OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

TeleTrusT
Pioneers in IT security.

Gemeinsame Arbeitskonferenz: GI | OCG | TeleTrusT

D·A·CH Security

Alpen-Adria-Universität Klagenfurt
26. und 27. September 2016

Aktuelle Informationen: http://www.syssec.at/dachsecurity2016

syssec
Alpen-Adria-Universität Klagenfurt
System Security Group

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

HISOLUTIONS

itsa 2016
Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Montag • 26. September 2016

08.30 Uhr **Registrierung, Kaffee und Tee**

08.55 Uhr **Begrüßung und Überblick**

Security Management • Leitung: K.-O. Detken — A

09.00 Uhr **Open-Source-SIEM im Eigenbau**

D. Mahrenholz
R. Schumann
rt-solutions.de GmbH

- Event Logging und Monitoring ist unverzichtbar für die IT-Security
- Kommerzielle Lösungen sind für Unternehmen oft zu teuer und komplex
- Für spezielle Anforderungen existieren teilweise gar keine Lösungen
- Ein Eigenbau mit Open-Source-Komponenten kann eine Alternative sein
- Möglichkeiten/Grenzen und Kosten/Nutzen sind vorab abzuwägen

09.30 Uhr **Prozessorientierte IT-Sicherheitsanalyse**

D. Simic-Draws
Universität Koblenz

- Herausforderungen bei der klassischen IT-Sicherheitsanalyse
- Differenzierte Berücksichtigung des Faktors Mensch
- Prozesse zur Abgrenzung von Organisation, Technik und Recht
- Sicherheitsoptimierung von Prozessen in sechs Schritten
- ProSA als Schnittstelle zwischen Fachabteilungen

10.00 Uhr **Anforderungen an eine IT-Lösung für den ISO27-Sicherheitsprozess**

M. Hofmann
A. Hofmann
CISO27

- Informationssicherheitsmanagement nach ISO/IEC 27001 nativ
- ISMS-Betrieb auf Basis des ISO27-Sicherheitsprozesses
- Literaturanalyse zu konkreten ISMS-Aufgaben und methodischen Hinweisen
- Anforderungen an ein ISO 27001 ISMS-Tool
- Forschungsausblick: Konzeption der IT-Lösung CISO27-Suite

10.30 Uhr **Kommunikationspause**

Schwachstellen & Angriffe • Leitung: K. Knorr — A

11.00 Uhr **Schwachstellen in SAML 2.0 Implementationen**

R. Bischofberger
E. Duss
Compass Security Schweiz AG

- SAML ist eine verbreitete Single Sign-On Technologie
- Den SAML Standard zu implementieren ist komplex
- Schwachstellen in der Signatur- und Zertifikatsvalidierung
- Eigenentwickeltes Tool, um SAML Service Provider einfach zu testen
- Empfehlungen bezüglich der Sicherheit von SAML Implementationen

11.30 Uhr **Sicherheit von ausgewählten OpenSource-SDN-Controllern**

J. Sell
FH Dortmund
E. Eren
HS Bremen

- SDN-Controller als Single-Point-of-Failure in SDN-Netzwerken
- Überprüfung von SDN-Controllern auf ihre Sicherheit
- Betrachtung von verschiedenen Controllern
- Floodlight und Opendaylight
- Möglichkeiten der Absicherung

12.00 Uhr **Angriff auf verschlüsselte Linux System-Partitionen**

T. Köhler
HS Darmstadt
A. Dörsam
Antago GmbH

- Angreifbarkeit des Linux Boot-Prozesses
- Informationsabfluss durch einmaligen Zugriff
- Evidence Injection auf verschlüsselten Linux System-Partitionen
- Keine angemessenen Schutzmechanismen
- Live-Demo des Angriffs

Montag • 26. September 2016

Netzwerk / Web-Sicherheit • Leitung: D. Mahrenholz — B

11.00 Uhr **Sehen heißt glauben: Aufdeckung von Webseiten Manipulation** — **T. Urban**
- Lernen des strukturellen Aufbaus einer Webseite — **N. Pohlmann**
- Erkennen von Webseiten Manipulation durch kollektive Intelligenz — Institut für Internet-
- Clustering von Webseiten — Sicherheit – if(is)
- Identifizierung von eingefügten HTML-Tags durch Malware
- Aufbau eines repräsentativen Webseiten Datensets

11.30 Uhr **Ordnungserhaltende Verschlüsselung in Cloud-Datenbanken** — **T. Waage**
- Der Wunsch nach Datenverwaltung durch Cloud-Datenbanken steigt — **L. Wiese**
- Konkurrierend: Sicherheitsgarantien vs. effiziente Datenverwaltung — Universität
- Eigenschaftsbewahrende Verschlüsselungsverfahren benötigt — Göttingen
- Insbesondere ordnungsbewahrende Verschlüsselung für Range Queries
- Modifikationen, Implementation und Benchmarks

12.00 Uhr **Reputation und Threat Information als Ergänzung zu Blacklists** — **I. Schiering**
- Risiko-Bewertung von Domains im Unternehmen — **J. Ohms**
- Untersuchung von Quellen, die aggregierte Informationen bieten — **P. Wentscher**
- Threat Intelligence Management Plattformen — Ostfalia HAW
- Kollaborative Web Reputation Systeme — **R. Kaltefleiter**
- Vergleich der beiden Ansätze und Prüfung des Einsatzes — NetUSE AG

12.30 Uhr **Gemeinsame Mittagspause**

Mobile Security • Leitung: W. Kühnhauser — A

14.00 Uhr **Verteilung von Benutzerzertifikaten auf Mobilgeräte** — **G. Jacobson**
- Ende-zu-Ende Verschlüsselung auf allen Geräten des Benutzers — Secardeo GmbH
- Benutzerkomfortable Nutzung von S/MIME auf Mobile Devices
- Automatisierte Verteilung von Zertifikaten und privaten Schlüsseln
- Sichere Schlüsselverteilung auf iOS im Apple MDM Protokoll
- Globaler Abruf von Partnerzertifikaten mit ActiveSync Proxy

14.30 Uhr **Instant-Messaging – Bedrohungen und Sicherungsmaßnahmen** — **P. Hartung**
- Sicherheit bei Instant-Messaging-Diensten wird immer wichtiger — **D. Fischer**
- Bedrohungsanalyse bei mobilen Instant-Messaging-Diensten — TU Ilmenau
- Erstellung eines Katalogs typischer Bedrohungen/Angriffe
- Vorschlag von Sicherungsmaßnahmen für Dienstanbieter und -nutzer
- Analyse ausgewählter Instant-Messaging-Dienste

15.00 Uhr **IT-forensische Erkennung modifizierter Android-Apps** — **H. Höfken, S. Becker**
- Erstellung einer Datenbank mit Informationen einer Original-App — **M. Schuba**
- Automatische Erkennung von Apps (Name, Version, Ersteller, ...) — FH Aachen
- Analyse der App-Berechtigungen — **P. Schütz**
- Statische Auswertung von weiteren App-Informationen (Bild, Video, Audio) — Landeskriminalamt
- Automatische Erkennung von Abweichungen von der Original-App — NRW

Montag • 26. September 2016

Studentische Abschlussarbeiten • Leitung: S. Schauer — B

14.00 Uhr **Betriebssystem-Sicherheitspolitiken formal analysieren** — **M. Rabe**, TU Ilmenau
- Die Korrektheit von Sicherheitspolitiken muss garantiert werden
- Eine formale Analyse ist dafür geeignet
- Die Sicherheitspolitik in ein formales Modell übertragen
- Die formalen Analyseergebnisse zurückübertragen
- Wie das geht und was dabei zu beachten ist

14.30 Uhr **Mindestanforderungen an das Incident Management in KMUs** — **S. Großmann**, Hochschule Furtwangen
- Information Security Incident Management (ISIM)
- Behandlung von Informationssicherheitsvorfällen
- Klein- und mittelständische Unternehmen
- Incident Management als Prozess
- Maßnahmenkatalog zum ISIM

15.00 Uhr **Entwicklung einer Android NFC-Signaturkarte** — **T. Uebel**, Hochschule Bonn-Rhein-Sieg
- Sicherheitsarchitektur und Schlüsselverwaltung unter Android
- Hardwaregestützte Speicherung von Schlüsselmaterial
- Drahtlose Kommunikation und Kartenemulation
- Verbesserung der Sicherheit durch erweiterte Benutzerinteraktion
- Sicherheitsbetrachtung der Implementierung

15.30 Uhr Kommunikationspause

Risikomanagement • Leitung: P. Schartner — A

16.00 Uhr **Ein Meta-Risiko-Datenmodell für IKT** — **M. Latzenhofer**, AIT
- Es werden unterschiedlichste Risikomodelle für IKT angewendet
- Praxis: Mangelnde Vergleichbarkeit, restriktive Organisationsgrenzen
- Kann ein Metamodell für IKT-Risikomanagement hier Abhilfe schaffen?
- Metamodellierungsansatz dargestellt als UML-Klassendiagramm
- Initiales Meta-Datenmodell, Testlauf mit COBIT for Risk-Integration

16.30 Uhr **Spieltheoretische Risikominimierung in IKT-Infrastrukturen** — **S. Schauer**, **S. König**, **M. Latzenhofer**, AIT, **S. Rass**, AAU Klagenfurt
- Einsatz von Spieltheorie unter Betrachtung von Unsicherheiten
- Verwendung von empirischen Verteilungen als Payoffs
- Identifikation einer optimalen Verteidigungsstrategie
- Einbindung von qualitativen Experten-Einschätzungen
- Einbindung von Schwachstellen-Informationen aus öffentlichen Quellen

17.00 Uhr **Risikobasierte Metapolitiken für spontane Kooperationen** — **M. Schlegel**, TU Ilmenau
- Vertrauliche Daten auf mobilen Geräten
- Zugriffsschutz durch risiko-adaptive Sicherheitspolitiken
- Spontane Kooperationen und Interaktionen mobiler Systeme
- Lösung von Politikkonflikten durch Metapolitiken
- Implementierung auf Android/MOSES-Plattformen

ACS-Workshop • Leitung: I. Münch — B

16.00 Uhr **IT-Sicherheitsanalysen von PLM-Systemen** — **K. Weber**, **M. Janik**, FHWS
- Informationssicherheit in der Automobilbranche
- Konzept zur Untersuchung produktiver PLM-Systeme auf Schwachstellen
- Common Criteria, OWASP – Testing Guide, IT-Grundschutz
- Prüfung von Richtlinien, Prüfung von Eigenentwicklungen, Penetrationstests
- Anwendungsbeispiel: Automobilzulieferer mit webbasiertem PLM-System

16.45 Uhr **Moderne Beschaffung mit Berücksichtigung von IT Security** — **E. Piller**, **G. Österreicher**, **G. Pötzelsberger**, FH St. Pölten
- Plattform zur Unterstützung der Beschaffung sicherer IT-Produkte
- Anforderungskataloge für IT-Sicherheit bei SW- und HW-Komponenten
- Schutzbedarfsklassifikation abhängig vom Anwendungsbereich
- Information über Sicherheitsvorfälle von Produkten
- Produkteintragung von Herstellern zur Schaffung von Transparenz

17.30 Uhr Ende erster Konferenztag • **19.30 Uhr** Gemeinsames Abendessen

Dienstag • 27. September 2016

Privacy & Anonymität • Leitung: S. Schwalm — A

09.00 Uhr **Privacy in sozialen Netzwerken**
- Verborgene Informationsflüsse in sozialen Online-Netzwerken
- Schwächen der Zugriffssteuerungssysteme
- Aufdeckung der Schwächen durch Informationsflussanalyse
- Ernüchternde Ergebnisse der Informationsflussanalyse
- Transparenz von Informationsflüssen durch Live Monitoring

P. Amthor
W. Kühnhauser
TU Ilmenau

09.30 Uhr **AnonDrop – Räumlich begrenzte anonyme Informationsverbreitung**
- Nichtdemokratische Staaten filtern oft die Internetkommunikation
- Vorstellung von AnonDrop als alternatives Kommunikationssystem
- Besonderer Fokus auf Teilnehmeranonymität
- Mögliche Angriffe und Schutzmaßnahmen
- Ergebnisse von Experimenten, auf Basis von einem Prototyp

A. Zeier
A. Heinemann
Hochschule Darmstadt

10.00 Uhr **Security- und Privacy Benchmarking IEC 62443-4-2**
- Entwicklung resilienter industrieller Automations- und Kontroll-Anlagen
- Vorläufig jüngster Teil der Norm IEC 62443-4-2 für IAC-System-Sicherheit
- ETSI ISG ISI Indikatorklassen für Sicherheit industrieller Produktionsanlagen
- Use Case: Identifikations- und Authentizitätskontrolle
- Benchmark des Foundation Requirements, Timely Response to an Event

J. B. de Meer
smartspacelab.eu GmbH
K. Waedt
AREVA GmbH

SECMGT WORKSHOP • Leitung: I. Münch — B

09.00 Uhr **Security Management as a Service**
- Die Öffentliche Verwaltung gehört zu den kritischen Infrastrukturen
- Ressourcen zur Umsetzung von IT-Sicherheit fehlen
- Neuartiges Vorgehen zum Etablieren eines ISMS
- Variable Gestaltung des IT-Verbunds durch skalierbare Auslagerung
- Cloud-basierte, benutzerzentrierte Schutzmaßnahmen

F. Otterbein
F. Kern
A. Heinemann
M. Margraf
S. Lange
Hochschule Darmstadt

09.45 Uhr **Anwendung von IT-Grundschutz bei einem TK-Dienstleister**
- Motivation zur Anwendung des IT-Grundschutzes in einem NMC
- Beherrschung als Prinzip zur Abgrenzung des IT/Informationsverbundes (IV)
- Betrachtung der Schnittstellen des IV nach dessen Abgrenzung
- Informationsflüsse und Schnittstellenübergänge des IV
- Betrachtung von Risiken, die von außen auf den beherrschten IV wirken

T. Milde
T-Systems International GmbH
W. Böhmer
TU Darmstadt

10.30 Uhr Kommunikationspause

Dienstag • 27. September 2016

Smart Grids & Smart Metering • Leitung: P. Horster — A

11.00 Uhr **Eine Architektur für sichere Smart Grids in Österreich** — **O. Jung, A. Hudic**
- Smart Grids sollen helfen, die Energiewende voranzubringen — AIT
- Interoperabilität und Sicherheit sind wichtige Kriterien — **S. Fenz**
- Konsolidierung nationaler und internationaler Modelle — SBA Research
- Digitales Modell bietet Schnittstellen für Sicherheitskomponenten — **M. Kammerstetter**
- Verifizierung der Anwendbarkeit durch Implementierung von Use Cases — TU Wien

11.30 Uhr **Integration von TNC in ein deutsches Smart Meter Gateway** — **C.-H. Genzel**, **O. Hoffmann**, **R. Sethmann**, Hochschule Bremen
- Architektur eines intelligenten Messsystems in Deutschland
- Sicherheitskonzept für das Smart Meter Gateway (SMGW)
- Nachweis der Integrität eines SMGW mit Trusted Network Connect (TNC)
- Praktische Implementierung von TNC in einem intelligenten Messsystem
- Herausforderungen bei der Integration von TNC in ein SMGW

12.00 Uhr **Integritätsmessung von Smart Meter Gateways** — **K.-O. Detken**, **M. Jahnke**, **M. Humann**, DECOIT GmbH
- Einführung in die Sicherheitsarchitektur von Smart Meters
- Vorstellung des BMWi-Projekts SPIDER
- Integritätskonzept mit Trusted Computing
- Smart Meter Gateway: vom F&E-Prototypen zum Produkt
- Testbed-Ergebnisse

Sichere Anwendungen • Leitung: S. Rass — B

11.00 Uhr **Technische Richtlinie – Sicherer E-Mail-Transport** — **F. Bierhoff**, **T. Gilles**, BSI
- Höhere E-Mail-Sicherheit ohne Einbußen für die Nutzerfreundlichkeit
- Kombination praxiserprobter Standards in einer offenen Infrastruktur
- Obligatorische Verschlüsselung durch DANE/TLSA
- Standardisierte Vertrauensanker und zeitgemäße Kryptographie
- Transparenz durch Prüfverfahren und Zertifizierung

11.30 Uhr **Automatisierte Erkennung von Sicherheitslücken mit CVE, CPE und NVD** — **K. Knorr**, Hochschule Trier
- Automatisierte Erkennung von bekannten Sicherheitslücken
- Betrachtung geeigneter Standards wie CVE, CPE und CVSS — **M. Scherf**, Universität Trier
- Herausforderungen bei der Nutzung der National Vulnerability Database
- Zunehmende Kommerzialisierung von Sicherheitslücken — **M. Ifland**, Siemens
- Software Vulnerability Tool

12.00 Uhr **Ein rekursiv approximatives Vorgehensmodell** — **A. Lunkeit**, OpenLimit SignCubes GmbH
- Vorgehensmodelle in der Softwareentwicklung, insbesondere IT-Sicherheit
- Risiken und Risikoabschätzungen bei sicherheitskritischen Anwendungen
- Review bestehender Methoden — **W. Zimmer**, UDZ
- Vorstellung eines Vorgehensmodells für sichere Komponenten
- Einbettung in entwicklungsbegleitende Sicherheitsevaluierungen

12.30 Uhr **Gemeinsame Mittagspause**

Dienstag • 27. September 2016

Industrie 4.0 & IoT • Leitung: W. Rankl — A

14.00 Uhr **Industrie 4.0 Schwachstellen: Basisangriffe und Szenarien** — **J. Dittmann**
- Sicherheit für komplexe Industrie 4.0 Umgebungen — **R. Fischer**
- Ansatz zur systematischen Beschreibung/Identifikation Angriffspunkte — Universität Magdeburg
- Ableitung komplexer Angriffsszenarien als Kombination Basis-Angriffe — **R. Clausing**
- Modellierung Angriffs-/Angreiferkontext (z.B. Wissen, Daten, Ressourcen) — **Y. Ding**
- Exemplarische Anwendung Ansatz, Diskussion und Ausblick — HS Magdeburg-Stendal

14.30 Uhr **Sicherheit für ROS-basierte Applikationen auf Anwendungsebene** — **B. Dieber**
- Sicherheit und Sicherheitsprobleme in Produktionssystemen — **M. Pichler**
- Spezielle Sicherheitsprobleme bei Mensch-Roboter Anwendungen — Joanneum Research
- Sicherheitsmängel im Robot Operating System — **S. Rass**
- Sicherheitsarchitektur für Publish/Subscribe Applikationen — **P. Schartner**
- Demonstration einer praktischen Anwendung — AAU Klagenfurt

15.00 Uhr **Risiko Smart Home – Angriff auf ein Babymonitorsystem** — **S. Nagel**
- Unser zu Hause wird intelligenter — **G. Bonney**
- Babymonitoring-Systeme als Teil des Smart Homes — **M. Schuba**
- Funktionsweise von Babymonitoring am Beispiel des Systems Babymoov — FH Aachen
- Schwachstellen-Analyse und Angriffsmöglichkeiten
- Empfehlungen zur Verbesserung der Sicherheit

Identifikation & Authentifikation • Leitung: G. Jacobson — B

14.00 Uhr **Beweiswerterhaltung im Kontext eIDAS – eine Case Study** — **S. Schwalm**
- Beweiswerterhaltung — **T. Kusber**
- Rechtlicher Rahmen — BearingPoint GmbH
- Technische Lösungswege — **U. Korte** BSI
- ETSI-Standards, RFC 4998/6283, BSI TR 03125 TR-ESOR — **D. Hühnlein**
- Migrationsansätze zwischen den technischen Lösungswegen — ecsec GmbH

14.30 Uhr **OAuth und OpenID Connect – Erfahrungen und Konzepte** — **R. Steinegger et al.**
- Überblick über OAuth und OpenID Connect — Karlsruher Institut
- Erfahrungen aus Industrie und Forschung — für Technologie
- Benutzerbestimmte Freigabe von Ressourcen
- Absicherung interner APIs mit OAuth
- Single-Sign On per sozialem Netzwerk

15.30 Uhr **Konferenzende**

… als Referenten haben sich zusätzlich zur Verfügung gestellt:

CyberSicherheitsCheck BSI und ISACA — **D. Schugardt**
- Praxisorientiertes Prüfwerkzeug für mittelständische Unternehmen — Konica Minolta
- Aufbau der IT-Basissicherheit mittelständischer Unternehmen — IT Solutions GmbH
- IT-Sicherheit begleitend zur Einführung von ISO27001/Notfallmanagement
- Auditierung von Industrial Control Systems (ICS) der Industrie 4.0
- Qualifikation der Auditoren durch den Cyber Security Practitioner

Anhalten unkooperativer Autos: Ein interaktives Bezugssystem — **M. Hildebrandt**
- Risiko- und Folgenabschätzung durch Ontologien im automotiven Umfeld — **R. Altschaffel**
- Strategische und operative Unterstützung im Krisenmanagement — **F. Rassek**
- Modellierung von Einflussfaktoren für den Einsatz von Stopptechniken — **S. Kiltz**
- Entscheidungsunterstützung beim Stoppen unkooperativer Fahrzeuge — **J. Dittmann**
- Ableitung von Entscheidungsbäumen im Kontext von Risiko & Alternativen — Universität Magdeburg

Die Beiträge dieser Referenten finden Sie auch im Tagungsband zur Konferenz.

Anmeldung & Teilnahmebedingungen

D·A·CH Security 2016

26. und 27. September 2016

Alpen-Adria-Universität Klagenfurt

Anmeldung zur Konferenz

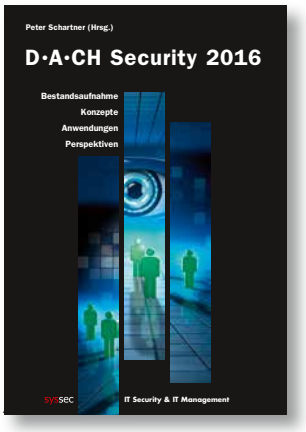
Telefon: +43 (0) 463 2700 3702
Online-Anmeldung unter:
http://www.syssec.at/ds16_anmeldung

Teilnahmebedingungen

Bei Anmeldung bis zum 8. August 2016 beträgt die Teilnahmegebühr € 440,– (Frühanmeldegebühr), danach € 530,–. Referenten zahlen die Referentengebühr von € 380,– (jeweils USt-frei gem. §6 Abs. 11 UStG). Die Teilnahmegebühr beinhaltet ein Exemplar des Tagungsbandes (Hardcover mit ISBN), Pausengetränke, Mittagessen an beiden Konferenztagen und ein gemeinsames Abendessen am ersten Konferenztag. Zudem ist die Teilnahme am Tag der Informatik, die Teilnahme an den wissenschaftlichen Veranstaltungen der INFORMATIK 2016 am 26. und 27.9.2016 und die Teilnahme am Empfang der INFORMATIK 2016 am 27.9.2016 sowie die freie Nutzung aller Buslinien der Stadtwerke Klagenfurt AG in der Zeit vom 26. bis 28.9.2016 enthalten. Bei Stornierung der Anmeldung bis 8. August 2016 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75,– erhoben. Nach dem 8. August 2016 ist die volle Tagungsgebühr zu entrichten. Es ist jederzeit die Benennung einer Ersatzperson ohne zusätzliche Kosten möglich.

Tagungsbände

Zusätzliche Tagungsbände
können bestellt werden unter:
http://www.syssec.at/tagungsbaende



Kontakt

Alpen-Adria-Universität Klagenfurt
Forschungsgruppe Systemsicherheit (syssec)
Universitätsstr. 65-67
A-9020 Klagenfurt
URL: http://www.syssec.at
E-Mail: konferenzen@syssec.at

Programmkomitee

Vorsitz: **P. Schartner** AAU Klagenfurt

P. Beenken Porsche AG • **J. Dittmann** Uni Magdeburg • **D. Engel** FH Salzburg • **J. Fuß** FH Hagenberg
M. Hartmann SAP • **P. Horster** AAU Klagenfurt • **D. Hühnlein** ecsec GmbH • **G. Jacobson** Secardeo GmbH
S. Janisch Uni Salzburg • **K. Knorr** HS Trier • **T. Kob** HiSolutions AG • **U. Korte** BSI
P. Kraaibeek secunet • **W. Kühnhauser** TU Ilmenau • **P.J. Kunz** Daimler • **S. Lechner** JRC
H. Leitold A-SIT • **K. Lemke-Rust** HS Bonn-Rhein-Sieg • **M. Meier** Uni Bonn • **B. Mester** Uni Oldenburg
H. Mühlbauer TeleTrusT • **I. Münch** BSI • **J. Neuschwander** HTWG Konstanz • **A. Philipp** Utimaco
N. Pohlmann FH Gelsenkirchen • **R. Posch** TU Graz • **W. Rankl** Infineon Technologies AG
S. Rass AAU Klagenfurt • **H. Reimer** DuD • **A. Roßnagel** Uni GH Kassel • **W. Schäfer** • **S. Schauer** AIT
H. Storck T-Systems GmbH • **S. Teufel** Uni Fribourg • **P. Trommler** TH Nürnberg • **M. Ullmann** BSI
G. Weck Infodas • **C. Wegener** Uni Bochum • **E. Weippl** SBA Research • **S. Wendzel** Fraunhofer FKIE
A. Wespi IBM CH • **B.C. Witt** it.sec GmbH • **K.-D. Wolfenstetter** DTAG

GI-FG SECMGT Workshop

Leitung: **I. Münch** BSI • **B.C. Witt** it.sec GmbH

K. Kirst PTLV • **D. Koschützki** HS Furtwangen
P. Reymann ITQS • **J. Voßbein** UIMC

Workshop der Allianz für Cyber-Sicherheit (ACS)

Organisatoren: **I. Münch** BSI • **S. Pötz-Schmitt** BSI

P.J. Kunz Daimler AG • **R. Szerwinski** Robert Bosch GmbH
B.C. Witt it.sec GmbH • **M. Meier** Uni Bonn
I. Münch BSI • **N. Pohlmann** FH Gelsenkirchen
H. Mühlbauer TeleTrusT

Organisation

B. Merl AAU Klagenfurt • **M. Möhlmann** • **P. Schartner** AAU Klagenfurt

Leitungsgremium der Konferenzreihe

P. Horster AAU Klagenfurt • **P. Schartner** AAU Klagenfurt

Bilder: shutterstock.com © Andrea Danti