

Cyber Security in der Industrie 4.0

„Durch die Vernetzung von Produktionsanlagen werden Cyber-Angriffe zu einem ernststen Sicherheitsrisiko. Diese Cyber-Angriffe können erhebliche Konsequenzen haben – von Verzögerungen im Produktionsablauf über komplette Ausfälle bis zum Extremfall, der physischen Zerstörung der Anlage. In unseren Trainings zu Cyber Security in der Industrie 4.0 erhalten Sie das nötige Know-how, um Ihr Unternehmen vor diesen Risiken zu schützen.“

Christina Eibert



Christina Eibert, DGQ-Produktmanagerin



- > Grundlagen Know-how Cyber Security
Seite 288
- > Cyber Security in der Industrie 4.0
Seite 289
- > Zertifizierung/Prüfung: DGQ-Spezialist Cyber Security in der vernetzten Produktion
Seite 290
- > Management Know-how Cyber Security
Seite 291

Ihr Weg zum Erfolg

CYBER SECURITY IN DER INDUSTRIE 4.0 (INDUSTRIAL CONTROL SYSTEMS)

LEHRGANGSREIHE

ZIELGRUPPE

Fachkräfte und Mitarbeiter mit technischem Ausbildungshintergrund in der industriellen Produktion, Mitarbeiter der Qualitätssicherung oder IT-Mitarbeiter mit Interesse an Cyber-Sicherheit in der vernetzten Produktion.

Optional
1 Tag Training

Grundlagen Know-how Cyber Security

S. 288

4 Tage Training

Cyber Security in der Industrie 4.0

S. 289

Prüfung am letzten Tag

DGQ-Spezialist Cyber Security in der vernetzten Produktion

Bitte separat buchen

S. 290

Trainings und Workshops zur Ergänzung/Vertiefung

EMPFEHLUNGEN

Datenschutzbeauftragter
S. 274

Datenschutz-Update
S. 276

Qualitätssicherung
S. 16 ff.

Lean Six Sigma
S. 150 ff.

Professionelle Integration von Datenschutz nach EU-DSGVO in ISO-Managementsysteme
S. 277

Interne Audits nach Datenschutzgrundverordnung (EU-DSGVO)
S. 278

Management Know-how Cyber Security
S. 291



Die Art und Weise, wie in Zukunft gearbeitet wird, hat sich durch die Digitalisierung grundlegend verändert. Das gilt auch für die industrielle Produktion. Intelligente und vernetzte Produktionsanlagen und Systeme bilden die Grundlagen für die Industrie 4.0. Diese Vernetzung bietet Unternehmen vielfältige Möglichkeiten. Gleichzeitig entstehen durch die eigenständige Kommunikation der Anlagen neue Sicherheitsrisiken.

Sogenannte „Smart Factories“ benötigen deshalb nicht nur eine sichere technische Infrastruktur, sondern auch Mitarbeiter, die den neuen Anforderungen gewachsen sind. Damit Cyber-Angriffe eine Produktion nicht zum Erliegen bringen, ist vor allem Know-how auf dem Gebiet der Cyber-Sicherheit gefragt. Das gilt sowohl für Fachkräfte, die in der vernetzten Produktion tätig sind, als auch für Führungskräfte, die ihr Unternehmen in der Industrie 4.0 sicher aufstellen wollen. Hierfür hat die Deutsche Gesellschaft für Qualität zusammen mit dem Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) ein spezielles Weiterbildungsangebot entwickelt. Dieses greift die „Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf.

Der Lehrgang „Cyber Security in der Industrie 4.0“ und das optionale Grundlagenseminar richten sich an Fachkräfte und Mitarbeiter in vernetzten Produktionen, die IT-Sicherheitslösungen umsetzen und die Produktion sichern wollen.

Sie sind Führungskraft und möchten Ihr Unternehmen vor Cyber-Kriminalität schützen? Im Seminar Management Know-how Cyber Security identifizieren Sie schnell umsetzbare Lösungsideen für Ihre Informationssicherheitsstrategie in der Industrie 4.0.



Grundlagen Know-how Cyber Security

CYBER SECURITY IN DER INDUSTRIE 4.0 (INDUSTRIAL CONTROL SYSTEMS)

S

Ihr Nutzen

- Sie verfügen über Grundlagenwissen zum Thema Cyber Security in der Produktion.
- Sie haben einen kompakten Überblick über relevante Cyber-Sicherheitsaspekte und Gefahrenlagen in der Industrie 4.0.
- Sie und Ihr Unternehmen profitieren von Best-Practice-Beispielen und konkrete Handlungsempfehlungen für die Praxis.

Sie wollen sich einen kompakten Überblick über das Thema Cyber Security in der Industrie 4.0 verschaffen? In unserem eintägigen Grundlagenseminar bringen Ihnen erfahrene Fraunhofer-Experten die Grundbegriffe und Gefahrenlagen der Cyber Security in Digitalisierung und Industrie 4.0 praxisnah näher. Sie steigen in aktuelle IT-Sicherheitsstandards ein und lernen relevante technische und organisatorische Schutzmaßnahmen kennen. Dabei profitieren Sie von aktuellen wissenschaftlichen Erkenntnissen und Beispielen aus der Praxis.

TEILNEHMER

Das Seminar richtet sich an alle, die sich mit den Grundbegriffen der Informations- und IT-Sicherheit vertraut machen möchten.

INHALTE

- Einführung Digitalisierung in der Produktion/Industrie 4.0
- Grundbegriffe der Informations- und IT-Sicherheit
- Überblick über geeignete Schutzmaßnahmen und relevante IT-Sicherheitsstandards zur Cyber Security
- Best-Practice-Beispiele und Handlungsempfehlung

BESONDERE HINWEISE

Sie möchten den Lehrgang „Cyber Security in der Industrie 4.0“ besuchen und benötigen noch Basiswissen zum Thema IT- und Informationssicherheit? Mit diesem Seminar erhalten Sie eine Grundlagenschulung, die Sie optimal auf den Lehrgang vorbereitet.

KOOPERATIONSPARTNER



AUF EINEN BLICK

Dauer: 1 Tag
 Gebühr: Euro 630,-
Ihr Plus: *Unterlagen, Mittagessen und Pausengetränke.*

PRODUKT-LINK

www.dgq.de/go/GKCS

Cyber Security in der Industrie 4.0

CYBER SECURITY IN DER INDUSTRIE 4.0 (INDUSTRIAL CONTROL SYSTEMS)



L

Ihr Nutzen

- Sie verfügen über praxisnahes Know-how zu Cyber Security in der vernetzten Produktion.
- Sie kennen Strategien, um mögliche Risiken und Angriffen zu erkennen und abzuwehren.
- Sie wissen über IT-Sicherheitsstandards Bescheid und wenden sie erfolgreich an.
- Sie vertiefen ihr Wissen praxisnah im Lernlabor Cyber Security des Fraunhofer Instituts und trainieren anhand der in der Produktion eingesetzten Hardware, Angriffe zu erkennen und abzuwehren.

Jede moderne und vernetzte Produktion muss Risiken von Cyber-Angriffen managen. Die besondere Komplexität von Industrial Control Systems (ICS) erfordert dafür spezielle Lösungen, denn der Einsatz klassischer IT-Sicherheitsmechanismen ist aufgrund der Echtzeitanforderungen schwierig bis unmöglich. Gefragt sind umfassende, unternehmensweite Sicherheitskonzepte, in denen die Mitarbeiter der Produktion eine zentrale Rolle spielen und mit den Verantwortlichen im Bereich Informationssicherheit eng zusammenarbeiten.

In diesem Lehrgang erwerben Sie das Know-how, um als „DGQ-Spezialist für Cyber Security in der vernetzten Produktion“ Gefahren zu erkennen, IT-Sicherheitslösungen umzusetzen und die Produktion zu sichern.

In praktischen Übungen an Demonstratoren des Lernlabors Cyber-Security lernen Sie realistische Angriffsszenarien auf Industrial Control Systems (ICS) zu identifizieren und mit geeigneten Gegenmaßnahmen zu reagieren. Dabei werden Sie von erfahrenen Fraunhofer-Experten begleitet. Durch den hohen Anteil praktischer Übungen können Sie das Erlernte schnell und effektiv in die Praxis umsetzen.

Darüber hinaus vermitteln wir Ihnen die Grundlagen der Netzwerktechnik im Automatisierungsbereich und die typischen Angriffsflanken. Sie profitieren von aktuellen wissenschaftlichen Erkenntnissen in den Bereichen Cyber Security und Automatisierung. Die im Training praktizierte Verzahnung von Forschung und Anwendungsorientierung ist einmalig und stellt einen direkten Nutzen für Ihr Berufsprofil und die Sicherheit Ihres Unternehmens dar.

TEILNEHMER

Der Lehrgang „Cyber Security in der Industrie 4.0“ und das optionale Grundlagenseminar richten sich an Fachkräfte und Mitarbeiter in vernetzten Produktionen, wie z. B. Produktions-CISO, Ingenieure, Infrastruktur-Betriebspersonal, Wartungstechniker, Instandhalter.

INHALTE

- Grundlagen der Cyber Security in der Industrie 4.0
- Basiswissen zur Industrie 4.0 IT-Sicherheit und IT-Kommunikation
- Bewusstsein für Bedrohungslagen und mögliche Lösungsstrategien
- Rechtlicher Rahmen
- Praktische Übungen von Angriffen auf Industrial Control Systems (ICS) und deren Auswirkungen

KOOPERATIONSPARTNER



AUF EINEN BLICK

Dauer: 4 Tage
 Gebühr: Euro 2.400,-
Ihr Plus: *Unterlagen, Mittagessen und Pausengetränke.*

PRODUKT-LINK

www.dgq.de/go/VEPR

Zertifizierung/Prüfung: DGQ-Spezialist Cyber Security in der vernetzten Produktion



CYBER SECURITY IN DER INDUSTRIE 4.0 (INDUSTRIAL CONTROL SYSTEMS)



Ihr Nutzen

- Sie weisen mit Ihrem DGQ-Zertifikat nach, dass Sie über praxisnahes Know-how zu Cyber Security in der vernetzten Produktion verfügen.
- Sie kennen Strategien, um mögliche Risiken und Angriffe zu erkennen und abzuwehren.
- Sie sind mit IT-Sicherheitsstandards vertraut und kennen Vorgehensweisen, um diese erfolgreich anzuwenden.

Mit Ihrem persönlichen Zertifikat **DGQ-Spezialist Cyber Security in der vernetzten Produktion** weisen Sie Kenntnisse zu realistischen Angriffsszenarien auf Produktionssysteme sowie zu deren Identifikation nach. Sie belegen, dass Sie Grundlagenwissen der Netzwerktechnik im Automatisierungsbereich besitzen, um insbesondere die typischen Angriffsflanken zu kennen. Darüber hinaus belegen Sie Ihr Wissen zu geeigneten Gegenmaßnahmen.

IHR WEG ZUM ZERTIFIKAT

Folgende Voraussetzungen müssen Sie erfüllen:

- Technischer (Fach-)Hochschulabschluss oder abgeschlossene technische Berufsausbildung
- 1 Jahr Berufserfahrung in einer Vollzeittätigkeit mit Aufgaben in der Automatisierungs- oder Informationstechnik
- Teilnahme an der DGQ-Veranstaltung „Cyber Security in der Industrie 4.0“

Nach bestandener Prüfung erhalten Sie das Zertifikat **DGQ-Spezialist Cyber Security in der vernetzten Produktion**.

PRÜFUNG

Die Prüfung erfolgt schriftlich.
Bitte buchen Sie die Prüfung separat.

HINWEIS

Das Zertifikat ist unbefristet gültig.

KOOPERATIONSPARTNER



AUF EINEN BLICK

Dauer: ½ Tag, am letzten Lehrgangstag
Gebühr: Euro 220,-
Die Gebühr bezieht sich auf das gesamte Zertifizierungsverfahren – von der Antragsbearbeitung über die Prüfung bis zur Ausstellung des Zertifikats.

PRODUKT-LINK

www.dgq.de/go/PSCS



Management Know-how Cyber Security

CYBER SECURITY IN DER INDUSTRIE 4.0 (INDUSTRIAL CONTROL SYSTEMS)

S

Ihr Nutzen

- Sie erkennen und verstehen IT-Sicherheitsrisiken und können Abwehrstrategien entwickeln.
- Sie überblicken den rechtlichen Rahmen, in dem Sie handeln und verantwortlich sind.
- Sie wissen über IT-Sicherheitsstandards Bescheid und können sich an der Fachdiskussion beteiligen.
- Anhand praktischer Demonstrationen identifizieren Sie schnell umsetzbare Lösungsideen für Ihre Informationssicherheitsstrategie in der Industrie 4.0.

Kein Tag vergeht, ohne dass Medien über Hackerangriffe und Lücken in der IT-Sicherheit berichten. Um im Wettlauf mit Cyberkriminellen die Oberhand zu behalten, müssen Sie Ihr Unternehmen strategisch schützen. Wie Ihnen das gelingt, erfahren Sie in diesem Seminar.

In nur zwei Tagen verschaffen Sie sich einen umfassenden Überblick über die wichtigsten Sicherheitsfragen in der digitalen Transformation und Industrie 4.0. Sie erkennen und verstehen die sicherheitstechnischen Herausforderungen und Risiken der stetig zunehmenden Vernetzung.

Praxisnahe Beispiele stehen im Mittelpunkt: Zusammen mit erfahrenen Fraunhofer-Experten durchleben Sie Angriffsszenarien auf Industrial Control Systems (ICS) und deren Auswirkungen auf das Unternehmen hautnah. Sie lernen mögliche Lösungsstrategien für Ihre Praxis zu entwickeln und profitieren von wissenschaftlichen Erkenntnissen in den Bereichen Cyber Security und Automatisierung. Die im Training praktizierte Verzahnung von Forschung und Anwendungsorientierung ist einmalig.

TEILNEHMER

Fach- und Führungskräfte sowie Produktionsverantwortliche, die sich mit dem Thema Cyber Security vertraut machen wollen

INHALTE

- Grundlagen der Cyber Security im Unternehmen im Industrie-4.0-Umfeld
- Bewusstsein für Bedrohungslagen und mögliche Lösungsstrategien
- Rechtlicher Rahmen
- Praktische Demonstration von Angriffen auf Produktionssysteme und deren Auswirkungen
- Mögliche Maßnahmen der Mitarbeitersensibilisierung

AUF EINEN BLICK

Dauer: 2 Tage

Gebühr: Euro 1.200,-

Ihr Plus: *Unterlagen, Mittagessen und Pausengetränke.*

PRODUKT-LINK

www.dgq.de/go/MKCS