits und Risikobeurteilung
- Die Behandlung von Informationssicherheitsvorfällen
- Haftungsrisiken für ICS-Betreiber
- Gefährdungen und Maßnahmen in ICS- und IT- Infrastrukturen

Abschluss: Teilnahmebestätigung

Optional: Prüfung mit Personenzertifikat (DGI®)

ZIELGRUPPE

- Verantwortliche für ICS / Automation Security
- Betriebspersonal für industrielle IT / ICS
- Verantwortliche im Risikomanagement
- Verantwortliche im Business Continuity Management
- Verantwortliche in der Informationssicherheit
- CISO / IT-Sicherheitsbeauftragte
- IT-Leitung / Administratoren
- Unternehmensberater / Wirtschaftsprüfer

IHR DOZENT

Herr Ronny Neid

Herr Neid ist Diplom-Betriebswirt sowie u. a. zertifizierter IT-Risk und Business Continuity Manager und IT-Sicherheitsbeauftragter. Als Vorstand | COO der DGI berät Herr Neid im Bereich der IT-Sicherheit und des Datenschutzes und entwickelt Sicherheitskonzepte. Herr Neid doziert zu zahlreichen korrelierenden Themen der Informationssicherheit.

© DGI AG 2020