Cyber Security in der Industrie 4.0

„Durch die Vernetzung von Produktionsanlagen werden Cyber-Angriffe zu einem ernsten Sicherheitsrisiko. Es drohen Verzögerungen im Produktionsablauf bis zu kompletten Ausfällen. Im digitalisierten Arbeitsumfeld benötigen wir neue Kompetenzen, um diese Risiken zu vermeiden.“

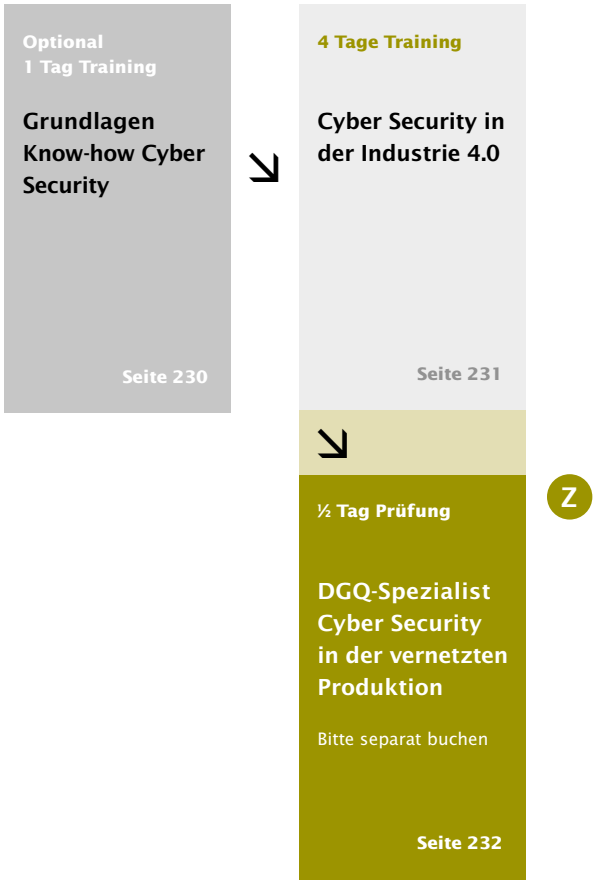
Christina Eibert, DGQ-Produktmanagerin

Lehrgang/Zertifizierung/Prüfung:

Ihr Weg zum Zertifikat

ZIELGRUPPE

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



Empfehlungen

Trainings und Workshops zur Ergänzung/Vertiefung

Qualitätssicherung
Seite 58 ff.

Lean Six Sigma
Seite 106 ff.

Management Know-how Cyber Security
Seite 233

Datenschutzbeauftragter Z
Seite 258

Datenschutz-Update
Seite 260

Professionelle Integration von Datenschutz nach EU-DSGVO in ISO-Managementsysteme
Seite 261

Interne Audits nach Datenschutzgrundverordnung (EU-DSGVO)
Seite 262

Aufbau und Ziele der Weiterbildung

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 auchBeschäftigte, 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 undBeschäftigte 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.

Fraunhofer IOSB

Grundlagen Know-how Cyber Security

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

L

Dauer: 1 Tag
Gebühr: Euro 660,–

Ihr Plus:
Unterlagen, Mittagessen und Pausengetränke

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.

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 konkreten Handlungsempfehlungen für die Praxis.

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.

TEILNEHMENDE UND VORAUSSETZUNGEN

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

www.dgq.de/go/GKCS

25.04.	Karlsruhe	**10.10.**	Karlsruhe

Fraunhofer IOSB

Cyber Security in der Industrie 4.0

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

L

Dauer: 4 Tage
Gebühr: Euro 2.500,–

Ihr Plus:
Unterlagen, Mittagessen und Pausengetränke

Jede vernetzte Produktion muss Risiken von Cyber-Angriffen managen. Die besondere Komplexität von Industrial Control Systems (ICS) erfordert dafür spezielle Lösungen. Der Einsatz klassischer IT-Sicherheitsmechanismen ist aufgrund der Echtzeit-Anforderungen schwierig. Gefragt sind umfassende, unternehmensweite Sicherheitskonzepte, in denen die Mitarbeiter der Produktion eine zentrale Rolle spielen und mit den Verantwortlichen im Bereich Informationssicherheit eng zusammenarbeiten. Sie erwerben das Know-how, um Gefahren zu erkennen, IT-Sicherheitslösungen umzusetzen und die Produktion zu sichern. An Demonstratoren des Lernlabors Cyber-Security lernen Sie, realistische Angriffsszenarien zu identifizieren und mit geeigneten Gegenmaßnahmen zu reagieren. Dabei werden Sie von Fraunhofer-Experten begleitet. Durch den hohen Anteil praktischer Übungen können Sie das Erlernte schnell und effektiv in die Praxis umsetzen. 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.

IHR NUTZEN

- Sie verfügen über praxisnahes Know-how zu Cyber Security in der vernetzten Produktion.
- Sie kennen Strategien, um mögliche Risiken und Angriffe 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.

TEILNEHMENDE UND VORAUSSETZUNGEN

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 und Instandhalter.

www.dgq.de/go/VEPR

26.04. – 29.04. Karlsruhe	**11.10. – 14.10.** Karlsruhe

Prüfung/Zertifikat

DGQ-Spezialist Cyber Security in der vernetzten Produktion

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.

Z

Dauer: **½ Tag, am letzten Lehrgangstag**
Gebühr: **Euro 230,–**

Die Gebühr bezieht sich auf das gesamte Zertifizierungsverfahren – von der Antragsbearbeitung über die Prüfung bis zur Ausstellung des Zertifikats.

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.

www.dgq.de/go/PSCS

29.04.	Karlsruhe	**14.10.**	Karlsruhe

Fraunhofer IOSB

Management Know-how Cyber Security

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

S

Dauer: 2 Tage
Gebühr: Euro 1.250,–

Ihr Plus:
Unterlagen, Mittagessen und Pausengetränke

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.

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.

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.

TEILNEHMENDE UND VORAUSSETZUNGEN

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

www.dgq.de/go/MKCS

04.04. – 05.04. Karlsruhe	**17.10. – 18.10.** Karlsruhe