

6. VDI-Fachkonferenz

Bildquelle: © iStock.com - iLexx

Industrial IT Security 2018

IT-Sicherheit in Produktions- und Automations-Systemen

Die Top-Themen:

- IT-Sicherheit bei Steuergeräten und Kommunikationssystemen
- Herausforderungen und Lösungsansätze bei Remote- und Fernwartssystemen
- Best Practices – Warum es besser ist in Vorbeugung zu investieren als in Reaktion
- Rollout von IT Sicherheit – Integration von Sicherheitsnormen und Best Security Practices Ansätzen
- Sichere Architektur von Produktionsnetzwerken

Konferenzleitung

Prof. Dr. rer. nat. Michael Waidner, Leiter, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Leiter Sicherheit in der Informationstechnik an der TU Darmstadt, Sprecher des Center for Research in Security and Privacy (CRISP)

+ buchbare Spezialtage

IT-Sicherheit in KRITIS & Industrie
durch Recht & Normung

Zertifizierung nach ISO 270XX –
Wie gehe ich es an und worauf
muss ich achten?

Alles neu im Datenschutz?
Einführung in DS-GVO und
BDSG-neu

Cyber War Game – Die Krise
als Übung

+ Parallele Veranstaltung

VDI-Fachtagung IT-Sicherheit für
Kritische Infrastrukturen 2018

+ Fachausstellung

Hören Sie Experten von:



Veranstaltung der VDI Wissensforum GmbH
www.vdi-wissensforum.de/it-security
 Telefon +49 211 6214-201 • Fax +49 211 6214-154

15. und 16. Mai 2018, Dorint Kongresshotel Neuss, bei Düsseldorf

1. Konferenztag Dienstag, 15. Mai 2018

08:15 Registrierung



Gemeinsame Eröffnung: 6. VDI-Fachkonferenz Industrial IT Security 2018 & VDI-Fachtagung IT-Sicherheit für Kritische Infra- strukturen 2018

09:15 Begrüßung und Eröffnung

Frank Winning, Produktmanager, VDI Wissensforum GmbH
Prof. Dr. rer. nat. Michael Waidner, Leiter, Fraunhofer-Institut für Sichere Informationstechnologie SIT, Leiter Sicherheit in der Informationstechnik an der TU Darmstadt, Sprecher des Center for Research in Security and Privacy (CRISP)



Plenarvorträge

09:30 Moderne Cyber Defense Services

- Digitalisierung und Cyber Attacks – Crime follows Business
- Strategie Prevent/Detect/Respond
- Ausrichtung der Cyber Defense in der Telekom Security
- erprobte Kooperationsmodelle

Dr. Rüdiger Peusquens, Vice President Cyber Defense Response, Telekom Security, Bonn

10:15 Die Sicherheit Kritischer Infrastrukturen – Forschung, Praxis und der Weg in die Zukunft

- Zahlen, Daten, Fakten aus den Studien „Monitor IT-Sicherheit für Kritische Infrastrukturen“ 1.0 und 2.0
- Effektivität und Effizienz – IT-Sicherheit implementieren – Ergebnisse der Fallstudienreihe
- Ein Rahmenwerk zu State of the Art Technologien der IT-Sicherheit
- Implikationen für die Innovationsfähigkeit

Prof. Dr. Ulrike Lechner, Professur für Wirtschaftsinformatik, Fakultät für Informatik, Universität der Bundeswehr München

11:00 Kaffeepause mit Besuch der Fachaussstellung

IT-Sicherheit im Spannungsfeld von Industrie 4.0

11:30 Industrie 4.0 Chancen und IT-Security Risiken der Digitalisierung

- Technologiefelder im Mittelpunkt der vernetzten Automatisierung
- Status Quo + die Welt im Wandel – Normen, Verbände und Gesetzgebung
- Lösungsvorschläge aus der Sicht eines Sensorherstellers

Andreas Teuscher, Chief Industrial Security Officer, SICK AG, Waldkirch

12:05 Industrie 4.0 ausprobieren – Aber sicher!

- Konzeption, Entwicklung und Aufbau von vernetzten Sensorknoten zur Datenerfassung für kundenspezifische Anwendungen
- Sichere Vernetzung von eingebetteten Systemen, wie Sensorknoten und Steuergeräte, durch drahtlose und leitungsgebundene Kommunikationssysteme
- Aufbau von sicheren Cloud-basierten Daten- und Steuerungs-lösungen
- Test von Konformität, Performance und Security in dedizierten Testumgebungen und Kundenszenarien

Dr. rer. nat. Daniela Pöhn, Projektleiterin Leistungszentrum Sichere Vernetzte Systeme, Fraunhofer AISEC, Garching bei München

12:40 Mittagsessen mit Besuch der Fachaussstellung

14:00 Entwicklung sicherer Produkte, was ist zu tun? – Nötige Anpassungen in Entwicklungsprozessen

- Nötige Analysen zur Identifikation geeigneter Schutzmaßnahmen
- Angemessene Dokumentation von Schutzkonzepten
- Ergänzende Vorgehensweise im Bereich Testing
- Maßnahmen zum Umgang mit Sicherheitsvorfällen

Dipl.-Inf. Paul Arndt, Leiter Center of Excellence Cyber Security, INVENSITY GmbH, Wiesbaden

Remote- & Fernwartssysteme sicher machen

14:35 Remote-Systeme und IoT-Security – Herausforderungen und Lösungsansätze

- Paradigmenwechsel: Den Wandel erkennen und adressieren
- Die Brennpunkte im Überblick: Anbindung – Daten – Übertragung – Speicherung.

- So geht's: Ein Blick in die Praxis
- Blue Print: Checkliste und Handlungsempfehlung

Dr. Christian J. Pereira, Geschäftsführer, Q-loud GmbH, Köln

15:10 Sichere Netzanbindung kritischer Infrastrukturen nach ISA 62443

- Vorstellung konzeptioneller Lösungsansätze zur sicheren Remote-steuerung industrieller Automatisierungssysteme
- Absicherung von Funktionalitäten wie Dateitransfer und VPN, die anwendungsbedingt sowohl kritische als auch unkritische Netze übergreifen
- Risikoanalyse der Teil- Gesamtsysteme mittels systematischer Bewertung relevanter Bedrohungsszenarien hinsichtlich Kritikalität und Häufigkeit anhand ISA 62443
- Ableitung und Umsetzung von Security Anforderungen im Rahmen von Secure Software Engineering konform zu ISA 62443

Dr. Falk Lindner, Senior Security Engineer, Alexander Winnicki, M.Sc., Security Engineer, Dipl.-Ing. Heiko Fimpel, Team Manager Communication Systems, Silver Atena Electronic Systems Engineering GmbH, Hamburg

15:45 Kaffeepause mit Besuch der Fachaussstellung

16:15 Von Null auf quantensicher – Unser Weg zu Standard und Referenzimplementierung Quantencomputer-resistenter Krypto-Signaturen

- Software-Updates mit sicheren Post-Quantum-Signaturen nach dem XMSS(ˆMT)-Verfahren
- Motivation der Themabearbeitung – der Weg des Forschungsprojekts
- Mögliche Alternativen zum gewählten Verfahren innerhalb der Code-, Gitter- oder Hash-basierten und weiterer Ansätze
- Ergebnisse des Forschungsprojekts zum Thema PQC-Signaturen: Referenzimplementation, IETF RFC und praktische Umsetzung

Stefan-Lukas Gazdag, M. Sc., Research Engineer/Firewall Developer, genua GmbH, Kirchheim bei München

Rollout von IT Sicherheit – Wie geht man voran?

16:50 Integriertes Vorgehensmodell zur Planung und Umsetzung eines Informationssicherheitsmanagementsystems am Beispiel der Pharmaproduktion

- Umsetzung eines Informationssicherheitsmanagement-system (ISMS) für KRITIS Infrastrukturen im pharmazeutischen Produktionsumfeld
- Risikomanagement und Risikobehandlung für Industrial Control Systems (ICS) im GMP-Umfeld
- Integration von Sicherheitsnormen, IT Standards und Best Security Practices Ansätze
- Beispiele und Szenarien unter Anwendung eines computer-gestützten Prozessmodells

Holger Mettler, Leiter Computer System Validation (CSV), M+W Central Europe GmbH, Stuttgart

17:25 Sicherheitskonzeption und Zonierung mithilfe der Vorgehensweise aus der IEC 62443-Standardfamilie

- Kurzer Überblick über die Standardfamilie IEC 62443
- Übersicht von allgemeinen Konzepten
- Ableiten eines Zonenkonzepts am praktischen Beispiel unter Berücksichtigung von ISA 62443-3-2 (Preview)
- Sicherheitskonzeption mit der IEC 62443-3 unter Anwendung von Sicherheitsanforderungen nach Security Level

Andreas Salm, Principal Consultant & Product Manager ICS-Security, HiSolutions AG, Berlin

ab 18:30 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.

2. Konferenztag

Mittwoch, 16. Mai 2018

08:30 Round Tables – Zukunftsdesigner im Dialog

Tisch 1 Veranstaltungsfeedback – Anmerkungen, Wünsche und Verbesserungen

Moderation: Frank Winning, Produktmanager, VDI Wissensforum GmbH, Düsseldorf

Tisch 2 Sensibilisierung von IT-Sicherheit von Mitarbeitern im Unternehmen – Wie nehme ich meine Mitarbeiter mit?

Moderation: Dr. Thomas Lapp, Rechtsanwalt, Fachanwalt für IT-Recht, Vorsitzender NIFIS, Nationale Initiative für Informations- und Internetsicherheit, IT-Kanzlei dr-lapp.de GbR, Frankfurt am Main

Tisch 3 Monitoring und Reaktion auf Anomalien in der Steuerkommunikation

Moderation: Dr. Frank Stummer, Mitgründer & Business Development, Rhebo GmbH, Leipzig

Tisch 4 ISO 27001 - Zertifizierung mit Aussagekraft oder nur Stempel für die Reputation?

Moderation: Hannes Hartung, CEO & IT-Sicherheitsspezialist, TÜV-SÜD zertifizierter Information Security Officer according to ISO/IEC 27000 series, INCREASE YOUR SKILLS, Leipzig

10:15 Kaffeepause mit Besuch der Fachaussstellung

IT-Sicherheit im industriellen Netzwerk

10:45 Absicherung von IoT-Netzwerken durch vertrauenswürdige Geräteidentitäten

- Sichere Prozesse für die Selbstorganisation ermöglichen
- Vertrauenswürdige Identitäten für Maschinen und Geräte kostengünstig erstellen
- Manipulationssicherheit auf Netzwerkebene garantieren mit IOTA Blockchain
- Übergeordnete Kommunikation über https-basiertes OPC UA

Sebastian Rohr, Chief Technology Officer, accessec GmbH, Groß-Bieberau

11:20 Architektur zum sicheren Zugriff auf Profinet-Produktionsnetze

- Praxisbeispiel zur Umsetzung von Fernzugriffen aus Intranet und Internet
- Separation auf allen Protokollebenen durch Kombination von Desktop-Sharing und VPN-Technologien
- Vereinfachtes Anwendermanagement durch Server-basierte Access Control
- Erfahrungen aus Pilotierung und Rollout

Dr.-Ing. Matthias Kabatnik, Entwicklung Digitalisierung und Security, Festo Didactic SE, Denkendorf

11:55 RiskViz: Risikolagebild der industriellen IT-Sicherheit in Deutschland

- Suchmaschine, die industrielle Systeme findet und Informationen zu ihnen und ihrer Bedrohungslage sammelt
- Internetweite Suche zum Aufspüren von ungeschützten Anlagen
- Einsatz im Firmennetzwerk ohne dabei den Betrieb dieser zu stören
- Rechtliche Fragestellungen und Cyber Versicherungen

Matthias Niedermaier, M.Sc., IT-Sicherheitsforscher, Hochschule Augsburg

12:30 Mittagessen mit Besuch der Fachaussstellung

Kosten und Nutzen – Was kostet IT-Sicherheit? Was bringt es an Nutzen?

14:00 Der Preis der IT-Sicherheit und der Unsicherheit

- Wie stehen Kosten und Nutzen für Security im Verhältnis?
- Lässt sich ein Return on Investment ermitteln?
- Prevent – Detect – Response: warum es besser ist, in Vorbeugung zu investieren als in Reaktion
- Gibt es Tools und Techniken in der Zukunft, die für höhere Effizienz sorgen?

Dr. Jürgen Kohr, Chief Operating Officer Central Europe, Fujitsu Technology Solutions GmbH, Düsseldorf

14:35 Notwendigkeit, Kosten und Nutzen von IT-Sicherheit

- Mit welchen Kosten rechnen Unternehmen in der Zukunft? Was bringt es an Nutzen?
- Mit welchen Risiken ist in Unternehmen zu rechnen?
- Inwieweit besteht eine persönliche Haftung von Vorständen/ Geschäftsführern und Mitarbeitern für Schäden?
- Können Versicherungen oder Rechtsformen wie GmbH die persönliche Haftung verhindern?

Dr. Thomas Lapp, Rechtsanwalt, Fachanwalt für IT-Recht, Vorsitzender NIFIS, Nationale Initiative für Informations- und Internetsicherheit, IT-Kanzlei dr-lapp.de GbR, Frankfurt am Main

15:10 Die Frage ist nicht ob man angegriffen wird, sondern was es kosten wird!

- Cyber Sicherheit ist defacto „Cost-of-Business“ – Bedrohungslage früher und heute
- Bedeutung der Business Resilienz im Kontext Industrie 4.0 und die Auswirkung auf die Produktionstechnologie
- Priorisierung von Security Maßnahmen – wie findet man die Balance zwischen Grundschutz und Fort Knox
- Cyber Security als permanente Übung – wie man sie nachhaltig im Produktionsumfeld verankert

Daniel Rüth, Senior Manager OT Cyber Security and Strategy GSA, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft, München

15:45 Zusammenfassung der Konferenz

16:00 Ende der Veranstaltung

Fachausstellung & Sponsoring

Sie möchten Kontakt zu den hochkarätigen Teilnehmern dieser VDI-Fachkonferenz 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 Konferenzgeschehens „Flagge zu zeigen“ und mit Ihren potenziellen Kunden ins Gespräch zu kommen.

Informationen zu Ausstellungsmöglichkeiten und zu individuellen Sponsoringangeboten erhalten Sie von:



Ansprechpartnerin:

Martina Slominski
Projektreferentin Ausstellungen & Sponsoring
Telefon: +49 211 6214-385
E-Mail: slominski@vdi.de



5 gute Gründe, warum Sie die Veranstaltung besuchen sollten

1. Austausch von aktuellen Erfahrungen und Wünschen – Branchen übergreifend.
2. Neue Erkenntnisse zur Reduzierung von Risiken in der Produktion.
3. Erfahren Sie, wie Sie die Produktion von morgen vor Angriffen schützen.
4. Sensibilisierung des Themas Social Engineering – Der Angriff kommt von Innen
5. Best Practices Berichte zum Rollout von IT-Sicherheit sowie den Kosten-Nutzen-Faktor



Parallele Veranstaltung

VDI-Tagung

IT-Sicherheit für Kritische Infrastrukturen 2018

15. und 16. Mai 2018

Besuchen Sie auch kostenlos die Vorträge der parallel stattfindenden Veranstaltung.

Die Top-Themen:

- Umsetzung des IT-Sicherheitsgesetzes – Best Practice
- Datenschutz – DS-GVO und BDSG-neu
- Cybersicherheit in Kritischen Infrastrukturen
- Krisen- und Ereignismanagement – Was tun wenn der Ernstfall eintritt?

Ihre Leitung:

Martin Schallbruch,

Deputy Director of the Digital Society Institute, Senior Researcher Cyber Innovation and Cyber Regulation, ESMT Berlin

Mit u.a. Experten von:

BSI | BERLINER WASSERBETRIEBE | Ernst & Young | INCREASEYOURSKILLS | LKA NRW | MOSAIK | RHEBO | SIDATE | T-SYSTEMS INTERNATIONAL | TÜV Nord | VeSiKi



Weitere interessante Veranstaltungen

6. VDI-Fachkonferenz

Big Data Technologien in der Produktion 2018

15. und 16. Mai 2018, Ettlingen bei Karlsruhe

<https://www.vdi-wissensforum.de/bigdata>

4. Internationale VDI-Fachkonferenz

IT Security for Vehicles

16. und 17. Mai 2018, Düsseldorf

www.vdi-international.com/itsecurityforvehicles

VDI-Spezialtage, Montag, 14. Mai 2018

Zertifizierung nach ISO 270XX – Best-Practices

09:00 bis 17:00 Uhr

Ihre Leitung:



Hannes Hartung, CEO & IT-Sicherheitsspezialist, Increase Your Skills UG, Leipzig

Dr. Frank Stummer, Business Development, Rhebo GmbH, Leipzig

Zielsetzung

Ziel des Spezialtages ist die praxisnahe Vermittlung des notwendigen Wissens und von Erfahrungsbeispielen aus unterschiedlichen Branchen, um die Zertifizierung nach der ISO 270XX-Reihe anzugehen. Dazu wird diese ISO-Reihe in ihrer Bedeutung als ein grundlegender Baustein auch für andere Normen eingeordnet und deren Aufbau einfürend gezeigt. Durch die Besprechung von Best-Practices sollen Stolpersteine vermieden und ein langfristiger Lebenszyklus des Informationssicherheitsmanagementsystems im Unternehmen erreicht werden.

Inhalte des Spezialtages

- Übersicht & Einordnung der ISO 270XX
- Best-Practices in der Einführung eines Informationssicherheitsmanagementsystems
- Best-Practices zur langfristig nachhaltigen Durchführung eines Informationssicherheitsmanagementsystems

IT-Sicherheit in KRITIS + Industrie durch Recht & Normung

09:00 bis 17:00 Uhr

Ihre Leitung:



Dr. Dennis-Kenji Kipker, Wissenschaftlicher Geschäftsführer, Universität Bremen

Dipl.-Ing. Sven Müller, DKE/VDE, Frankfurt am Main

Zielsetzung

Ziel des Spezialtages ist die praxisnahe Vermittlung der wesentlichen regulatorischen Anforderungen für sichere IT-Systeme. Zunächst werden hierzu die aktuellen rechtlichen Vorgaben im Bereich der IT-Sicherheit betrachtet, dies sowohl auf europäischer wie auch auf nationaler Ebene. Anhand konkreter Anwendungsbeispiele soll so auch Fachfremden der Zugang zum Recht eröffnet werden. Des Weiteren stellen die Teilnehmer einen passiven Zugang zum Cyberlaw her – Erklärung der wesentlichen Werkzeuge der juristischen Rechtsanwendung, Auslegung und Systematisierung.

Inhalte des Spezialtages

- Strukturen des IT-Sicherheitsrechts & Grundlagen der Rechtsanwendung
- IT-Sicherheitsrecht an der Schnittstelle zur Technik
- Strukturen und Grundlagen der Normenlandschaft im IT-Sicherheitsbereich
- Normen in den Bereichen Energie, Gesundheitswesen und Industrie 4.0

VDI-Spezialtage, Donnerstag, 17. Mai 2018

Alles neu im Datenschutz? Einführung in DS-GVO und BDSG-neu

09:30 bis 17:00 Uhr

Ihre Leitung:



Prof. Dr. Benedikt Buchner, LL.M. (UCLA); Professor für Bürgerliches Recht an der Universität Bremen, Direktor des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR)

Zielsetzung

Der Spezialtag soll Datenschutz- und IT-Verantwortliche in Unternehmen dabei unterstützen, sich in die neuen datenschutzrechtlichen Rahmenbedingungen einzuarbeiten. Im Fokus stehen die DS-GVO und auf nationaler Ebene das neue BDSG. Den Teilnehmern werden die zentralen Regelungsprinzipien und -inhalte des neuen Rechts vermittelt. Schwerpunktthemen sind dabei die Grundsätze und Rechtmäßigkeit einer Datenverarbeitung, die Betroffenenrechte, der technische Datenschutz sowie die Organisation des Datenschutzes im Betrieb.

Inhalte des Spezialtages

- Das neue Datenschutzrecht – eine erster Überblick
- Grundsätze und Rechtmäßigkeit einer Datenverarbeitung
- Betroffenenrechte, Technischer Datenschutz & Datenschutzorganisation im Betrieb

Cyber War Game – Die Krise als Übung

09:00 bis 17:00 Uhr

Ihre Leitung:



Dr. Sebastian Pape, Senior Researcher, Goethe Universität Frankfurt am Main

Zielsetzung

Cyberattacken betreffen, so die weit verbreitete Vorstellung, nur die Technik und die in ihr integrierten IT-Systeme. Doch beim Social Engineering richten sich die Angriffe über Internet oder Telefon zuallererst auf die zwischenmenschliche Kommunikation, indem versucht wird das Vertrauen eines Mitarbeiters zu gewinnen, um auf diese Weise Zugriff auf sensible Daten zu erhalten. Lernen Sie im Spezialtag auf spielerische Weise einen ganzheitlichen Ansatz zur Abwehr von Social Engineering. Führen Sie anhand des Spiels HATCH Bedrohungsanalysen durch und schöpfen Sie dabei Verbesserungspotenziale für die Sicherheit Ihres Unternehmens aus.

Inhalte des Spezialtages

- Einführung in Social Engineering
- HATCH: Spielrunde Awareness (Virtuelles Szenario)
- Gegenmaßnahmen, Policies und Incident Management
- Bedrohungsanalyse mit HATCH & Ganzheitlicher Ansatz gegen Social Engineering

Sie haben noch Fragen?
Kontaktieren Sie uns einfach!

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
www.vdi-wissensforum.de/it-security

**Nutzen Sie die
Kombibuchung! Sparen
Sie bis zu 200 EURO**

Ich nehme wie folgt teil (zum Preis p. P. zzgl. MwSt.):

| 6. VDI-Fachkonferenz: „Industrial IT Security 2018“ | Bitte wählen Sie unten Ihre Spezialtage aus! | | |
|--|--|---|--|
| <input type="checkbox"/> 15. und 16. Mai 2018, Neuss (02K0704018) | <input type="checkbox"/> pro Spezialtag | <input type="checkbox"/> Kombipreis Konferenz + 1 Spezialtag | <input type="checkbox"/> Kombipreis Konferenz + 2 Spezialtage |
| EUR 1.490,- | EUR 890,- | EUR 2.230,- | EUR 3.070,- |

- VDI-Spezialtag Zertifizierung nach ISO 270XX – Wie gehe ich es an? am 14.05.2018 (02ST171001) oder
- VDI-Spezialtag IT-Sicherheit in KRITIS & Industrie durch Recht & Normung am 14.05.2018 (02ST172001) oder
- VDI-Spezialtag Alles neu im Datenschutz? Einführung in DS-GVO und BDSG-neu am 17.05.2018 (02ST373001) oder
- VDI-Spezialtag Cyber War Game – Die Krise als Übung am 17.05.2018 (02ST374001)

Ich bin VDI-Mitglied und erhalte **pro Veranstaltungstag EUR 50,- Rabatt** auf die Teilnahmegebühr: Mitgliedsnr.* _____
* Für den VDI-Mitglieder-Rabatt ist die Angabe der VDI-Mitgliedsnummer erforderlich.

Ich interessiere mich für **Ausstellungs- und Sponsoringmöglichkeiten**

1111

Meine Kontaktdaten:

Nachname _____ Vorname _____

Titel _____ Funktion/Jobtitel _____ Abteilung/Tätigkeitsbereich _____

Firma/Institut _____

Straße/Postfach _____

PLZ, Ort, Land _____

Telefon _____ Mobil _____ E-Mail _____ Fax _____

Abweichende Rechnungsanschrift _____

Datum _____ Unterschrift _____

Teilnehmer mit einer Rechnungsanschrift außerhalb Deutschlands, Österreichs oder der Schweiz bitten wir, mit Kreditkarte zu zahlen. Bitte melden Sie sich über www.vdi-wissensforum.de an. Auf unserer Webseite werden Ihre Kreditkartendaten verschlüsselt übertragen, um die Sicherheit Ihrer Daten zu gewährleisten.

Die **allgemeinen Geschäftsbedingungen** der VDI Wissensforum GmbH finden Sie im Internet: www.vdi-wissensforum.de/de/agb/

Veranstaltungsort/ Zimmerbuchung

Neuss: Dorint Kongresshotel Düsseldorf Neuss, Selikumer Str. 25, 41460 Neuss, Tel. +49 2131 262-0, E-Mail: info.neuss@dorint.com
Ein Zimmerkontingent ist in den Hotels unter dem Stichwort „VDI“ bis zum 19.03.2018 abrufbar. Bitte beachten Sie, dass dieses begrenzt ist.

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



Leistungen: Im Leistungsumfang der Konferenz (zweitägig) sind die Pausengetränke, das Mittagessen und der Abendimbiss am 15. Mai 2018 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.

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

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 widersprechen.

Nutzen Sie dazu die E-Mail Adresse wissensforum@vdi.de oder eine andere oben angegebene Kontaktmöglichkeit.

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.

