



#### 4. VDI-Fachkonferenz mit Fachaussstellung

# Industrial IT Security 2016

## IT-Sicherheit in Produktions- und Automations-Systemen

28. und 29. Juni 2016, Darmstadt

### Top-Themen der Konferenz

- Absicherung unternehmensübergreifender Wertschöpfungsnetzwerke
- Industrial Security als zentrale Komponente der Industrie 4.0
- Sichere Kommunikation in verteilten Produktionsumgebungen
- Cyberangriffe, Spionage und Sabotage: Bedrohungen erkennen
- Standardisierung und Normierung sicherer Referenzarchitekturen
- Sichere Fernwartung und Monitoring durch standardisierten Zugriff
- Best practice Tipps für den shop floor level

### Leiter der Konferenz

#### Prof. Dr. rer. nat. Michael Waidner

Leiter, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Leiter Sicherheit in der Informationstechnik an der TU Darmstadt, Direktor CASED, Leiter EC SPRIDE

### Mit Vorträgen von diesen Experten

ABB Automation • Bayer • Bosch Rexroth • Bundesamt für Sicherheit in der Informationstechnik (BSI) • Daimler • genua • PHOENIX CONTACT Cyber Security • Pilz • PROFI Engineering Systems • secunet Security Networks • Siemens • Unified Automation • WTS Legal Rechtsanwaltsgesellschaft • ZF Friedrichshafen

### + VDI-Spezialtage

am 27. Juni 2016

- IT-Sicherheitsmanagement auf dem Weg zur Industrie 4.0

am 30. Juni 2016

- IT-Sicherheit von industriellen Steuerungen: Grundlagen SCADA Security und ICS
- Digitale Transformation: Auswirkungen auf Unternehmen und die Rolle des Chief Digital Officers



# 1. Konferenztag

## Dienstag, 28. Juni 2016

08:45 Anmeldung

### 09:45 Begrüßung und Eröffnung durch den Konferenzleiter



**Prof. Dr. rer. nat. Michael Waidner**, Leiter, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Leiter Sicherheit in der Informationstechnik an der TU Darmstadt, Direktor CASED, Leiter EC SPRIDE

## Rechtliches, Standards und Prozessmodellierung

### 10:00 Netzwerksicherheit in verteilten Produktionsumgebungen im Kontext von Industrie 4.0

- Reifegrad der Organisation und Prozesse als Schlüssel für den Einstieg in die digitale Transformation
- Prozess-Standardisierung als wichtige Voraussetzung für Effizienzsteigerung
- Netzwerksicherheit als Herausforderung bei global verteilten Standorten
- Effiziente Verwaltung von Firewall, IPS und Content Security am Bsp. eines global Players im Mittelstand

**Dipl.-Kfm. Udo Bungert**, Senior Vice President Consulting, Dipl.-Inf. Marcus Hock, CISSP, Senior Consultant, Leiter Kompetenzteam Netzwerk & Security, PROFI Engineering Systems AG, Darmstadt

### 10:45 Normierte sichere Infrastruktur für Industrie 4.0

- Aktuelle Sicherheit von Fertigungsanlagen
- Abbildung ISO 2700x auf die diskrete Fertigung
- Herausforderungen für die Organisation in der Fertigung
- Standardisierter Remote Access Zugang für die Fernwartung
- Ausblick ögP IUNO und die Erwartungshaltung eines Betreibers

**Dipl.-Inform. Michael Jochem**, Director Projekt Industrie 4.0@Bosch, Bosch Rexroth AG, Lohr am Main

### 11:30 Rechtliche Herausforderungen für die Industrie an der Schnittstelle zur IT-Sicherheit

- Bedrohung durch Cyberangriffe, Spionage und Sabotage: Wie können sich Unternehmen rechtlich absichern?
- Herausforderung Datenschutz: Wie lassen sich multinationale Datentransfers bei vernetzten Produktionsprozessen rechtskonform ausgestalten?
- Haftung und Verantwortlichkeiten: Wie lassen sich IT- und datenschutzrechtliche Haftungsrisiken unter den Beteiligten von vernetzten Produktionsprozessen interessengerecht verteilen?
- Herausforderung Exportkontrolle: Lassen sich Verschlüsselungstechnologien rechtssicher verwenden?

**RA Dr. Thorsten B. Behling**, Datenschutz- und IT-Recht, Partner, Rechtsanwalt der WTS Legal Rechtsanwalts-gesellschaft mbH, Köln

### 12:15 Mittagspause mit Besuch der Fachausstellung

## Umsetzungen von IT-Sicherheitsmaßnahmen

### 13:45 Start small, keep on growing, think big – Wie die Absicherung gelingt

- Quick Wins durch andere Blickwinkel
- Der Weg von Checklisten über Richtlinien zum ganzheitlichen Sicherheitsmanagement
- Sensibilisierung jenseits von Postern und schlaun Sprüchen
- IT-Sicherheitsgesetz: eine erste Bilanz

**Dipl.-Inform. Holger Junker**, Referatsleiter, Cyber-Sicherheit in kritischen IT-Systemen, Anwendungen und Architekturen, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

### 14:30 Shopfloor Security – Zellschutz zur Risikoreduzierung in Profinet vernetzten Automatisierungsanlagen

- Löst das Security Update von Industrie 4.0 auf Industrie 4.0.1 unsere Probleme?
- Gefährdung der Produktionsprozesse durch extrem gesteigerte Zugriffsmöglichkeiten
- Möglichkeiten der Separierung und Trennung zur Risikoreduktion
- IT Prozesse zur Aufrechterhaltung der Systemstabilität in den Instandhaltungsbereichen: Patching, AV-Schutz, Incident Management, Asset Management, Vulnerability Management
- Anforderungen an Automatisierungskomponenten und Tools, um Schwachstellen nachhaltig zu schließen

**Dipl.-Ing.(FH) Nachrichtentechnik Alexander Rinker**, Entwicklung Mercedes ME Virtual Car & Security, Daimler AG – Research & Development, Mercedes Benz Werk Sindelfingen

### 15:15 Kaffeepause mit Besuch der Fachausstellung

## Sichere Kommunikation – Maßnahmen für Cybersicherheit

### 15:45 OPC UA – integrierte Security für Industrie 4.0

- Warum ist Sicherheit in der Industrie wichtig?
- Was ist OPC UA und warum ist es sicher?
  - » Bedrohungen und Schutzziele
  - » Maßnahmen von OPC UA um diese Schutzzeile zu gewährleisten
- Wartung und Pflege von OPC UA Security
- Was die Industrie noch zu lernen hat
- Verfügbarkeit vs. Security
- Ausblick von OPC UA Security

**Gerhard Gappmeier**, Chief Software Architect, Unified Automation GmbH, Schwabach

### 16:30 Sichere unternehmensübergreifende Kommunikation für Industrie 4.0

- Etablierung sicherer Kommunikationsbeziehungen ohne manuelle Vorkonfiguration zur Absicherung unternehmensübergreifender Wertschöpfungsnetzwerke
- Gewährleistung von Authentizität, Integrität und Vertraulichkeit der Daten an Endpunkten und während der Weiterverarbeitung
- Kommunikationspartner müssen sich über Unternehmensgrenzen hinweg sicher identifizieren auch unter der Prämisse wechselnder Rollen und Aufgaben von Personen
- Verlagerung von Informationsverarbeitung in Echtzeit in die Cloud oder zu anderen Unternehmen erfordert höhere Verlässlichkeit der Kommunikationswege

**Dr.-Ing. Lutz Jänicke**, Industrie 4.0 Security Technologies, PHOENIX CONTACT Cyber Security AG, Berlin

### 17:15 Safety und Security – gemischtes Doppel für Industrie 4.0

- Abgrenzung Safety und Security: Woher stammen die Anforderungen an Safety und Security?
- Wichtige Normen und Standards: Was gibt es bezüglich Funktionaler Sicherheit zu beachten?
- Gemeinsamkeiten und Unterschiede: Abläufe und Prozesse – auf bewährtem und vertrautem aufbauen
- Herausforderungen und Lösungsansätze: Was muss für eine sichere Automatisierung erfüllt sein?

**Dipl.-Ing. (FH) Martin Frey**, Regionalleiter, Tochtergesellschaft Deutschland, Vertriebsregion Südwest, Pilz GmbH & Co. KG, Ostfildern

### Ca. 18:00 Get-Together

Zum Ausklang des ersten Veranstaltungstages lädt Sie das VDI Wissensforum zu einem Get-Together ein. Nutzen Sie die entspannte Atmosphäre, um Ihr Netzwerk zu erweitern und mit anderen Teilnehmern und Referenten vertiefende Gespräche zu führen.

### 19:00 DINNER SPEECH

#### „ICS-Live-Hacking“

##### Angriffe auf Prozessnetze verstehen

- Neuralgische Punkte in Kritischen Infrastrukturen erkennen
- Demonstration potenzieller Angriffspunkte
- Fehlverhalten oder mangelnden organisatorischen Maßnahmen führen zu Betriebsstörungen und Sicherheitsvorfällen
- Verbindungen zwischen Prozess- und Office-Netzen bedeuten höhere Anforderung an die Sicherheit

**Markus Linnemann**, Leiter Division Kritische Infrastrukturen, Dirk Reimers, Leiter Bereich Pentest und Forensik, secunet Security Networks AG, Essen

## 2. Konferenztag Mittwoch, 29. Juni 2016

### Sicherheit in der Produktion und in eingebetteten Systemen

#### 08:30 Erfahrungsbericht IT Security in der Produktion als Voraussetzung für Industrie 4.0

- hochgradige Vernetzung der Maschinen und Anlagen bringt Produktivitätssteigerung durch hochflexible und effiziente Fertigungsprozesse
- Anspruch an Verfügbarkeit und Robustheit der IT-Komponenten erfordert besondere Maßnahmen gegen Malware und Angriffe
- Schwierigkeiten beim Umgang mit alten Steuerungen, nicht mehr supporteten Betriebssystemen und leistungsschwacher Hardware
- Technische Herausforderungen und organisatorische Lösungen für die IT-Sicherheit im Produktionsumfeld
- Vorgehen bei einem Automobilzulieferer und Vorstellung von praktikable Lösungen

**Rainer Rodler, Betriebswirt (VWA)**, Projektleiter PITS, Production Management ZF-Konzern, Dr.-Ing. Nils Macke, Senior Manager Corporate Production, Production Network Solutions (OPS), Production Management and System, Technik ZF-Konzern, ZF Friedrichshafen AG

#### 09:15 Industrielle Kommunikation im Wandel: Auswirkung von Industrie 4.0 auf IT-Sicherheitskonzepte

- Industrielle Kommunikation und IT-Sicherheitskonzepte vor Industrie 4.0
- Wandel von Kommunikationsarchitekturen ausgelöst durch Industrie 4.0-Anwendungen
- Grenzen bestehender IT-Sicherheitskonzepte
- Ableitung von Anforderungen in Bezug auf IT-Sicherheit
- Aufzeigen von Lösungsansätzen

**Dr.-Ing. Holger Flatt**, Gruppenleiter Eingebettete Systeme für die Automation, Fraunhofer-Anwendungszentrum Industrial Automation (IOSB-INA), Lemgo

#### 10:00 Kaffeepause mit Besuch der Fachaussstellung

### Sicherheit vernetzter Systeme durch Design und Referenzarchitekturen

#### 10:30 Security by Design: Herausforderung für viele Beteiligte

- „Security by Design“ als Umsetzungsstrategie für die IT-Security in Produkten
- Bedrohungsanalyse und Definition von Schutzzielen
- Erforderliche Anpassung bestehender Unternehmensprozesse
- Typische Randbedingungen für Industrial Security
- Verankerung von Security in Standards

**Dr. Wolfgang Klasen**, Corporate Technology, Technology Field IT-Security, Siemens AG, München

#### 11:15 Security by Design – Was bedeutet das für die Automatisierungstechnik?

- Modelle und Konzepte zur horizontalen und vertikalen Integration in Industrie 4.0 Wertschöpfungsnetzwerken
- Ergänzung des Defense-in-Depth-Ansatzes durch integrierte Sicherheitsfunktionen
- Auswirkungen von Security by Design auf Komponenten der Automatisierungstechnik
- Mögliche Lösungsansätze zur Realisierung

**Prof. Dr. Karl-Heinz Niemann**, Fachgebiet Prozessinformatik und Automatisierungstechnik, Fakultät 1 Elektro- und Informationstechnik, Hochschule Hannover

#### 12:00 Mittagspause mit Besuch der Fachaussstellung

#### 13:30 Secure Reference Architecture for Production IT

- (Kritische) Infrastrukturen im Wandel von Industrie 4.0: Warum sind segmentierte Netzwerke eine Erfordernis?
- Wie sehen sichere Architekturen aus und mit welchen Technologien kann man sie implementieren?
- Was bedeutet es für Hersteller?
- Der lange Weg zum Ziel: Methodologie des Designs und Learnings aus der Praxis der Netzwerk-Segmentierung
- Wichtiger denn je: was macht eine gute Beziehung zwischen Hersteller und Anlagenbetreiber aus?

**Dr. rer. nat. Walter Speth**, Senior Project Manager, Manufacturing IT, Bayer AG, Leverkusen, Dipl.-Ing. (FH) Mirko Brcic, Technology Manager, Forschung und Entwicklung, Endress + Hauser Process Solutions AG, Reinach, Schweiz, Achim Patzner, Geschäftsführer, Systems, Networks and Security, BNC Network Consulting GmbH, Rheinbach

### Wirkungsvolle Schutzmaßnahmen und Lösungsansätze für Automatisierung und Produktion

#### 14:15 Neue IT-Technologien für sichere Vernetzung bei Industrie 4.0

- Steigende Bedeutung von Netzwerken und -technologien durch höhere Vernetzungsgrade
- Neben dem Transfer von Sicherheitstechnologie aus dem Office-Netz werden weitere Technologien benötigt
- Entwicklung neuer Geschäftsmodelle werden erst realisierbar mit nachhaltiger (Netzwerk-)Sicherheit
- Vorstellung von Netzwerksicherheitstechnologien am Beispiel Fernwartung und Monitoring

**Matthias Ochs**, Gruppenleiter und Product Owner, genua gmbh, Kirchheim bei München

## 15:00 Aufbau eines Sicherheitsmanagement-Systems für Industrieanlagen

- Kennen Sie Reifegradmodelle zur Beschreibung unterschiedlicher Ausbaustufen von Sicherheitsmanagement-Systemen (SMS) gemäß Standards wie ISO 27000 oder IEC 62443?
- Wie kann ein Betriebsverantwortlicher für eine Industrieanlage ein solches SMS aufbauen?
- Wie motiviert er gegenüber seinem Management die dafür notwendigen Mittel?
- Wie kann er dabei gleichzeitig sicherstellen, dass der laufende Betrieb nicht überfordert wird?
- Und wie kann er sicherstellen, dass trotzdem die mittelfristig notwendigen Ziele erreicht werden?

**Maximilian Wolodin**, Automation Security Expert, ABB Automation GmbH, Frankfurt

## 15:45 Zusammenfassung der Konferenz und Schlusswort

**Prof. Dr. rer. nat. Michael Waidner**

**Ca. 16:00 Ende der Konferenz**

## Gründe, warum Sie die Veranstaltung besuchen sollten:

- Erkennen Sie, welche neuen Gefahren und Risiken drohen
- Nutzen Sie Praxiswissen zur effizienteren Nutzung von Firewalls und IPS
- Lernen Sie, wie Komponenten und Anlagen von Grund auf sicher geplant werden
- Erfahren Sie, welche aktuellen Entwicklungen es zu Industrie 4.0 gibt
- Informieren Sie sich über den neuesten Stand der Technik für sichere Prozesskommunikation
- Erhalten Sie Einblick in die Architektur sicherer Prozesse, Komponenten und Protokolle

## Fachausstellung/Sponsoring

Sie möchten Kontakt zu den hochkarätigen Teilnehmern dieser VDI-Tagung aufnehmen und Ihre Produkte und Dienstleistungen einem Fachpublikum Ihres Marktes ohne Streuverluste präsentieren? Vor, während und nach der Veranstaltung bieten wir Ihnen vielfältige Möglichkeiten, rund um das Tagungsgeschehen „Flagge zu zeigen“ und mit Ihren potenziellen Kunden ins Gespräch zu kommen.

Informationen zu Ausstellungsmöglichkeiten und zu individuellen Sponsoring Angeboten erhalten Sie von:

### **Antonia Schlemmer**

Ansprechpartnerin Ausstellungen/Sponsoring

Telefon: +49 211 6214-592, E-Mail: [schlemmer@vdi.de](mailto:schlemmer@vdi.de)

## IT-Sicherheitsmanagement auf dem Weg zur Industrie 4.0

10:00 bis ca. 17:30 Uhr

### Ihr Leiter

**Dipl.-Ing. oec. Sebastian Rohr**, CISA/CISM/CISSP, technischer Geschäftsführer, accessec GmbH, Gross-Bieberau

### Thema

Die Sicherheit Industrieller Fertigungsanlagen und ihrer IT Komponenten ist durch eine Vielzahl Schwachstellen und Bedrohungen gefährdet. Der Spezialtag „IT-Sicherheitsmanagement auf dem Weg zur Industrie 4.0“ zeigt auf, wie auf Basis erster Erkenntnisse aus Risikoanalysen nach FMEA Methodik sowie unter Anwendung der Vorgaben und Leitlinien aus VDI 2182, IEC 62443 sowie der ISO27000er Reihe sinnvolle Maßnahmen abgeleitet, priorisiert und umgesetzt werden können, um das Sicherheitsrisiko auf ein akzeptables Niveau zu senken.

### Inhalt

#### Einführung in IT-Risikoanalyse und Risikomanagement

- Begriffsdefinitionen und Unterschiede im Analyse Ansatz
- Risikoanalyse unter Nutzung der FMEA Methodik
- Risiko-Maturität im Management Prozess

#### Ausgewählte IT-Risiken in der Produktion

- Gruppenarbeit: Unterschiede zwischen Office und Industrial IT
- Schutzbedarf, mögliche Schutzmaßnahmen und ihre Wirksamkeit
- Bedrohungen und ihre Handhabung in Produktionsnetzen
- Änderungen durch Industrie 4.0

#### Maßnahmen für IT-Sicherheit

- Offene Diskussion: Basisanforderungen für IT-Sicherheit in der Produktion
- Organisation und Verantwortlichkeiten
- Zonenmodell, Netzwerk Segregation und Netzwerk-Überwachung
- Client und Systemsicherheit: Antivirus, Whitelisting und ihre Grenzen

#### Mini-Workshop nach Mehrheitsbeschluss

- Remote Access für Anlagen vs. Benutzerverwaltung und Monitoring in der Produktion
- Kurze Anforderungsanalyse
- Schlüsselfunktionen und „Wünschenswertes“
- Erarbeitung der Ergebnisse am Whiteboard



### IT-Sicherheit von industriellen Steuerungen: Grundlagen SCADA Security und ICS

09:00 bis ca. 17:00 Uhr

Ihr Leiter

**Dipl.-Ing. Hans Hoefken**, Institutsleitung, Instituts für IT-Sicherheit in Industrial Control Systems, Aachen

#### Thema

Experten für die IT-Sicherheit von Office-IT UND ICS sind heute rar gesät. Beide sprechen nur vordergründig die gleiche Sprache, die Probleme und deren Lösungen sind oft sehr unterschiedlich. In diesem Spezialtag „IT-Sicherheit von industriellen Steuerungen: Grundlagen SCADA Security und ICS“ erhalten Sie einen Überblick, wo die Unterschiede liegen und wie deren Lösung aussieht. Werden Sie Vermittler zwischen den IT-Welten.

#### Inhalt

##### Übersicht über Industrielle Steuerungssysteme

- Aufbau und Komponenten von ICS
- Kommunikationslevel im ICS
- SCADA-Server/Master Terminal Unit (MTU)
- Control Server (CS)
- Input/Output Server (I/O)
- Programmierbare Steuerungen (PLC/SPS)
- Intelligente elektronische Geräte (IED)
- Human Machine Interface (HMI)
- Data Historian
- Remote Terminal Unit (RTU)
- Engineering Workstation (EWS)
- Feldbusse

##### ICS Protokolle

- Modbus:
  - » Aufbau und Funktionscodes
  - » Protokollvarianten
  - » Sicherheitsbetrachtung
- OPC:
  - » Was ist OPC?
  - » Sicherheitsbetrachtung von OPC
- Industrial Ethernet
  - » Ethernet vs. Industrial Ethernet: Gemeinsamkeiten und Unterschiede
  - » Typen von Industrial Ethernet: EtherCat, Profinet

##### Bedrohungen und Schwachstellen von Industriellen Steuerungen

- Sicherheitsterminologie und -konzepte: Authentifizierung, Verschlüsselung, Integrität und Autorisierung
- Software-, Hardware- und Konfigurationsschwachstellen und Gegenmaßnahmen
  - » Der Sicherheits-Lifecycle
  - » Zugriffskontrollen
  - » Was darf ein Benutzer oder System tun?
- Risikofaktoren

##### Angriffe auf SCADA

- Grundsätzlicher Ablauf eines IT-Angriffs
- Sicherheitsprobleme mit ICS wie Buffer Overflow, ungepatchte Systeme und Angriffe auf Passworte
- Penetrationstests im ICS Umfeld
- Praktische Beispiele
  - » Scannen eines SCADA Netzes
  - » SQL Injection auf SPS
  - » Angriff auf eine Beckhoff SPS CS5020

##### Sicherheitsmaßnahmen zur ICS Sicherung

- Defense in Depth – Das Zonenkonzept
- Firewalls im ICS Umfeld
- Was ist SIEM? Vorstellung, Nutzen und Probleme mit der Technik
- Standards und Best Practices für die IT-Sicherheit in ICS

### Digitale Transformation: Auswirkungen auf Unternehmen und die Rolle des Chief Digital Officers

09:00 bis ca. 16:30 Uhr

Ihr Leiter

**Albert Brenner**, Geschäftsführer, Digital Transformation Group GmbH, München

#### Thema

Der VDI-Spezialtag befasst sich mit der Frage, welche Bedeutung die Position des Chief Digital Officers (CDO) für die Digitalisierung eines Unternehmens innehat. Welche Funktionen und Aufgaben sollte der CDO übernehmen? Wie lässt sich die Position optimal in das Tagesgeschäft einbinden? Und wie kann man den kulturellen Wandel in Unternehmen am besten gestalten? Anschaulich und mit vielen Praxisbeispielen untermalt, werden die wichtigsten digitalen Transformationshebel behandelt.

#### Inhalt

##### Einfluss der Digitalisierung auf Unternehmen

- Transformative Wirkung der Digitalisierung auf Unternehmen: Veränderung von Geschäftsmodellen, Transformation von Aufbau- und Ablauforganisation und Vernetzung im und außerhalb des Unternehmens
- Die Wellen der Digitalisierung und Ihre wechselnden Paradigmen (Digitalisierung gestern, heute und morgen)
- Geschwindigkeit und Volatilität der Veränderung von Markt-Chancen und -Risiken, Geschäftsmodellen, Organisationsformen, Vernetzung und Interaktionen durch die Digitalisierung

##### Systematische Bewertung von digitalen Trends in Bezug auf tatsächliche und erwartete Entwicklung für das eigene Unternehmen

- Vorgehensmodell zur Identifikation und Bewertung von Digitalisierungstrends
- Auswirkungen der Trends auf die Wertschöpfungskette und die Funktionsbereiche der Organisation
- Die Veränderung von „Außen und Innen“ durch Digitalisierung
- Möglichkeiten und Grenzen von Trend-Analysen, Trendstudien und Trend-Radar

##### Überblick über die wichtigsten digitalen Transformationshebel

- Marketing: Social Media und digitales Marketing als Treiber von Customer Centricity
- Vertrieb: Die nächste(n) Welle(n) des E-Commerce und E-Business
- F&E: Augmented Reality intern und extern sinnvoll einsetzen
- Produktion und Logistik: Internet der Dinge und Industrie 4.0
- HR: Digital Collaboration
- IT: Big Data, Cloud

##### Digitalisierung als Treiber für Customer Centricity

- Das Anlagevermögen in der digitalen Welt: Digital Assets
- Der Konsument 2.0 – Fluch und Segen zugleich: Social Media, Shitstorms, Community & Influencer Management, Reviews & Ratings und Crowd-Sourcing
- Die Medien-Eruption: Der veränderte Medienmix
- Die Renaissance des CRM: Mit Kunden vernetzen, Kundendaten sammeln und nutzen, Social CRM

##### Datenintelligenz in allen Funktionsbereichen

- Tracking von Customer Journey und Customer Touchpoints
- E-Commerce Daten intelligent nutzen
- Der Sockel des Eisbergs: Optimierung der Wertschöpfungskette aus Daten vernetzter Objekte

##### Der Chief Digital Officer

- Digitalisierung im Unternehmen: Die Transformations-Roadmap
- Blockaden der Digitalisierung: Der Bedarf einer neuen digitalen Struktur und Denke
- Beschreibung einer neuen Rolle im Unternehmen
- Warum ein CDO? Wo macht er Sinn / wo nicht?
- Der CDO als Organisationsstruktur
- Herausforderungen des CDO und Lösungsansätze

## 4. VDI-Fachkonferenz Industrial IT Security 2016



Mit dem FSC® Warenzeichen werden Holzprodukte ausgezeichnet, die aus verantwortungsvoll bewirtschafteten Wäldern stammen, unabhängig zertifiziert nach den strengen Kriterien des Forest Stewardship Council® (FSC). Für den Druck sämtlicher Programme des VDI Wissensforums werden ausschließlich FSC-Papiere verwendet.

**Gedruckt auf 100 % Recycling-Papier, versehen mit dem Blauen Engel.**

Günstige  
Kombipreise  
nutzen!

Ja, ich nehme wie folgt teil: (Bitte Veranstaltung und Preiskategorie wählen)

4. VDI-Fachkonferenz „Industrial IT Security 2016“, 28.–29.06.2016 (02KO704016)  
 VDI-Spezialtag „IT-Sicherheitsmanagement auf dem Weg zur Industrie 4.0“, 27.06.2016 (02ST264003)  
 VDI-Spezialtag „IT Sicherheit von industriellen Steuerungen: Grundalgen SCADA Security und ICS“, 30.06.2016 (02ST265003)  
 VDI-Spezialtag „Digitale Transformation: Auswirkungen auf Unternehmen und die Rolle des Chief Digital Officers“, 30.06.2016 (02ST261001)

Preis p./P. zzgl. MwSt.	PS	Einzelbuchung 4. VDI-Fachkonferenz Industrial IT Security 2016 am 28.–29.06.2016 (02KO704016)	Einzelbuchung VDI-Spezialtage (Preis je Spezialtag)	Kombibuchung Konferenz + 1 Spezialtag  Sparen Sie 150 Euro!	Kombibuchung Konferenz + 2 Spezialtage  Sparen Sie 200 Euro!
Teilnahmegebühr	1	<input type="checkbox"/> EUR 1.390,-	<input type="checkbox"/> EUR 890,-	<input type="checkbox"/> EUR 2.130,-	<input type="checkbox"/> EUR 2.970,-
persönliche VDI-Mitglieder	2	<input type="checkbox"/> EUR 1.290,-	<input type="checkbox"/> EUR 840,-	<input type="checkbox"/> EUR 1.980,-	<input type="checkbox"/> EUR 2.770,-
VDI-Mitgliedsnummer*					

\* Für die Preisstufe (PS) 2 ist die Angabe der VDI-Mitgliedsnummer erforderlich.

1111

Ich interessiere mich für Ausstellungs- und Sponsoringmöglichkeiten.

Nachname

Vorname

Titel

Funktion

Abteilung

Tätigkeitsbereich

Firma/Institut

Straße/Postfach

PLZ, Ort, Land

Telefon

Fax

Mobilnummer

E-Mail

Abweichende Rechnungsanschrift

Teilnehmer mit Rechnungsanschrift außerhalb von Deutschland, Österreich und der Schweiz zahlen bitte mit Kreditkarte.

- Visa  Mastercard  
 American Express

Karteninhaber

Kartenummer

Prüfziffer

gültig bis (MM/JJ)

Datum

× Unterschrift

## VDI Wissensforum

VDI Wissensforum GmbH  
 Kundenzentrum  
 Postfach 10 11 39  
 40002 Düsseldorf  
 Telefon: +49 211 6214-201  
 Telefax: +49 211 6214-154  
 E-Mail: [wissensforum@vdi.de](mailto:wissensforum@vdi.de)  
[www.vdi.de/IT-Security](http://www.vdi.de/IT-Security)

**Anmeldungen** müssen schriftlich erfolgen. Anmeldebestätigung und Rechnung werden zugesandt. Gebühr bitte erst nach Rechnungseingang unter Angabe der Rechnungsnummer überweisen.

#### Veranstaltungsort/Zimmerreservierung

Maritim Rhein-Main Hotel Darmstadt, Am Kavalleriesand 6, 64295 Darmstadt, Tel. +49 6151 303-0, Fax +49 6151 303-111, E-Mail: [info.dam@maritim.de](mailto:info.dam@maritim.de)

Für Sie als Konferenzteilnehmer haben wir im genannten Hotel s.o. Zimmerkontingente reserviert. Bitte reservieren Sie bis zum 23.05.2016 unter dem Stichwort „VDI“. Bitte nehmen Sie die Reservierung selber direkt im Hotel vor.

Weitere Hotels in der Nähe des Veranstaltungsortes finden Sie auch über unseren kostenlosen Service von HRS, [www.vdi-wissensforum.de/hrs](http://www.vdi-wissensforum.de/hrs)



**Exklusiv-Angebot:** Als Teilnehmer dieser Veranstaltung bieten wir Ihnen eine 3-monatige, kostenfreie VDI-Probemitgliedschaft an. (Dieses Angebot gilt ausschließlich bei Neuaufnahme).

**Leistungen:** Im Leistungsumfang der Konferenz (zweitägig) sind die Pausengetränke, das Mittagessen und der Abendimbiss am 28. Juni 2016 enthalten. Im Leistungsumfang der Spezialtage sind die Pausengetränke und das Mittagessen enthalten. Die Konferenzunterlagen werden den Teilnehmern vor der Veranstaltung via Download zur Verfügung gestellt. Die Spezialtagunterlagen erhalten Sie vor Ort.

**Geschäftsbedingungen:** Mit der Anmeldung werden die Geschäftsbedingungen der VDI Wissensforum GmbH verbindlich anerkannt. Abmeldungen müssen schriftlich erfolgen. Bei Abmeldungen bis 14 Tage vor Veranstaltungsbeginn erheben wir eine Bearbeitungsgebühr von € 50,- zzgl. MwSt. Nach dieser Frist ist die volle Teilnahmegebühr gemäß Rechnung zu zahlen. Maßgebend ist der Posteingangsstempel. In diesem Fall senden wir die Veranstaltungsunterlagen auf Wunsch zu. Es ist möglich, nach Absprache einen Ersatzteilnehmer zu benennen. Einzelne Teile des Seminars können nicht gebucht werden. Muss eine Veranstaltung aus vorvorhersehbaren Gründen abgesagt werden, erfolgt sofortige Benachrichtigung. In diesem Fall besteht nur die Verpflichtung zur Rückerstattung der bereits gezahlten Teilnahmegebühr. In Ausnahmefällen behalten wir uns den Wechsel von Referenten und/oder Änderungen im Programmablauf vor. In jedem Fall beschränkt sich die Haftung der VDI Wissensforum GmbH ausschließlich auf die Teilnahmegebühr.

**Datenschutz:** Die VDI Wissensforum GmbH erhebt und verarbeitet Ihre Adressdaten für eigene Werbezwecke und ermöglicht namhaften Unternehmen und Institutionen, Ihnen im Rahmen der werblichen Ansprache Informationen und Angebote zukommen zu lassen. Bei der technischen Durchführung der Datenverarbeitung bedienen wir uns teilweise externer Dienstleister. Wenn Sie zukünftig keine Informationen und Angebote mehr erhalten möchten, können Sie bei uns der Verwendung Ihrer Daten durch uns oder Dritte für Werbezwecke jederzeit wider sprechen.

Nutzen Sie dazu die E-Mail Adresse: [wissensforum@vdi.de](mailto:wissensforum@vdi.de) oder eine andere oben angegebene Kontaktmöglichkeit.