Fachhochschule
Brandenburg
University of
Applied Sciences

Security Forum X.0

Status und Perspektiven der Sicherheit

21. Januar 2016

Wir danken unseren Partnern und Unterstützern:

EUROPÄISCHE UNION

Europäischer Fonds für
Regionale Entwicklung

THE GERMAN CAPITAL REGION
excellence in ict • media • creative industries

Willkommen zum Security Forum X.0

10 Jahre Sicherheit an der Fachhochschule Brandenburg

In den vergangenen zehn Jahren haben sich Kollegen aller Fachbereiche in verschiedener Weise mit dem Sicherheitsthema befasst. Die erfolgreichen Arbeiten und Projekte auf diesem Gebiet haben „Sicherheit" zu einem der Schwerpunkte im Profil der Hochschule gemacht. Das Security Forum, zu dem wir Sie heute willkommen heißen, trägt den Titel

Status und Perspektiven der Sicherheit.

Welche Perspektiven ergeben sich für die Sicherheitsbranche und die Sicherheitsforschung in den nächsten Jahren?

Zwei Megatrends, die fortschreitende Vernetzung diverser technischer Systeme und der Lebens- und Wirtschaftsbereiche einerseits und die optimierte Auswertung immer größerer Datenbestände (Big Data) andererseits, bergen Chancen und Risiken für die Sicherheit von Unternehmen, Bürgern und Verbrauchern. Diese Umbrüche wollen wir in ihrer technischen, ökonomischen und sozialen Dimension ansprechen - und dabei den Blick aus verschiedenen Perspektiven wagen.

In der Zusammenstellung unserer Vortragenden aus Politik, Wissenschaft und Wirtschaft spiegelt sich dies wider. In der einführenden Keynote wird Dr. Maaßen, Präsident des Bundesamtes für Verfassungsschutz, über das Verhältnis von Freiheit und Sicherheit reflektieren. Die aktuellen Herausforderungen für die Cyber-Außenpolitik wird Karsten Geier aus dem Auswärtigen Amt darstellen. Wolfgang Reibenspies von der EnBW stellt ein zeitgemäßes Informationssicherheitsmanagement in Unternehmen vor.

In den Panels wollen wir zeigen, wie vielschichtig und breit die Fachhochschule Brandenburg mit ihren Partnern aktuelle Themen auf diesem Feld behandelt.

In den Abschlussvorträgen werden die technischen und sozialen Aspekte von Industrie 4.0, vernetzten Automobilen und dem Spannungsverhältnis von Predictive Analytics und der Privatheit thematisiert.

Veranstalter und Unterstützer des Security Forums X.0

Das Security Forum X.0 wird vom Masterstudiengang Security Management zusammen mit den drei Fachbereichen der Hochschule ausgetragen.

Die Sponsoren und Aussteller sind überwiegend langjährige Kooperationspartner des Studiengangs - ohne ihre Unterstützung wäre diese Veranstaltung nicht möglich gewesen.

Wir danken der Zukunftsagentur Brandenburg, die vor Ort ist, um all jene Teilnehmer zusammenzubringen und zu unterstützen, die das Forum für die Akquise neuer Projekte und Partnerschaften nutzen möchten. Dabei wird Sie auch das Zentrum für Gründung und Transfer unterstützen.

Die Referenten der HiSolutions, der KPMG, EASC, der Deloitte Touche und der ICT-Facilities geben interessante Einblicke in aktuelle Projekte und Entwicklungen in der (IT-)Sicherheitsberatung. Insbesondere für Studierende kann sich ein Besuch der Stände dieser potenziellen Arbeitgeber lohnen.

Anwender finden in unserem Ausstellerbereich Lösungen für Sicherheitsprobleme von der Zutrittskontrolle bei Elock2 bis hin zu ganzheitlichen Beratungsangeboten.

Besonderer Dank gilt nicht zuletzt den Studierenden des Masterstudiengangs Security Management, die durch ihr freiwilliges Engagement zum Gelingen der Veranstaltung beitragen.

Wir freuen uns auf einen anregenden Tag mit Ihnen und hoffen, dass Sie viele neue Ideen in Ihren sicheren Arbeitsalltag mitnehmen können.

Fachhochschule
Brandenburg
University of
Applied Sciences

Hier studier’ ich!

Security Management (M.Sc.)

IT-Security und Unternehmenssicherheit. Interdisziplinär, praxisnah, schnell, flexibel und berufsbegleitend zum akkreditierten Master of Science.

Zielgruppe und Studieninhalte

Wer studiert „Security Management (M.Sc.)" an der FH Brandenburg?

Sicherheitsverantwortliche, die eine systematische Managementausbildung suchen, Bachelors mit Informatik-, Technik-, Wirtschafts- oder juristischer Vorbildung. Aber auch Meistern aus Handwerk, Technik oder Verwaltungsberufen steht der Zugang unter bestimmten Bedingungen offen.

Studiert wird meist neben dem Beruf in Blockveranstaltungen. An etwa 30 Wochenenden im Jahr treffen die Studierenden auf hochkarätige Experten, um in einem ganzheitlichen Ansatz praxisnah und sehr zielführend ausgebildet zu werden.

Unternehmenssicherheit benötigt zunächst Managementkompetenz, dann erst eine sichere IT. So werden die Kernfächer

- Security Management
- IT-Sicherheit
- Mathematische und technische Grundlagen
- Recht und Betriebswirtschaftslehre
- Wissenschaftliches Arbeiten

ergänzt durch ein übergreifendes Angebot an Wahlpflichtfächern

- Business Analytics und Privatheit
- Sicherheitsanforderungen an kerntechnische Anlagen
- IT-Sicherheit im BOS Umfeld
- Systemkompetenz und sicherheitsbewusstes Handeln
- Working for Life
- Payment Card Industry Data Security Standard (PCI DSS)
- Informationssicherheitsmanagementsysteme
- Technische Aspekte der IT-Forensik
- Sicherheitsveranstaltungen
- Sicherheit von Rechenzentren
- Risikoanalysen und Risikomanagement
- Cyberwar
- IT-Infrastructure Library (ITIL)
- Know How-Schutz.

Nahezu alle der etwa 25 Dozenten sind hauptberuflich in Unternehmen aktiv, die mit dem Studiengang kooperativ verbunden sind.

Als geradezu außergewöhnlich gut ist das Lernklima zu bezeichnen. Überzeugen Sie sich selbst.

https://www.security-management.de

Programm zum Security Forum X.0

08:30	Einlass		
09:00 - 09:15	Begrüßung Prof. Dr.-Ing. Wieneke-Toutaoui (Präsidentin der Hochschule) Prof. Dr.-Ing. habil. Mieke (Dekan des Fachbereichs Wirtschaft) Dr. Ivo Keller (stellv. Studiendekan Security Management)		
09:15 - 10:00	Keynote „Freiheit ohne Sicherheit - eine Illusion" Dr. Hans-Georg Maaßen (Präsident des Bundesamts für Verfassungsschutz)		
10:00 - 10:45	„Aktuelle Herausforderungen der Cyber-Außenpolitik" Karsten Geier (Koordinierungsstab Cyber-Außenpolitik, Auswärtiges Amt)		
10:45 - 11:00	Kaffeepause		
11:00 - 11:45	„Informationssicherheit heute" Wolfgang Reibenspies (CISO EnBW)		
11:45 - 12:00	Pause, Zeit für Raumwechsel zu den Panels		
Panels	IT-Sicherheitsgesetz und Kritis	Produkt- und Prozesssicherheit	Aufklärung und Forensik
12:00 - 12:20	„Umsetzung des IT-Sicherheitsgesetzes in kleineren KRITIS-Unternehmen" Wilhelm Dolle (KPMG)	„Methoden der technischen Risikoanalyse" Prof. Dr.-Ing. Katharina Löwe (FH Brandenburg)	„Globale Risikoanalyse - Folgerung für die Sicherheitsplanung" Thomas Wandinger (IAP-Dienst)
12:20 - 12:40	„Kritische Infrastrukturen - live gehackt" Prof. Dr. Reiner Creutzburg (FH Brandenburg)	„Prozesssicherheit im Krankenhaus" Prof. Dr. Eberhard Beck / Prof. Dr. Thomas Schrader (FH Brandenburg)	„Organisatorische Aspekte der IT-Forensik" Prof. Dr. Igor Podebrad (Commerzbank)
12:40 - 13:30	Mittagspause - ggf. Zeit für Raumwechsel zwischen den Panels		

Panels	IT-Sicherheitsgesetz und Kritis	Produkt- und Prozesssicherheit	Aufklärung und Forensik
13:30 - 13:50	„Sicherheitsrisiken beim Outsourcing“ Torsten Gründer (GRÜNDER Consulting)	„Security Guideline für Rechenzentrenprojekte“ Ralph Wölpert (ICT-Facilities)	„Herausforderungen an die europäischen Luftsicherheitsforschung“ Prof. Dr. Wolfgang Rehak (EASC)
13:50 - 14:10	„Europäische Sicherheitslösungen“ Guido Gluschke (Institut für Security und Safety)	„Mehr als nur SAP-Security: Segregation of Duties (SoD)“ Alexander Huffer (Deloitte und Touche)	„Datenbanken-Forensik“ Alexander Kornbust (Red-Database-Security)
14:10 - 14: 30	Pause, Zeit für Raumwechsel, Abschlussvorträge im Audimax		
14:30 - 14:55	„Automotive IT-Security“ Prof. Dr.-Ing. Jana Dittmann/ Dr. Sven Kuhlmann (Otto-von-Guericke-Universität Magdeburg)		
14:55 - 15:20	„Sicherheit von Cyberphysical Systems/ Industrie 4.0“ Frank Rustemeyer (HiSolutions)		
15:20 - 15:45	„Predictive Analytics im Spannungsfeld zur Privatheit“ Holger Berens (Kompetenzzentrum Internationale Sicherheit, RFH Köln)		
15:45- 16:10	„Kann man Amokläufe vorhersagen? Nein! Aber vielleicht verhindern.“ Prof. Dr. Herbert Scheithauer (Freie Universität Berlin)		
16:10 - 16:20	Zusammenfassung und Schlusswort		
16:20 - 16:30	Kaffeepause		
Ab 16:30	Verabschiedung von Prof. Dr. Friedrich Holl, im Anschluss Sektempfang und Get-together		

Freiheit ohne Sicherheit - eine Illusion

Nach den jüngsten Terroranschlägen von Istanbul und Paris steht die Frage: „Wieviel Freiheit werden wir für die Sicherheit aufgeben müssen" einmal mehr im Raum. Die Werte Freiheit und Sicherheit stehen offensichtlich in einem Spannungsverhältnis - aber ist der oft angenommene Gegensatz wirklich zutreffend?

Dr. Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz

Dr. Hans-Georg Maaßen wurde 1962 in Mönchengladbach (Nordrhein-Westfalen) geboren. Nach dem Abitur studierte er in Köln und Bonn Rechtswissenschaften. Das Studium schloss er 1987 mit dem ersten juristischen Staatsexamen ab, das anschließende Rechtsreferendariat beendete er 1991 mit dem zweiten juristischen Staatsexamen.
Seit 1991 war er in verschiedenen Abteilungen im Bundesministerium des Innern tätig. Nach Verwendungen als Referent in der Abteilung für Ausländerangelegenheiten und in der Polizeiabteilung wurde er im Jahr 2000 persönlicher Referent des Sicherheitsstaatssekretärs. 2001 übernahm er die Leitung der Projektgruppe Zuwanderung und wurde 2002 zusätzlich Referatsleiter für Ausländerrecht.
Im August 2008 wurde er Leiter des Stabes Terrorismusbekämpfung in der Abteilung Öffentliche Sicherheit im Bundesministerium des Innern.

Seit 1. August 2012 ist Dr. Hans-Georg Maaßen Präsident des Bundesamtes für Verfassungsschutz.

Aktuelle Herausforderungen der Cyber-Außenpolitik

Karsten Geier

Karsten Geier is head of the Cyber Policy Coordination Staff in Germany's Federal Foreign Office and deputy to the Special Commissioner on Cyber Foreign Policy. He is also a member of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.
A career Foreign Service officer, Karsten Geier has held a variety of posts. His most recent overseas assignment took him to New York, where he helped set up the European Union Delegation, and subsequently worked at Germany's Mission to the United Nations. In immer stärkerem Ausmaß werden auch die internationalen Beziehungen durch die Digitalisierung und die zunehmende Vernetzung der Welt bestimmt. Die Cyber-Außenpolitik ist dabei als Querschnittsaufgabe zu verstehen.

Ziele der Cyber-Außenpolitik

Ziel dieser Politik ist es:

- die wirtschaftlichen Chancen des Internets auszubauen,
- universelle Menschenrechte wie den Schutz der Privatsphäre und Meinungs-und Pressefreiheit auch im Internet zu schützen und die freiheitsstiftenden Wirkungen des Internets verantwortungsvoll zu nutzen,
- sowie die Sicherheit des Cyberraums zu gewährleisten und aus der zunehmenden Digitalisierung entstehende Bedrohungen einzudämmen.

Informationssicherheit heute

Security Management X.0

Informationssicherheit ist weit mehr als IT-Sicherheit. Ohne Risikoorientierung wird die Informationssicherheit zum Schrankenwärter. 100% Sicherheit gibt es nicht – es gibt Prozesse, Werkzeuge und Methoden, um die gesamte IKT „beherrschbar" zu gestalten. Das bedeutet am Ende, eine flexible, ganzheitlich integrierte und gesteuerte Informationssicherheit zu gestalten, die sich stetig an die Komplexität und die sich ständig ändernden Vektoren anpasst. Im Mittelpunkt stehen die Menschen – und nicht die Technik. Die Technik liefert, was das Business anfordert. Der Security-Manager 5.0 ist kreativ, selbständig und verantwortlich in gemischten Netzwerken unterwegs. Kein Spezialist – er ist ein Generalist.

„Ich bin sicher, dass ein CISO/ein Security-Manager auch mit „weichen" Fähigkeiten überzeugen muss. Wesentliche Voraussetzungen sind Wertschätzung, Achtsamkeit und Einfühlungsvermögen, gepaart mit einer hohen Authentizität. Aber auch Durchsetzungsfähigkeit mit entsprechendem Durchgriff ist notwendig, wenn es zu einem Security-Vorfall gekommen ist. Hier ist vor allem eine hohe Prozesskompetenz gefragt, die in Notfallsituationen die schnellstmögliche Rückkehr in den Normalbetrieb organisiert und sicherstellt. Informationssicherheit braucht einen Anführer."

Wolfgang Reibenspies

Wolfgang Reibenspies ist CISO und Konzernexperte Informationssicherheit bei der EnBW, der Energie Baden-Württemberg AG. In dieser Funktion ist er verantwortlich für die Sicherheit der Informations- und Kommunikationssicherheit des Gesamtkonzerns.

Das IT-Sicherheitsgesetz in kleineren KRITIS-Unternehmen

Klein, aber kritisch für die Sicherheit

Das IT-Sicherheitsgesetz führt eine Reihe neuer Verpflichtungen für Betreiber Kritischer Infrastrukturen (KRITIS) ein, u.a. den Aufbau von Informationssicherheitsmanagementsystemen oder die Meldung von Vorfällen. In dem Vortrag wird auf die besonderen Umsetzungsschwierigkeiten und Lösungen für die Vielzahl mittelständischer KRITIS-Unternehmen eingegangen.

Wilhelm Dolle

Wilhelm Dolle ist seit Oktober 2011 als Partner Advisory bei der KPMG AG tätig. Zuvor war Herr Dolle bei der HiSolutions AG als Director Security Management. Herr Dolle ist ausgebildeter CISA, CISM, CISSP sowie lizenzierter BSI-Grundschutz-/ISO 27001- sowie BS 25999-Auditor.

Er ist Experte sowohl für technische, als auch organisatorische Aspekte der Informationssicherheit. Dazu gehören Risiko- und Sicherheitsanalysen, der Aufbau von Informationssicherheitsmanagementsystemen bis hin zur Zertifizierungsvorbereitung, aber auch Themen wie Penetrationstests und digitale Forensik. Zudem publiziert er als Autor zahlreiche Artikel in Fachzeitschriften und hat Lehraufträge an verschiedenen Hochschulen inne. Im Sommersemester wird er im „Master Security Management" an der Technischen Hochschule Brandenburg ein Modul zum Penetration Testing anbieten.

Kritische Infrastrukturen - live gehackt

Live-Hacking

Statt durch einen Vortrag wird hier die Verwundbarkeit einer Kritischen Infrastruktur live demonstriert.
Erleben Sie mit, wie zertifizierte Spezialisten Angriffswege, Schwachstellen und Gegenmaßnahmen suchen!

Prof. Dr. Reiner Creutzburg

Reiner Creutzburg studierte Mathematik und Physik an der Universität Rostock und war in Forschung und Lehre an mehreren Hochschulen und Forschungseinrichtungen in Berlin, Karlsruhe und Tampere (Finnland) tätig.

Prof. Creutzburg ist seit der Gründung der Fachhochschule Brandenburg 1992 Professor für angewandte Informatik.

Europäische Sicherheitslösungen

In diesem Vortrag wird Guido Gluschke den Blick über die Grenzen Deutschlands richten und über internationale und europäische Entwicklungen zur Sicherung Kritischer Infrastrukturen im Energiesektor vortragen.

Guido Gluschke

Guido Gluschke is one of the directors of the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences, where he teaches in the field of cyber and nuclear security. Serving also as the university's program manager on international cyber security, he is responsible for joint projects with international organisations. Mr. Gluschke's main areas of expertise are IT and cyber security, especially in the energy context. He holds a Master of Science degree in Security Management from the Brandenburg University of Applied Sciences and a diploma in Computer Science from the Dortmund University of Applied Sciences. Mr. Gluschke is an expert in cyber security in the nuclear context and a member of the Energy Expert Cyber Security Platform - Expert Group of the European Commission Directorate Generale Energy.

„Outsourcing ist eine gute Sache - wenn es gut gemacht wird.“

Sicherheitsrisiken beim Outsourcing

Thorsten Gründer

Zwei von drei Outsourcing-Deals aber erfüllen die gestellten Erwartungen nicht – häufigste Ursachen: Fehlende Erfahrung, überhasteter Abschluss, untaugliche Verträge, Naivität.

Statt Problemlösung entstehen neue Probleme und die IT-Kosten steigen.

Praxisbeispiele zeigen, welche typischen Risiken im Markt bestehen, wie sie erkannt und beherrscht werden können.

Herr Gründer ist Outsourcing-Experte, Fachbuchautor und Hochschuldozent an der Fachhochschule Brandenburg.

Seit fast 20 Jahren berät er Unternehmen bei der Ausgestaltung, Durchführung und Optimierung ihrer IT-Outsourcing-Vorhaben. Mit der GRÜNDER Consulting GmbH etablierte er die erste Outsourcing-Spezialberatung und entwickelte das OMIT-Referenzmodell, eine Projektmanagementmethode zur erfolgreichen Umsetzung von Outsourcing-Projekten.

Methoden der technischen Risikoanalyse

Prof. Dr. Katharina Löwe, Prof. Dr. Thomas Schrader, Prof. Dr. Eberhard Beck, Fachhochschule Brandenburg, Brandenburg an der Havel

Prozesstechnische Anlagen, wie z.B. der chemischen und petrochemischen Industrie, sind durch eine sehr hohe Komplexität sowie ein hohes Gefahrenpotential gekennzeichnet, wobei Unfälle verheerende Konsequenzen haben können. Aus diesem Grund existiert ein umfangreiches Regelwerk für die Genehmigung prozesstechnischer Anlagen.

Für die sicherheitstechnische Bewertung von technischen Anlagen ist eine Vielzahl von Methoden entwickelt worden. Ziel dabei ist, systematisch alle Gefahren, die eintreten können, im Vorfeld zu identifizieren, diese zu bewerten und ereignisverhindernde Maßnahmen abzuleiten.

Schwere Unfälle in der Prozessindustrie erfolgen meist aus einem Zusammenspiel mehrerer verschiedener Fehler und der gleichzeitigen Wechselwirkung mit falschem menschlichen Handeln. Dabei sind diese Fehlhandlungen nicht als Unfallursache anzusehen, sondern sie resultieren aus Fehlern, die in dem System selbst zu finden sind. Aus diesem Grund kann bei der Sicherheitsanalyse die technische Analyse nicht unabhängig von der Betrachtung des Human Factors durchgeführt werden. Um eine Reduzierung der Fehlhandlungen zu erreichen, müssen das Anlagendesign, die Bedienbarkeit und die Arbeitsumgebung an die menschlichen Fähigkeiten angepasst werden.

Dieser Vortrag gibt einen Überblick über die wichtigsten Methoden der Sicherheits-, Risiko- sowie der Human-Factors-Analyse.
Mit dem Ziel, eine Verbesserung der Patientensicherheit in Krankenhäusern zu erreichen, wurde an der Fachhochschule Brandenburg ein interdisziplinäres Forschungsprojekt erfolgreich durchgeführt.

Prof. Dr.-Ing. habil. Katharina Löwe

Katharina Löwe ist Professorin für Energie- und Verfahrenstechnik an der Fachhochschule Brandenburg und Prodekanin Forschung des Fachbereichs Technik. Nach ihrem Studium der Energie- und Verfahrenstechnik an der TU Berlin hat sie auf dem Gebiet der dynamischen Optimierung thermischer Trennprozesse im Fachgebiet Dynamik und Betrieb technischer Anlagen der TU Berlin promoviert.

Während ihrer Promotion sowie ihrer Tätigkeit als wissenschaftliche Mitarbeiterin und Leiterin der Arbeitsgruppe „Thermische Trenntechnik" erlangte sie umfangreiche Erfahrungen auf den Gebieten der Modellierung, Prozessführung und Optimierung verfahrenstechnischer Anlagen. Anschließend war sie Leiterin der Arbeitsgruppe Human Factors am Fachgebiet Anlagen- und Sicherheitstechnik, Beraterin für die Bayer CropScience AG und Projektleiterin verschiedener Forschungsprojekte auf den Gebieten der Sicherheitsanalysen, Sicherheits-Management-Systeme und des Human Factors und hat mit dem Forschungsschwerpunkt „Der Human Factor in der Anlagentechnik" 2008 habilitiert.

Ihre jetzigen Forschungstätigkeiten sind auf den Gebieten der Energieeffizienz, der prozess- und sicherheitstechnischen Optimierung verfahrenstechnischer Anlagen sowie der Entwicklung von Alarmmanagement- und Operatorunterstützungssystemen angesiedelt.

Darüber hinaus ist sie in ein aktuelles, interdisziplinäres Forschungsprojekt im Bereich der Patientensicherheit eingebunden. Seit 2014 ist sie berufenes Mitglied der Kommission für Anlagensicherheit (KAS) beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit zur Beratung der Bundesregierung.

Prozesssicherheit im Krankenhaus

Prof. Dr. Eberhard Beck,
Prof. Dr. Thomas Schrader,
Prof. Dr. Katharina Löwe,
Fachhochschule Brandenburg, Brandenburg an der Havel

Erst als im Jahr 2000 das Buch „To err is human" veröffentlicht wurde, rückte die Bedeutung der Sicherheit von medizinischen Prozessen ins Zentrum der Aufmerksamkeit. Noch 2014 weist die Statistik aus, dass ca. 19.000 Menschen im Rahmen der medizinischen Versorgung durch Fehler in der Diagnostik und/oder Ausführung sterben. Es gibt Schätzungen, die von einer Fehlerrate von 5 bis 10% in medizinischen Prozessen ausgehen, wobei nicht alle einen fatalen Ausgang für die Patientinnen und Patienten aufweisen. Die meisten Fehler werden rechtzeitig erkannt und können korrigiert werden. Bisheriges Risikomanagement im Krankenhaus konzentriert sich darauf, retrospektiv – nach Auftreten eines Fehlers oder eines Schadens – medizinische Prozesse bezüglich der Risiken zu analysieren und daraus Veränderungen abzuleiten. Ein Methodenset für eine prospektive Analyse medizinischer Prozesse gibt es noch nicht.
Im Rahmen des interdisziplinären Forschungsprojektes wurde begonnen, das Wissen aus der Sicherheitsanalyse prozesstechnischer Anlagen in die Medizin zu überführen und nach Gemeinsamkeiten und Unterschieden zu suchen. Dabei gilt es sprachliche, terminologische Probleme zu überwinden.

Mit dem Ziel, eine prospektive Risikoanalyse in medizinischen Umgebungen zu ermöglichen, wurden erste Modelle und Werkzeuge entwickelt. Sie erlauben es, ausgehend von Prozessmodellen, einzelne Aufgaben zu analysieren, sie in den vielfältigen Dimensionen medizinischer Aufgaben zu beschreiben und ein Risikoprofil zu erstellen. Dieses kann verwendet werden, um verschiedene Aufgaben zu vergleichen, kritische Eigenschaften der Aufgaben zu identifizieren und auch die Risiken für einen medizinischen Prozess zu beschreiben.
Die Präsentation gibt zunächst einen Überblick über Sicherheit in medizinischen Prozessen und die Schwierigkeiten der Verständigung über Fachdomänen hinweg. Die Möglichkeiten der Anwendung gehen über die medizinischen Bereiche hinaus.

Security Guidelines für Rechenzentrums-Projekte

Ausgehend von einer Fachplanung eines Rechenzentrums werden die „Lead-to-Sucess" Phasen zur Vor- und Detailplanung von Sicherheitsaspekten sowie verschiedene Umsetzungsprozesse, beginnend bei der Grundlagenermittlung und der Risikoanalyse über die Baustellen-Sicherheit, Business Impacts, Logistik-Vorgänge, Test- und Betriebsprozesse bis hin zum integralen Notfallmanagement vorgestellt. Das Ergebnis ist ein Sicherheitsleitfaden für RZ-Projekte gleich welcher Dimension.

Ralph Wölpert

Ralph Wölpert ist bei ICT-Facilities GmbH für die Vermarktung von IT-Infrastrukturlösungen für Rechenzentren verantwortlich.

2007 wurde Ralph Wölpert eine Lehrtätigkeit an der FH Brandenburg im Masterstudiengang „Security Management" übertragen. 2011 übernahm er eine weitere Dozentur an der FH Aalen (HTW), Fachbereich Informatik. Er lehrt dort ebenfalls „Sicherheit von Rechenzentren".
Im BITKOM ist er Gründungs- und Vorstandsmitglied des Arbeitskreises „Betriebssicheres Rechenzentrum und Infrastruktur" (2005) und seit 2012 dessen Vorsitzender. Seit 2014 ist Ralph Wölpert Jury-Mitglied für die Verleihung des Deutschen Rechenzentrumspreises. Er ist Verfasser und Mitautor verschiedener Publikationen in diesen Fachbereichen und hält nationale und internationale Vorträge zur physischen IT-Sicherheit, Standardisierung von IT-Infrastrukturen, Energieeffizienz, Nachhaltigkeit und Compliance in der IT.

Mehr als nur SAP-Security: Segregation of Duties (SoD)

Alexander Huffer

Alexander Huffer ist Director für Governance, Risk Management und Compliance und leitet den Bereich GRC Technology in Deutschland. Er berät Unternehmen zu Themen wie Design und Redesign von SAP-Berechtigungskonzepten und IT-Applikations-Zugriffsmanagement, Funktionstrennung (SoD) Strategie und Umsetzung, Entwicklung interner Kontrollsysteme und -automatisierung, Implementierung von Sicherheits- und Compliance-Konzepten für IT-Anwendungen sowie IAM-Lösungen.

Nicht oder unzureichend definierte Rechte sind eine häufige Ursache für Sicherheitsvorfälle in Unternehmen. In dem Vortrag wird Alexander Huffer anhand eines Beispiels aus der Beratungspraxis aufzeigen, was bei der Entwicklung eines Rechtekonzepts zu beachten ist.

Globale Risikoanalyse - Folgerungen für die Sicherheitsplanung

General Threat Assessment

Thomas Wandinger wird ein globales Bild der Bedrohungen entwickeln und zeigen, wie diese im Rahmen einer Risikoanalyse in eine Sicherheitsplanung eingehen können.

Thomas M. Wandinger

Thomas M. Wandinger studierte an den Universitäten München und Berlin (FU Berlin) Politik- und Wirtschaftswissenschaften und Neuere Geschichte sowie in Genf Internationale Beziehungen. Er war wissenschaftlicher Mitarbeiter im Bereich „Stabilitätsorientierte Sicherheitspolitik" am Max-Planck-Institut sowie Mitarbeiter am Sonderforschungsvorhaben „SVP III" der Stiftung Wissenschaft und Politik (SWP).

Im Anschluss war er Leiter „Internationale Beziehungen" der Deutschen Aerospace AG (DASA) in München. Seit 1994 ist er Leiter des Institut für Politik und Internationale Studien (IPIS) und seit 2002 Geschäftsführender Gesellschafter der IAP GmbH
Er ist ferner Absolvent der Führungsakademie der Bundeswehr, des „Institute Universitaire des Hautes Etudes" (IUHEI) in Genf sowie des „Joint Services Command and Staff College" (UK). Thomas Wandinger absolvierte zahlreiche Spezialverwendungen und steht als Oberst i.G. (d.R.) seit 2007 in der „Division Schnelle Kräfte" (DSK) ununterbrochen in Kommando- und Führungsfunktion. Im Verlauf von zahlreichen Publikationen und Auslandsaufenthalten sowie durch eine Vielzahl von Radio- und Fernsehbeiträgen zu Fragen der Außen- und Sicherheitspolitik und Terrorabwehr wurde er einem überregionalen Publikum bekannt.

Organisatorische Aspekte der IT-Forensik

In seinem Vortrag beleuchtet Herr Podebrad aktuelle Herausforderungen IT-forensischer Untersuchungen. Hierbei geht er insbesondere auf Fragestellungen im Zusammenhang mit

- gestiegenen gesetzlichen Anforderungen,
- erfolgskritischen Eingangsvoraussetzungen und
- Wirkungshebeln bei IT-forensischen Analysen

ein.

Prof. Dr. Igor Podebrad

Herr Podebrad ist Group Chief Information Security Officer und Bereichsleiter Information Security bei der Commerzbank AG.

In seiner Funktion hat er die globale und unternehmensweite Verantwortung für alle wesentlichen Aufgaben der Informationssicherheit.
Zuvor arbeitete Prof. Dr. Igor Podebrad als IT-Security-Architecture Spezialist in diversen Projekten, gefolgt von Managementpositionen in den Themen IT-Sicherheitsstandards, Bedrohungsanalysen und Forensik sowie Threats Defense.

Er hat einen Lehrauftrag für die Themengebiete "IT-Forensik" und „Cyber Crime" an der Fachhochschule Brandenburg.

Herausforderungen an die europäische Luftsicherheitsforschung

Prof. Dr. Wolfgang Rehak

- 2010 Berufung zum Professor im Department of Electrical Engineering an der Universität New Hampshire
- 2004 Gründung des Netzwerkes „nesis" Eine Initiative dieses Netzwerkes ist die Bildung des europäischen Luftsicherheitszentrums Schönhagen (eascSchönhagen e.V.). Darüber hinaus wurden die Netzwerke von Tunneln und unterirdischen Verkehrsanlagen initiiert.
- 1991 Gründung des Industrieforschungsverein „Optotransmitter Umweltschutz Technologie - OUT e.V." mit weiteren Partnern.

In seinen Vortrag wird Herr Rehak aus verschiedenen laufenden Forschungsprojekten im Bereich der Luftsicherheit berichten. Die inhaltlichen Herausforderungen, die in diesem Bereich beforscht werden, sind z.B. die Integration des Personalmanagements in das Sicherheitsmanagement, Entscheidungshilfen in kaskadierenden Notfallsituationen oder die optimierte Nutzung von RFID und Videotechnik. Nicht zuletzt sind Chancen und Risiken der fortschreitenden Entwicklung unbemannter Flugsysteme zu nennen.

Datenbank-Forensik

Alexander Kornbrust

Alexander Kornbrust ist Gründer und Geschäftsführer der Red-Database-Security GmbH, ein Unternehmen, das sich auf IT-Sicherheit mit dem Schwerpunkt Oracle spezialisiert hat.

Er ist verantwortlich für Oracle-Security-Audits und Oracle-Antihacker-Trainings. Davor war er etliche Jahre bei Oracle Deutschland und Oracle Schweiz sowie bei IBM Global Services, jeweils als Consultant, beschäftigt. Alexander Kornbrust arbeitet mit Oracle-Produkten als DBA und Entwickler seit 1992.

Während der letzten sechs Jahre entdeckte er mehr als 200 Sicherheitslücken in verschiedenen Oracle Produkten wie Datenbank- oder Applikationsservern.

In seinem Vortrag wird Herr Kornbrust auf Angriffsmuster in Datenbanken und deren forensische Spuren eingehen.

Automotive IT-Security

Prof. Dr. Jana Dittmann/ Dr. Sven Kuhlmann, Otto-von-Guericke Universität Magdeburg

Jana Dittmann ist Leiterin des Advanced Multimedia and Security Lab (AMSL) der Otto-von-Guericke Universität Magdeburg mit dem Fokus auf multimediaspezifische Sicherheitsaspekte der IT-Technik, Anwenderinteraktion und -wahrnehmung, aber auch gesellschaftlichen Dimensionen wie Datenschutzaspekte oder die Rechte und Pflichten der Beteiligten. In den Forschungsarbeiten spielen Automotive und IT-Security eine wesentliche Rolle, die auch das Zusammenspiel von Gefährdungen auf Leib und Leben (safety) verdeutlichen sollen. Sie arbeitet zusammen mit Dr. Sven Kuhlmann in Projekten zur Erforschung der Sicherheit im Automobil, wie zum Beispiel Untersuchungen zur elektronischen Manipulationen von Fahrzeug- und Infrastruktursystemen. Ihre Expertise umfasst auch die Analyse von Vorgehensmodellen bei der Aufklärung von Sicherheitsvorfällen und Systematisierung von Schwachstellen. Die Analyse von Sicherheitsaspekten aus der Sicht von Basisangriffen und deren Kombination, die Klassifikation von Angriffsmodellen und Schutzmaßnahmen sowie das Design und die Umsetzung von Werkzeugen spielt in ihrer Forschung eine wesentliche Rolle.

Herr Kuhlmann ist seit 2009 wissenschaftlicher Mitarbeiter bei AMSL im Schwerpunkt Automotive IT Security. Von 2006 bis 2009 war er bei der Volkswagen Konzernforschung tätig und hat an der TU Chemnitz zusammen mit der Universität Bochum zum Thema Human Factors in Automotive Crime and Security promoviert. Er beschäftigt sich neben der Analyse

von IT-Sicherheit im Automobil auf der technischen Ebene auch mit den psychologischen Herausforderungen, die damit einhergehen. Dazu zählen Fragen, wie eine Security-Warnung gestaltet werden sollte, oder wie Fahrer in kritischen Situationen nach IT-Angriffen auf ein Fahrzeug reagieren.

Im Vortrag werden grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen im Automobil zusammengefasst sowie Angriffs- und Schutzziele erläutert. Darauf aufbauend werden ausgewählte Angriffsmethoden und Eigenschaften von automotivem IT-Schadecode dargelegt sowie Praxisbeispiele aufgezeigt, um die Relevanz und den Forschungsbedarf zu verdeutlichen. Am Beispiel werden verschiedene Herausforderungen von Sicherheitskonzepten im Design, Implementierung und Konfiguration angesprochen. Darüber hinaus werden Datenschutzaspekte, wie Verkettbarkeit, Unbeobachtbarkeit, Anonymisierung, Integrität, Transparenz, Wahlfreiheit und der Schutzbedarf des „Berechneten" vor dem Hintergrund multilateraler Interessen verdeutlicht. Abschließend wird Security und Datenschutz auch als Herstellerschutz motiviert.

Sicherheit von Cyberphysical Systems/ Industrie 4.0

Informationstechnologie und Automatisierungstechnik konvergieren in der „Industrie 4.0". An die Stelle von Computern und Maschinen treten „Cyber-Physische Systeme". Davon profitieren viele Beteiligte:

- Anlagenhersteller können sich mit neuen Lösungen profilieren.
- Produzenten können schnell und flexibel fertigen.
- Kunden bekommen maßgeschneiderte Produkte.
- Cyberkriminelle können ganze Fabriken aus der Ferne lahmlegen.

Der Vortrag zeigt typische Sicherheitsrisiken Cyber-Physischer Systeme auf und verdeutlicht den Handlungsbedarf für Betreiber.

Frank Rustemeyer

Frank Rustemeyer leitet bei der HiSolutions AG als Director den Geschäftsbereich „System Security", der die Beratungsleistungen zur technischen Umsetzung von Sicherheit in Informationssystemen bündelt. Neben technischen Risikoanalysen, Audits und Penetrationstests gehört dazu auch das IT-Forensik-Team der HiSolutions, das seit vielen Jahren Kunden im Fall von Cyberangriffen tatkräftig unterstützt. Seit mehreren Jahren ist die Sicherheit von industriellen Steuerungssystemen (ICS) ein Schwerpunkt des Teams.

Frank Rustemeyer hat nach einem Studium der Wirtschaftsinformatik seine Laufbahn zunächst im Bereich IT-Revision begonnen und ist von dort ins Consulting gewechselt. Seit dem Jahr 1999 beschäftigt er sich mit Themenbereichen der Informationssicherheit, wobei seine Schwerpunkte bei Public-Key-Infrastrukturen und IT-Grundschutz liegen. Frank Rustemeyer ist vom BSI zertifizierter Audit-Teamleiter für ISO 27001/IT-Grundschutz und IS-Revisor. An der TU Berlin hat er einen Lehrauftrag zum Thema „Grundlagen des Information Security Management". An der Frankfurt School of Management and Finance unterrichtet er zum Thema „Informationssicherheit und Social Engineering".

Predictive Analytics im Spannungsfeld zur Privatheit

In der datenbasierten unternehmerischen Entscheidungsfindung werden personenbezogene Daten genutzt, um für wichtige Entscheidungen im Unternehmen eine greifbare und bewertbare Grundlage zu schaffen und Probleme zu lösen. Aber nicht alles, was technisch möglich ist, kann rechtlich umgesetzt werden. Anhand von Fallbeispielen werden die Vor- und Nachteile speziell der Human Resources Analytic dargestellt und mit dem bestehenden nationalen und deutschen Rechtsrahmen sowie der aktuellen Rechtsprechung abgewogen und einem rechtssicheren Ergebnis zugeführt.

Holger Berens

Holger Berens ist Studiengangsleiter für Wirtschaftsrecht und Leiter des Studiengangs Compliance und Corporate Security (LL.M.) an der Rheinischen Fachhochschule Köln. Darüber hinaus ist er Leiter des Kompetenzzentrums Internationale Sicherheit der Rheinischen Fachhochschule Köln. Ebenfalls ist er Vorstandsmitglied von ASIS International Germany e.V. und Mitglied verschiedener Gremien im Bereich der Corporate Security.

Seit nunmehr 25 Jahren berät er internationale Unternehmen, aber auch KMU, in allen Bereichen des Compliance und Security Managements und ist Autor entsprechender Fachbücher sowie gefragter Experte der Medien im Bereich Compliance und Security.

Kann man Amokläufe vorhersagen? Nein! Aber vielleicht verhindern.

Network against School Shootings

Die retrospektive Analyse deutscher Fälle von School Shootings hat gezeigt, dass bestimmte Faktoren im Vorfeld einer Tat bei verschiedenen Tätern beobachtet werden konnten. Diese Faktoren sind jedoch so unspezifisch, dass eine Vorhersage einer konkreten Tat nicht möglich ist. Allen Taten ist eine längere krisenhafte Entwicklung vorangegangen, in deren Verlauf die späteren Täter ihre Pläne sowohl durch verbale Äußerungen als auch durch subtile Anzeichen angedeutet haben. Da es sich bei diesen so genannten Leakings um beobachtbare Verhaltensmerkmale handelt, ist eine Möglichkeit der Anwendung von Präventionsstrategien gegeben. In dem Vortrag wird das Programm NETWASS (Networks Against School Shootings) vorgestellt, welches ein systematisches Krisenpräventionsverfahren für Schulen darstellt. Ziel ist es, Lehrpersonal und andere Berufsgruppen darin zu schulen, Leaking zu erkennen, zu beurteilen sowie Hilfestellung geben zu können, um krisenhafte Entwicklungen von Schülern rechtzeitig erkennen und verhindern zu können.

Prof. Dr. Herbert Scheithauer

Herr Scheithauer ist seit 2004 als Professor an der FU Berlin tätig mit den Schwerpunkten Entwicklungspsychologie und Klinische Psychologie Er leitet den Arbeitsbereich Entwicklungswissenschaft und Angewandte Entwicklungspsychologie
Seit 2006 Faculty Member an der International Max Planck Research School "The Life Course: Evolutionary and Ontogenetic Dynamics" am Max Planck Institute for Human Development, Berlin. Seit 2004 beratende Funktion für die Stiftung Deutsches Forum für Kriminalprävention (DFK), seit 2007 in den wissenschaftlichen Beirat des DFK berufen. Erfahrungen in verschiedenen Präventions- und Forschungsprojekten und Beteiligung an der Entwicklung von Präventions- und Fördermaßnahmen. Prof. Dr. Scheithauer verfasste zahlreiche Publikationen im Bereich der Klinischen Kinderpsychologie, Pädagogischen und Entwicklungspsychologie und ist u.a. Editor-in-Chief des International Journal of Developmental Science (www.ijds.net).

Unsere Aussteller

Auf den folgenden Seiten finden Sie eine kurze Darstellung zu den Firmen, die Ihnen in unserem Ausstellerbereich als Ansprechpartner zur Verfügung stehen. Sie finden den Ausstellerbereich im Audimax hinter der Rednerbühne .

- Cluster IKT, Medien und Kreativwirtschaft vertreten durch das Clustermanagement bei der ZukunftsAgentur Brandenburg GmbH
- HiSolutions AG
- Deloitte & Touche
- KPMG
- ELOCK2
- ICT-Facilities

HISOLUTIONS AG

Firmenprofil, Kompetenzen und Erfahrungen

Die HiSolutions AG bietet ein umfassendes Portfolio an Dienstleistungen rund um die Themen Governance, Risk und Compliance (GRC). Dabei vereinen wir strategische Beratungskompetenz mit fundierten methodischen Vorgehensweisen und technischer Expertise. Als inhabergeführtes Unternehmen sind wir frei von Marktinteressen Dritter und erbringen unsere Leistungen mit größtmöglicher Objektivität. Seit unserer Gründung im Jahr 1994 haben wir unsere Leistungsfelder und die Stärke unseres Teams beständig erweitert.

HISOLUTIONS

Unsere Kundenstruktur ist geprägt von großen Unternehmen und Konzernen mit hohen Sicherheitsanforderungen. So gehören mehr als die Hälfte der DAX-Unternehmen, 75 % der deutschen Top-20-Banken und fast alle deutschen Landesbanken zu unseren Kunden.

Im Jahr 2011 erhielt HiSolutions als erstes Unternehmen vom BSI eine Zertifizierung als IT-Sicherheitsdienstleister. Wir arbeiten grundsätzlich nur mit fest angestellten Mitarbeitern zusammen. Die HiSolutions AG hat derzeit ca. 100 Mitarbeiter. Sitz der Gesellschaft ist Berlin.

HISOLUTIONS AG

Firmenprofil, Kompetenzen und Erfahrungen

Das Leistungsportfolio der HiSolutions AG im Bereich Sicherheitsberatung umfasst die folgenden Geschäftsfelder:

- Information Security & IT-Risk Management: Aufbau und Einführung von ISMS, Audits und Zertifizierung, Sicherheitskonzepte und Richtlinien, Security Management Consulting
- System Security: Technische Sicherheitskonzepte und Risikoanalysen, Audits zur Umsetzung von Sicherheit in elektronischen Systemen, Penetrationstests, IT-Forensik und Vorfallsbewältigung
- Business Continuity & Risk Management: Absicherung und Steigerung des kontinuierlichen Geschäftsbetriebs, Durchführung von Audits, Übungen und Tests sowie Schulungen und Sensibilisierungen
- Business Security Management: Aufbau und Optimierung von Unternehmenssicherheitsabteilungen, präventives und reaktives Krisenmanagement/ präventiver und reaktiver Krisenkommunikation

Zu allen unseren Kompetenzfeldern bieten wir auch kundenspezifische Schulungen und Seminare an.

ZAB
ZukunftsAgentur
Brandenburg

Cluster IKT, Medien und Kreativwirtschaft Berlin-Brandenburg

Berlin-Brandenburg gehört zu den führenden Standtorten der Informations- und Kommunikationstechnologie in Deutschland. Mittlerweile sind in den über 7.000 Unternehmen der Branche mehr als 63.000 hochqualifizierte Fachkräfte tätig.

Das länderübergreifende Cluster IKT, Medien und Kreativwirtschaft Berlin-Brandenburg umfasst Wirtschaft, Wissenschaft und Netzwerke in der deutschen Hauptstadtregion und fördert die Sichtbarkeit und Entwicklung der digitalen Wirtschaft in Berlin-Brandenburg.

Mit seinen über 300 Unternehmen in der Sicherheitswirtschaft, davon etwa die Hälfte im Bereich IT-Sicherheit, liegt ein inhaltlicher Schwerpunkt mit hoher Querschnittsrelevanz für alle Branchen in der Hauptstadtregion.

In vom Clustermanagement gesteuerten Arbeitsgruppen wird, auch im Bereich Sicherheit, eine Vielzahl von neuen Projekten von und zwischen den Clusterakteuren entwickelt.

Das Berlin-Brandenburger Cluster IKT, Medien und Kreativwirtschaft ist organisatorisch durch das Clustermanagement in der ZAB ZukunftsAgentur Brandenburg GmbH vertreten.

Kontakt:

Dennis Bohne, T. +49 331 660 3828, dennis.bohne@zab-brandenburg.de

EUROPÄISCHE UNION

Europäischer Fonds für
Regionale Entwicklung

THE GERMAN CAPITAL REGION
excellence in ict • media • creative industries

KPMG: Globales Know-how für Unternehmen vor Ort
KPMG ist ein Firmennetzwerk mit mehr als 162.000 Mitarbeitern in 155 Ländern. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen. Unser Ziel: eine komplexe Welt für Unternehmen verständlicher machen. Unser Anspruch: den weltweit besten Service zu bieten. Unser Handwerkszeug: Qualität, Innovation und Leidenschaft. Unser fundiertes Fach- und Branchenwissen gibt unseren Kunden Sicherheit. Sicherheit, die sie brauchen, um ihre Ziele zu verwirklichen. Unsere Experten zeigen Unternehmen geschäftliche Chancen auf und helfen ihnen, Entwicklungen mitzubestimmen und ihre Wachstumsziele zu erreichen.

Im Blickpunkt: Der Bereich Security Consulting von KPMG
Weltweit arbeiten über 2000 Sicherheitsexperten des KPMG-Netzwerks – davon mehr als 100 in Deutschland – an Lösungen und Konzepten, mit denen sich Unternehmen und Organisationen gegen Cyber-Angriffe und Sicherheitsbedrohungen schützen können.

Unsere Experten begleiten Sie umfassend: von der Entwicklung und Umsetzung Ihrer Sicherheitsstrategie über den Aufbau Ihrer Sicherheitsorganisation bis hin zur Auswahl, Implementierung und Konfiguration geeigneter technischer Tools und Sicherheitskomponenten. Mithilfe eigener Cyber Defense und Security Labs testen wir die Wirksamkeit von Maßnahmen zum Schutz Ihrer kritischen Infrastruktur, Industrieanlagen und Informationswerte. Darauf aufbauend entwickeln wir mit Ihnen Sicherheitslösungen, die individuell auf die Gefahren für Ihr Unternehmen ausgerichtet sind.

Unsere Teams stehen für Sie bereit. Sprechen Sie uns an!
www.kpmg.de/cybersecurity

ICT Facilities GmbH wurde im Jahr 2015 von einer Gruppe von erfahrenen Ingenieuren und Architekten gegründet und hat sich auf die Planung und die Realisierung von Rechenzentren spezialisiert.

Alle Mitarbeiter unseres Unternehmens verfügen über langjährige Führungskompetenz in der Umsetzung von Großprojekten in diesem speziellen Marktsegment. Wir verfügen über einen Erfahrungsschatz von der frühen Beratungsleistung, über die Rolle des Hauptauftragnehmers (General contractor) bis zur Vermittlung der gesamten Projektfinanzierung.

Unser wachsendes Team von Projektmanagern, Senior-Experten und Entwicklern hat tiefgreifende Berufserfahrung im Projektmanagement und im Bau von Rechenzentren.

Deloitte.

Making an impact that matters. Unser Anspruch ist, jeden Tag das zu tun, was wirklich zählt – für Kunden, unsere Mitarbeiter und die Gesellschaft. Mit unserem breiten Leistungsspektrum - von Wirtschaftsprüfung über Tax & Legal bis Corporate Finance und Consulting - unterstützen wir Kunden auf einzigartige Weise: Wir liefern innovative Denkansätze, lösen komplexe Herausforderungen und ermöglichen nachhaltiges Wachstum. Wir bieten unseren hochqualifizierten Mitarbeitern ein inspirierendes Umfeld, in dem sie für Kunden echten Mehrwert schaffen, wir fördern außergewöhnliche Berufserfahrungen und Karrierechancen sowie eine integrative und gemeinschaftliche Kultur. Wir leisten einen Beitrag für die Gesellschaft – wir stärken Vertrauen und Zuversicht in die Märkte, wahren die Integrität von Organisationen und engagieren uns für die Gemeinschaft.

ELOCK2

Zutrittskontrolle, Mobile Datenerfassung, NFC-Anwendungen und digitale Sicherheitstechnik - wir von ELOCK2 bieten Lösungen, die bereits seit Jahren marktreif, praxiserprobt und bei Kunden im Alltagsbetrieb sind, an. Mit unserer umfassenden ELOCK2-Access-Control Produktpalette sind wir Experten in der Sicherheitstechnik. Einzigartige Mechanik, Hardware für alle Türen - und das bei kabelloser Montage.