



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



D·A·CH Security

EWE Forum „Alte Fleiwa“ und OFFIS – IT-Quartier Oldenburg
20. und 21. September 2011



Aktuelle Informationen: <http://www.syssec.at/ds11>





Dienstag • 20. September 2011

08.30 Uhr Registrierung, Kaffee und Tee

09.15 Uhr Grußwort des Oberbürgermeisters Prof. Dr. Gerd Schwandner
Begrüßung und Überblick durch die Veranstalter

Mobile Datenträger • Leitung: K.-D. Wolfenstetter

A

09.35 Uhr Datenträgerschleusen: Firewalls für mobile Datenträger

- Sicherheitsrisiko mobile Datenträger
- Übersicht zu aktuellen Schutzmaßnahmen
- Perimeter-basierte Absicherung
- Schutzmaßnahme Datenträgerschleusen
- Aufgaben und Funktionen von Datenträgerschleusen

T. Warns
T. Dörge
PRESENSE
Technologies
GmbH

10.00 Uhr Kostengünstiger Datenschutz auf USB-Sticks

- Schutz vor Gelegenheitsangriffen im Büro oder auf Reisen
- Schutz gegen forensische Analyse
- Einsatz auf handelsüblichen USB-Sticks, keine Spezialhardware
- Schneller als Verschlüsselung
- Einfach im Management

H. Langweg
R. Søybe
Ø. Nilsen
K. Borg
NISlab

10.25 Uhr Optimierte Fehleremulation zur Verifikation von Chipkarten

- Verifikation von Sicherheitsprozessoren im Entwicklungsstadium
- Abstraktion von Fehlerattacken durch Fehlermodelle
- Implementierung einer FPGA-basierten Fehleremulationsumgebung
- Individuelle Anpassung der Fehleremulation während der Hardware-Synthese
- Optimierungsansätze zur Verbesserung der Emulationsgeschwindigkeit

R. Nyberg
D. Rabe
Hochschule
Emden/Leer

10.50 Uhr Kommunikationspause

Digitale Signaturen • Leitung: A. Philipp

A

11.20 Uhr Mobile Authentisierung und Signatur

- Mobile Nutzung des neuen Personalausweises
- Mobiltelefon als Chipkartenterminal oder mobile AusweisApp
- Mobiltelefon als aktives Authentisierungstoken
- Verteilter Komfort-Chipkartenleser zur (mobilen) Signaturerzeugung
- Rechtliche Aspekte des PIN-Sharing zur Signaturerzeugung

M. Horsch
J. Braun
A. Wiesmaier
TU Darmstadt
D. Hühnlein
ecsec GmbH

11.45 Uhr Elektronisch signierende Endgeräte im Forschungsprozess

- Gute wissenschaftliche Praxis und digitale Forschungsdaten
- Sicherung der Integrität über den gesamten Scientific Data Lifecycle
- Steigerung des Beweiswerts durch signierende Endgeräte
- BeLab: Webservice zur Überprüfung und Klassifizierung von Forschungsdaten
- Webservice als Middleware zwischen elektr. Laborbuch und Langzeitarchiv

S. Rieger
J. Potthoff
Karlsruher (KIT)
P.C. Johannes
Uni Kassel
M. Madiesh PTB

12.10 Uhr IDS-Signaturen für automotive CAN-Netzwerke

- Anwendung von Intrusion Detection auf automotive On-Board-Netzwerke
- Untersuchung der Anwendbarkeit signaturbasierter IDS-Konzepte
- Konzepterstellung und Anwendung auf beispielhafte Security-Vorfälle
- Implementierung auf Prototypingssystem für das Controller Area Network (CAN)
- Evaluierung von Konzept und Umsetzung hinsichtlich Funktion und Performanz

T. Hoppe
F. Exler
J. Dittmann
Uni Magdeburg

Modellierung und Frameworks • Leitung: G. Welsch

B

11.20 Uhr Wechselwirkungsmodell der Safety und Security

- Wechselwirkungsmodell der Safety und Security für eingebettete Systeme
- Bedrohungsmodell der Security eingebetteter Systeme nach der CERT-Taxonomie
- Gefährdungsmodell der Safety eingebetteter Systeme auf Basis von CERT
- Exemplarische Wechselwirkungsmodellierung für automotive Systeme
- Exemplarische Risikoanalyse auf Basis des Wechselwirkungsmodells

C. Neubüser
J. Fruth
T. Hoppe
J. Dittmann
Uni Magdeburg

11.45 Uhr Kontextmodellierung und Policies für die Langzeitarchivierung

- Digitale Langzeitarchivierung
- Konstruktion von Kontextmodellen
- Use-case-getriebene Kontextualisierung
- Ableitung von hierarchischen Sicherheitspolicies aus Use-cases
- Implementation und Durchsetzung von Policies

M. Schott
C. Krätzer
K. Qian
J. Dittmann
Uni Magdeburg

Dienstag • 20. September 2011

12.10 Uhr Entwicklung eines Industrial Information Security Frameworks

- Industrial Automation and Control Systems
- Automatisierungs- und IT-Systeme – Unterschiede und Gemeinsamkeiten
- I2S Framework
- Secure by Design
- Information Security: Technik vs Management

H. Dirnberger

K. Flieder

Ferdinand Porsche
FernFH

12.35 Uhr Gemeinsame Mittagspause

Schwachstellenanalyse • Leitung: N. Pohlmann

A

13.35 Uhr Mustererkennungsverfahren zur Angriffsdetektion im Smart Grid

- Angriffsdetektion im Smart Grid
- Angriffspotenziale auf die kritische Infrastruktur der Energieversorgung
- Exemplarische Betrachtung eines domänenspezifischen Angriffs
- Intrusion Detection auf Basis von IEC 62351-7
- Ontologiebasierte Mustererkennung

C. Rosinger

P. Beenken

S. Lehnhoff

OFFIS – Institut
für Informatik

14.00 Uhr Zustandsbasierte Anomalieerkennung im HTTP Protokoll

- Problemstellung: Bekannte Ansätze, Erweiterung und Abgrenzung
- Markov Modelle
- Aufbau des Hidden Markov Modells zur Anomalie-Erkennung im HTTP Protokoll
- Implementierung eines Prototyps
- Testergebnisse des Prototyps

B. Vamos

FH Hagenberg

14.25 Uhr Automatisierung von Penetrationstest-Berichten mittels CWE

- Ziele und Klassifikation von Penetrationstests
- Bestehende Verfahren für Penetrationstests
- Common Weakness Enumeration: Historie, Struktur und Inhalte
- Automatisierung der Erstellung von Penetrationstest-Berichten
- Erfahrungen aus der toolunterstützten Erstellung von Berichten

K. Knorr

FH Trier

U. Rosenbaum

Siemens AG

14.50 Uhr Neue Angriffe auf interne Daten erfordern adäquate Lösungsarchitekturen

- Angriffe von mobilen Datenträgern und Anwendungen verhindern
- Sicherheitsprobleme von Funkschnittstellen, PDAs und portablen Geräten
- Unerwünschten Datenabfluss erkennen und verhindern
- Automatische Virtualisierung problematischer Daten und Anwendungen
- Vertraulichkeit mobiler Information/Datenträger unterwegs gewährleisten

R. Mörl

itWatch

Zugriffskontrolle • Leitung: J. Pohle

B

13.35 Uhr Zugriffskontrolle in der Datenbank: Vamos eine Fallstudie

- VAMOS: Internetbasierte Pflegeunterstützung
- Modell der Zugriffskontrolle für einzelne Datensätze
- Zugriffskontrolle mit Hilfe von parametrisierten Views
- Sprache zur Spezifikation der Zugriffskontrolle
- Ausblick zur Integration in einen Softwareentwicklungsprozess

P. Trommler

S. Prijovic

Georg-Simon-Ohm-
Hochschule
Nürnberg

14.00 Uhr Implementierung von Zugriffskontrollen für Legacy OGC WS

- Sicherheitsaspekte von Geodaten in Webservices
- Problematik von Legacy (OGC) Webservices
- Bestehende Ansätze zur Lösung der Problematik
- Vereinheitlichte Sicherheitsarchitektur für alte und neue OGC Webservices
- Mögliche Nutzung von existierenden FOSS Komponenten und Standards

C. Wagner

A. Bonitz

Z. Ma, T. Bleier

AIT Austrian
Institute of
Technology GmbH

14.25 Uhr Gesundheitsdaten in der Cloud

- Praxisbeispiele aus Europa und den USA
- Chancen des Cloud Computing für Leistungserbringer und Leistungsbezüger
- Risiken aus rechtlicher Sicht betrachtet
- Rechtliche Rahmenbedingungen für eine Migration in die Cloud
- Effiziente Umsetzung, Grenzen und rechtlicher Handlungsbedarf

U. Widmer

Dr. Widmer

& Partner

14.50 Uhr Data Loss Prevention – Geheimnisschutz, Konkurrenzschutz, Datenschutz

- Data-Loss-Prevention-Systeme und Information-Rights-Management
- Deep Packet Inspection, Session Tracking, linguistische Analyse
- Geheimnisschutz und Konkurrenzschutz im Beschäftigungsverhältnis
- IT-Sicherheitsmaßnahmen und DSGVO – Was ist (noch) zulässig?
- Mitarbeiterinformation vs. heimlicher Schutz durch den Arbeitgeber

I. Conrad

SSW München

15.15 Uhr Kommunikationspause



Rechtliche Aspekte • Leitung: J. Taeger

A**15.45 Uhr Cmc – Compliance meets Cloud**

- Verfügbarkeit, Garantiehaftung und Service Level Agreements
- Datenschutz, Datensicherheit und sektorspezifische Anforderungen
- Urheber- und telekommunikationsrechtliche Aspekte
- Rechtsprobleme im internationalen Kontext
- Kartellrechtliche Fragen und vieles mehr

J. Pohle
DLA Pipe**16.10 Uhr Rechtliche Aspekte der Netzneutralität**

- Begriffsdefinition der Netzneutralität
- Rechtliche Rahmenbedingungen in den USA und EU
- Die Netzneutralität in der Novelle zum TKG 2011
- Benötigen wir eine stärkere Regulierung der Netzneutralität?
- Ausblick über die weitere Entwicklung

M. Baumgärtel
Justiziar
EWE TEL GmbH**16.35 Uhr Sensible Unternehmensdaten präventiv schützen**

- Rollen erkennen, Rechte festlegen, sensible Daten kennzeichnen
- Transparenz über den Umgang mit sensiblen Daten erlangen
- Rollenbedingte Regeln zur Verarbeitung sensibler Daten festlegen
- Die Verarbeitung und Speicherung sensibler Daten kontrollieren
- Regeln technisch durchsetzen – präventiv ungewollten Datenabfluss vermeiden

R. Krüger
secunet AG
U. Oesing
FH Jena**17.00 Uhr Kontrolle von Beschäftigten mittels Videoüberwachung**

- Bedarf der Videoüberwachung zum Schutz eines Unternehmens
- Rechtfertigung der Mitarbeiterkontrolle
- Unterscheidung von öffentlichem und nicht-öffentlichem Raum
- Schutz der Privatsphäre von Mitarbeitern
- Videokontrolle nach dem Entwurf zum BeschäftigtendatenschutzG

B. A. Mester
Carl von Ossietzky
Universität
Oldenburg

Risiko- und Sicherheitsmanagement • Leitung: J. Schneider

B**15.45 Uhr Studie zu IT-Risikobewertungen in der Praxis**

- Verwendete Bewertungsverfahren, Kriterien und Daten in der Praxis
- Identifikation von Risiken
- Subjektivität von IT-Risikobewertungen
- Sicherheitsanforderungen und Prozessmodelle für die IT-Risikobewertung
- IT-Risikobewertungen kombiniert mit Compliance- und Risikomanagement

S. Taubenberger
Open University
J. Jürjens
TU Dortmund**16.10 Uhr Ein standardkonformer Patch Management Prozess**

- Betrachtung der gängigen Industriestandards für das Patch Management
- Berücksichtigung der Anforderungen großer Industrieunternehmen
- Einbeziehung technischer und organisatorischer Fragen
- Ableitung eines standardkonformen Patch Management Prozesses
- Vorstellung einer industrieübergreifenden Lösung

M. Bühler
G. Rohrmair
HS Augsburg
M. Ifland, N. Lode
K. Lukas
Siemens AG**16.35 Uhr ISO/IEC 27033 und IT-Grundschutz: Ein Vergleich**

- Neuer ISO-Standard zur Netzwerksicherheit
- Überschneidung/Gemeinsamkeiten mit den IT-Grundschutzkatalogen
- Unterschiede in der Behandlung und Aufbereitung der Thematik
- Exemplarische Gegenüberstellung anhand von Beispielen
- Ansätze für eine ergänzende Anwendung beider Standards in Risikoanalysen

F. Rustemeyer
HiSolutions AG**17.00 Uhr Werkzeuggestützte Identifikation von IT-Sicherheitsrisiken**

- Vereinfachung der Risikoidentifikation und -behandlung
- Verknüpfung mit Standards wie BSI-Grundschutz sowie Expertenwissen
- Integration der Informationssicherheitsprozesse in Geschäftsprozesse
- Flexible Anpassung an das Risikomanagement des Unternehmens
- Steuerung der Risiken im Cloud Computing

J. Jürjens
Fraunhofer ISST**17.25 Uhr Ende erster Konferenztag****18.00 Uhr Gemeinsames Abendessen****19.30 Uhr Konzert der Big Band der Liebfrauenschule Oldenburg**

Clouds und Crowds • Leitung: W. Schäfer

A**09.00 Uhr Cloudsicherheit ohne vertrauenswürdige Administration**

- Eigenschaften des Cloud-Computing
- Bisherige Ansätze zum Schutz von Daten in der Cloud
- IT-Administration, Vertrauensmodelle für privilegierte User
- Ansatz des DaPriM-Projektes zur Cloud-Administration
- Präsentation des Prototypen

U. Greveler**B. Justus****D. Löhr**

FH Münster

09.25 Uhr Sec2 – Ein sicheres Speicherkonzept für die Cloud

- Mobiles Konzept für sichere, nutzerkontrollierte Cloud Speicher
- Sicherheit in Händen des Nutzers – unabhängig vom Diensteanbieter
- Flexibel, skalierbar und nahtlos zu integrieren
- Mehrstufiges Schlüsselkonzept
- Aufbauend auf bestehenden Technologien

C. Meyer, J. Somorovsky, B. Driessen,**J. Schwenk**

Uni Bochum

T. Tran, C. Wietfeld

TU Dortmund

09.50 Uhr SkIDentity – Vertrauenswürdige Identitäten für die Cloud

- Angriffe gegen schwache Authentisierung in der Cloud
- SkIDentity – die Brücke zwischen eID und Cloud
- Rechtliche Aspekte für eID in der Cloud
- Geschäftsmodelle für eID in der Cloud
- „Trusted Cloud“ Wettbewerb des BMWi

J. Schmölz, T. Wich

ecsec GmbH

G. Hornung Uni Passau**H. Roßnagel****J. Zibuschka**

Fraunhofer IAO

10.15 Uhr Crowds mit beeinflussbarer Empfängeranonymität

- Kombination von Crowds und Mix-Net
- Verbesserte Empfängeranonymität durch Secret Sharing
- Keine Verwendung von asymmetrischer Kryptographie
- Vom Sender beeinflussbarer Anonymitäts-Level
- Empfängeranonymität ohne Verwendung von Padding

R. Wigoutschnigg**P. Schartner****S. Rass**

Uni Klagenfurt

Daten- und Jugendmedienschutz • Leitung: B. Mester

B**09.00 Uhr Technische Möglichkeiten des Jugendmedienschutzes**

- Sachstand nach der gescheiterten Novellierung des JMStV in 2010
- Zukunft von Jugendschutzprogrammen (Anerkennung, Verbreitung)
- Freiwillige Alterskennzeichnung von Telemedien-Angeboten (Tools, Labels)
- Altersverifikationssysteme – ohne Medienbruch?
- Technik und Recht – Was braucht der Jugendmedienschutz?

N. Schüttel

Referentin für Internet- und Medienrecht, eco Verband der deutschen Internetwirtschaft e.V.

09.25 Uhr Nutzung des elektronischen Rechtsverkehrs durch Rechtsanwälte

- Betrachtung aus datenschutz-/sicherheitsrechtlicher Perspektive
- Status Quo der Nutzung elektronischen Rechtsverkehrs
- (Sicherheits-)Rechtliche Verpflichtungen
- E-Mail, EGVP, De-Mail & Co.
- Anforderungen an Alternativen zur qualifizierten elektronischen Signatur

J. D. Roggenkamp

Referent im Bundesministerium der Justiz

09.50 Uhr Mobile Gewalt als Herausforderung für den Jugendmedienschutz

- Erscheinungsformen mobiler Gewalt
- Bedeutung mobiler Gewalt für Jugendliche
- Rechtliche Einordnung der mobilen Gewalt
- Möglichkeiten des Schutzes von Jugendlichen bei mobiler Gewalt
- Aufgaben für den Jugendmedienschutz

A. Ackermann

Kanzlei für Medien- und IT-Recht

10.15 Uhr Effizienter Datenschutz durch Einbeziehung betrieblicher Mitbestimmung

- Datenschutz im Spannungsfeld der betrieblichen Mitbestimmung
- Zukunft der Betriebsvereinbarung als Rechtsgrundlage
- Ansätze für eine effiziente Einbindung der Interessenvertretungen
- Konkrete Beispiele für mögliche Regelungsstatbestände in der Praxis
- Datenschutz in der Arbeit der betrieblichen Interessenvertretungen

J. Schultze-Melling

Leiter Mitarbeiterdatenschutz (CDM) DB Mobility LogisticsAG

10.40 Uhr Kommunikationspause



Mittwoch • 21. September 2011

Biometrie I • Leitung: P. Schartner

A

11.10 Uhr Abgleich im Erfassungsgerät

- Automatisierte Erfassung biometrischer Charakteristika
- Biometrische Systeme für Gefahrenabwehr und Strafverfolgung
- Dezentrale Verarbeitung biometrischer Daten
- Informationelle Selbstbestimmung und informationelle Gewaltenteilung
- Verfassungsverträgliche Technikgestaltung

M. Pocs
Uni Kassel

11.35 Uhr Fingerspurenfälschungsdetektion: Ein erstes Vorgehensmodell

- Rechtliche Grundlagen zur Zulassung von Beweismitteln in Verhandlungen
- Derzeitige ACE-V Methodologie für daktyloskopische Experten
- Einsatz von Modellen biometrischer Systeme in forensischen Untersuchungen
- Vorgehensmodell zur Detektion gefälschter Fingerspuren
- Integration der Detektion in aktuelle und zukünftige forensische Prozesse

S. Kiltz, J. Dittmann
Uni Magdeburg
I. Großmann
LKA Sachsen-Anhalt
C. Vielhauer
FH Brandenburg

12.00 Uhr Ausgewählte Biometrieverfahren zu Fingerspurdetektion

- Digitale Daktyloskopie
- Unterstützung forensischer Experten
- Biometrische vs. forensische Fingerspur-Analyse
- Detektion und Lokalisierung von Fingerabdrücken
- Erzeugung von ROI als Basis zur weiteren forensischen Analyse

R. Fischer
C. Vielhauer
FH Brandenburg

Mobilität und Überwachung • Leitung: F. Rustemeyer

B

11.10 Uhr Sichere Plattform zur Smartphone-Anbindung auf Basis von TNC

- Quarantänenetz zur Erhöhung des Sicherheitsgrades
- Einbindung unterschiedlicher Policies
- Neue Sicherheitsanforderungen für Smartphones
- Systemarchitektur des F&E-Projektes VOGUE
- Einbeziehung von Trusted Computing

K.-O. Detken
DECOIT GmbH

11.35 Uhr Zur Komplexität der Mobilfunkforensik am Beispiel des iPhone

- Daten- und Informationsauswertung
- Sensibilisierung und Weiterbildung
- Computer-Forensik
- Mobile Endgeräte
- Privacy und Datenschutzaspekte

H. Baier
CASED
A. Brand
C. Dichtelmüller
B. Roos
Hochschule Darmstadt

12.00 Uhr Spionage via Webcam

- Malware-Zugriff auf Webcam
- Virens Scanner und Personal Firewall
- Laborumgebung und Testergebnisse
- Ausnutzbare OS-Schnittstelle
- Gegenmaßnahmen

U. Greveler
M. Wellmeyer
FH Münster

12.25 Uhr Gemeinsame Mittagspause

Biometrie II • Leitung: U. Korte

A

13.25 Uhr Automatisierte Lokalisierung und Erfassung von Fingerspuren

- Gesamtprozess der automatisierten kontaktlosen Fingerspurerfassung
- Aufteilung der Fingerspurerfassung in Grob- und Feinscan
- Automatische Scanparameterbestimmung & Lokalisierung des Spurenträgers
- Fingerspurenlokalisierung im Grobscan (Regions-of-Interest)
- Fingerspurerfassung im Feinscan zur daktyloskopischen Untersuchung

M. Hildebrandt
S. Kiltz
J. Dittmann
Uni Magdeburg

13.50 Uhr Lebenderkennungsverfahren zur Gesichtsverifikation

- Lebenderkennung steigert die Sicherheit von biometrischen Systemen
- Spoofing-Attacken: Fotos, Videos, Gesichtsmasken, 3D-Modelle
- Beschreibung/Vergleich aktueller Lösungsansätze
- Evaluierung der aktuellen Lösungsansätze nach vordefinierten Kriterien
- Bewertung der Ergebnisse/Fazit/Ausblick

M. Rybnicek
C. Fischer
J. Kaufmann
FH St. Pölten

Mittwoch • 21. September 2011

14.15 Uhr Experimentelle Machbarkeitsstudie eines BioHash Algorithmus

- Anwendung biometrischer Kryptosysteme
- Dynamische Handschrift als Biometrie
- Eingebettetes biometrisches System auf einer Java Card
- Untersuchung der Leistungsfähigkeit/Machbarkeit
- Ergebnis einer exemplarischen Evaluierung

K. Kümmel
C. Arndt
T. Scheidat
C. Vielhauer
FH Brandenburg

Sicherheitsinfrastrukturen • Leitung: P. Beenken

B

13.25 Uhr Sicherheit in kritischen Infrastrukturen

- Smart Grid und Smart Meter verstärken die IT-technische Vernetzung
- Historisch gewachsene Arbeitsweisen bergen hohe Sicherheitsrisiken
- Customized Malware erfordert Umdenken bei Betreibern und Herstellern
- Holistische Ansätze zur Absicherung der Versorgungssicherheit
- Prozessorientierte Zertifizierung des Sicherheitsstatus statt Annahmen

J. Müller
M. Pietsch
BTC AG

13.50 Uhr Nutzerfreundliche Authentisierung für den Krankenhausalltag

- Authentisierungsverfahren im Krankenhaus: Überblick und Bewertungskatalog
- Untersuchung der Schutzbedürftigkeit von sensiblen Patientendaten
- Nutzbare Sicherheit: Berücksichtigung der speziellen Arbeitsbedingungen
- Konkurrierende Anforderungen: Verfügbarkeit, Vertraulichkeit, Integrität
- Rechtliche Rahmenbedingungen

S. Gerdes
O. Bergmann
Uni Bremen

14.15 Uhr Technikgestaltung bei Vorratsdatenspeicherung & Quick Freeze

- Bedeutung verfassungskonformer Technikgestaltung
- Technische Umsetzung datenschutzrechtlicher Anforderungen bei VDS und QF
- Spezifische Herausforderungen an die Technik
- Präsentation technischer Gestaltungsvorschläge
- Grenzen technischer Sicherheit

A. Knierim
Uni Kassel, provet

14.40 Uhr Kommunikationspause

E-Government und sichere E-Mail • Leitung: D. Hühnlein

A

15.10 Uhr Ein virtuelles Testframework für E-Government Komponenten

- Anforderungen von E-Government Komponenten an das Benutzersystem
- Plattformübergreifende Tests von E-Government Client-Komponenten
- Systematisches Auffinden umgebungsbedingter Sicherheitsschwachstellen
- Testframeworks basierend auf virtuellen Maschinen
- Evaluierung des Frameworks und Erfahrungsbericht

T. Zefferer
V. Krnjic
B. Zwattendorfer
TU Graz

15.35 Uhr Identity Certified Encryption

- PKI Interworking
- Spontane E-Mailverschlüsselung
- Ad-hoc Zertifikate
- Identity Based Encryption mit X.509
- Zertifikatsserver

G. Jacobson
Secardeo GmbH

16.00 Uhr Elektronisches Einschreiben im DACH-Raum

- Elektronisches Einschreiben zur sicheren und verlässlichen Zustellung
- OSCI, De-Mail und Postbrief als dominante Systeme in Deutschland
- E-Zustellung (ZUSE) und der ERV als dominante Systeme in Österreich
- IncaMail als Beispiel der Schweiz
- Vergleich und Diskussion der beschriebenen Zustellsysteme

A. Tauber
B. Zwattendorfer
T. Zefferer
TU Graz

16.25 Uhr Konferenzende

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

- **Attributbasierter Schlüsselaustausch in VPN** | **M. Roßberg, T. Köllmer, G. Schäfer** TU Ilmenau
- **Zertifizierung hochverfügbarer globaler Rechenzentren** | **C. Meinig** BTC AG
- **Ein Internet-Kennzahlensystem für Deutschland** | **S. Feld, N. Pohlmann, M. Deml** Institut f. Internetsicherheit
- **IT-Riskmanagement in der 4. Dimension: IdM-as-a-service** | **G. Rossa** iSM – Institut für System Management GmbH
- **Konsolidierung von Metadaten** | **K.-O. Detken** DECOIT GmbH

Die Beiträge dieser Referenten finden Sie auch im Tagungsband zur Konferenz



Anmeldung & Teilnahmebedingungen

D·A·CH Security 2011

20. und 21. September 2011

IT-Quartier Oldenburg

Anmeldung zur Konferenz

Telefon: +43 (0) 463 2700 3702

Fax: +43 (0) 463 2700 993702 oder

Online-Anmeldung unter: http://www.syssec.at/ds11_anmeldung

Teilnahmebedingungen

Bei Anmeldung bis zum 20. August 2011 beträgt die Teilnahmegebühr € 385.– (Frühmeldegebühr), danach € 470.– jeweils zuzüglich der gesetzlichen MwSt. Referenten zahlen nur die Referentengebühr von € 335.– 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 18. August 2011 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75.– erhoben. Nach dem 18. August 2011 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

Universität Klagenfurt

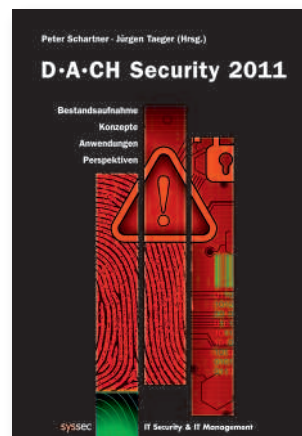
Forschungsgruppe Systemsicherheit (syssec)

Universitätsstr. 65-67

A-9020 Klagenfurt

URL: <http://www.syssec.at>

E-Mail: konferenzen@syssec.at



Programmkomitee:

J. Taeger Uni Oldenburg/DSRI • **P. Scharfner** Uni Klagenfurt

R. Ackermann SAP Research • **P. Beenken** OFFIS Oldenburg • **C. Busch** Fraunhofer IGD • **J. Dittmann** Uni Magdeburg • **W. Feiel** RTR GmbH • **S. Fenz** SBA Research • **J. Fuß** FH Hagenberg • **D. Gabel** White & Case
M. Hartmann SAP • **P. Horster** Uni Klagenfurt • **D. Hühnlein** ecsec GmbH • **S. Janisch** Uni Salzburg
D. Jäpel IBM CH • **T. Kob** HiSolutions • **U. Korte** BSI • **P. Kraaibeek** secunet • **W. Kühnhauser** Uni Ilmenau
P. J. Kunz Daimler • **S. Lechner** JRC • **H. Leitold** A-SIT • **C. Meinig** BTC AG • **H. Mühlbauer** TeleTrust
I. Münch BSI • **J. Neuschwander** HTWG Konstanz • **A. Philipp** Utimaco • **J. Pohle** DLA Piper Köln • **N. Pohlmann** FH Gelsenkirchen • **R. Posch** TU Graz • **W. Rankl** Giesecke & Devrient • **S. Rass** Universität Klagenfurt • **M. Rath** Luther RA-Gesellschaft • **H. Reimer** DuD • **J. Ritter** BTC AG • **A. Roßnagel** Uni GH Kassel • **W. Schäfer** DATEV
M. Schaffer NXP Semiconductors • **J. Schneider** SSW München • **H. Storck** Nokia Siemens • **S. Teufel** Uni Fribourg
G. Weck Infodas • **C. Wegener** Uni Bochum • **E. Weippl** SBA Research • **G. Welsch** BMI • **U. Widmer** RAe Dr. Widmer, Bern • **K.-D. Wolfenstetter** DTAG • **M. Zeilinger** FH Hagenberg

Organisation:

P. Beenken Uni Oldenburg • **D. Cechak** Uni Klagenfurt • **P. Scharfner** Uni Klagenfurt • **J. Taeger** Uni Oldenburg/DSRI