



Gemeinsame Arbeitskonferenz: GI | BITKOM | OCG | SI | TeleTrust



D·A·C·H Security

Hochschule Bonn-Rhein-Sieg | Campus St. Augustin
8. und 9. September 2015



Aktuelle Informationen: <http://www.syssec.at/dachsecurity2015>





Dienstag • 8. September 2015

08.30 Uhr **Registrierung, Kaffee und Tee**

09.30 Uhr **Begrüßung und Überblick**

Cloud & Big Data • Leitung: K.-D. Wölfenstetter

A

09.35 Uhr **Sicherheitsanalyse der Private Cloud Inter faces von openQRM**

- Vorteil von Private Clouds gegenüber Public Clouds?
- Standards und Umsetzung
- XSS, CSRF und SQLi
- Einfluss von Schwachstellen in den Schnittstellen auf den Workflow
- Interface-übergreifende Lücken

D. Felsch
F. Schulz
J. Schwenk
Ruhr-Uni Bochum

10.00 Uhr **Benutzerfreundliche Verschlüsselung für Cloud-Datenbanken**

- Der Wunsch nach Datenverwaltung durch Cloud-Datenbanken steigt
- Eine Anforderung sind möglichst hohe Sicherheitsgarantien
- Eine weitere Anforderung ist effiziente Datenverwaltung in der Cloud
- Durchsuchbare, ordnungsbewahrende und homomorphe Verschlüsselung
- Proxy-Client zwischen Benutzer und Clouddatenbank

L. Wiese
T. Waage
Universität Göttingen

10.25 Uhr **Themis – Sicheres Vererben in der Cloud**

- Verschwommene Grenzen des Besitztums und Kontrolle über Cloud-Inhalte
- Backups erstellen und teilen mit der Themis Security-First Architektur
- Umsetzung des Elasticsearch Index-Per-User Modells und Implikationen
- Deine Daten in deiner Hand: Themis mit PGP Verschlüsselung
- Themis Generationenbackup und juristisch geregelter Nachlass-Workflow

A. Lindley, M. Bartha
AIT
W. Eibner
X-Net Services GmbH
S. Pimminger
FH OÖ

10.50 Uhr **Kommunikationspause**

Identifikation & Biometrie • Leitung: U. Kor te

A

11.20 Uhr **SkIDentity – Mobile eID as a Ser vice**

- Elektronische Ausweise vermeiden Identitätsdiebstahl und Missbrauch
- Ableitung von Cloud Identitäten aus elektronischen Ausweisen
- Cloud Identitäten für Smartphones und mobilen Einsatz
- Portal ermöglicht effiziente eID-Integration mit wenigen Mausklicks
- Verschlüsselung, elektronische Signatur und mehr

M. Tuengerthal et al.
ecsec GmbH

11.45 Uhr **Elektronische Identifizierung und ver trauenswürdige Dienste**

- Mit eIDAS zu Privatsphäre-konformen Bankentransaktionen
- Vertrauenswürdige Transaktionen für den Euro-Zahlungsverkehrsraum
- Erweiterung von eIDAS um biometrisch authentifizierte Transaktionen
- Verbessertes Benutzerkomfort und Vertrauen für eBanking
- Datenschutz und Privatsphäre-konforme biometrische Technologien

N. Buchmann
H. Baier
HS Darmstadt

12.10 Uhr **BioMe – Kontinuierliche Authentifikation mittels Smartphone**

- Biometrische Authentifizierung anhand von Touchgesten bei Smartphones
- Möglichkeiten und Herausforderungen bei der Datenaufnahme
- Klassifikation von Touchgesten
- Erstellung eines Scoring Systems zum Erkennen von BenutzerInnen
- Ausblick und weitere Entwicklung

M. Temper
M. Kaiser
FH St. Pölten

12.35 Uhr **Gemeinsame Mittagspause**

Datenschutz & Signaturen • Leitung: G. Jacobson

A

13.35 Uhr Ersetzendes Scannen und Beweiswerterhaltung

- Beweiswerterhaltung mit SAP
- Ersetzendes Scannen
- Elektronische Vertrauensdienste
- BSI-TR 03138 (TR-RESISCAN)
- BSI-TR 03125 (TR-ESOR)

S. Schwalm

BearingPoint GmbH

U. Korte

BSI

D. Hühnlein

ecsec GmbH

14.00 Uhr Informationelle Selbstbestimmung auch auf der Straße

- Die Vernetzung der Mobilität – auf der Straße in eine vernetzte Welt
- Informationelle Selbstbestimmung bei der Fahrzeugvernetzung
- Datenschutz als Showstopper in der modernen Verkehrsinfrastruktur?
- Zukünftige Herausforderungen eines globalen Datenschutz(-rechts)
- Datenschutztechnik und Recht – eine Allianz im Fahrzeug

S. Kroschwald

Porsche AG

14.25 Uhr Nachweisbarkeit in Smart Grids auf Basis von XML-Signaturen

- Sicherheitsanforderungen für Smart Grids
- Übersicht über IEC 61850 und Smart Grid Security Standards
- Sicherheitsprobleme
- Sicherheitslösung für MMS
- Einbindung von XML-Signaturen

C. Ruland

J. Saßmannshausen

Uni Siegen

Studentische Abschlussarbeiten • Leitung: M. Ullmann

B

13.35 Uhr Analyse und Simulation dynamischer RBAC-Zugriffssteuerungsmodelle

- Rollenbasierte Zugriffssteuerung in IT-Systemen (RBAC)
- Modellierung dynamischen Verhaltens
- Analyse dynamischer Rechteausbreitungen
- Werkzeuggestützte Analyse und Simulation dynamischer RBAC-Modelle
- Evaluierung der praktischen Machbarkeit

M. Schlegel

TU Ilmenau

14.00 Uhr Blinde Turingmaschinen

- Verarbeitung verschlüsselter Daten mit Blinden Turingmaschinen
- Funktionsweise von Blinden Turingmaschinen
- Anwendung des Prinzips auf verschlüsselten Assembler-Code
- Sicherheitsprobleme und Angriffsmöglichkeiten
- Gegenmaßnahmen zur Absicherung

M. Brodbeck

AAU Klagenfurt

14.25 Uhr Industrie 4.0 und deren Umsetzung

- Vier grundlegende Veränderungen für Unternehmen
- Telekommunikationsbranche als Vorreiter der Industrie 4.0
- Strategische Umsetzung mit Hilfe der Enterprise Architecture
- Standardisierung als größte Herausforderung von Industrie 4.0
- Datensicherheit – Die Rolle von Open Innovation und Open Source

A.-C. Ritter

TU München &

Haselhorst

Associates GmbH

14.50 Uhr Kommunikationspause





Dienstag • 8. September 2015

Risikoanalyse, Sicherheitsmodelle & Zertifizierung • Leitung: B. Mester

A

15.20 Uhr IKT-Risikoanalyse am Beispiel APT

- Meta-Risiko-Modell für kritische Infrastrukturen
- Graphenbasiertes Risiko-Modell
- Identifikation von Sicherheitslücken über Organisationsbereiche
- Advanced Persistent Threats (APT)
- Risikomanagement

S. Schauer et al.

AIT

15.45 Uhr Zertifizierung nach VdS 3473

- Richtlinie für den Mittelstand
- Bindeglied zwischen Audit und Erlangung eines ISO-27001-Zertifikats
- Unterteilung in kritische und unkritische Systeme
- Wichtige Einzelaspekte im Überblick
- Vorgehensmodell bis zur Zertifizierung

U. Greveler

HS Rhein Waal

R. Reiner mann

VdS GmbH

M. Semmler

Mark Semmler GmbH

16.10 Uhr Das KIARA Security- Modell

- Sicherheitsinfrastrukturen
- Sichere Middleware
- Sicherheitspolitiken
- Informationsfluss
- Security-by-Design

A. Nonnengart

W. Stephan

P. Slusallek

D. Rubinstein

DFKI

16.35 Uhr eHealth – Zertifizierungskonzept für Kartengeneration G2

- Neugestaltung der Sicherheitszertifizierung von eHealth-Karten
- Schlanke, effiziente, transparente und flexible Prozesse
- Zertifizierung der Karten-Plattform nach Common Criteria
- Zertifizierung der Karten-Produkte nach Technischer Richtlinie
- Aktueller Sachstand der Umsetzung des Zertifizierungskonzepts

S. Pingel

BSI

ACS WORKSHOP • Leitung: I. Münch

B

15.20 Uhr Vertraulichkeitsschutz durch Verschlüsselung

- Wirtschaftsspionage als gravierendes IT-Risiko auch für KMU
- Verschlüsselung als wichtigste Maßnahme zum Schutz der Informationsbestände
- Elemente einer risikoorientierten Anwendung von Verschlüsselung
- Aufbau einer Verschlüsselungsarchitektur für KMU
- Vorstellung einer laientauglichen Lösung für Nutzer in KMU

M. Stöwer

T. Rubinstein

Fraunhofer SIT

15.45 Uhr Software-Whitelisting mit Microsoft AppLocker

- Grundlagen des Software-Whitelisting
- Anwendungsszenarien
- Microsoft AppLocker
- Schwachstellenanalyse
- Handlungsempfehlungen

M. Reuter

D. Loevenich

M. Ullmann

HS Bonn-Rhein-Sieg

16.10 Uhr Den Erfolg von Sicherheitsmaßnahmen messen – ein Praxisansatz

- Investitionen in IT-Sicherheit rechtfertigen – aber wie?
- Herausforderung: Entwicklung eines Kennzahlensystems
- Komplexität reduzieren durch Risikoszenarien
- Kennzahlen entwickeln mit kombiniertem Top-Down- und Bottom-up-Ansatz
- Handlungsfähigkeit gewinnen durch ebenengerechtes Lagebild

R. Schumann

rt-solutions.de GmbH

N. Nagel

16.35 Uhr ISMS-Notfall (IT-Notfallmanagement)

- Schnelle Initialumsetzung und geringe Kosten, Mittelstandslösung
- Notfallvorsorge nach BSI-Grundschriftkatalog (100-4)
- Faktor Mensch: Einsicht ist wichtigster Faktor für Akzeptanz und Erfolg
- Volle Integration des IT-Notfallmanagements in die tägliche Arbeit
- Qualitätsgesicherte Freigabeprozesse mit Eskalationsstufen

H. Huber

J. Schmalz GmbH

17.00 Uhr Ende erster Konferenztag • Gemeinsames Abendessen

Mittwoch • 9. September 2015

Mobile Security & Chipkarten • Leitung: M. Spritzenbarth

A

09.00 Uhr Kryptografisches Zugriffskontrollsystem für mobile Endgeräte

- Anforderungen bei Smartphones und Tablets
- Verfügbare Lösungen, Neuartigkeit der eigenen Lösung
- Effektives Schlüsselmanagement
- Sicheres und benutzerfreundliches Backup kryptographischer Schlüssel
- Prototyp (App) für vertrauliche Datenspeicherung in einer Cloud

E. Piller

FH St. Pölten

A. Westfeld

HTW Dresden

09.25 Uhr Sicherheitsanforderung an Messenger Apps

- Wie mobile Messenger das Kommunikationsverhalten verändern
- Sicherheitslücken in mobilen Messengern
- Sicherheitsanforderungen an mobile Messenger
- Evaluation ausgewählter Messenger
- Ausblick und weitere Entwicklungen

T. Bötner

H. Pohl

softScheck GmbH

M. Ullmann

BSI

09.50 Uhr Mobile Devices in Unternehmen mit erhöhtem Security-Bedarf

- Sichere Kommunikation von Daten auf mobilen Endgeräten
- Sicherheitsarchitekturen von mobilen Plattformen
- Benutzer- und Schlüsselmanagement auf mobilen Plattformen
- Mechanismen zur Zugriffskontrolle und App Wrapping
- Mobile Device Management

S. Schauer et al.

AIT

10.15 Uhr Offene Software-Architektur für moderne Smartcards

- Strikte Lizenzbedingungen häufiges Hindernis für Smartcard-Einsatz
- OpenSC-Unterstützung unter Linux nur durch individuelle Kartentreiber
- Ansatz: Generisches JavaCard-Applet mit generischer OpenSC-Integration
- ISO-7816-basierte Schnittstelle
- Flexibles Dateisystem durch Objektorientierung

P. Wendland

M. Roßberg

G. Schäfer

TU Ilmenau

SECMGT WORKSHOP • Leitung: B. Witt

B

09.00 Uhr IT-Risiko-Check

- Informationssicherheit in mittelständischen Unternehmen
- Ganzheitliches Risikomanagement in der Informationssicherheit
- Identifizierung und Wissen um geschäftskritische Prozesse
- Verfahren zur Risikobewertung mittels Schwachstellen und Gefährdungen
- Status der Risikolage hinsichtlich Informationssicherheit

J. Stocker

HS Albstadt-Sigmaringen

J. Jürjens

TU Dortmund

S. Wenzel

Fraunhofer ISST

09.50 Uhr Schatten-IT

- Schatten-IT beschreibt im Fachbereich autonom entwickelte Systeme
- Relevanz wird oftmals unterschätzt
- IT-Sicherheit wird nur wenig betrachtet
- Schatten-IT unterläuft die Kontrollsysteme
- Bessere Awareness und Management sind notwendig

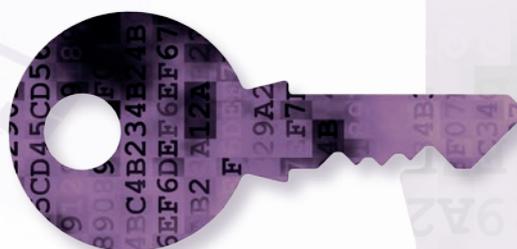
C. Rentrup

S. Zimmermann

M. Huber

HTWG Konstanz

10.40 Uhr Kommunikationspause





Mittwoch • 9. September 2015

Web- & Netzwerksicherheit • Leitung: R. Szerwinski

A

11.10 Uhr Dynamische Trackererkennung im Web durch Sandbox-Verfahren

- Überblick von aktiven Trackingverfahren im Web
- Grenzen aktueller Tools zum Selbstschutz
- Vorstellung der Sandbox als Messinstrument von Web-Tracking
- Analyse von Trackingverfahren auf Webseiten durch die Sandbox
- Evaluierung

T. Wambach

Uni Koblenz-Landau

11.35 Uhr Netzwerksicherheit mit probabilistischen Angriffsgraphen

- Zielgerichtete Angriffe stellen aktuell für Firmen große Bedrohungen dar
- Angreifer bewegen sich in mehreren Schritten durch Firmen-Netzwerke
- Automatische Analyse der Netzwerke auf Schwachstellen und Angriffspfade
- Weitestgehende automatische Vorschläge für Absicherung
- Probabilistische Berücksichtigung von unbekanntem Schwachstellen

A. Schmitz

Fraunhofer ISST

H. Pettenpohl

TU Dortmund

12.00 Uhr Aktuelle Probleme und Potentiale von Web-App Scannern

- Schwachstellenerkennung in Web-Applikationen
- Entwicklung einer Infrastruktur zur Analyse von Web-App Scannern
- Entwicklung einer unsicheren Web-Applikation
- Evaluation frei erhältlicher Web-App Scanner
- Analyse möglicher Verbesserungspotentiale

M. Schneck

Fraunhofer SIT

M. Ullmann

BSI

K. Lemke-Rust

HS Bonn-Rhein-Sieg

Security Incident & Event Management • Leitung: R. Welter

B

11.10 Uhr Intelligentes Monitoring der IT-Sicherheit durch SIEM-Einsatz

- Einführung in SIEM
- SIEM-Architektur des iMonitor-Projektes
- Zeitreihenbasierte Anomalie-Erkennung
- Erkennung von Vorfallvariationen durch KI-Nutzung
- Ein Anwendungsfallbeispiel

K.O. Detken

DecoIT GmbH

C. Eifers

neusta GmbH

M. Humann

Uni Bremen

11.35 Uhr Incident Response im SIEM-Kontext – Ein Erfahrungsbericht

- Erfolgreiche Angreifer erreichen meist innerhalb von 24 Stunden ihr Ziel
- Ein SIEM-System erlaubt, Angriffe in nahezu Echtzeit zu erkennen
- Eine zeitnahe Behandlung ermöglicht eine effektive Schadensreduktion
- Geeignete Prozessgestaltung reduziert den Personalbedarf signifikant
- Automatisierung kann die Incident Response effektiv unterstützen

D. Mahrenholz

rt-solutions.de GmbH

12.00 Uhr Android in SIEM-Umgebungen

- Monitoring von Smartphones und Tablets in SIEM-Umgebungen?
- Einbindung in Icinga- und TNC IF-MAP-basierte Lösungen
- Zustandsbewertung durch Metadaten und Events
- Umsetzung und Implementierung (DECOmap for Android)
- Einsatz in SIEM-Projekten und Ausblick

M. Schölzel

E. Eren

FH Dortmund

K.O. Detken

DecoIT GmbH

12.25 Uhr Gemeinsame Mittagspause



Mittwoch • 9. September 2015

Angriff & Abwehr • Leitung: K. Knorr

A

13.25 Uhr Forensische Sicherung von DSL-Routern

- Entwicklung von Methoden zur Systemanalyse von DSL-Routern
- Ermittlung von forensisch relevanten Hard- und Softwarekomponenten
- Kommunikation mit dem DSL-Router – JTAG und UART
- Welches Gerät liegt vor – Bootloader- und Betriebssystemanalyse
- Einfache Möglichkeiten zur Anfertigung von forensischen Sicherungen

H. Hoefken

S. Braun

M. Schuba

FH Aachen

M. Breuer

LKA NRW

13.50 Uhr Bedrohungslage von SAP Systemen durch ABAP Eigenentwicklungen

- Übersicht über die kritischsten ABAP Risiken
- Statistische Datenbasis von über 200 Unternehmen weltweit
- Vorstellung der BIZEC APP/11 und der BSI Top 20 ABAP Risiken
- Live-Demonstration ausgewählter ABAP Risiken
- Praxisbezogene Empfehlungen für die sichere Entwicklung mit ABAP

A. Wiegstein

Virtual Forge GmbH

14.15 Uhr Schutz eingebetteter Systeme gegen physische Angriffe

- IoT-Protokolle wie LWM2M nutzen DTLS-PSK als Security-Layer
- Schlüssel sind im Flash aber nicht vor physischen Angriffen geschützt
- Hardware-Security-Module bieten Schutz
- Schnittstellen und Mechanismen verfügbarer HSM sind aber proprietär
- Integration solcher HS-Module in DTLS ohne Protokolländerungen

J. Bauer

Bosch Software

Innovations GmbH

F. Freiling

Uni Erlangen-

Nürnberg

14.40 Uhr Kommunikationspause

Internet of Things & Automatisierung • Leitung: H. Storck

A

15.10 Uhr Autorisierungsmanagement für das Internet of Things

- Sicherstellen von Integrität und Vertraulichkeit im Internet der Dinge
- Besondere Anforderungen durch die Einsatzszenarien von Smart Objects
- Autonome Umsetzung von Autorisierungsentscheidungen durch die Geräte
- Dynamischer Wechsel der Entscheider von Autorisierungsregeln
- Maßnahmen zum Schutz der Autorisierungsübergänge im Gerätelebenszyklus

S. Gerdes

O. Bergmann

Uni Bremen

R. Hummen

RWTH Aachen

15.35 Uhr OPC UA vs. MTConnect – Sicherheit von Standards für Industrie 4.0

- Webservice- vs. Webtechnologien für M2M-Kommunikation
- Welche Sicherheit für die Automatisierung?
- Schwachstellen und Risiken in den Standards im Vergleich
- Was macht einen guten Standard aus?
- Lessons learned für sichere Industrie 4.0

D. Fuhr

HiSolutions AG

16.00 Uhr BACtag – Data Leakage Protection für Gebäude

- Data Leakage in der Gebäudeautomation als Gefahr
- BACnet als Referenzprotokoll für die Untersuchung von DLP
- Vorstellung eines Ansatzes für ein Plus an Sicherheit
- Filterung des Traffic im Gebäudenetzwerk
- Praktischer Ansatz für DLP in der Gebäudeautomation

E. M. Anhaus

FU Hagen

S. Wendzel

Fraunhofer FKIE

16.25 Uhr Konferenzende

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

• Big Data und Datenschutz

M. Steinebach Fraunhofer SIT

• Event-Korrelation in SIEM-Systemen auf Basis von IF-MAP

K.O. Detken, T. Rix Decoit GmbH

F. Heine, L. Renners Hochschule Hannover

Die Beiträge dieser Referenten finden Sie auch im Tagungsband zur Konferenz



Anmeldung & Teilnahmebedingungen

D·A·CH Security 2015

8. und 9. September 2015

Hochschule Bonn-Rhein-Sieg
Campus St. Augustin

Anmeldung zur Konferenz

Telefon: +43 (0) 463 2700 3702

Online-Anmeldung unter:

http://www.syssec.at/ds15_anmeldung

Teilnahmebedingungen

Bei Anmeldung bis zum 3. August 2015 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 3. August 2015 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75,- erhoben. Nach dem 3. August 2015 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. Schar tner** Uni Klagenfurt • **K. Lemke-Rust** HS Bonn-Rhein-Sieg • **M. Ullmann** BSI

P. Beenken Porsche AG • **J. Dittmann** Uni Magdeburg • **D. Engel** FH Salzburg • **W. Fischer** Infineon
J. Fuß FH Hagenberg • **M. Hartmann** SAP • **D. Henze** TÜV TRUST IT GmbH • **P. Horster** Uni Klagenfurt
D. Hühlein ecsec GmbH • **G. Jacobson** Secardeo GmbH • **S. Janisch** Uni Salzburg • **B. Klein** KPMG
K. Knorr HS Trier • **T. Kob** HiSolutions AG • **U. Korte** BSI • **P. Kraaibeek** secunet • **W. Kühnhauser** Uni Ilmenau
P.J. Kunz Daimler • **S. Lechner** JRC • **H. Leitold** A-SIT • **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** Giesecke & Devrient • **S. Rass** Uni Klagenfurt
H. Reimer DuD • **A. Roßnagel** Uni GH Kassel • **W. Schäfer** • **M. Spreitzenbarth** Siemens CERT
H. Stor ck T-Systems GmbH • **R. Szerwinski** Bosch • **S. Teufel** Uni Fribourg • **P. Trommler** GSO HS Nürnberg
T. Tschersich Deutsche Telekom • **G. Weck** Infodas • **C. Wegener** Uni Bochum • **E. Weippl** SBA Research
S. Werth BM des Innern • **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 & Co. KG

K. Kirst PTLV • **D. Koschützki** HS Furtwangen
S. Leuchter HS Rhein-Waal • **P. Reymann** ITQS
J. Voßbein UIMC • **C. Stark** Citigroup AG
R. Welter IABG mbH

Workshop der Allianz für Cyber-Sicherheit (ACS)

Organisatoren: **I. Münch** BSI • **K. Alberts** BSI

P.J. Kunz Daimler AG • **M. Meier** Uni Bonn
S. Werth BM des Innern • **R. Szerwinski** Robert Bosch GmbH
N. Pohlmann FH Gelsenkirchen • **H. Mühlbauer** TeleTrust
B. C. Witt it.sec GmbH & Co. KG • **I. Münch** BSI

Organisation

D. Cechak Uni Klagenfurt • **K. Lemke-Rust** HS Bonn-Rhein-Sieg • **M. Möhlmann** • **P. Schar tner** Uni Klagenfurt
M. Ullmann BSI

Leitungsgremium der Konferenzreihe

P. Horster Uni Klagenfurt • **P. Schar tner** Uni Klagenfurt