



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



# D·A·C·H Security

TU Graz | 16. und 17. September 2014



Aktuelle Informationen: <http://www.syssec.at/dachsecurity2014>





# Dienstag • 16. September 2014

08.30 Uhr **Registrierung, Kaffee und Tee**

09.30 Uhr **Begrüßung und Überblick**

## Sicherheitsmanagement • Leitung: R. Welter

A

### 09.35 Uhr **SIEM – Technik allein ist keine Lösung**

- Zielgerichtete Angriffe (APT) stellen die aktuell größte Bedrohung dar
- SIEM-Systeme können APT erkennen, um Schäden und Kosten zu minimieren
- Effektive SIEM-Systeme benötigen geeignete und effiziente Prozesse
- Bei der Umsetzung lauern viele Fallstricke und Hindernisse
- Geschicktes Prozessdesign hilft, die Herausforderungen zu meistern

**D. Mahrenholz**

**R. Schumann**

**A. Brüggemann**

rt-Solutions.de

GmbH

### 10.00 Uhr **SIEM-Ansätze zur Erhöhung der IT-Sicherheit auf MAP-Basis**

- SIEM-Definition und Ansätze
- SIEM-Technologien (u.a. Event Correlation, Identity Mapping)
- SIEM-Architektur auf Basis von IF-MAP
- Mehrwerte von SIEM-Systemen für Unternehmen
- Herausforderungen bei der Einführung

**K.O. Detken**

DECOIT GmbH

### 10.25 Uhr **Security Patch Management in Großunternehmen**

- Produkte und Lösungen setzen vermehrt auf Drittanbieter-Komponenten
- IT-Sicherheitsschwachstellen treten in Drittanbieter-Komponenten auf
- Eine zentralisierte Patch-Management-Lösung spart Zeit und Geld
- Schnittstellen zur Anbindung verschiedener Workflow-Systeme
- Einheitliche und unternehmensweite Namensgebung von Komponenten

**M. Ifland**

Siemens AG

10.50 Uhr **Kommunikationspause**

## Digitale Signaturen & Öffentliche Verwaltung • Leitung: R. Posch

A

### 11.20 Uhr **Design und Implementierung eines Localhost Signaturgateways**

- FutureID Client auf Basis des Open eCard Framework
- Add-on für elektronische Signaturen
- OASIS DSS Request-/Responseformat
- Abstraktion der Signaturerstellung mittels diverser Karten
- Integration der österreichischen Handy-Signatur

**D. Derler, C. Rath**

IAIK – TU Graz

**M. Horsch**

TU Darmstadt

**T. Wich**

Ecsec GmbH

### 11.45 Uhr **Standards und Lösungen zur langfristigen Beweiswerterhaltung**

- Beweiswerterhaltung elektronischer Unterlagen
- Standards und Normen zur vertrauenswürdigen Langzeitspeicherung
- Lösungsvorschläge zur vertrauenswürdigen Langzeitspeicherung
- Associated Signature Container+Evidence Records – ein Austauschformat
- Interoperabilität technischer Beweisdaten

**S. Schwalm**

**T. Kusber**

Bearing Point GmbH

**U. Korte, BSI**

**D. Hühnlein**

Ecsec GmbH

### 12.10 Uhr **Security by Isolation in der öffentlichen Verwaltung**

- Migration zu virtualisierten Anwendungen bei bestehendem Betrieb
- Schutz gegen Malware beim Laden von Dokumenten von Datenträgern
- Sicheres Surfen bei vollständigem Abtrennen des Browsersystems
- Unaufdringliche Integration in eine bestehende IT-Infrastruktur
- Der öffentliche Bereich: sanfte Integration im großen Maßstab

**O. Maurhart**

**R. King**

**M. Bartha**

AIT Austrian

Institute of

Technology

12.35 Uhr **Gemeinsame Mittagspause**

## Sicherheitsinfrastrukturen & Anwendungen • Leitung: P. Lipp

A

### 13.35 Uhr Absicherung von einer M2M-Telematikplattform

- Zentralisierte M2M-Kommunikationsinfrastruktur zwischen Landmaschinen
- Kommunikationsszenarien im landwirtschaftlichen Bereich
- Exemplarische IT-Infrastruktur und Komponenten
- Implementierung etablierter Protokolle und Tools
- Datenkommunikation und Ablage

J. Sell

E. Eren

S. Gansemer

T. Horster-Möller

FH-Dortmund

### 14.00 Uhr Anonymität und Mehrwegeübertragung

- Gesteigerte Anonymität durch Mehrwegeübertragung?
- Auswirkungen für Sender und Empfänger
- Gefahren durch den Predecessor-Angriff
- Evaluation durch Simulationen
- Vergleich mit bestehenden Systemen

R. Wigoutschnigg

Uni Klagenfurt

### 14.25 Uhr Absicherung von Smart-Meter-Umgebungen durch TC

- Einführung in ein Smart-Meter-Szenario
- Bewertung geeigneter Schutzverfahren (TCG versus BSI)
- SMGW-Integritätsprüfung mit Trusted-Computing-Verfahren
- Einsatz von Trusted Network Connect (TNC)
- Ausblick von Trusted Computing im Smart-Meter-Umfeld

K.O. Detken

DECOIT GmbH

K.H. Genzel

HS Bremen

### 14.50 Uhr Sicherheit von industriellen Steuerungssystemen

- Kritische Betrachtung des ICS-Security-Kompendiums
- BSI IT-Grundsicherheits-Vorgehensweise bei ICS
- Best-Practice Maßnahmen
- Gefährdungen und Risikoanalyse für ICS
- Ausblick für weitere Aktivitäten

A. Floß

HiSolutions AG

### 15.15 Uhr Kommunikationspause

## Digitale Forensik & Angriffstechniken • Leitung: K. Lemke-Rust

A

### 15.45 Uhr Digitalisierte Forensik: Sensorbildfusion und Benchmarking

- Design eines Fusionsframeworks für die intra-/inter Sensorfusion
- Subjektiver und objektiver Vergleich von Sensor-/Featurelevelfusion
- Benchmarking zerstörungsfreier, kontaktloser, optischer Messtechnik
- Untersuchung der Reproduzierbarkeit von Sensorsignalen und Artefakten
- Evaluation anhand latenter Fingerspuren als ausgewählter Tatortspur

C. Krätzer

M. Hildebrandt

A. Dobbert

J. Dittmann

Uni Magdeburg

### 16.10 Uhr Angriffsszenarien auf Truecrypt

- Ist das Team hinter TrueCrypt ein Phantom?
- Angriffe via Trojaner, Analyse des RAM, IO Control Codes, Kopien von Images
- Kommerzielle Software „gewinnt“ Schlüssel für BitLocker, TrueCrypt und PGP
- Gegenmaßnahmen in GUI und Treiber sind noch weitestgehend unbekannt
- Konkrete Maßnahmen, mit denen TrueCrypt effektiv gehärtet werden kann

B. Röllgen

Global IP

Telecommunications

### 16.35 Uhr Ende erster Konferenztag

### 18.30 Uhr Gemeinsames Abendessen



Mittwoch • 17. September 2014

**Compliance & Risikomanagement • Leitung: G. Jacobson**

**A**

**09.00 Uhr IT Compliance mit kontextuellen Sicherheitsanforderungen**

- Ganzheitliches Sicherheitsmanagement auf Basis von Unternehmensmodellen
- Kooperative Definition und Verwaltung kontextueller Sicherheitsanforderungen
- Hoher Automatisierungsgrad beim Überwachen von Sicherheitsanforderungen
- Frei konfigurierbare change-getriebene Workflows
- Demonstration des Tools adamant

**M. Brunner**

**R. Breu**

Uni Innsbruck

**09.25 Uhr Kennzahlen im Informationssicherheitsmanagement**

- Sicherheitskennzahlen ergänzen Audits
- Sie sind Bestandteil eines standardkonformen ISMS
- Ziele der Nutzung von Kennzahlensystemen
- Gute Kennzahlen
- Erfahrungen aus Beispielimplementationen

**M. Stöwer**

**R. Kraft**

Fraunhofer-  
Institut SIT

**09.50 Uhr Entwicklung einer Test-Umgebung für Risiko-Assessmenttools**

- Risiko-Management
- Generische Test-Umgebung für Risiko-Assessments
- Evaluation von Risiko-Assessmentmethoden
- Identifikation von Angriffsstrategien durch das Doppelvektor-Modell
- CIA+-Sicherheitsbewertung von Kommunikationskanälen in Unternehmen

**S. Schauer**

AIT

**A. Peer, J. Göllner**

BMLVS

**S. Rass**

Uni Klagenfurt

**10.15 Uhr Kommunikationspause**

**Datenkontrolle & Rechtliche Aspekte • Leitung: P. Schartner**

**A**

**10.45 Uhr Datenkontrolle mit Software für Informationsrechteverwaltung**

- Verschlüsselungsverfahren beim Formular- und Dokumentenschutz
- Identitäts- und Schlüsselmanagement der Informationsrechteverwaltung
- Planung und Implementierung von Informationsrechten in Organisationen
- Abgrenzung Data Leakage Prevention und Informationsrechteverwaltung
- Beispiele Informationsrechteverwaltung verschiedener Plattformen

**D. Scherrer**

BLUESITE

**11.10 Uhr Wahrnehmung der Richtlinien von Facebook**

- Facebook's Datenverwendungsrichtlinien aus der Perspektive der Nutzer
- Besorgnis der Nutzer über die Datenweitergabe seitens Facebook
- Ursache und Hintergründe für das Akzeptieren der Facebook AGBs
- Wahrnehmung der Facebook Nutzungsbedingungen aus Sicht der Mitglieder
- Ausblick und weitere Entwicklung

**N. Hintz**

**W. Schwarz**

Uni Erlangen-  
Nürnberg

**11.35 Uhr Schutz nicht nur der Inhalte, sondern auch der Metadaten**

- Datenschutz-Herausforderungen für Cloud-Dienste
- Die Sealed-Cloud-Versiegelung
- Betreibersicherheit
- Pseudonymisierung von Fremdschlüsseln
- Versiegelte Dekorrelation

**H. Jäger**

Unicon GmbH

**12.00 Uhr Outsourcing im Massengeschäft sicher und rechtskonform**

- Outsourcing ist datenschutzrechtliche Auftragsdatenverarbeitung
- Das Gesetz passt für große Outsourcing-Vorhaben, nicht für die Cloud
- Umfangreiche Verträge und Kontrollen des Anbieters sind vorgeschrieben
- Massenverkehr braucht Standard-Verträge und Standard-Sicherheitsniveaus
- Die Kontrolle der Sicherheit können Zertifikate Dritter übernehmen

**M. Bergt**

von BOETTICHER

Rechtsanwälte

## Workshop der GI-FG SECMGT • Leitung: I. Münch & B. Witt

B

### 10.45 Uhr Ganzheitliche Informationssicherheit bei Banken

- Zahlreiche Anforderungen für Banken
- Haftungsentlastung durch best practices (statt good practice)
- Cross-Control-Mapping beim IT-GRC-Management nötig
- Herausforderungen an die IT-GRC-Infrastruktur
- Beispiele guter Praxis

**B.C. Witt**

it.sec GmbH&Co.KG

### 11.35 Uhr Cyber-Sicherheits-Check

- Reflektion des Leitfadens Cyber-Sicherheits-Check
- Einführung in die Cyber-Sicherheit und aktuelle Lage
- Grundsätze und Voraussetzungen zur Durchführung
- Durchführung eines Cyber-Sicherheits-Checks
- Weiterbildung zum Cyber-Security-Practitioner

**M. Becker**

BSI

### 12.25 Uhr Gemeinsame Mittagspause

## eGovernment & Identitätsmanagement • Leitung: H. Leitold

A

### 13.25 Uhr Umsetzung von vertrauenswürdigen Open Government Data

- Open Government Data (OGD) für Veröffentlichung von öffentlichen Daten
- Authentizität und Integrität fanden bisher wenig bis keine Beachtung
- Vertrauenswürdige OGD mittels elektronischer Signaturen
- Signaturfähigkeit von OGD Formaten
- Architektur und Umsetzung eines vertrauenswürdigen OGD

**K. Stranacher**

**B. Zwattendorfer**

**S. Fruhmann**

**P. Koch**

EGIZ

### 13.50 Uhr Föderiertes Identitätsmanagement in der Cloud

- Identitätsmanagement-Modelle in der Cloud
- Föderation von unterschiedlichen Cloud Identity Brokern
- Prototypische Implementierung mit OpenID/Twitter als Identity Provider
- Schutz der Daten durch Verwendung von Proxy Re-Encryption
- Daten unter der Kontrolle des Benutzers

**B. Zwattendorfer**

**K. Stranacher**

EGIZ

**F. Hörandner**

TU Graz

### 14.15 Uhr IdP zur Verifikation der vertrauenswürdigen digitalen Identität

- Vertrauenswürdige digitale Identität
- Identity Provider Modell mit Trusted Third Party (TTP)
- Verifikation der vertrauenswürdigen digitalen Identität
- Identity Provider Modell mit dem neuen Personalausweis (nPA)
- Modell auf andere TTP und Objekt-IDs des Internet der Dinge anwenden

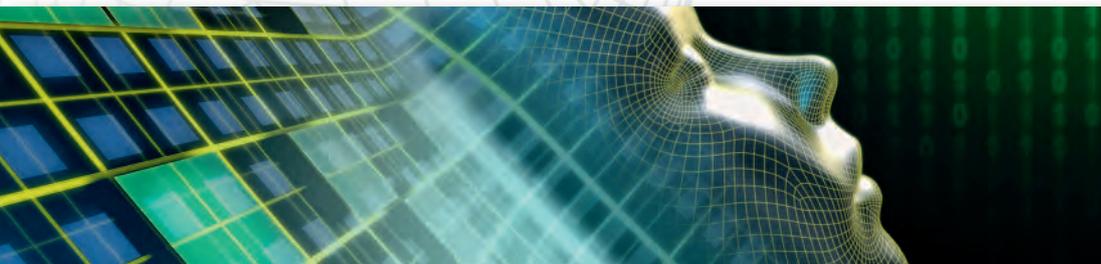
**A. González Robles**

**N. Pohlmann**

if(is) – Westfälische  
Hochschule

Gelsenkirchen

### 14.40 Uhr Kommunikationspause





Mittwoch • 17. September 2014

**Mobile (Un)Sicherheit • Leitung: H. Storck**

**A**

**15.10 Uhr Zum sicheren Löschen auf Smartphones**

- Sicherheit der vom Android System bereit gestellten Löschmöglichkeiten
- Konzeptionierung unterschiedlicher sicherer Löschrategien
- Prototyp zum sicheren Löschen von Daten im Flashspeicher
- Blockweises Löschen auf NAND Flashspeicher
- Verteilung der Daten durch Wear Leveling und Bad Block Management

**15.35 Uhr Architekturelle Sicherheitsanalyse für Android Apps**

- Automatische Extraktion der Sicherheitsarchitektur von Android Apps
- Architekturelle Sicherheitsanalyse von (hybriden) Android Apps
- Konzeptionelle Sicherheitsprobleme in Software identifizieren
- Frameworkspezifische Sicherheitsprobleme in Software identifizieren
- Wissensdatenbank mit architekturellen Sicherheitsregeln

**16.00 Uhr Aktuelle Grenzen der mobilen Sicherheit**

- Status Quo und Herausforderungen
- State-of-The-Art Abwehr und protektive Technologien
- Grenzen rechtlicher und ethischer Zulässigkeit von Sicherheitslösungen
- Wie können Schwachstellen eliminiert werden?
- Die zukunftsgerichtete Lösung für die wahre mobile Sicherheit

**16.25 Uhr Konferenzende**

**B. Roos**

**H. Baier**

**P. Lyko**

Hochschule

Darmstadt/CASED

**B. Berger**

**K. Sohr**

Uni Bremen

**U. Kalinna**

ifAsec GmbH

**P. Papagrigoriou**

EMPELOR GmbH

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

**Risikokommunikation**

- Besondere Merkmale von Risikokommunikation in einer IT Schadenslage
- Mögliche Folgen für das Krisenmanagement
- Ursachen für Problemquellen
- Methoden zur Messung
- Lösungsvorschläge zur Prävention

**ISMS im Bereich der Energieversorgung und -messung**

- Vorgaben für Smart Meter Gateway Betreiber
- Vergleich ISO 27019 und BSI TR 03109
- BSI IT-Grundschutz-Vorgehensweise im Bereich Smart Meter
- Best Practice Maßnahmen
- Ausblick und notwendige weitere Aktivitäten

**N. Wlczek**

IABG mbH

**T. Goldschmidt**

HiSolutions AG

Die Beiträge dieser Referenten finden Sie auch im Tagungsband zur Konferenz

## Programmkomitee

Vorsitz: **P. Schartner** Uni Klagenfurt • **P. Lipp** TU Graz

**R. Ackermann** SAP Research • **P. Beenken** Porsche AG • **R. Bloem** TU Graz • **J. Dittmann** Uni Magdeburg  
**D. Engel** FH Salzburg • **J. Fuß** FH Hagenberg • **M. Hartmann** SAP • **P. Horster** Uni Klagenfurt  
**D. Hühlein** 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** Uni Ilmenau • **P.J. Kunz** Daimler  
**S. Lechner** JRC • **H. Leitold** A-SIT • **K. Lemke-Rust** HS Bonn-Rhein-Sieg • **S. Mangard** TU Graz  
**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** Universität Klagenfurt • **H. Reimer** DuD • **A. Roßnagel** Uni GH Kassel • **W. Schäfer** DATEV  
**H. Storck** T-Systems GmbH • **S. Teufel** Uni Fribourg • **P. Trommler** GSO HS Nürnberg • **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  
**C. Stark** Citigroup AG • **J. Voßbein** UIMC • **R. Welter** IABG mbH

## Organisation

**D. Cechak** Uni Klagenfurt • **P. Lipp** TU Graz • **P. Schartner** Uni Klagenfurt • **M. Möhlmann**

## Leitungsgremium der Konferenzreihe

**P. Horster** Uni Klagenfurt • **P. Schartner** Uni Klagenfurt





# Anmeldung & Teilnahmebedingungen

## D·A·CH Security 2014

16. und 17. September 2014

TU Graz – Campus Inffeldgasse

### Anmeldung zur Konferenz

Telefon: +43 (0) 463 2700 3702

Online-Anmeldung unter:

[http://www.syssec.at/ds14\\_anmeldung](http://www.syssec.at/ds14_anmeldung)

### Teilnahmebedingungen

Bei Anmeldung bis zum 14. August 2014 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 Konferenztage.

Bei Stornierung der Anmeldung bis 8. August 2014 (Datum des Poststempels) wird eine Bearbeitungsgebühr von € 75,- erhoben. Nach dem 8. August 2014 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/tagungsbände>

### Kontakt

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

