OESTERREICHISCHE COMPUTER GESELLSCHAFT
AUSTRIAN COMPUTER SOCIETY

TeleTrusT
Pioneers in IT security.

Gemeinsame Arbeitskonferenz: GI | OCG | TeleTrusT

D·A·CH Security

Westfälische Hochschule Gelsenkirchen
4. und 5. September 2018

Aktuelle Informationen: http://www.syssec.at/dachsecurity2018

syssec
Alpen-Adria-Universität Klagenfurt
System Security Group

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen

DB

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Bundesministerium des Innern, für Bau und Heimat

Dienstag • 4. September 2018

08.30 Uhr **Registrierung, Kaffee und Tee**

09.30 Uhr **Begrüßung und Überblick: N. Pohlmann & P. Schartner**

Awareness & Schulung • Leitung: B. Mester — A

09.35 Uhr **Informationssicheres Verhalten automatisiert messen** — **M. Janik**
- Effektivität von Security Awareness Maßnahmen beurteilen — **K. Weber**
- Kritisches Verhalten identifizieren — **A. Schütz**
- Sicherheitsrelevantes Verhalten automatisch messen — **T. Fertig**
- Verhalten von Beschäftigten datenschutzkonform aufzeichnen — HS Würzburg-
- Prototyp demonstriert Machbarkeit — Schweinfurt

10.00 Uhr **CT2 Projekt für Lehre, Forschung und Studium von Kryptologie** — **N. Kopal**
- Geschichte des CrypTool-Projekts — **B. Esslinger**
- Kryptologie verstehen mit Toolunterstützung — Uni Kassel
- CrypTool 2 an Schulen und Universitäten
- Historische Chiffren analysieren und brechen
- Verteilte Kryptoanalyse mit CrypTool 2

10.25 Uhr **Neue Narrative für Informationssicherheit** — **D. Scribane**
- Steigerung der Reslilienz durch organisatorische Beidhändigkeit — etomer GmbH,
- Überwinden der Fachsprache – mehr Semantik durch weniger Fachbezug — Secutain
- Awareness für Informationssicherheit als Kulturwandel begreifen
- Den Unterschied zwischen Schuld und Scham erkennen und begegnen
- Einstellungsänderung durch Sympathie und Wissen um das Thema

10.50 Uhr **Kommunikationspause**

Software- & Security-Engineering • Leitung: K. Knorr — A

11.20 Uhr **Eine Programmiersprache zur souveränen Datenverarbeitung** — **F. Bruckner, D. Krüger**
- Usage Control kein fester Bestandteil klassischer Programmiersprachen — **R. Nagel, S. Wenzel**
- Statt den Daten können Applikationen und Ergebnisse verschickt werden — Frauenhofer ISST
- DSL für die Datenverarbeitung mit erweiterbaren Subsystemen — **B. Otto**
- Definition neuer Typen, Aktivitäten und Policies bei Bedarf — TU Dortmund
- Cross-Compilation in komplexe Applikationen welche Policies einhalten

11.45 Uhr **Security-Engineering in Software-Entwicklung und Betrieb** — **A. Lunkeit**
- Nutzung modellbasierter Ansätze im Security Engineering — Rohde & Schwarz
- Einfluss betrieblicher Randbedingungen auf die Systemsicherheit — Cybersecurity
- Review bestehender Ansätze
- Vorstellung eines modellbasierten Ansatzes für Entwicklung und Betrieb
- Nutzung des Ansatzes in einer Fallstudie

12.10 Uhr **Techniken zur Vermeidung von ROP-Angriffen** — **J. Klemkow**
- Neue OpenBSD Sicherheitsmechanismens der letzten Jahre — genua GmbH
- Mit besonderem Fokus auf anti-ROP Techniken
- Veränderungen im Kernel bzw. Userland
- Einblick in die aktuelle Entwicklung
- Veränderungen im Bereich der Technik

12.35 Uhr **Gemeinsame Mittagspause**

Dienstag • 4. September 2018

Angriff & Abwehr • Leitung: K. Lemke-Rust — A

13.35 Uhr **Erkennung von Hardwaremanipulationen durch Lötzinn-Analyse** — **T. Kuhn**, HTV GmbH

- Analyse der Lötstellen von Testleiterplatten nach Manipulation
- Darstellung unterschiedlicher Analysemethoden (z.B. Mikroskopie, RFA)
- Vergleich der Ergebnisse von zwei unterschiedlichen Rework-Anlagen
- Austausch von BGA-Bauteilen mit Underfill
- Austausch von gelöteten Schutzblechen bei Mobiltelefonen

14.00 Uhr **Erkennung von Android-Malware mit maschinellem Lernen** — **T. Straub**, Duale Hochschule Baden-Württemberg; **M. Stahlberger**, Fiducia & GAD IT AG

- Trends bei Android-Malware, bestehende Erkennungsansätze
- Klassifizierung von Malware mit Machine Learning
- Trainingsset mit Schadklassen und Kernelaufrufsequenzen
- Lösungsarchitektur und Datenerfassung am Android-Gerät
- Parametervergleich Support Vector Machine & Logistic Regression

14.25 Uhr **fishy – Ein Framework zur Umsetzung von Verstecktechniken in Dateisystemen** — **A. Kailus**, **C. Hecht**, **T. Göbel**, **L. Liebler**, HS Darmstadt

- Open Source Framework für Dateisystem-basierte Verstecktechniken
- Bereitstellung von Schnittstellen zur Manipulation von Datenstrukturen
- Aktuelle Unterstützung unterschiedlicher Dateisysteme: EXT, FAT, NTFS
- Vorstellung und Evaluation des Frameworks anhand konkreter Techniken
- Grundlage zukünftiger Qualitätssicherungen von Forensik-Software

Studentische Abschlussarbeiten • Leitung: S. Schauer — B

13.35 Uhr **Secret-Sharing: Sicherheitsbetrachtungen und Tools** — **V. Pachatz**, Alpen-Adria-Universität Klagenfurt

- Erläuterung von Secret-Sharing-Protokollen und Commitment-Verfahren
- Diskussion eines Chosen-Instruction-Angriffs
- Anwendbarkeit von Chosen-Instruction-Angriffen auf Secret-Sharing
- Vorstellung einer Bibliothek zur Durchführung von Secret-Sharing
- Live-Demo eines Prototyps zur Ausführung verteilter Berechnungen

14.00 Uhr **Automatisierte Erkennung von Daten-Exfiltration** — **N. Rogmann**, HS Darmstadt, Controlware GmbH

- Weltweit immer häufiger Systemeinbrüche mit dem Ziel eines Datendiebstahls
- Bisher keine zuverlässige Erkennung von Netzwerk-Steganographie
- Ein neuer Lösungsansatz: Statistische Analyse & maschinelles Lernen
- Wissenschaftliche Untersuchung zur Identifizierung statistischer Merkmale
- Fokus auf bisher unzureichend überwachte Netzwerk-Protokolle wie DNS und ICMP

14.50 Uhr **Kommunikationspause**

Sicherheitsmanagement • Leitung: R. Benzmüller A

15.20 Uhr **Der IT-Security-Navigator** — **D.-K. Kipker**, Uni Bremen
- Interdisziplinäre Herausforderungen für die IT-Sicherheit
- Auslegungsschwierigkeiten im Hinblick auf unbestimmte Rechtsbegriffe — **A. Harner**
- Konkretisierung des „Standes der Technik“ im Sinne des IT-SiGn — **S. Müller**, DKE/VDE
- Domänenübergreifende technische Normung in der IT-Sicherheit
- Lösungsmodelle zur praxisnahen Gesetzeskonkretisierung für KMU

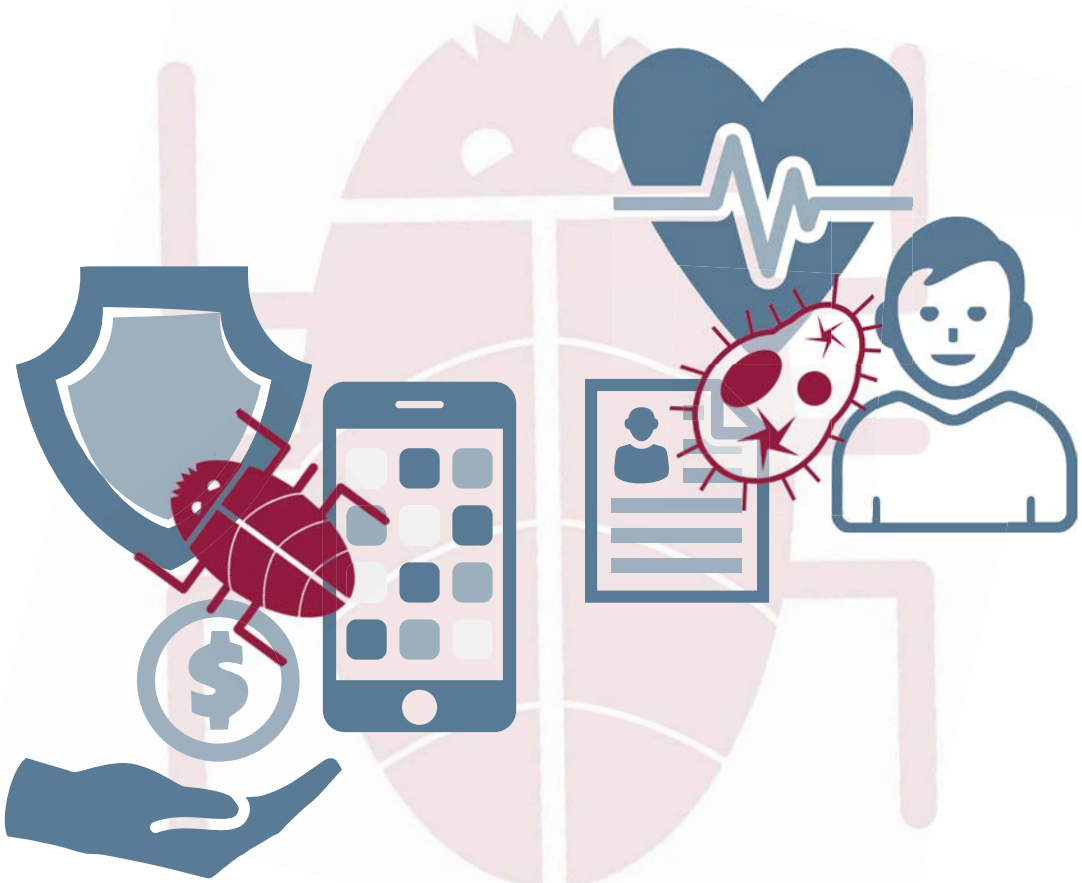
15.45 Uhr **Einführung eines KMU-CERTs in Österreich** — **E. Huber et al.**, Donau-Universität Krems
- Computer Emergency Response Teams
- Bedarfsanalyse bei den österreichischen KMUs
- Struktur eines KMU-CERTs
- Cybersicherheit
- Organisation

16.10 Uhr **Sei gewarnt! Vorhersage von Angriffen im Online-Banking** — **T. Urban, R. Riedel, N. Pohlmann**, Institut für Internet-Sicherheit, **C. Paulisch**, TU Berlin
- Aktive Warnungen vor tagesaktuellen Angriffen im Online-Banking
- Bestimmung geeigneter Kennzahlen, die das Gefahrenlevel beschreiben
- Vergleich unterschiedlicher KI-Verfahren zur Bestimmung der Gefahrenlage
- Studie zur Nutzerfreundlichkeit des Systems im praktischen Einsatz
- Kritische Betrachtung der Ergebnisse und Hindernisse bei der Einführung

16.35 Uhr **Erfüllung von IT-Compliance durch automatische Vorfall-Bearbeitung** — **K.-O. Detken, M. Jahnke, T. Rix**, DECOIT GmbH, **M. Steiner**, IT-Security@Work GmbH
- Automatisierte Überwachung und Steuerung von Compliance-Aspekten
- Zentrale Sammlung aller sicherheitsrelevanten Informationen
- Generierung verstehbarer Handlungsempfehlungen
- Anomalien erkennen und diese melden
- Anbindung an ein NAC-System im Forschungsprojekt CLEARER

17.00 Uhr Ende erster Konferenztag

18.30 Uhr Gemeinsames Abendessen



Mittwoch • 5. September 2018

Beweiswerthaltung • Leitung: G. Jacobson — A

09.00 Uhr **High-Level Risikoanalyse im Bereich Internet of Things** — **T. Kusber**
- Blockchain, insbesondere Private Chain — **S. Schwalm**
- Nachweis- und Aufbewahrungspflichten — Fraunhofer FOKUS
- EU-Verordnungen zur Digitalisierung (eIDAS, DSGVO...) — **C. Berghoff**
- Lösungsansätze zum Erhalt des Integritätsschutzes — **U. Korte**
- Lösungsansätze zum Beweiswerterhaltung — BSI

09.25 Uhr **Anforderungen an eine vertrauenswürdige Langzeitarchivierung** — **P. Kathmann**
- Integrität und Nicht-Abstreitbarkeit einer VoIP-Kommunikation — **G. Gritzan**
- Integrität und Authentizität über die Phasen des OAIS-Modells — **O. Hoffmann**
- Digitale Langzeitarchivierung nach DIN-Norm 31644 — **R. Sethmann**
- Anforderungen an die Archivierung von VoIP-Daten nach DIN-31644 — HS Bremen
- Integritätsprüfung über PCR-Check eines TPMs

09.50 Uhr **Ein sicherer Datenrekorder** — **S. Taurer**
- Datenschreiber für intelligente Robotersysteme — **B. Dieber**
- Sicheres Aufzeichnen und Speichern des Systemzustandes — Joanneum Research – Robotics
- Transparenz in der Entscheidungsfindung von durchzuführenden Aktionen
- Nachvollziehbarkeit in komplexen (Roboter-) Systemen
- Unterstützung von forensischen Untersuchungen nach Fehlverhalten

10.15 Uhr **Vertrauenswürdige E-Akte auf Basis von TR-RESISCAN /TR-ESOR** — **D. Hühnlein**
- EU-Verordnungen zur Digitalisierung (eIDAS, DSGVO...) — ecsec GmbH
- Ersetzendes Scannen (BSI TR-03138, TR-RESISCAN) — **J. Ahmad**
- Elektronische Vorgangsbearbeitung (E-AKTE) — **U. Korte**
- Beweiswerterhaltung für Signaturen (BSI TR-03125, TR-ESOR) — BSI
- ETSI-Standards für Vertrauens- und Bewahrungsdienste

Workshop KRITIS • Leitung: U. Lechner & S. Dännart — B

09.00 Uhr **IT-Sicherheit bei den Kliniken des Bezirks Oberbayern** — **T. Kehr**
- Schutz von Patientendaten in Kliniken — **S. Dännart**
- Reaktionen auf Ransomwareattacke auf Krankenhäuser — UniBw München
- Strategie des ausgewogenen Risikomanagements
- Einsatz eines multiprofessionellen IT-Sicherheitskomitees
- Schnelle, transparente Entscheidungen von IT und Anwendern ermöglichen

IT-Sicherheit für Geschäftsprozesse im Finanzsektor — **T. Bollen**
- Unterstützung des Risikomanagements in Banken — Wincor Nixdorf
- Ganzheitliche Risikobewertung durch die Managementlösung PREVENT — **S. Rudel**
- Vielzahl an Datenquellen im Unternehmen aggregieren — UniBw München
- Wechselwirkungen zwischen Ebenen im Unternehmen darstellen
- Verschiedene Sichten bedarfs- und anwendergerecht erzeugen

Ausfallsicherheit in der Zentralen Leitstelle Ostthüringen — **S. Müller**
- Vorstellung einer zentralen Rettungsleitstelle als KRITIS — Stadtverwaltung Gera
- Ausfallsicherheit des Alarmierungsprozesses — **T. Gurschler**
- Weiterentwicklung der Informations- und Kommunikationstechnologie — UniBw München
- Disponentenarbeitsplätzen
- Rückfallebenen und Redundanzen

Transfer in die Praxis — **U. Lechner**
- Lösungen zur IT-Sicherheit, wie sie konkret angewendet werden — **S. Dännart**
- Bandbreite von Good Practices — UniBw München
- Zusammenspiel Technik, Organisation, Mensch
- Weitere Beiträge von Experten
- Kostenfreie Bezugsquelle der Fallstudien

10.40 Uhr **Kommunikationspause**

Mittwoch • 5. September 2018

Automatisierung, Industrie 4.0 & IoT • Leitung: H. Storck — A

11.10 Uhr **Biometrie in der Industrie 4.0** — **S. Schindler**, **J. Schneider**, **T. Goeble**, Uni Kassel
- Neue Herausforderung durch die Datenschutzgrundverordnung
- Rechtliche Erlaubnis zur Nutzung biometrischer Daten
- Datenverarbeitung im Rahmen eines Beschäftigungsverhältnisses
- Neue technische Gestaltungsvorgaben für den Datenschutz
- Rechtskonforme Technikgestaltung im Bereich der Industrie 4.0

11.35 Uhr **Security-Demonstrator Industrie 4.0** — **R. Fischer**, **K. Lamshöft**, **J. Dittmann**, Otto von Guericke Universität Magdeburg
- Sicherheit für komplexe Industrie 4.0 Umgebungen
- Sichere Steuerung von Industrie-Prozessen
- Kommunikations-basierte Szenarien mit Basis-Angriffen
- Security-Demonstrator für experimentelles Security-Testing
- Demonstrative Umsetzung und experimentelle Auswertung

12.00 Uhr **OT-Security: Von der Norm ins Leitsystem** — **S. Fluchs**, **H. Rudolph**, admeritia GmbH
- Pragmatische Umsetzung der IEC 62443 durch Komplexitätsreduktion
- Managementsystem: Was es kann, was nicht – und wo man anfängt
- Risikoanalyse: Ingenieurmethoden statt Glaskugel
- Maßnahmen: Wenn Security die Arbeit mit dem Leitsystem erleichtert
- Security für Safety-Systeme: Keine Parallelstrukturen aufbauen

12.25 Uhr Gemeinsame Mittagspause

Risikomanagement • Leitung: N. Pohlmann — A

13.25 Uhr **Risikobewertungen in Datennetzwerken** — **D. Tebernum**, **M. Spiekermann**, **S. Wenzel**, ISST Frauenhofer, **B. Otto**, TU Dortmund
- Metadatenbasierte Risiko- und Sicherheitsbewertung von Datenressourcen
- Flexibilisierung von metadatenbasierten Metriken
- Unterstützung des unternehmensübergreifenden Datenaustausches
- Datenkataloge zur qualitativen Risikobewertung von Data Supply Chains
- Kollaboratives Risikomanagement in Datennetzwerken und -ökosystemen

13.50 Uhr **Ansatz zur Auswahl von Risikomanagement-Methoden** — **S. Schauer**, **M. Latzenhofer**, **S. König**, **C. Kollmitzer**, AIT
- Vergleich von Risikomanagementframeworks
- Aktualisierung des ENISA Vergleichs (2006)
- Diskussion der Vergleichskriterien
- Diskussion der Praxisanwendung
- Fokus auf Risikomanager in KMUs

14.15 Uhr **Risikobewertung für vernetzte kritische Infrastrukturen** — **S. Schauer et al.**, AIT
- Vernetzte kritische Infrastrukturen
- Identifikation von Kaskadeneffekten
- Statisches und dynamisches Risikomodell
- Simulation und Visualisierung
- Ganzheitliche Risikoanalyse

Workshop ACS • Leitung: T. Kleinert & S. Becker — B

13.25 Uhr **Die Wirtschaft im Fokus von Cyber-Angriffen** — **S. Becker**, **T. Kleinert**, BSI
- Bedrohungslage
- Aktuelle Vorfälle
- Tätertypologie
- Angebote von BSI & Ermittlungsbehörden
- Skizzierung Incident Response

Incident Response – Workshop zum korrekten Verhalten im Ernstfall — **S. Becker**, **T. Kleinert**, BSI
- Vorstellung eines Fallbeispiels
- Kurzfristige Maßnahmen
- Zusammensetzung eines Krisenstabs
- Erarbeitung eines Notfallplans
- Übung erzeugt Kompetenz

14.40 Uhr Kommunikationspause

Mittwoch • 5. September 2018

Authentifikation & Identifikation • Leitung: U. Korte — A

15.10 Uhr **Mehr Sicherheit und Benutzerfreundlichkeit für Fernsignaturen** — **T. Wich**
- Die eIDAS-Verordnung – der „Digitalisierungsmotor“ im Überblick — **S. Schuberth**
- Die Fernsignatur – das „Killer-Feature“ der eIDAS-Verordnung — **R. Lottes**
- Bedrohungsmodell: Wie sicher ist die Fernsignatur eigentlich? — **T. Hühnlein**
- Mehr Sicherheit und Benutzerfreundlichkeit für die Fernsignatur — **D. Hühnlein**
- SkIDentity – Gestern, heute, morgen – von eID zu eIDAS! — ecsec GmbH

15.35 Uhr **Kontextsensitive CAPTCHAs im Online-Banking** — **T. Urban, R. Riedel**
- Darstellung von aktuellen Angriffen im Online-Banking — **N. Pohlmann**
- Konzeption eines Protokolls zur Absicherung von Transaktionen durch CAPTCHAs — Institut für Internet-
- Konzeption von Angriffen auf das entwickelte Protokoll — Sicherheit
- Berechnungen des Restrisikos eines erfolgreichen Angriffs — **C. Paulisch**
- Umfangreiche Nutzerstudie zum praktischen Einsatz des Systems — TU Berlin

16.00 Uhr **Risikobasierte und adaptive Authentifizierung** — **R. Riedel**
- Maßnahmen für eine frustfreie Multi-Faktor Authentifizierung — **N. Pohlmann**
- Synergien durch Zentralisierung der Identifikation und Authentifikation — Institut für Internet-
- High-Level Design eines adaptiven Identity Providers — Sicherheit
- Anwendungsfälle mit Blick auf gesetzliche Rahmenbedingungen
- Vergleich bestehender Systeme und deren IT-Sicherheitskonzepte

16.25 Uhr **Konferenzende**

... als Referenten haben sich zusätzlich zur Verfügung gestellt:

ML-gestützte Authentifizierung mit QR Code und Smartphone — **M. Hertlein**, XignSys GmbH
- Profilbildung anhand von Smartphonesensoren
- Vereinfachung und Absicherung von Authentifizierung durch maschinelles Lernen
- Adaptive Authentifizierung mit maschinellem Lernen
- Authentifizierung mittels Smartphonesensordaten – Vergleich von Algorithmen
- Ergebnisdaten durch die Nutzung von XignQR

Using Geolocation Data as a Threat Enlargener — **M. Cagnazzo**, **N. Pohlmann**, Institut für Internet-Sicherheit
- Privacy Leaks in Geolocation Data
- Operational Security Risks
- Open Source Data Risks
- Social Engineering Attacks
- Enlarging Attack Surface through Data Analysis

Integrität und Nicht-Abstreitbarkeit von VoIP-Kommunikation — **K.-O. Detken**, **M. Jahnke**, DECOIT GmbH, **B. Röllgen**, Global IP Telecommunications
- Nicht-Abstreitbarkeit mündlicher Konversation
- Integritätsschutz mittels Trusted-Computing-Technologie
- Sichere Authentifizierung der Kommunikationspartner
- Revisionssichere Speicherung der Kommunikation
- Umsetzung im Forschungsprojekt INTEGER

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

Anmeldung & Teilnahmebedingungen

D·A·CH Security 2018

4. und 5. September 2018

Westfälische Hochschule Gelsenkirchen

Anmeldung zur Konferenz

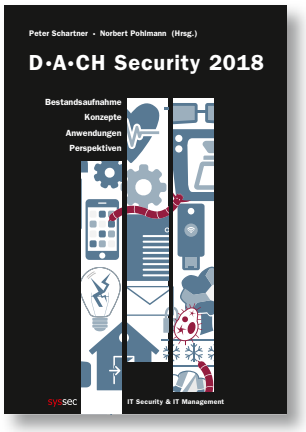
Telefon: +43 (0) 463 2700 3702
Online-Anmeldung unter:
http://www.syssec.at/ds18_anmeldung

Teilnahmebedingungen

Bei Anmeldung bis zum 13. August 2018 beträgt die Teilnahmegebühr € 395,- (Frühanmeldegebühr), danach € 480,- jeweils zuzüglich der gesetzlichen Mwst. Referenten zahlen nur die Referentengebühr von € 345,- zzgl. Mwst.
Die Teilnahmegebühr beinhaltet ein Exemplar des Tagungsbandes (Hardcover mit ISBN), Pausengetränke, Mittagessen an beiden Konferenztagen und ein gemeinsames Abendessen am ersten Konferenztag. Bei Stornierung der Anmeldung bis 13. August 2018 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75,- erhoben. Nach dem 13. August 2018 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 | **N. Pohlmann** Westfälische Hochschule Gelsenkirchen

A. Alkassar TeleTrusT • **R. Baumgart** Secunet AG • **A. Baumann** UniBw München • **P. Beenken** Porsche AG
R. Benzmüller GDATA AG • **J. Dittmann** Uni Magdeburg • **D. Engel** FH Salzburg • **K. Frintrop** AFCEA
J. Fuß FH Hagenberg • **M. Hartmann** SAP • **P. Horster** AAU Klagenfurt • **G. Jacobson** Secardeo GmbH
S. Janisch Uni Salzburg • **A. Kreth** AFCEA • **K. Knorr** HS Trier • **U. Korte** BSI • **W. Kühnhauser** TU Ilmenau
P.J. Kunz HiSolutions AG • **S. Lechner** JRC • **H. Leitold** A-SIT • **K. Lemke-Rust** HS Bonn-Rhein-Sieg • **M. Meier** Uni Bonn
B. Mester datenschutz nord • **H. Mühlbauer** TeleTrusT • **I. Münch** BSI • **J. Neuschwander** HTWG Konstanz
A. Philipp PrimeKey Labs GmbH • **R. Posch** TU Graz • **W. Rankl** Infineon Technologies AG • **S. Rass** AAU Klagenfurt
A. Roßnagel Uni GH Kassel • **S. Rudel** UniBw München • **S. Schauer** AIT • **H. Storck** Schneider Electric Systems
S. Teufel Uni Fribourg • **P. Trommler** TH Nürnberg • **M. Ullmann** BSI • **G. Weck** Infodas • **C. Wegener** Uni Bochum
E. Weippl SBA Research • **S. Wendzel** HS Worms/FKIE • **S. Werth** FH Lübeck • **A. Wespi** IBM CH
T. Wich ecsec GmbH • **B.C. Witt** it.sec GmbH • **K.-D. Wolfenstetter** DTAG

Workshop KRITIS

Organisatorinnen: **U. Lechner** UniBw München • **S. Rudel** UniBw München

Workshop der Allianz für Cyber-Sicherheit (ACS)

Organisatoren: **S. Becker** BSI • **T. Kleinert** BSI

Organisation

M. Möhlmann • **N. Pohlmann** Westfälische Hochschule Gelsenkirchen

Leitungsgremium der Konferenzreihe

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

Titelbild: Sebastian Wacowski