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

D·A·CH 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** — **D. Mahrenholz**, **R. Schumann**, **A. Brügmann**, rt-Solutions.de GmbH

- 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

10.00 Uhr **SIEM-Ansätze zur Erhöhung der IT-Sicherheit auf MAP-Basis** — **K.O. Detken**, DECOIT GmbH

- 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

10.25 Uhr **Security Patch Management in Großunternehmen** — **M. Ifland**, Siemens AG

- 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

10.50 Uhr **Kommunikationspause**

Digitale Signaturen & Öffentliche Verwaltung • Leitung: R. Posch — A

11.20 Uhr **Design und Implementierung eines Localhost Signaturgateways** — **D. Derler, C. Rath**, IAIK – TU Graz

- 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

11.45 Uhr **Standards und Lösungen zur langfristigen Beweiswerterhaltung** — **S. Schwalm**, **T. Kusber**, Bearing Point GmbH, **U. Korte,** BSI, **D. Hühnlein**, Ecsec GmbH

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

12.10 Uhr **Security by Isolation in der öffentlichen Verwaltung** — **O. Maurhart**, **R. King**, **M. Bartha**, AIT Austrian Institute of Technology

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

12.35 Uhr **Gemeinsame Mittagspause**

Dienstag • 16. September 2014

Sicherheitsinfrastrukturen & Anwendungen • Leitung: P. Lipp — A

13.35 Uhr **Absicherung von einer M2M-Telematikplattform** — **J. Sell**
- Zentralisierte M2M-Kommunikationinfrastruktur zwischen Landmaschinen — **E. Eren**
- Kommunikationsszenarien im landwirtschaftlichen Bereich — **S. Gansemer**
- Exemplarische IT-Infrastruktur und Komponenten — **T. Horster-Möller**
- Implementierung etablierter Protokolle und Tools — FH-Dortmund
- Datenkommunikation und Ablage

14.00 Uhr **Anonymität und Mehrwegeübertragung** — **R. Wigoutschnigg**
- Gesteigerte Anonymität durch Mehrwegeübertragung? — Uni Klagenfurt
- Auswirkungen für Sender und Empfänger
- Gefahren durch den Predecessor-Angriff
- Evaluation durch Simulationen
- Vergleich mit bestehenden Systemen

14.25 Uhr **Absicherung von Smart-Meter-Umgebungen durch TC** — **K.O. Detken**
- Einführung in ein Smart-Meter-Szenario — DECOIT GmbH
- Bewertung geeigneter Schutzverfahren (TCG versus BSI) — **K.H. Genzel**
- SMGW-Integritätsprüfung mit Trusted-Computing-Verfahren — HS Bremen
- Einsatz von Trusted Network Connect (TNC)
- Ausblick von Trusted Computing im Smart-Meter-Umfeld

14.50 Uhr **Sicherheit von industriellen Steuerungssystemen** — **A. Floß**
- Kritische Betrachtung des ICS-Security-Kompendiums — HiSolutions AG
- BSI IT-Grundschutz-Vorgehensweise bei ICS
- Best-Practice Maßnahmen
- Gefährdungen und Risikoanalyse für ICS
- Ausblick für weitere Aktivitäten

15.15 Uhr **Kommunikationspause**

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

15.45 Uhr **Digitalisierte Forensik: Sensorbildfusion und Benchmarking** — **C. Krätzer**
- Design eines Fusionsframeworks für die intra-/inter Sensorfusion — **M. Hildebrandt**
- Subjektiver und objektiver Vergleich von Sensor-/Featurelevelfusion — **A. Dobbert**
- Benchmarking zerstörungsfreier, kontaktloser, optischer Messtechnik — **J. Dittmann**
- Untersuchung der Reproduzierbarkeit von Sensorsignalen und Artefakten — Uni Magdeburg
- Evaluation anhand latenter Fingerspuren als ausgewählter Tatortspur

16.10 Uhr **Angriffszenarien auf Truecrypt** — **B. Röllgen**
- Ist das Team hinter TrueCrypt ein Phantom? — Global IP
- Angriffe via Trojaner, Analyse des RAM, IO Control Codes, Kopien von Images — Telecommuni-
- Kommerzielle Software „gewinnt“ Schlüssel für BitLocker, TrueCrypt und PGP — cations
- Gegenmaßnahmen in GUI und Treiber sind noch weitestgehend unbekannt
- Konkrete Maßnahmen, mit denen TrueCrypt effektiv gehärtet werden kann

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** — **M. Brunner, R. Breu**, Uni Innsbruck

- 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

09.25 Uhr **Kennzahlen im Informationssicherheitsmanagement** — **M. Stöwer, R. Kraft**, Fraunhofer-Institut SIT

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

09.50 Uhr **Entwicklung einer Test-Umgebung für Risiko-Assessmenttools** — **S. Schauer**, AIT, **A. Peer, J. Göllner**, BMLVS, **S. Rass**, Uni Klagenfurt

- 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

10.15 Uhr **Kommunikationspause**

Datenkontrolle & Rechtliche Aspekte • Leitung: P. Schartner — A

10.45 Uhr **Datenkontrolle mit Software für Informationsrechteverwaltung** — **D. Scherrer**, BLUESITE

- 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

11.10 Uhr **Wahrnehmung der Richtlinien von Facebook** — **N. Hintz, W. Schwarz**, Uni Erlangen-Nürnberg

- 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

11.35 Uhr **Schutz nicht nur der Inhalte, sondern auch der Metadaten** — **H. Jäger**, Uniscon GmbH

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

12.00 Uhr **Outsourcing im Massengeschäft sicher und rechtskonform** — **M. Bergt**, von BOETTICHER Rechtsanwälte

- 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

Mittwoch • 17. September 2014

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

10.45 Uhr **Ganzheitliche Informationssicherheit bei Banken** — **B.C. Witt**, it.sec GmbH&Co.KG

- 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

11.35 Uhr **Cyber-Sicherheits-Check** — **M. Becker**, BSI

- 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

12.25 Uhr **Gemeinsame Mittagspause**

eGovernment & Identitätsmanagement • Leitung: H. Leitold — A

13.25 Uhr **Umsetzung von vertrauenswürdigem Open Government Data** — **K. Stranacher**, **B. Zwattendorfer**, **S. Fruhmann**, **P. Koch**, EGIZ

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

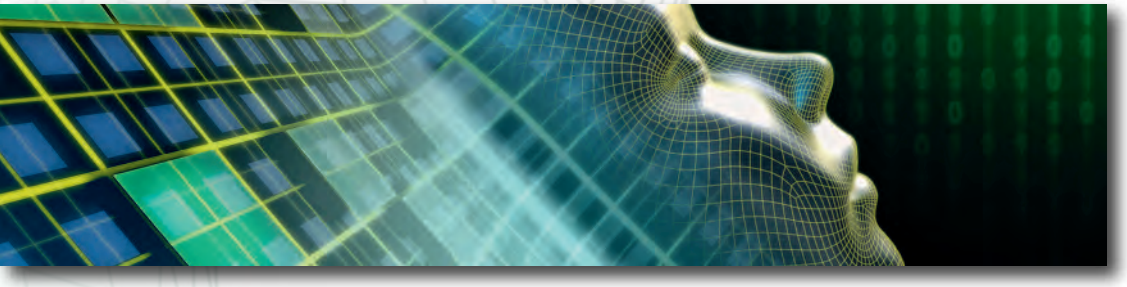
13.50 Uhr **Föderiertes Identitätsmanagement in der Cloud** — **B. Zwattendorfer**, **K. Stranacher**, EGIZ, **F. Hörandner**, TU Graz

- 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

14.15 Uhr **IdP zur Verifikation der vertrauenswürdigen digitalen Identität** — **A. González Robles**, **N. Pohlmann**, if(is) – Westfälische Hochschule Gelsenkirchen

- 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

14.40 Uhr **Kommunikationspause**



Mobile (Un)Sicherheit • Leitung: P. Horster — A

15.10 Uhr **Zum sicheren Löschen auf Smartphones** — **B. Roos**
- Sicherheit der vom Android System bereit gestellten Löschmöglichkeiten — **H. Baier**
- Konzeptionierung unterschiedlicher sicherer Löschstrategien — **P. Lyko**
- Prototyp zum sicheren Löschen von Daten im Flashspeicher — Hochschule
- Blockweises Löschen auf Nand Flashspeicher — Darmstadt/CASED
- Verteilung der Daten durch Wear Leveling und Bad Block Management

15.35 Uhr **Architekturelle Sicherheitsanalyse für Android Apps** — **B. Berger**
- Automatische Extraktion der Sicherheitsarchitektur von Android Apps — **K. Sohr**
- Architekturelle Sicherheitsanalyse von (hybriden) Android Apps — Uni Bremen
- Konzeptionelle Sicherheitsprobleme in Software identifizieren — **U. Kalinna**
- Frameworkspezifische Sicherheitsprobleme in Software identifizieren — ifAsec GmbH
- Wissensdatenbank mit architekturellen Sicherheitsregeln

16.00 Uhr **Aktuelle Grenzen der mobilen Sicherheit** — **P. Papagrigoriou**
- Status Quo und Herausforderungen — EMPELOR GmbH
- 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**

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

Risikokommunikation — **N. Wlczek**
- Besondere Merkmale von Risikokommunikation in einer IT Schadenslage — IABG mbH
- Mögliche Folgen für das Krisenmanagement
- Ursachen für Problemquellen
- Methoden zur Messung
- Lösungsvorschläge zur Prävention

ISMS im Bereich der Energieversorgung und -messung — **T. Goldschmidt**
- Vorgaben für Smart Meter Gateway Betreiber — HiSolutions AG
- Vergleich ISO 27019 und BSI TR 03109
- BSI IT-Grundschutz-Vorgehensweise im Bereich Smart Meter
- Best Practice Maßnahmen
- Ausblick und notwendige weitere Aktivitäten

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. 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** 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

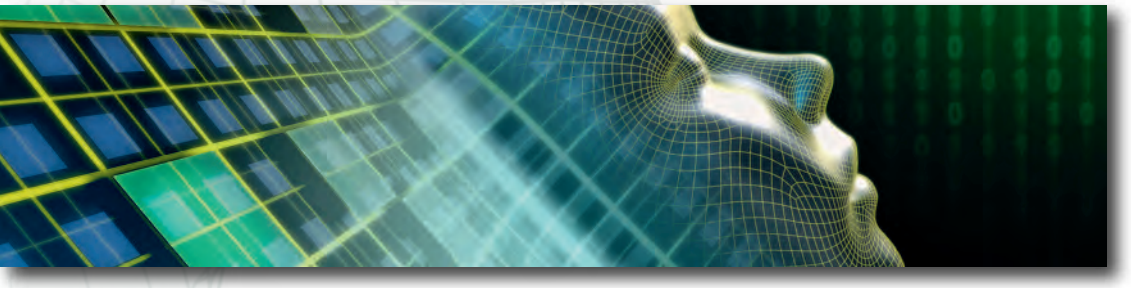
K. Kirst PTLV • **D. Koschützki** HS Furtwangen • **S. Leuchter** HS Rhein-Waal • **P. Reymann** ITQS
C. Stark Citigroup AG • **J. Voßbein** UIMC • **R. Welter** IABG mbH

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

Teilnahmebedingungen

Bei Anmeldung bis zum bis 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 Konferenztag.
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/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