Institut für ISICS
IT-Sicherheit in Industrial Control Systems

In dieser Broschüre finden Sie die Schulungsangebote des Instituts für IT-Sicherheit in Industrial Control Systems (ISICS).

Alle Schulungen können online oder in Präsenz durchgeführt werden. Es gibt regelmäßige Termine in Aachen, aber auch Inhouse-Schulungen sind möglich.

Termine und Preise finden Sie auf unserer Webseite scada-secure.de

@yet Industrial IT Security

Certified SCADA Security Engineer (CSSE)

Einführung in die IT-Sicherheit von industriellen Steuerungen

SCADA-Ingenieure und IT-Administratoren müssen jeweils vom anderen lernen. Genau dazu haben wir unsere Kurse geschaffen. In 5 Tagen werden im Seminar ***Certified SCADA Security Engineer*** alle notwendigen Sachverhalte vorgestellt und besprochen und Sie werden auf die ISICS-Zertifizierung *Certified SCADA Security Engineer* (CSSE) vorbereitet.

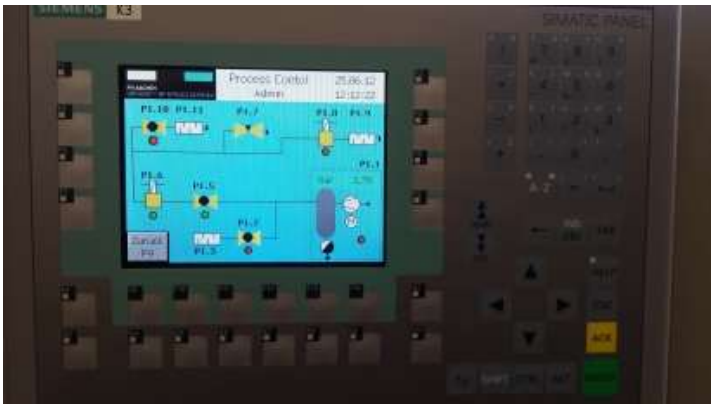
Das IT-Sicherheitsgesetz verpflichtet Betreiber kritischer Infrastrukturen zur IT-Sicherung ihrer Anlagen. Das Personal ist dabei häufig überfordert. Diejenigen, die sich mit IT-Sicherheit auskennen, kennen die industriellen Anlagen und deren Besonderheiten nicht. Die, die die Anlagen kennen, sind meist keine IT-Spezialisten.

SCADA-Ingenieure und IT-Administratoren müssen jeweils vom anderen lernen. Genau dazu haben wir unsere Kurse geschaffen. In 5 Tagen werden im Kurs ***Certified SCADA Security Engineer*** alle notwendigen Sachverhalte vorgestellt und besprochen und Sie werden auf die ISICS-Zertifizierung *Certified SCADA Security Engineer* (CSSE) vorbereitet. Neben den theoretischen Grundlagen werden auch praktische Übungen durchgeführt, die konkret zeigen, wie und was zu tun ist. Dabei führen die Teilnehmer selber z.B. Angriffe auf Systeme durch, entwerfen ein Firewallszenario, bewerten eine Geräteschwachstelle oder bewerten (toolgesteuert) ein gesamtes Produktionsnetz. Dazu werden u.a. virtuelle Maschinen verwendet.

Angriff auf das MODBUS Protokoll

SQL-Injection-Angriff auf ein HMI Web-Login

Wir haben aber auch richtige Hardware, die angegriffen werden kann (siehe Bilder unten).

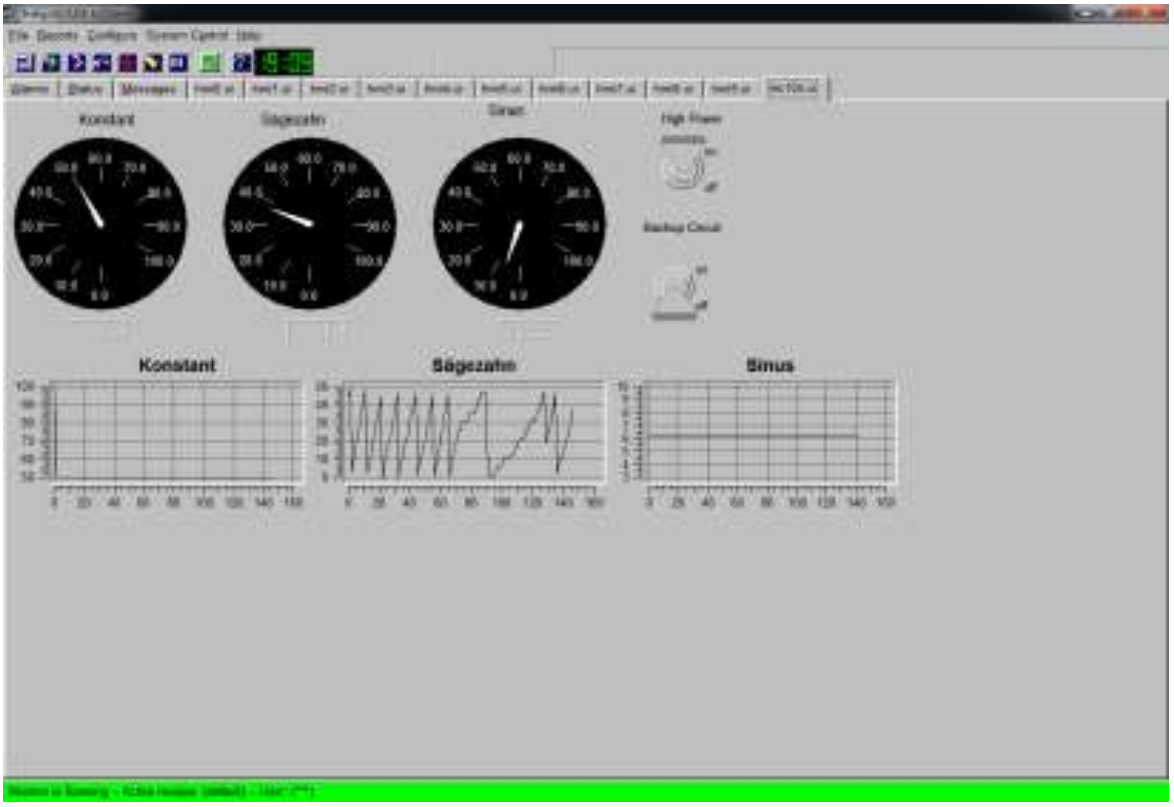


Angriff auf eine Siemensanlage

Institut für ISICS
IT-Sicherheit in Industrial Control Systems

Angriff auf ein VPN (Beckhoff)

Angriff auf ein HMI (WindowsXP)



Angriff auf das Protokoll IEC 60870-5-104

Der Kurs wendet sich an SCADA-Ingenieure, die auch wissen müssen, wie sie ihre Systeme sichern, und an IT-Sicherheitsadministratoren, die die Unterschiede zwischen ihrer Office-IT und einem SCADA-Netz kennen müssen. Er wendet sich aber auch an diejenigen, die in ihrer Funktion für die IT-Sicherheit einer Organisation verantwortlich sind. Unsere Dozenten sind ausgewiesene Experten, die die Probleme und deren Lösung kennen.

Der Kurs wird mit der Prüfung zum CSSE abgeschlossen.

Kurze Zusammenfassung der Inhalte (Kurse auf Deutsch oder Englisch):

1. Einführung
    a. Entwicklung von SCADA-Systemen
2. Übersicht über industrielle Steuerungssysteme
3. ICS-Protokolle
4. Übersicht Informationssicherheit
5. Bedrohungen und Schwachstellen von industriellen Steuerungen
6. SCADA Schwachstellen
    a. Vorstellen typischer Angriffstechniken
    b. Praktische Beispiele
7. Sicherheitstechnik für ICS
    a. Firewall
    b. IDS
    c. Authentifizierungsserver
    d. Security Information and Event Management (SIEM)
    e. Sichern der Feldebene
    f. Sichern von Remote-Zugängen
8. Sicherheitsmaßnahmen zur ICS-Sicherung
    a. Defense-in-Depth
9. Patchmanagement
10. Sicherheitsstandards und Best Practices
    a. Standards
    b. 21 typische Schritte
    c. IT-Sicherheitsgesetz
        - Branchenspezifische Standards
11. Pentests und IT-Forensik für ICS
12. Einführung: Aufbau und Umsetzung eines CERT im ICS-Umfeld
    a. Praxis: Verwendung des *Cyber Security Evaluaton Tools* zur Feststellung des aktuellen Sicherheitszustandes eines ICS

Praktische Aufgaben

Im Rahmen des Kurses führen Sie u.a. folgende Aufgaben aus:

- Angriff auf das Protokoll Modbus
- Angriff auf das Protokoll IEC 60870-5-104
- Finden von SPS-Systemen über Shodan
- Angriff auf eine SPS
- Brute Force Angriff auf SPS-VPN
- Angriff auf einen SPS-Webserver
- Anfgriff auf eine SCADA-Workstation
- Angriff auf eine HMI über die Webseite
- Scannen mit nmap
- Man-in-the-Middle Angriff auf SCADA-Kommunikation
- Erstellung eines Firewall-Regelwerks für SCADA
- Bewertung von ICS-Schwachstellen mit CVSS
- Bewertung des Sicherheitszustands eines kleinen ICS mit CSET.

Um das Zertifikat *CSSE* zu erlangen, muss der Kurs mit einem Online-Test abgeschlossen werden (ca. 100 Fragen/180 Minuten).

Testvorbereitung und Test finden am letzten Tag des Kurses statt.

Institut für IT-Sicherheit in Industrial Control Systems

Zertifikat

Certified SCADA Security Engineer

CSSE

Frau Marion Mustermann

hat erfolgreich die Prüfung zum

Certified SCADA Security Engineer

abgelegt.

Aachen, 25.09.2015

Prof. Dr. Marko Schuba
Kursleiter

Dipl.-Ing. Hans Höfken
Trainer

Kursinhalt des 5-tägigen CSSE Kurses:

1. Einführung
   a. Entwicklung von SCADA Systemen
   b. Das IT Sicherheitsgesetz
2. Übersicht über Industrielle Steuerungssysteme
3. ICS Protokolle
4. Bedrohungen und Schwachstellen von Industriellen Steuerungen
5. Angriffe auf SCADA
   a. Vorstellen typischer Angriffstechniken
   b. Praktische Beispiele
6. Sicherheitstechnik für ICS
   a. Firewall
   b. IDS
   c. Authentifizierungsserver
   d. Security Information and Event Management (SIEM)
   e. Sichern der Feldebene
   f. Sichern von Remote Zugängen
7. Sicherheitsmaßnahmen zur ICS Sicherung
   a. Defense-in-Depth
8. Anti-Malware und Patchmanagement
9. SCADA Sicherheitsstandards und Best Practices
   a. Standards: IEC 62443
   b. 21 typische Schritte
10. Pentests und IT Forensik für ICS
11. Einführung : Aufbau und Umsetzung eines CERT im ICS Umfeld
    a. Praxis: Verwendung des *Cyber Security Evaluation Tools* zur Feststellung des aktuellen Sicherheitszustandes eines ICS.
    b. Vorstellung: *LARS*

Der Abschlusstest wurde mit 89% erfolgreich bestanden.

Was haben Sie davon?

Nach dem Seminar sind die Teilnehmer in der Lage, die Probleme der Sicherheit von SCADA-Systemen zu erkennen und zu beheben. Sie kennen die relevanten Verfahren um die IT-Sicherheit weiter zu entwickeln und die Grundlagen, die für ein ICS Informations-sicherheitsmanagement notwendig sind. Ob SCADA-Ingenieur oder IT-Mitarbeiter, Sie kennen und verstehen die Probleme des Anderen.

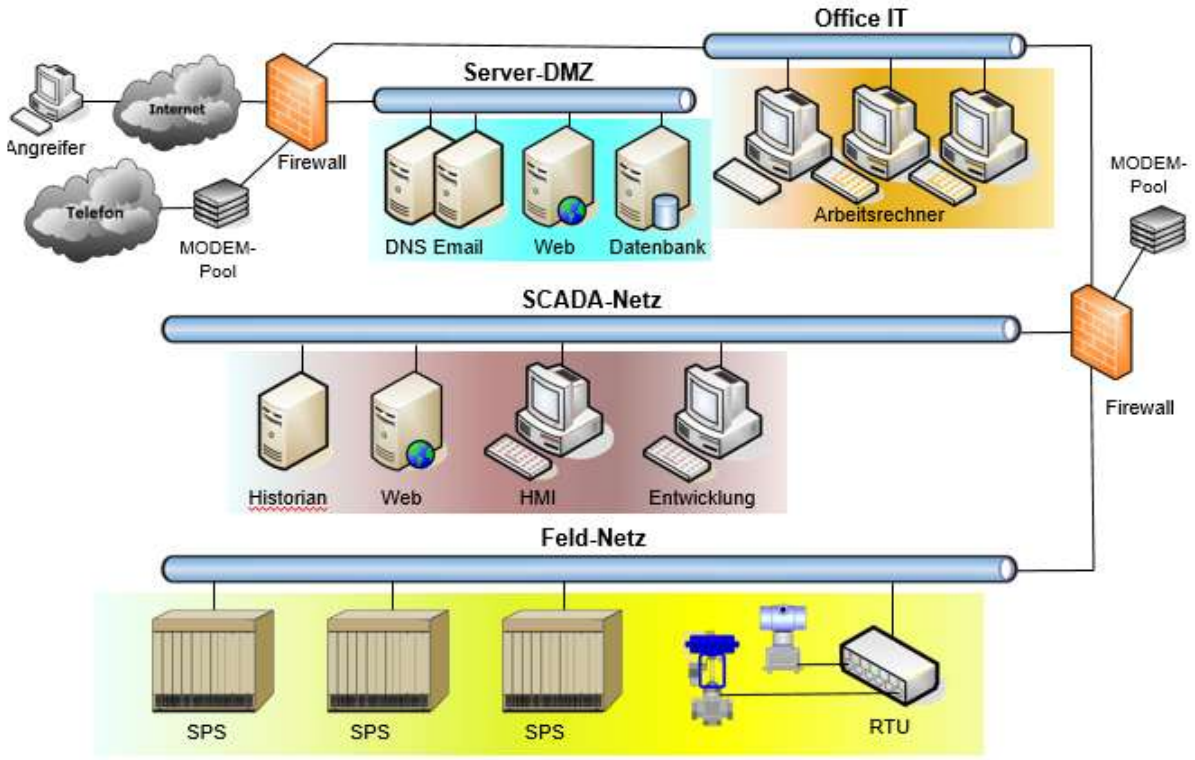
Cyber Security *Seminar* für industrielle Steuerungssysteme (CSSIS)

Einführung in die IT-Sicherheit von industriellen Steuerungen

IT-Sicherheit ist neben der technischen auch eine organisatorische Herausforderung. Es ist wichtig zu wissen, wie ein Angreifer vorgeht, um entscheiden zu können, auf welche Szenarien man sich vorbereiten soll. Welche Standards gibt es und wie können sie umgesetzt werden?

Als verkürzte Version unseres Kurses *Certified SCADA Security Engineer (CSSE)*, ist dieses 3-tägige Seminar eine fundierte Einführung in das Thema IT-Sicherheit für industrielle Steuerungssysteme.

Nach einer Einführung in die IT-Sicherheit von ICS und der kurzen Darstellung von Angriffszenarien, wird sinnvolle Technik, die einen sicherheitstechnischen Vorteil bringt, vorgestellt. Weiterhin wird ein Cybersicherheitsmanagement-System (CSMS) vorgestellt, das zum Managen der IT-Sicherheit im ICS notwendig ist (siehe neues IT-Sicherheitsgesetz für kritische Infrastrukturen der Bundesregierung).



SCADA Zonenkonzept

Dann stehen in diesem Seminar die organisatorischen Aspekte im Vordergrund.

Best Practices, Policy Management, Schwach-stellentests und Aufbau/Aufgaben eines Computer Emergency Response Teams (CERT) für ICS sind die weiteren Hauptthemen. Sie erfahren aber auch, wie Angreifer vorgehen. Dazu führen die Teilnehmer selber z.B. Angriffe auf Systeme durch.

Unsere Dozenten sind Experten, die sich mit der Materie und deren Vermittlung sehr gut auskennen.

Inhalt dieses Seminars:

1. Einführung
2. Übersicht über industrielle Steuerungssysteme
3. ICS-Protokolle
4. Bedrohungen und Schwachstellen von industriellen Steuerungen
5. Angriffe auf SCADA
   - Angriff auf eine SCADA-Workstation
   - Angriff auf Geräte der Feldebene
6. Sicherheitstechnik für ICS
7. Sicherheitsmaßnahmen zur ICS-Sicherung
8. Patchmanagement
9. SCADA-Sicherheitsstandards und Best Practices
10. Einführung in den Aufbau und Umsetzung eines CERT

Was haben Sie davon?

Nach dem Seminar kennen die Teilnehmer die Probleme der Sicherheit von industriellen Steuerungssystemen. Weiterhin sind sie in der Lage, organisatorisch und technisch den Bedrohungen und deren Auswirkungen, entgegenzuwirken.

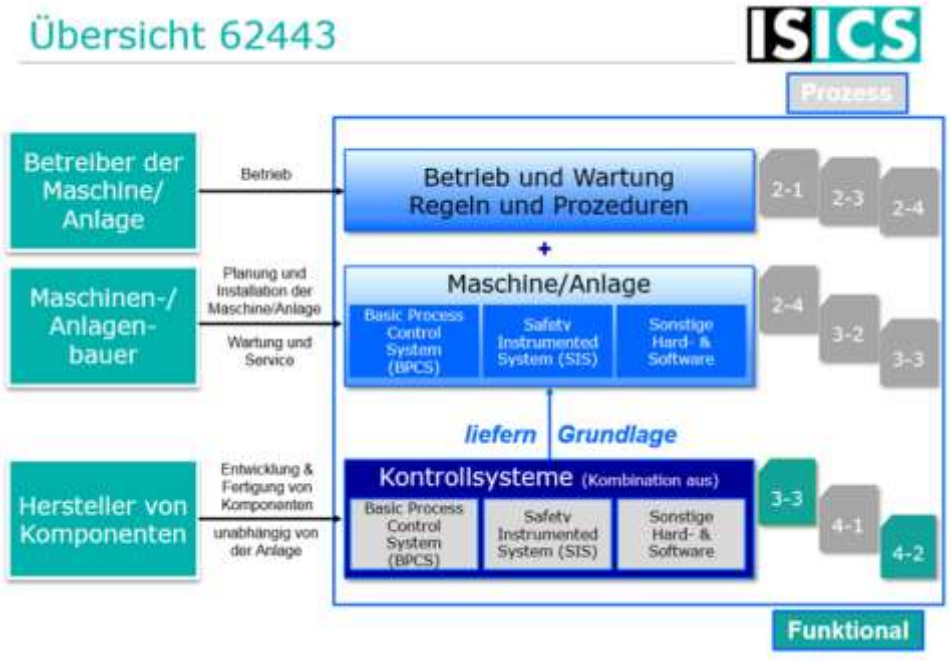
Einführung in den Standard IEC 62443

Der Standard IEC62443 beschreibt einen ganzheitlichen Ansatz zur Herstellung und Konsolidierung von IT-Sicherheit im industriellen Umfeld. Dabei berücksichtigt sie alle Beteiligten wie Betreiber, Hersteller und Integrator. In unserem Seminar erhalten Sie eine Übersicht über die wichtigen Dinge in diesem Zusammenhang.

In diesem 2-tägigen Seminar erhalten Sie eine ausführliche Einführung im den Standard IEC62443.

IT- und Informationssicherheit im industriellen Umfeld

Im Bereich Informationssicherheit in der Office-IT hat sich die ISO 27000 durchgesetzt. Für den Bereich ICS ist dieser Standard allerdings nur begrenzt einsetzbar, es fehlt die Berücksichtigung der speziellen Anforderungen in einer Produktionsanlage. Aufbauend auf der ISO 27002 beschreibt der Standard IEC 62443 wie Sie auch hier erfolgreich Sicherheit managen können.

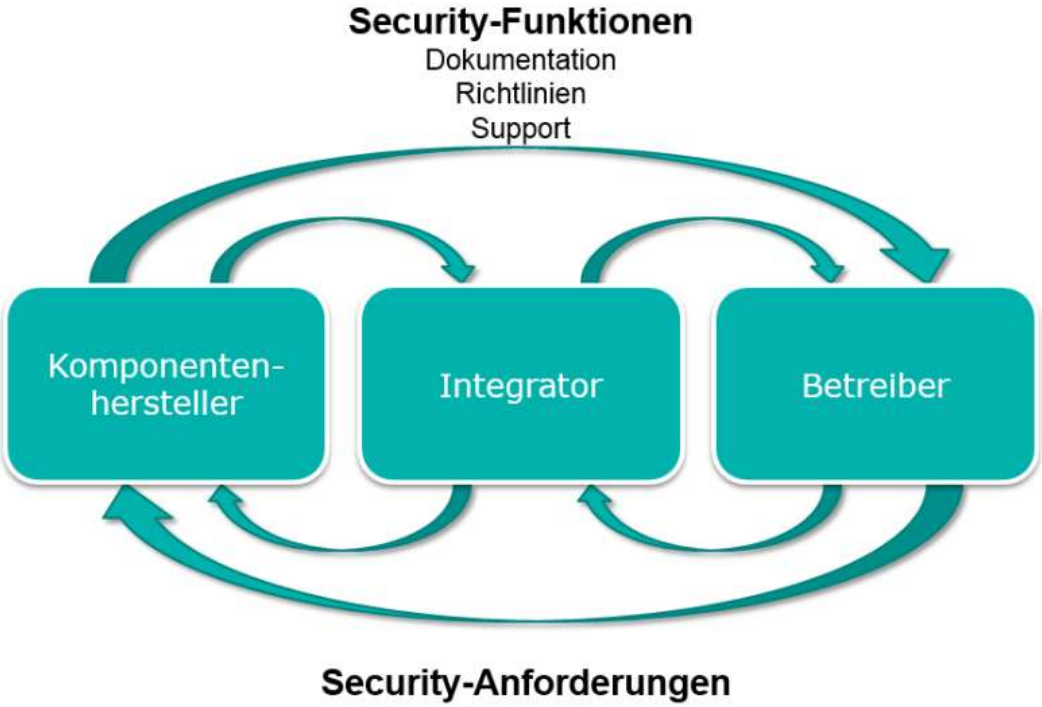


IT-Sicherheit für Industriesteuerungen, Gefährdungen und Gegenmaßnahmen

Der Standard IEC62443 beschreibt einen ganzheitlichen Ansatz zur Herstellung und Konsolidierung von IT-Sicherheit im industriellen Umfeld. Dabei berücksichtigt sie alle Beteiligten wie Betreiber, Hersteller und Integrator. Diese 3 sind auch in vielen Dingen voneinander abhängig.

Institut für ISICS
IT-Sicherheit in Industrial Control Systems

Security-Lebenszyklus



In unserem Seminar erhalten Sie eine Übersicht über die wichtigen Dinge in diesem Zusammenhang.

Inhalte des Seminars:

In diesem Seminar lernen Sie:

- Einführung in die Informationssicherheit
- Überblick IEC 62443
- IEC 62443-1 Konzepte und Methoden
- IEC 62443-2 ISMS und Patchmanagement
- IEC 62443-3 Technische Grundlagen
- IEC 62443-4 Herstelleranforderungen

Für wen ist das Seminar geeignet?

Angesprochen sind alle Personen, die mit der Planung und Umsetzung von IT- und Informationssicherheit im industriellen Umfeld befasst sind, wie:

- IT-Management/Management
- IT-Administratoren
- SCADA-Ingenieure
- Softwareentwickler für SCADA und Industrial Control Systeme
- IT-Netzarchitekten
- IT-Sicherheitsbeauftragte in Unternehmen mit Industrieanlagen

Übersicht über die Probleme bei der Vernetzung von ICS

Sie suchen Antworten auf diese Fragen?

- Wie stelle ich IT- und Informationssicherheit im industriellen Umfeld her?
- Welche Konzepte können dabei verwendet werden?
- Welche Prozesse zur Erhaltung der Sicherheit sind wichtig?
- Wie können Sie sich vor Angriffen schützen?
- Was sind die größten Probleme bei der IT-Sicherheit von ICS?

Dann sollten Sie sich gleich hier zu unserem Seminar „*Einführung in den Standard IEC 62443* " anmelden!

Cybersicherheit für CE-Koordinatoren

Grundkurs

Diese Schulung ist für CE-Koordinatoren ausgerichtet. CE-Koordinatoren kommen i.d.R. aus dem Maschinenbau. Mit den neuen Gesetzen der EU (Maschinenverordnung und Cyber Resilience Act) sind weitere Kompetenzen im Bereich Cybersicherheit notwendig. Die notwendigen Kompetenzen in diesem Bereich für einen CE-Koordinator, werden in dieser Schulung aufgebaut. Dazu sind nur grundlegende IT-Kenntnisse notwendig! Alles Weitere ist Inhalt der Schulung.

Inhalt:

1. Die Rolle des CE-Koordinators in Bezug auf Cyber-Sicherheit
2. Ermittlung der relevanten gesetzlichen Anforderungen
   a. Cybersicherheit in der neuen Maschinenverordnung
   b. Cyber Resilience Act
   c. Zusammenspiel der Gesetze
3. Koordination der Cyber-Risikobeurteilung
   a. Von der ISO 12100 zur Cybersicherheit von Maschinen
   b. Bedrohungsanalyse im Cyber-Umfeld
4. Nachweis der Umsetzung
   a. Maßnahmenplan
5. Dokumentation
   a. Einbindung in den CE-Prozess
6. Cybersicherheitsgrundlagen
   a. Vorgehensweise von Angreifern (nicht technisch!)
   b. Schutzziele
   c. **Common Vulnerability Scoring System (CVSS)**
7. Prüfung harmonisierter Normen
   a. Vorstellung IEC 62443
   b. Vorstellung prEN 50742 (für MVO)
   c. Vorstellung prEN 40000-1-x (für CRA)
8. Schwachstellenmanagement
9. Zusammenarbeit mit anderen Fachbereichen
   a. Von Softwareentwicklung bis Qualitätssicherung
10. Unterstützung bei der Konformitätserklärung
    a. Die Rolle des CE-Koordinators

Zur Schulung werden über 20 Beispieldokumente ausgeliefert.

- Ca. 8 Dokumente zum Thema Cybersecurity-Screening
- Ca. 10 Dokumente zum Thema Cyber-Risikobeurteilung
- Cybersecurity-Freigabe zur Konformitätserklärung
- Ermittlung projektbezogener Anforderungen aus Normen
- Protokollvorlage – Cybersecurity-Review
- Verantwortungsmatrix Cybersecurity CE-Prozess
- Vollständigkeitsprüfung der technischen Dokumentation
- Zuordnung von Nachweisen zu normativen Cybersecurity-Anforderungen

Anhand der Dokumente werden die einzelnen Schritte von den Teilnehmern während der Schulung durchgeführt.
Die Dokumente werden im Word-Format DOCX ausgeliefert.
Sie beinhalten beispielhafte Informationen. **Diese Daten müssen beim Einsatz natürlich an das konkrete Projekt angepasst werden!**

Es werden weitere praktische Übungen in der Schulung durchgeführt.
- Ermittlung eines CVSS-Wertes
- Durchführung einer Cyber-Bedrohungsanalyse im industriellen Umfeld

Demos

Es werden Demos von Cyberangriffen durchgeführt.
(Zeitabhängig!)
- Angriffe gegen OT-Protokolle
- Angriff auf eine Produktionsanlage
- Angriff über eine HMI-Schwachstelle

Durchführung

- Online
- vor Ort (ab 8 Teilnehmenden)

Dauer der Schulung: 2 Tage

Weitere Informationen zur Schulung finden Sie auf der Webseite unseres Ausbildungsinstituts **ISICS**. (www.scada-secure.de)

Schulungsinhalt „Cybersicherheit für CE-Koordinatoren

Erweiterungskurs

Diese Schulung ist für CE-Koordinatoren ausgerichtet, die den Grundkurs „Cybersicherheit für CE-Koordinatoren“ erfolgreich absolviert haben.
CE-Koordinatoren kommen i.d.R. aus dem Maschinenbau. Mit den neuen Gesetzen der EU (Maschinenverordnung und Cyber Resilience Act) sind weitere Kompetenzen im Bereich Cybersicherheit notwendig.
Der Grundkurs war eine Einführung, wie ein CE-Koordinator die Cybersicherheit managen kann. Typischerweise führt der CE-Koordinator viele Aufgaben nicht selber durch, das machen entsprechende Spezialisten.

Es gibt aber weitere Kompetenzen, die für einen CE-Koordinator wichtig sind, um die Ergebnisse der Spezialisten einordnen und beurteilen zu können.
Diese Kompetenzen werden in dieser Schulung aufgebaut. Dazu sind nur grundlegende IT-Kenntnisse notwendig! Alles Weitere ist Inhalt der Schulung.

Inhalt:

1. Abgrenzung CRA vs. MVO
   a. Wann gilt der CRA, wann Anhang III Ziff. 1.1.9 MVO, wann beides? Verweisstruktur zwischen den Rechtsakten, "eingebettete" vs. "eigenständige" Digitalkomponenten einer Maschine, Praxisbeispiele (SPS, HMI, Cloud-Anbindung)
2. Wesentliche Anforderungen CRA
   a. Anhang I Teil I (sichere Konfiguration, Datenschutz, Verfügbarkeit, Angriffsflächenminimierung) und Teil II (Schwachstellenmanagement-Prozesse)
3. Cybersicherheit in der Maschinenverordnung
   a. Anhang III Ziff. 1.1.9 "Schutz vor Korrumpierung" im Detail: Schutz sicherheitsrelevanter Steuerungen, Integrität von Sicherheitsfunktionen, Bezug zu IEC 62443 und harmonisierten Normen (z. B. EN ISO 12100, prEN-Normen zur Maschinen-Cybersicherheit)
4. Integrierte Risikobeurteilung
   a. Zusammenführung klassischer Maschinen-Risikobeurteilung (ISO 12100) mit Cybersicherheits-Risikobewertung; Bedrohungsmodellierung für sicherheitsrelevante Steuerungen; Wechselwirkung Safety ↔ Security
5. Technische Dokumentation & SBOM
   a. Anforderungen an technische Dokumentation nach CRA und MVO, Aufbau einer SBOM, Nachweisführung "Schutz vor Korrumpierung" in Betriebsanleitung/Risikobeurteilungsakte
6. Konformitätsbewertung & Meldepflichen
   a. Konformitätsbewertungsverfahren (inkl. Fälle mit notifizierter Stelle bei sicherheitsrelevanter Software, Anhang I Teil A MVO); CRA-Meldepflichten (24h/72h/14-Tage-Fristen), ENISA-Meldeplattform

7. Praxis-Simulation
   a. End-to-End-Fallstudie: vernetzte Maschine mit sicherheitsrelevanter Steuerung – von Risikobeurteilung über Anforderungscheck (CRA + MVO) bis zur CE-Kennzeichnung
8. Stolperfallen & Best Practices
   a. Häufige Fehler, typische Abgrenzungsfehler CRA/MVO, Audit-Erfahrungen, Q&A

Praktische Übungen

Zu jedem Modul gibt es eine praktische Übung die in Kleingruppen (2-4) Teilnehmenden durchgeführt wird.

Erfolgskontrolle

- Abschließendes Quiz (ca. 40 Fragen, Multiple Choice + 2 offene Fragen, mit Fragen zu beiden Rechtsakten) zur Wissensüberprüfung
- Bewertung der Gruppenpräsentation aus Übung 7 (qualitatives Feedback, keine Benotung)
- Teilnahmezertifikat bei Anwesenheit an beiden Tagen und aktiver Teilnahme an den Übungen

Durchführung

- Online
- vor Ort (ab 8 Teilnehmenden)

Dauer der Schulung: 2 Tage

Weitere Informationen zur Schulung finden Sie auf der Webseite unseres Ausbildungsinstituts **ISICS**. (www.scada-secure.de)

IT-/OT-Security Schulung für Führungskräfte

Einführung in die Cybersicherheit für Manager

Neue Gesetze und Richtlinien in der EU sollen ein hohes Sicherheitsniveau für Netz- und Informationssysteme (NIS-2) und Produkte mit digitalen Elementen (CRA) schaffen. Auch die Maschinenverordnung verlangt nun Cybersicherheit.

Dies umzusetzen ist nicht einfach. Wichtig ist dabei auch die Unterstützung der Führungskräfte. NIS-2 fordert sogar explizit eine Schulung.

Da IT-Security nicht gleich OT-Security ist, ist es auch sinnvoll, bei einer entsprechenden Schulung auf spezielle Szenarien einzugehen.

Das BSI hat Anforderungen für die Inhalte von NIS-2 Schulungen erstellt. Unsere Schulung richtet sich danach,

Auch der CRA stellt Anforderungen an das Management.

In unserer Schulung werden beide Gesetze berücksichtigt.

Schulungsdauer

Die Schulung wird online durchgeführt und hat 6 Module je 45 Minuten. Sie kann auf 2 verschiedene Arten durchgeführt werden.

1. 3 Termine je 2 Module

2. 2 Termine je 3 Module

Während der Schulung werden online Fragen gestellt, die von den Teilnehmenden beantwortet werden müssen. So wird sichergestellt, dass die Teilnehmenden die Schulung (auch wenn sie online ist) die gesamte Zeit verfolgen.

Schulungsinhalt

Der Kern der Schulung:
Haftung vermeiden, Überblick behalten, richtig steuern.
Ohne Technik-Overkill.

Folgende Themen sind Inhalt der Schulung:

· Was ist das NIS2-2-Umsetzungs- und

Cybersicherheitsstärkungsgesetz ((NIS2UmsuCG)

· Wer ist in Deutschland betroffen

· Zentrale Pflichten nach deutschem Recht

· Verantwortung & Organisation

· Umsetzung & Betrieb

· Sicherheitsstrategie

· Risikobeurteilung

· Melde- & Krisenfähigkeit

· Persönliche Haftungsrisiken vermeiden

· Checkliste für Geschäftsführer

Die Teilnehmenden erhalten nach der erfolgreichen Teilnahme an der Schulung ein Zertifikat.

Infos zu unseren Veranstaltungen (CSSE, CSSIS, CSTIS, Einführung IEC 62443):

Teilnehmer kamen z.B. aus folgenden Bereichen:

- Einer der fünf führenden Strom- und Gasanbieter in Europa
- Bundeskriminalamt (BKA)
- Einer der weltgrößten Hersteller von Windturbinen
- Einer der führenden Anbieter in den Bereichen Produktions- und Fertigungsautomation
- Mittelständisches Ingenieurbüro für Automation
- Stadtverwaltung
- Deutsche Bank
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Technische Universität
- Landeskriminalamt (LKA NRW)
- Fachhochschule
- Stadtwerk
- Bundesweite Ermittlungsbehörde
- Betreiber Kernkraftwerk
- Mineralwasserproduzent
- Gastransporteur
- Ernst&Young
- Centralschweizerische Kraftwerke AG
- R+V Versicherung
- Innogy
- Swissgrid

Die Teilnehmer kamen ausfolgenden Bereichen:

IT (Technisch): 29%
IT (Management): 20%
SCADA (Technisch): 29%
SCADA (Management): 22%

Auf einer Skala *sehr zufrieden/zufrieden/eher unzufrieden/sehr unzufrieden* gab es folgende Bewertungen:

97% der Teilnehmer waren mit den Dozenten sehr zufrieden, **3%** waren zufrieden.

87% der Teilnehmer waren mit der Veranstaltung sehr zufrieden, **13%** zufrieden!

Es gab bisher nur einen unzufriedenen Teilnehmer!

Kommentare begeisterter Teilnehmer:

"Sehr gelungene Veranstaltung!"
"Alles drin was man braucht."
"Besonders die praktischen Angriffe sind sehr eindrucksvoll."
"Schnelle Einführung in den Bereich der Security industrieller Steuerungssysteme."
"Die Begeisterung der Dozenten für das Thema steckt an!"
"Hat sehr gut die Problematik, die Risiken und den Aufwand zur Vermeidung/Behebung von Sicherheitslücken bei ICS verdeutlicht."
"Die Praxistests zu den jeweiligen Themen und die durchgeführten Angriffe auf SCADA Systeme waren besonders interessant."
"ICS-IT-Sicherheit sehr gut, anschaulich und hochaktuell behandelt."
"Vielen Dank für diese sehr informativen und spannenden Tage!"
"Sehr umfangreiches Seminar über die aktuelle Situation und zukunftsweisende Konzepte zur Absicherung von ICS."
"Übersichtliche und umfangreiche Info-Veranstaltung zum Thema Sicherheit in ICS-Anlagen."
"Erschreckend, wie wenig IT-Sicherheit in ICS-Systemen vorhanden ist."
"Die Veranstaltung war sehr informativ und gibt einen guten Einblick und Start in das Thema."

"Eine sehr informative, lehrreiche und unterhaltsame Veranstaltung."
"Ich bin sehr zufrieden mit dem Seminar und werde dies in meiner Firma so kund tun, damit Kollegen aus der Automatisierung auch geschult werden."
"Sehr angenehme Atmosphäre"
"Eine sehr interessante Woche, welche das Interesse an SCADA-Sicherheit gesteigert hat."
"Hervorragend auf meine firmeninternen Bedürfnisse abgestimmt."
"Top!"
"Guter Einblick in die Welt der SCADA Security. Schafft Awareness für Sicherheitsproblematik, sowie Maßnahmen um das Risiko zu minimieren."
"Must have."
"Hätten wir das Geld dazu, würde ich jeden unserer SCADA-Admins nach Aachen schicken."
"Ein MUSS für jeden SCADA-Betreiber."
"Sehr interessant und kurzweilig."
"Praxiserfahrung vom Referenten ist sehr nützlich und interessant."
"Viele praktische Übungen und Praxistipps."
"Es war ein klares und umfassendes Training, sowohl aus technischer, als auch aus organisatorischer Sicht."
"Sehr gute und qualitativ hochwertige Schulung."