Mitarbeiter effizient & erfolgreich für eine sichere Fabrik qualifizieren

13. Juli 2021

bayern innovativ

UNIVERSITY 4 INDUSTRY

University4Industry: Das Gründungsteam und seine Mission

Dr. Wolfgang Huhn

- Gründer und Geschäftsführer von University4Industry, München (seit 2015)
- Senior Partner bei McKinsey & Company, Frankfurt (1988-2015)
- Promoviert in Theoretischer Physik, Vordiplom in Elektrotechnik, RWTH Aachen

Jan Veira

- Gründer und Geschäftsführer von University4Industry, München (seit 2015)
- Junior Partner bei McKinsey & Company, München/Berlin (2007-2015)
- MBA von der University of California Berkeley, Diplom in Physik, TU Berlin

Unsere Mission

Aufbau von Fähigkeiten für die ambitioniertesten Innovationen mit …

… dem richtigen **„Was“** aus Sicht der **Industrie**

… dem richtigen **„Wie“** aus Sicht von **Mitarbeitern im Unternehmen**

University4Industry – auf einen Blick

UNIVERSITY 4 INDUSTRY

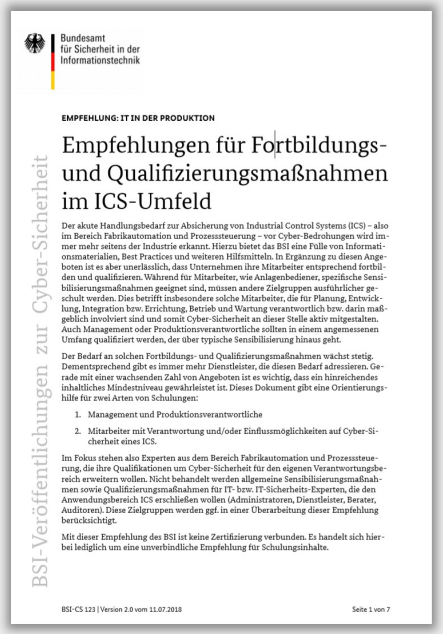
Angebot	**Aufbau von Fähigkeiten** für die ambitioniertesten Innovationen in (Groß-)**Unternehmen**	
Format	**Online-Lernangebot** (weitgehend “self-paced”) als aktiv betreutes **Programm** mit innovativer Nutzung digitaler Möglichkeiten zum Experimentieren und Erfahren	
Inhalte	**>950h** im Themenfeld „Digitalisierung“, produziert mit **>300** Experten aus **>90** Institutionen Fokusbereiche: Digitalisierung, Industrie 4.0, Connectivity, Machine Learning, SW-Engineering & Cloud, Blockchain, Additive Fertigung, Industrial Security, Digital Sales & Marketing, Digital Strategy	
Ausgewählte KPIs	**>100’000 Nutzer** mit Zugang (über SSO oder direkter Sign-In) **>80-90% Net Promoter Score** der Nutzer	**>80% Aktivierungsrate** **>80% Abschlussquote**
Team	>45 Mitarbeiter in München, Frankfurt und Krakau, gegründet 2015	
Starke Partner	Fraunhofer, LNI4.0 Labs Network Industrie 4.0, ZVEI Die Elektroindustrie, DETECON Consulting, edutech, VDMA, Microsoft, eit InnoEnergy Knowledge Innovation Community, FESTO, Technische Universität München	

Mitarbeiter effizient & erfolgreich für eine sichere Fabrik qualifizieren

“Never touch a running system”

Mitarbeiter effizient & erfolgreich für eine sichere Fabrik qualifizieren

Die richtigen Inhalte



Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IN DER PRODUKTION

Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld

Der akute Handlungsbedarf zur Absicherung von Industrial Control Systems (ICS) – also im Bereich Fabrikautomation und Prozesssteuerung – vor Cyber-Bedrohungen wird immer mehr seitens der Industrie erkannt. Hierzu bietet das BSI eine Fülle von Informationsmaterialien, Best Practices und weiteren Hilfsmitteln. In Ergänzung zu diesen Angeboten ist es aber unerlässlich, dass Unternehmen ihre Mitarbeiter entsprechend fortbilden und qualifizieren. Während für Mitarbeiter, wie Anlagenbediener, spezifische Sensibilisierungsmaßnahmen geeignet sind, müssen andere Zielgruppen ausführlicher geschult werden. Dies betrifft insbesondere solche Mitarbeiter, die für Planung, Entwicklung, Integration bzw. Errichtung, Betrieb und Wartung verantwortlich bzw. darin maßgeblich involviert sind und somit Cyber-Sicherheit an dieser Stelle aktiv mitgestalten. Auch Management oder Produktionsverantwortliche sollten in einem angemessenen Umfang qualifiziert werden, der über typische Sensibilisierung hinaus geht.

Der Bedarf an solchen Fortbildungs- und Qualifizierungsmaßnahmen wächst stetig. Dementsprechend gibt es immer mehr Dienstleister, die diesen Bedarf adressieren. Gerade mit einer wachsenden Zahl von Angeboten ist es wichtig, dass ein hinreichendes inhaltliches Mindestniveau gewährleistet ist. Dieses Dokument gibt eine Orientierungshilfe für zwei Arten von Schulungen:

1. Management und Produktionsverantwortliche
2. Mitarbeiter mit Verantwortung und/oder Einflussmöglichkeiten auf Cyber-Sicherheit eines ICS.

Im Fokus stehen also Experten aus dem Bereich Fabrikautomation und Prozesssteuerung, die ihre Qualifikationen um Cyber-Sicherheit für den eigenen Verantwortungsbereich erweitern wollen. Nicht behandelt werden allgemeine Sensibilisierungsmaßnahmen sowie Qualifizierungsmaßnahmen für IT- bzw. IT-Sicherheits-Experten, die den Anwendungsbereich ICS erschließen wollen (Administratoren, Dienstleister, Berater, Auditoren). Diese Zielgruppen werden ggf. in einer Überarbeitung dieser Empfehlung berücksichtigt.

Mit dieser Empfehlung des BSI ist keine Zertifizierung verbunden. Es handelt sich hierbei lediglich um eine unverbindliche Empfehlung für Schulungsinhalte.

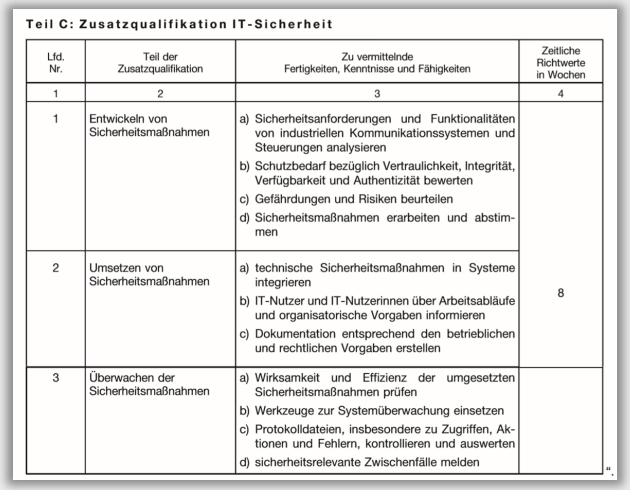
BSI-CS 123 | Version 2.0 vom 11.07.2018 Seite 1 von 7

BSI-Veröffentlichungen zur Cyber-Sicherheit

Leitfaden Industrie 4.0 Security

Handlungsempfehlungen für den Mittelstand

Auszug



Teil C: Zusatzqualifikation IT-Sicherheit

Lfd. Nr.	Teil der Zusatzqualifikation	Zu vermittelnde Fertigkeiten, Kenntnisse und Fähigkeiten	Zeitliche Richtwerte in Wochen
1	2	3	4
1	Entwickeln von Sicherheitsmaßnahmen	a) Sicherheitsanforderungen und Funktionalitäten von industriellen Kommunikationssystemen und Steuerungen analysieren b) Schutzbedarf bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität bewerten c) Gefährdungen und Risiken beurteilen d) Sicherheitsmaßnahmen erarbeiten und abstimmen	
2	Umsetzen von Sicherheitsmaßnahmen	a) technische Sicherheitsmaßnahmen in Systeme integrieren b) IT-Nutzer und IT-Nutzerinnen über Arbeitsabläufe und organisatorische Vorgaben informieren c) Dokumentation entsprechend den betrieblichen und rechtlichen Vorgaben erstellen	8
3	Überwachen der Sicherheitsmaßnahmen	a) Wirksamkeit und Effizienz der umgesetzten Sicherheitsmaßnahmen prüfen b) Werkzeuge zur Systemüberwachung einsetzen c) Protokolldateien, insbesondere zu Zugriffen, Aktionen und Fehlern, kontrollieren und auswerten d) sicherheitsrelevante Zwischenfälle melden	

- ✓ **Umfassendes Angebot an Lerninhalten**
- ✓ **>100h** Lerninhalte
- ✓ **Modular aufgebaut** für Kunden- & Zielgruppen-spezifische Konfiguration
- ✓ **>50 beitragende Experten**
- ✓ **>30 beitragende Unternehmen** & Institutionen

HISOLUTIONS
SICK Sensor Intelligence.
Fraunhofer AISEC
VDMA
Weidmüller
accessec powerful security solutions
@yet
Rexroth Bosch Group
SIEMENS

Mitarbeiter effizient & erfolgreich für eine sichere Fabrik qualifizieren

Mitarbeiter sind eine besondere Zielgruppe

Große Zahl von Arbeitnehmern
braucht zusätzliche Fähigkeiten

Die Zielgruppen sind beschäftigt:
Nur wenig Zeit für den Aufbau von Fähigkeiten verfügbar

Jede Zielgruppe und jede Person braucht ihren **persönlichen Zuschnitt:**
Themen, Tiefe, Format

- ✓ **Online**
- ✓ **Konfiguration je Unternehmen & Zielgruppe**
- ✓ **Effizientes Umsetzungsformat**

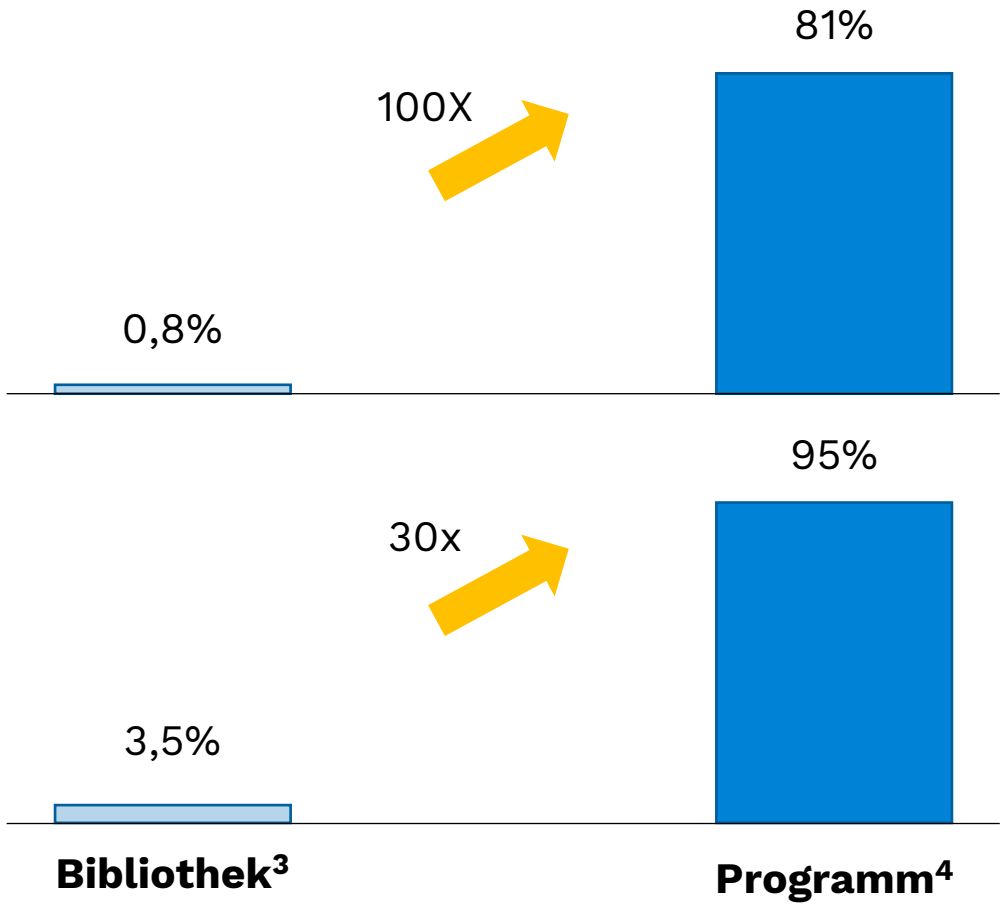
Konfiguration je Zielgruppe (Kundenbeispiel)

	Thema	Erläuterung	Thematische Relevanz für: Bediener	Instand-halter	Planer	OT- Security-verantwort-licher	Produktions-verantwort-licher
1	**Awareness** einschätzen	Bewusstsein entwickeln Relevanz für mich verstehen Potentielle Angriffsziele Potentielle Angreifer	■■■■□□	■■■■■□	■■■■■■	■■■■■■	■■■■□□
2	**Identify** identifizieren	Asset Management Risiken beschreiben Sicherheitsrelevante Führungsaufgaben Risikiobewertung Risikomanagementstrategie entwickeln	■■■□□□	■■■□□□	■■■■■■	■■■■■□	■■■□□□
3	**Protect** schützen	Access Control implementieren Schulung von Mitarbeitern Datensicherheit herstellen Informationsschutzprozesse	■■□□□□	■■■■■□	■■■■■■	■■■■■■	■■■□□□
4	**Detect** aufdecken	Erkennen von Anomalien kontinuierliche Sicherheitsüberwachung Implementeren von Erkennungsprozessen	■□□□□□	■■■□□□	■■■■■■	■■■■■■	■■□□□□
5	**Response** reagieren	Reaktionsplanung Schaden- und Angriffsanalyse Schadenbegrenzung und Schadensabwehr	■□□□□□	■■■□□□	■■■■■□	■■■■■■	■■□□□□
6	**Recover** wiederherstelllen	WIederherstellungsplan Verbesserung Kommunikation	■□□□□□	■■■□□□	■■■■■□	■■■■■■	■■□□□□

Mitarbeiter effizient & erfolgreich für eine sichere Fabrik qualifizieren

Wir haben gelernt, welche Online-Schulungsformate im Unternehmenskontext zum Erfolg führen: Programme

KPIs von Industrial Security Schulungen



1 Nutzer, die mind. 1 Kurs gestartet haben
2 Nutzer, die angefangene Kurse beenden
3 Bei Automatisierungs-Unternehmen(schwach betreut)
4 bei Automobil-OEM (freiwillig)

Beispielprojekt: “Industrial Security” bei einem deutschen Automobilhersteller

Industrial Security Schulung

- **6 Zielgruppen**
  - Führungskräfte
  - Security
  - Verantwortliche Planer
  - Instandhalter
  - Produktions-IT
  - Auszubildende
- Starke Anpassung von Format und Inhalten je Zielgruppe
- Ca. **1/4 kunden-spezifische Inhalte**

Zielsetzung

1. Überblick & Verständnis
2. Echtes Up-Skilling hin zur Anwendung im Betrieb

Rahmenbedingungen

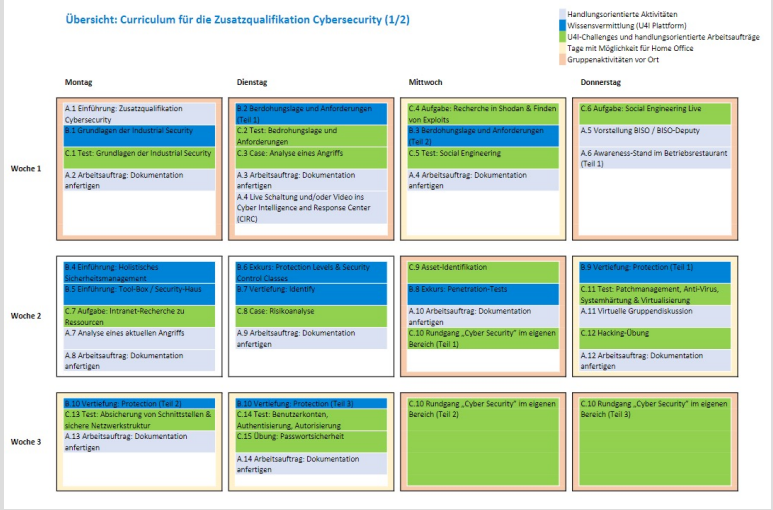
- Minimaler zeitlicher Einsatz der Lerner
- Anbindung an existierende Systeme & Prozesse

U4I Lösung

- Programm Design
- Definition Lernziele
- Bereitstellung & Konfiguration Inhalte aus Bestand
- Produktion von unternehmensspezifischen Inhalten
- Projektmanagement
- Infrastruktur für Durchführung

Endergebnis

- 6-Wochen Training für Auszubildende
- Blended Learning Angebot (Online + Präsenzaufgaben)
- Anpassung in 2h-18h Module für Instandhalter, Planer, etc.



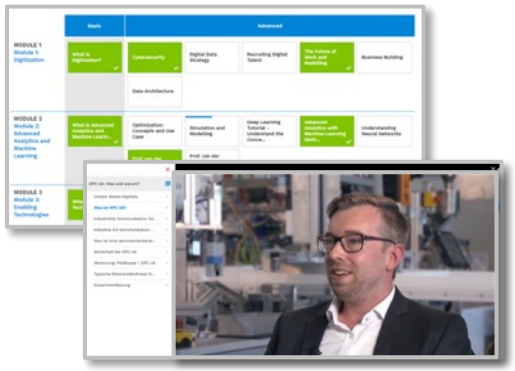
Programme nutzen eine Kombination an Formaten, um konkrete Handlungen im Unternehmen vorzubereiten und umzusetzen

LEARN

Online Lerninhalte

- Video-basierte Module: Experten erklären
- Übungsaufgaben

Online, selbstgesteuert, flexible Nutzung

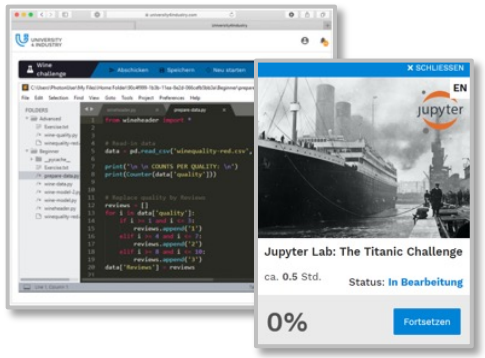


EXPLORE

Online Labs

- Praxiserfahrung
- Experimente mit Daten, Software & Hardware

Online, selbstgesteuert, flexible Nutzung



DISCUSS

Gruppenarbeit & Diskussion

- Verständnis im eigenen Kontext diskutieren und vertiefen
- Gruppenprojekte zur Anwendung der neuen Fähigkeiten

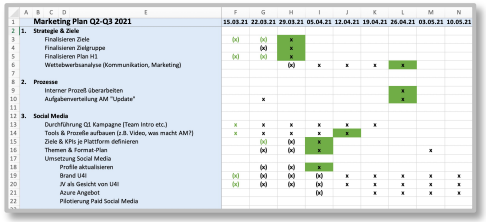
Online & Präsenz

ACT

Definition der nächsten Schritte

- Transfer ins eigene Arbeitsumfeld
- Handlungsbedarf im eigenen Unternehmen festlegen
- Projekte definieren

Online & Präsenz



U4I Cloud-Plattform + Integration mit Microsoft Teams für effiziente Durchführung

Unser Ansatz funktioniert: Feedback aus einem Kundeprojekt

- **>80%** Aktivierungsrate in freiwilligem Training
- **>80%** Abschlussquote in freiwilligem Training
- **>90%** der Lerner würde das Training an Kollegen weiterempfehlen

> Die Themen sind inhaltlich sehr gut aufbereitet, sodass sie auch für Nicht-IT-Experten gut zu verstehen sind. Man bekommt eine ganz andere Sichtweise darauf, wie wichtig Security für unser Unternehmen ist.

> Fantastic, a good reminder of the basics of it all.

> The course is very detailed and the use of reading, videos, and user interaction helps to make the concepts concrete.

UNIVERSITY
4 INDUSTRY

Industrial Security – Verfügbare Inhalte (1/2)

Grundlagen	Vertiefung	
Einführung Industrial Security • Bedrohungslage • Angriffstypen • Ablauf eines Angriffs • Rechtlicher Rahmen (IT-Sicherheitsgesetz) • Einführung IEC 62443	**Risikoanalyse**	**Kryptographie**
	Netzsegmentierung	**Incident Response**
	Benutzerkonten, Authentisierung, Autorisierung	**Monitoring & Logging**
	Sichere Netzwerk-kommunikation & Schnittstellen	**Dokumentation**
	Sichere Fernwartung	**Penetrationtests**
	Schutzmaßnahmen (AV, Komponentenhärtung, etc.)	**Deep-Dives: OPC UA & MQTT**

Industrial Security – Verfügbare Inhalte (2/2)

Vertiefung

IEC 62443
- Technologie, Prozesse & Menschen
- Struktur des Standards IEC 62443
- Defense-in-Depth-Konzept
- Protection Levels
- Security Control Classes
- Holistic Security Concept

Sicherer Produktlebenszyklus
- Beobachtung von Schwachstellen & Bedrohungen
- Patchmanagement
- Kommunikationskanäle & Verantwortlichkeiten
- EoS, Phase-out-Management

Embedded System Security

Einführung Embedded System Security

Angriffe & Security bei Embedded System Hardware

Angriffe & Security bei Embedded System Software

Sicherer Entwicklungsprozess für Embedded Systems
- Einführung
- Tests (Unit-, Integration-, & Acceptance Test, Penetrationtest)
- Organisatorische Maßnahmen
- Best Practices