VDI Wissensforum

2. VDI-Fachkonferenz mit Fachausstellung

Industrial IT Security 2014

IT-Sicherheit in Produktions- und Automationssystemen

07. und 08. Mai 2014, Frankfurt a.M.

TOP-THEMEN DER KONFERENZ

- Bedrohungen und Schwachstellen des eigenen Produktionsnetzwerkes erkennen
- Anhand der Richtlinien und Normen die richtigen Tools auswählen und in die Praxis umsetzen
- Mensch und Maschine gegen Angriffe auf die Produktions-IT mit den richtigen Technologien sichern
- Industriespionage und Produktschutz – Konsequenzen für Automatisierung, Prozesstechnik und Produktion
- Tiefgestaffelte Sicherheitskonzepte für komplexe Bedrohungssituationen in Shopfloor, industriellen IT- und Office-Systemen
- Chancen und Risiken der Industrie 4.0 für Ihre Produktionssicherheit
- IT-Sicherheit in der Industrieautomatisierung im Vergleich mit anderen Embedded-Branchen wie z.B. der Automobilindustrie

LEITER DER KONFERENZ

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

TREFFEN SIE EXPERTEN VON

ABB AG • AGT R&D GmbH, AGT International • ENCS – European Network for Cyber Security • ESCRYPT GmbH – Embedded Security • genua Gesellschaft für Netzwerk-und Unix-Administration mbH • ondeso GmbH • Safety Network International e.V. • Siemens AG • Symantec (Deutschland) GmbH • T-Systems GEI GmbH • TÜV SÜD AG – Embedded Systems

+ SPEZIALTAGE

- **Rechtsfragen der IT-Sicherheit in Produktionsumgebungen,** 06. Mai 2014, Frankfurt a.M.
- **IT-Sicherheit in der Industrie – Erste-Hilfe-Kurs gegen Cyberbedrohungen,** 06. Mai 2014, Frankfurt a.M.
- **Industrielle IT-Sicherheit – Gefahren und Schutzmöglichkeiten,** 09. Mai 2014, Frankfurt a.M.

Veranstaltung der VDI Wissensforum GmbH
www.vdi.de/IT-Security
Telefon +49 211 6214-201 | Fax +49 211 6214-154

1. Konferenztag

MITTWOCH
07. MAI 2014

08:45 Anmeldung

09:45 Begrüßung und Eröffnung durch den Konferenzleiter

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

Reale Angriffe aus der virtuellen Welt – Gefahren, Risiken und Konsequenzen von Cyber Threats und Cyber Spionage für Industrie und Gesellschaft

10:00 Status quo der Industrial-IT Security

- Aktuelle Bedrohungslage: ICS Top 10 Bedrohungen 2014
- Ein Blick in die Trickkiste der Angreifer
- Empfehlungen für Hersteller, Integratoren und Betreiber
- Aktuelle Aktivitäten für Bestandsanlagen und Industrie 4.0

Holger Junker, Referatsleiter C12 – Cyber-Sicherheit in kritischen IT-Systemen, Anwendungen und Architekturen, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

10:45 Industrial IT Security – ein Wunsch oder schon Realität?

- Welchen Security Bedrohungen ist die Industrie heute ausgesetzt? War Stuxnet nur der Anfang oder das Ende?
- Wie ist die Position deutscher und internationaler Unternehmen im Vergleich? Welche Maßnahmen und Prozesse sind implementiert?
- Wie weit kann die VDI 2182 bei der Einführung einer Security Lösung helfen? Risikobewertung von Industrial IT

Olaf Mischkovsky, CISSP, CCSK, TSO Technical Specialist, Symantec (Deutschland) GmbH, München

11:30 Von Botnetzen und industrieller Schadsoftware: Risiken erkennen und Gefahren vermeiden

- Gefahren durch Botnetze und Schadsoftware für die Industrie: Risiko, Erkennung und Gegenmaßnahmen
- Herausforderungen für stark vernetzte Industrieanlagen und Produktionssysteme durch automatisierte Angriffe und Industrial Malware
- Early Warning, Intrusion Detection und Industrial Honeypots zum Schutz und zur Überwachung komplexer Automations- und Produktionsanlagen: State-of-the-Art und Erkenntnisse für die Industrie, offene Probleme, Zukunftsausblick

Prof. Dr. rer. nat. Michael Meier, Leiter der Abteilung Cyber Security & Defense bei Fraunhofer FKIE, Wachtberg/Bonn

12:15 Mittagspause und Besuch der Fachausstellung

Industrie 4.0 – IT-Sicherheit als integraler Bestandteil für die Produktion und Automation der Zukunft

13:45 IT Security und Wissensschutz – Auf dem Weg zu Industrie 4.0

- Neue Herausforderungen durch Industrie 4.0
- Security, Safety und Wissensschutz als kritische Erfolgsfaktoren
- Forschungsansätze und Anwendungsszenarien

Prof. Dr.-Ing. Reiner Anderl, Fachgebietsleiter, Fachgebiet Datenverarbeitung in der Konstruktion (DiK), Fachbereich Maschinenbau, Technische Universität Darmstadt

14:30 Ganzheitlicher Sicherheitsbegriff im Kontext Industrie 4.0

- Sicherheit in der Automatisierung gestern und heute
- Automatisierung morgen und übermorgen
- Kommunikation unbegrenzt – Sicherheitsanforderungen unendlich?
- Handlungsfelder für die Zukunft und Aufgaben für die Gegenwart

Dipl.-Ing. Jochen Streib, Vorstand, Safety Network International e.V., Ostfildern

15:15 Kaffeepause und Besuch der Fachausstellung

Spannungsfeld IT-Sicherheit in der industriellen Produktion und kritische Infrastrukturen

15:45 Smart Buildings: Sichere Gebäudeautomation und Gebäudemanagement im Industrieumfeld

- Schwachstellen und sicherer Einsatz von Building Automation Systems (BAS), offene Industriestandards (BACnet, LON)
- Sicherheitsrisiken bei der Integration und dem Zusammenschluss von BAS
- Sichere Integration von Kommunikationsschnittstellen und deren sichere und verlässliche Einbindung in die Gebäude/Anlagen-Infrastruktur
- Zukunft der industriellen Gebäudeautomation, Lösungsansätze sowie Herausforderungen (insb. BAS Wardriving, Covert und Side Channels)

Dr. rer. nat. Steffen Wendzel, Head of Secure Smart Buildings, Cyber Defense Research Group, Fraunhofer FKIE, Bonn

16:30 Protecting Critical Infrastructures against determined aggressors – Challenges and Opportunities

- Which are the challenges that Critical Infrastructures (CI) Operators are facing in protecting their systems?
- What is the current Threatscape and how it evolves
- Is the data the next security perimeter?
- How big data technologies are affecting cyber security for Critical Infrastructures
- How the convergence of Operational, Physical and Cyber Security is redefining the Modus Operandi of CI Operators

Dr. Panayotis Kikiras, Research Director, AGT R&D GmbH, AGT International, Darmstadt
(Vortrag in englischer Sprache)

17:15 Security Challenges and Roadmap for Smart Grid Security

- Where are the special security issues, and where is the difference to "classical" security?
- How is the security of current systems? What are realistic threats and threat actors?
- How do we get to a secure smart grid in an economically viable way?

Dr. Klaus Kursawe, Director Research and Development, ENCS – European Network for Cyber Security, The Hague, Netherlands
(Vortrag in englischer Sprache)

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.

19:15 Dinner Speech: Neue Cyberrisiken für die Industrie

- Eine Vorstellung aktueller Angriffsmodelle, ihrer Taktiken und Strategien
- Wann ist Industrial IT ein Ziel?
- Cyber-Risikomodellierung für Industrieanlagen
- Konzeption einer strategischen Cyber Security für Industrial IT
- Wie lässt sich die Effizienz und Sicherheit von Sicherheitsprodukten messen?

Dr. phil. Sandro Gaycken, Senior Researcher, Fachbereich Mathematik und Informatik, FU Berlin

2. Konferenztag

DONNERSTAG
08. MAI 2014

Identifikation wirkungsvoller Schutzmaßnahmen und Lösungsansätze für Automatisierung und Produktion

08:30 IT Sicherheit – Die Hydra der Produktion

- IT Sicherheit als vielschichtiges Problem – Mensch, Prozesse, Technologie
- IT Sicherheit als kontinuierlicher Prozess – Produktentwicklung, Systemintegration und Betrieb
- IT Sicherheit im regulatorischen Rahmen – Branchenempfehlungen, Normen und Gesetze

Dr. Inf. Ragnar Schierholz, Cyber Security Analyst, ABB AG, Minden

---

09:15 Erfahrungen und Technologien aus anderen Embedded-Branchen für die sichere Industrieautomation nutzen!

- IT-Sicherheit in der Industrieautomatisierung im Vergleich mit anderen Embedded-Branchen wie der Automobilindustrie, der Avionik oder der Medizintechnik
- Mögliche Beschränkungen & Synergien für die sichere Industrieautomatisierung: Was können wir von den anderen Branchen lernen?
- Industrial-Security-Komponenten & Technologien wie Softwareschutz, Hardwaresicherheit, Sichere Kommunikation oder Domainseparation
- Industrial-Security-Entwicklung & Prozesse wie Security-Engineering, Security-Deployment, Lifecycle-Support oder Security-Zertifizierung
- Ausblick: Gemeinsamer Security-Standard? Brauchen wir ein Industrial Security Incident Response Team (ISIRT)?

Dr.-Ing. Marko Wolf, Head of Branch Office Munich, Dr. rer. nat. Frederic Stumpf, Head of Branch Office Stuttgart, B.Sc. Mirko Lange, Senior Security Engineer, München, ESCRYPT GmbH – Embedded Security

---

10:00 Kaffeepause und Besuch der Fachausstellung

Ganzheitliche Strategien zur Abwehr von Angriffen und Betriebssicherheit zum Schutz von Mensch und Maschine

10:30 Innere Härtung als zentrale Komponente der Industrial IT-Security durch Industrial-IT-Management

- Inventarisierung mit organisations- und prozessorientierter Strukturierung
- Sicheres und valides Patch- und Releasemanagement der Industrial IT, einheitliches Systemmanagement
- Multi-Vendor Systemmanagement der Industrial IT Komponenten mit vendorspezifischer Ausprägung
- Implementierung einheitlicher Sicherheitsstandards auf der Grundlage eines Industrial IT Betriebskonzeptes
- Dokumentation aller relevanten LifeCycle Steps der IT-Komponenten

Rolf-Dieter Metka, CEO, ondeso GmbH, Regensburg

11:15 When Safety meets Security!

- Vorstellung der Sicherungsproblematik von Internetverbindungen mittels ICS-Systemen
- Schwierigkeiten von Safetyaussagen aufgrund von nicht klar definierten Einsatzumgebungen und Schnittstellen
- Überforderung klassischer IT-Sicherheitssysteme für die Industrial IT Security
- Potentiale von minimalen Separationssystemen auf Microkern-Basis durch minimale Schnittstellen und definierte Umgebungsmöglichkeiten
- Funktion und Kontext von Separationssystemen im Zusammenhang von Industrie 4.0 und kritischen Infrastrukturen

Dr. rer. nat. Magnus Harlander, Geschäftsführer, genua Gesellschaft für Netzwerk-und Unix-Administration mbH, Kirchheim bei München

---

12:00 Mittagspause und Besuch der Fachausstellung

Von der Norm in die Praxis – Sicherheitslücken von industriellen Produktions- und Automationssystemen erkennen und beseitigen

13:30 IEC 62443 Standard Familie – Hilfe oder neues Ungemach?

- Einführung in den Standard
- Neueste Tendenzen z.B. eine Beschreibung einer Risikoanalyse in Dokument 3-2
- Wie hängen die verschiedenen Dokumente (z.B. die Dokumente 2-1,3-2 und 3-3 für die Security von Anlagenbetreibern) zusammen?
- Wie kann IEC 62443 genutzt werden?

Dr. rer. nat. Thomas Störtkuhl, Product Manager Industrial IT Security, TÜV SÜD AG – Embedded Systems, München

---

14:15 IEC 62443 und VDI 2182: Einsatz in der Praxis

- Rollen und Verantwortungen
- Defense-in-Depth
- Entwicklungsphase und Anlagen-Lebenszyklus
- Risiko-Assessments und Abhängigkeiten

Dr.-Ing. Pierre Kobes, Product and Solution Security Officer, Advanced Technologies and Standards, Siemens AG, Karlsruhe

---

15:00 Sind Daten mehr wert als Waren? – Ein Praxisbericht

- Erfahrungen aus Auditdurchführungen und veränderte Sicherheitsanforderungen
- Aktuelle gefundene Schwachstellen und wie man ihnen begegnen kann
- Der Umgang mit Spannungsfeldern: Kein ROI ohne Risikoabschätzung – Keine Kosteneffizienz ohne Sicherheit – keine Betriebssicherheit ohne Schutz vor Angriffen
- Der weite Weg bis zu Industrie 4.0
- Sicherheit als Prozess aufgefasst

Dipl.-Math. Winfried Stephan, Security Consultant, Security Consulting & Engeneering, T-Systems GEI GmbH, Bonn, Dipl.-Ing. (FH) Volker Zimmer, Security Consultant, T-Systems International GmbH, Darmstadt

---

15:45 Zusammenfassung der Konferenz und Schlusswort

Prof. Dr. Michael Waidner

Ca. 16:00 Ende der Konferenz

KONFERENZLEITER

Prof. Dr. Michael Waidner
Michael Waidner ist seit 2010 Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie (Fraunhofer SIT) und Inhaber des Lehrstuhls für Sicherheit in der Informationstechnik an der Technischen Universität Darmstadt. Zudem ist er verantwortlich für die Kompetenzzentren European Center for Security and Privacy by Design (ECSPRIDE) und das LOEWE Center for Advanced Security Research Darmstadt (CASED). Vorher war er in New York als IBM Distinguished Engineer und Chief Technology Officer for Security verantwortlich für die technische Sicherheitsstrategie und -architektur der IBM Corporation. Von 1994 bis 2006 war er am IBM Zurich Research Lab in Rüschlikon und leitete die Forschung im Bereich der IT Sicherheit und des Datenschutzes und war einer der Initiatoren des Zürich Information Security Centers (ZISC) an der ETH.

Industrial IT Security 2014

07. und 08. Mai 2014, Frankfurt a.M.

GRÜNDE, WARUM SIE DIE VERANSTALTUNG BESUCHEN SOLLTEN

- Schätzen Sie die Risiken von Angriffen auf Ihre Produktion richtig ein und verschaffen Sie sich Kenntnisse über Angreifer, Angriffsmotivation und Angriffsziele
- Informieren Sie sich über die maßgeblichen internationalen Standards, Maßnahmenkataloge und Bewertungsrichtlinien zur IT-Sicherheit
- Erfahren Sie, wie Sie Sicherheitstechnologien und -dienste integrieren können
- Tauschen Sie sich mit anderen Unternehmen aus, wie Sie Ihre Sicherheit optimal managen und integrieren können
- Informieren Sie sich über ganzheitliche Strategien für mehr IT-Sicherheit und aktuellen Methoden des ganzheitlichen Sicherheitsmanagements.

FÜNF FRAGEN, AUF DIE SIE EINE ANTWORT WÄHREND DER VERANSTALTUNG ERHALTEN

- Welche Bedrohungen und Schwachstellen hat Ihr Produktionsnetzwerk?
- Was für Chancen und Risiken biete Industrie 4.0 für Ihre Produktion?
- Was können Normen zur Sicherheit Ihrer Produktions- und Automatisierungsysteme beitragen?
- Wie lässt sich die Effizienz und Sicherheit von Sicherheitsprodukten messen?

VERTIEFEN SIE IHR KNOWHOW DURCH DEN BESUCH EINES SPEZIALTAGES:

- **Rechtsfragen der IT-Sicherheit in Produktionsumgebungen,** 06. Mai 2014, Frankfurt a.M.
- **IT-Sicherheit in der Industrie – Erste-Hilfe-Kurs gegen Cyberbedrohungen,** 09. Mai 2014, Frankfurt a.M.
- **Industrielle IT-Sicherheit – Gefahren und Schutzmöglichkeiten,** 09. Mai 2014, Frankfurt a.M.

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 Sponsoringangeboten erhalten Sie von:

Antonia Schlemmer
Projektreferentin Ausstellung & Sponsoring
Telefon: +49 211 6214-592
E-Mail: schlemmer@vdi.de

Spezialtag

IT-Sicherheit in der Industrie – Erste-Hilfe-Kurs gegen Cyberbedrohungen

Dienstag, 06. Mai 2014

THEMA

Zunehmende Vernetzung, smarte Geräte, Netze & Fabriken, noch smartere Angreifer – die Kampfzone der Cybersicherheit hat sich ausgeweitet. Nicht nur kleinere und mittlere Betreiber von Automatisierungstechnik (ICS) stehen den neuen Herausforderungen oft in einer Mischung aus Unsicherheit und trotziger Zuversicht gegenüber.

ZIELSETZUNG

Dieser eintägige Intensivkurs führt unterhaltsam, aber sehr ernst gemeint in das Thema Cybersicherheit für ICS ein. In einem anschaulichen Minds- und Hands-on-Vorgehen werden wir uns die aktuelle Bedrohungslage und notwendige Heilmittel anschauen. Neben praktischen Demonstrationen finden auch aktuelle Hype-Themen wie Industrie 4.0 ihren Platz und werden gründlich auf ihre Security-Nebenwirkungen abgeklopft. Ausdrücklich erwünscht: Erfahrungen, Fragen und spezielle Interessen der Teilnehmer – frei nach dem Motto „Was Sie schon immer über Cyber* wissen wollten." Da eine Crash-Kurs-Einführung in das Thema Cybersicherheit erfolgt, sind spezielle Vorkenntnisse nicht unbedingt notwendig, jedoch wird aufgrund der Dichte des Stoffs ein Tiefgang erreicht, der auch für Experten genügend neue Ideen, Erkenntnisse und Fragen beinhalten dürfte.

SEMINARLEITER

Dipl.-Math. David Fuhr, CISA, HiSolutions AG, Berlin

David Fuhr studierte Mathematik, Informatik und Politikwissenschaft in Köln und an der FU Berlin. Nach Stationen am Fraunhofer Institut für Software- und Systemtechnik (ISST Berlin, heute FOKUS) und am Fraunhofer Institut für Produktionsanlagen und Konstruktionstechnik (IPK) war er jahrelang als freiberuflicher Softwarearchitekt und Projektleiter im Bereich Web, Datenbanken und Cloud tätig. Seine Expertise als Senior Consultant im Bereich System Security bei der HiSolutions AG umfasst neben dem Sicherheitsmanagement insbesondere die technische Sicherheit von Standard- und Industrial IT in Form von Risikoanalysen, technischen Audits und Penetrationstests sowie Sicherheitsanalysen von Infrastrukturen, Systemen und Protokollen.

SEMINARINHALT

06. Mai 2014, 09:00 bis ca. 16:30 Uhr

Erste Hilfe für ICS
- Incoming! – Die aktuelle Bedrohungslage
- Das Rescue-Pack – Sofortmaßnahmen zum Selbermachen

Vorbeugen ist besser als Heilen: Cybersecurity-Management-Systeme (CSMS)
- One management system to rule them all – Wo fange ich an?
- The nice thing about standards is that you have so many to choose from. (Andrew S. Tanenbaum) – Standards für CSMS
- Wir suchen uns unsere Freuden und Leiden aus, lange bevor wir sie durchleben. (Khalil Gibran) – Welcher Standard taugt für mich?

Praxisblock I: Bin ich schon drin?
- DIY Reconnaissance, oder: Was das Internet über meine Systeme weiß
- Eine gute Schwäche ist besser als eine schlechte Stärke. (Charles Aznavour) – Wie finde ich meine Schwachstellen?

Gestaffelte Verteidigung: Maßnahmen für Cybersicherheit
- Niemand hat die Absicht, eine Firewall zu errichten – Zonen und Kommunikationskanäle
- Pflaster gefällig? – Patchmanagement für ICS
- Impfen? Sport? Vitamine? – Virenschutz im Prozessnetz
- Einmal husten, bitte! – Detektion von Schädlingen und Anomalien
- Nachts sind alle Katzen grau – Blacklisting, Whitelisting, Greylisting
- The code has been subverted (Bruce Schneier) – Sichere Softwareentwicklung für ICS

Praxisblock II: Attacke!
- Praktische Angriffe auf Protokolle, Systeme und Anwendungen

Skandal um ROSI
- Wie sag ich's meinem Management? – Einbindung der Leitungsebene
- Can't buy me love – Wie bekomme ich Budget für Sicherheitsmaßnahmen?
- Von schwarzen Schwänen und weißen Mäusen – Das Leben, das Universum und das ganze Restrisiko

Spezialthemen
- Industrie 4.0
  - » Was bedeutet das wirklich (aus Sicherheitssicht)?
  - » Too much love will kill you – Die wahren Bedrohungen
  - » Hoffnungen, Hausaufgaben, Herausforderungen
- PRISM, Tempora, XKeyscore
  - » Was bedeutet die totale Kommunikationsüberwachung für die Industrie?
  - » Ist Widerstand zwecklos?

5 GRÜNDE, WARUM SIE DAS SEMINAR BESUCHEN SOLLTEN

- Informieren Sie sich über aktuelle Trends, Bedrohungen, Schwachstellen im Bereich der Automatisierungstechnik.
- Erhalten Sie eine realistische Einschätzung der Risikolage für ICS allgemein und für Ihr Unternehmen im Besonderen.
- Erfahren Sie mehr über Notwendigkeit, Effektivität und Wirtschaftlichkeit empfohlener praktischer Maßnahmen wie Zonierung, Patchmanagement, Virenschutz und sicherer Softwareentwicklung.
- Profitieren Sie von unserer Praxiserfahrung aus zahlreichen Sicherheitsanalysen, Audits, Penetrationstests, Forensik- und Incident-Response-Einsätzen in einer Vielzahl von Branchen.
- Erleben Sie praktische Demonstrationen zur Auflockerung und Vertiefung der Inhalte.

Spezialtag

Rechtsfragen der IT-Sicherheit in Produktionsumgebungen

Dienstag, 06. Mai 2014

THEMA

IT-Sicherheitsvorfälle in der (vernetzten) industriellen Produktion können zu Entwicklungen führen, die den Fortbestand des Unternehmens gefährden. Die Absicherung der eigenen Anlagen lohnt, denn es drohen neben Reputationsverlusten auch immense wirtschaftliche Schäden. Themen der IT-Sicherheit rücken deswegen verstärkt in das Blickfeld des Managements.

ZIELSETZUNG

In der jüngsten Vergangenheit hat sich unter Beweis gestellt, dass Produktionsanlagen in Deutschland teilweise erheblichen IT-Sicherheitsrisiken ausgesetzt sind. Die reine Reaktion auf Sicherheitsvorfälle erscheint aus rechtlicher Sicht als ungenügend. Betroffene Unternehmen sehen sich schnell dem Vorwurf der Fahrlässigkeit ausgesetzt. Zu spät getroffene Maßnahmen exponieren jedoch nicht nur das Unternehmen, auch die IT-Verantwortlichen können bei fahrlässigem Handeln zum Ausgleich verpflichtet sein. Für die Zukunft wird deswegen eine wirkungsvollere Herangehensweise gefordert. IT-Security Vorfälle sollten im Idealfall durch präventiv wirkende Maßnahmen bereits im Vorfeld verhindert werden.

Sie lernen in diesem Seminar:

- die rechtlichen Anforderungen an die IT-Sicherheit von Produktionsanlagen
- die rechtlichen Grundsätze der IT-Sicherheit
- die Haftungsgrundsätze bei IT-Sicherheitsvorfällen
- die Informationspflichten bei IT-Sicherheitsvorfällen in der Produktion
- die strafrechtlichen Grenzen bei IT-Sicherheitsanalysen
- das rechtliche Risiko vermindernde Maßnahmen

SEMINARLEITER

Rechtsanwalt Tim Faulhaber, Niedermeier & Faulhaber Rechtsanwaltskanzlei, München

Rechtsanwalt Tim Faulhaber studierte Rechtswissenschaften an der Ludwigs-Maximilians-Universität in München. Er bearbeitet als Rechtsanwalt in München überwiegend Rechtsfragen der IT-Branche. RA Faulhaber war mehrjährig in der IT-Branche als Freiberufler tätig und kann auf ein fundiertes technisches Sachverständnis zurückgreifen. Er beschäftigte sich unter anderem mit der proaktiven IT-Security und der Datensicherheit und implementierte bei Unternehmen der Hochtechnologie IT-Sicherheitskonzepte.

SEMINARINHALT

06. Mai 2014, 09:00 bis 17:00 Uhr

IT-Sicherheit – Pflicht oder Kür?

- Begrüßung und Vorstellung
- Agenda
- Aktuelle rechtliche Beispiele

Rechtliche Grundlagen der IT-Sicherheit

- Grundsätzliche Anforderungen an die IT-Sicherheit
- Organisationsverpflichtung
- Technische, organisatorische, strategische und rechtliche Aspekte

Deutsche und Europäische Vorschriften

- Normenpyramide
- Betriebssicherheit im europarechtlichen Kontext
- Haftungsrisiken
- Internes Kontrollsystem
- Geplantes Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Datenschutz

- Grundlagen
- Technische und organisatorische Maßnahmen
- Auftragsdatenverarbeitung
- Informationspflichten bei DS-Verstößen
- Geplante europäische Datenschutzgrundverordnung

Strafrecht

- Strafrechtliche Grundlagen der IT-Sicherheit
- Strafrechtliche Grenzen der Sicherheitsanalyse

Maßnahmen zur rechtlichen Risikominimierung

- Grundsätzliche Verantwortungsverteilung
- Datenschutzrechtliche Besonderheiten
- Einhaltung von Informationspflichten
- Vertragliche Ausgestaltung

FÜNF FRAGEN, AUF DIE SIE EINE ANTWORT ERHALTEN

- Welche rechtlichen Anforderungen bestehen zur IT-Sicherheit von Produktionsanlagen?
- Wie sieht die Verantwortungsverteilung in Fragen der IT-Sicherheit aus?
- Wodurch kann ein IT-Sicherheitsdefizit zu einem rechtlichen Risiko werden?
- Was darf ich im Rahmen der IT-Sicherheitsanalyse machen?
- Womit kann ich das rechtliche Risiko für mein Unternehmen verringern?

Spezialtag

Industrielle IT-Sicherheit – Gefahren und Schutzmöglichkeiten

Freitag, 09. Mai 2014

THEMA

Durch die steigende Vernetzung stehen sowohl Geräte- und Anlagenhersteller als auch Betreiber vernetzter Automatisierungssysteme vor großen Herausforderungen hinsichtlich IT-Security. Im Seminar wird durch das Aufzeigen der aktuellen Situation vor Augen geführt, wie brisant die momentane Lage ist und dass enormer Handlungsbedarf bezüglich IT-Sicherheit im industriellen Umfeld besteht. Das Bewusstsein der Teilnehmer soll geschärft werden, um das Risiko bestehender Gefahren abschätzen zu können und so angemessen auf die jeweiligen Gegebenheiten zu reagieren.

ZIELSETZUNG

Im Seminar wird gezeigt, wie Industrienetze gegen Cyber-Attacken geschützt werden. Mit den gewonnenen Erkenntnissen sind die Teilnehmer in der Lage, Ausfallzeiten durch mögliche Sicherheitsprobleme in Ethernet-basierten Netzwerken zu vermeiden. Der präsentierte systematische Ansatz hilft bei der deutlichen Steigerung der Funktionalen Sicherheit durch die Verbesserung der Security-Maßnahmen (mit einfachen Mitteln). Dazu wird dem Publikum Schritt für Schritt gezeigt, vorhandene Sicherheitsprobleme zu identifizieren, zu beheben und den erreichten Schutz nachhaltig zu pflegen. Die nötige Theorie hinter den zunehmend komplexeren Problemstellungen wird dabei stets durch praktische Beispiele untermauert.

Ziel des Seminars ist es, sowohl einen Einblick in potentielle Gefahren und Angriffe als auch in mögliche Schutzmaßnahmen zu geben. Dazu soll die Live Demonstration die Verhaltensweise und das Vorgehen von Angreifern näherbringen. Im Anschluss werden basierend auf den gewonnenen Erkenntnissen denkbare Abwehrmechanismen vorgestellt. Dadurch werden im Seminar beide Blickwinkel (Offensive und Defensive) beleuchtet.

FÜNF GUTE GRÜNDE, WARUM SIE DAS SEMINAR BESUCHEN SOLLTEN

- Erfahren Sie mehr über die wesentlichen Unterschiede zur klassischen IT-Security
- Lernen Sie den Sicherheitszustand Ihres Netzwerks zu erfassen
- Verstehen Sie das Vorgehen von Angreifer, um industrielle Netzwerke zu kompromittieren
- Lernen Sie geeigneten Schutzmaßnahmen umzusetzen
- Vermeiden Sie Stillstandszeiten durch mangelhafte Sicherheitskonzepte

SEMINARLEITER

Karl Leidl, M.Sc., wissenschaftlicher Mitarbeiter, Technische Hochschule Deggendorf, Fakultät Elektrotechnik und Medientechnik

Karl Leidl ist wissenschaftlicher Mitarbeiter an der Technischen Hochschule Deggendorf in der Fakultät Elektrotechnik und Medientechnik. Er verfügt über mehrjährige Erfahrung im Bereich IT-Sicherheit aus nationalen Förderprojekten. Sein Fokus liegt dabei auf Trusted Computing und industrielle Netzwerksicherheit. Innerhalb der Projekte werden Maßnahmen entwickelt, um Anomalien in industriellen Netzwerken zu erkennen und die Sicherheit von eingebetteten Systemen zu erhöhen.

SEMINARINHALT

09. Mai 2014, 09:00 bis 17:00 Uhr

Einführung
- Was bedeutet Security im industriellen Umfeld?
- Welche Begriffe sind zu unterscheiden?
- Aufzeigen bekannter Cyberangriffe
- Aktuelle Bedrohungslage für industrielle Netzwerke

Gegenüberstellung von industrieller IT-Sicherheit und klassischer IT-Sicherheit
- Wo liegen die Unterschiede in diesen Bereichen?
- Bedrohungen für Industrie- und Office-IT im Vergleich
- Die wichtigsten Schutzziele in der Industrie (inkl. Ranking)
- Überblick der wichtigsten nationalen und internationalen Standards und Normen (VDI/VDE 2182, ISO/IEC 27000 Serie, IEC 62443, ISA 99, usw.)
- Werkzeuge und Vorgehen zur Erfassung des Ist-Zustandes im Netzwerk

Live Demonstration eines Angriffs
- Auffinden eines angreifbaren Systems über das Internet
- Gezielter Angriff durch die Ausnutzung bekannter Schwachstellen für den initialen Zugang zum Netzwerk
- Vordringen in andere Subnetze durch Aufspüren von Lücken in Firewalls
- Vorführung eines gezielten Denial-of-Service-Angriffs gegen die im industriellen Netzwerk eingesetzten Komponenten
- Manipulation von Daten (z.B. industrielle Steuerung)

Mögliche Schutzmaßnahmen
- Monitoring des Netzwerkverkehrs
- Überwachung industrieller Kommunikationsprotokolle durch geeignete Schutzmaßnahmen (z.B. Deep Packet Inspection)
- Zugriffskontrolle durch geeigneten Fernwartungszugang
- Industrie-Firewalls als Zugriffsschutz für kritische Systeme (z.B. SPS)
- Härtung von Geräten

Gemeinsame Diskussion
- Vertiefung ausgewählter Themen nach Teilnehmerwunsch
- Zusammenfassung und Fazit des Seminars

VDI Wissensforum

INDUSTRIAL IT SECURITY 2014

Ich nehme wie folgt teil:

Bitte Preiskategorie wählen

Preis p./P. zzgl. MwSt.	PS	Spezialtag Rechtsfragen der IT-Sicherheit in Produktionsumgebungen 06.05.2014 (02ST223002)	Spezialtag IT-Sicherheit in der Industrie – Erste-Hilfe-Kurs gegen Cyberbedrohungen 06.05.2014 (02ST264001)	Einzelbuchung VDI-Fachkonferenz Industrial IT Security 2014 07.–08.05.2014 (02KO704014)	Spezialtag Industrielle IT-Sicherheit – Gefahren und Schutzmöglichkeiten 09.05.2014 (02ST265001)	Kombibuchung: Fachkonferenz + 1 Spezialtag	Kombibuchung: Fachkonferenz + 2 Spezialtage
Teilnahmegebühr	1	☐ EUR 890,–	☐ EUR 890,–	☐ EUR 1.390,–	☐ EUR 890,–	☐ EUR 2.180,–	☐ EUR 2.870,–
persönliche VDI-Mitglieder	2	☐ EUR 840,–	☐ EUR 840,–	☐ EUR 1.290,–	☐ EUR 840,–	☐ EUR 2.030,–	☐ EUR 2.770,–
VDI-Mitgliedsnummer*							

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

www

☐ **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

Kartennummer

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
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
Relexa Hotel Frankfurt/Main, Lurgiallee 2, 60439 Frankfurt, Telefon +49 69 957780, Telefax +49 69 95778878, E-Mail:Frankfurt-Main@relexa-hotel.de

Für Sie als Konferenzteilnehmer haben wir im genannten Hotel s.o. Zimmerkontingente reserviert. Bitte reservieren Sie bis zum 16.04.14 unter dem Stichwort „VDI". Bitte nehmen Sie die Reservierung selber direkt im Hotel vor.

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 07. Mai 2014 enthalten. Im Leistungsumfang der Seminare/Zusatztage sind die Pausengetränke und das Mittagessen enthalten. Die Konferenzunterlagen werden den Teilnehmern vor der Veranstaltung via Download zur Verfügung gestellt. Die Seminarunterlagen 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 unvorhersehbaren 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 widersprechen.

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