



Call for Papers – Vorabversion

D•A•CH Security 2017

Universität der Bundeswehr München

5. und 6. September 2017

Ziel der Veranstaltung ist es, eine interdisziplinäre Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft in Deutschland, Österreich und der Schweiz zu geben. Insbesondere sollen Aspekte aus den Bereichen Forschung und Entwicklung, Lehre, Aus- und Weiterbildung vorgestellt, relevante Anwendungen aufgezeigt sowie neue Technologien und daraus resultierende Produktentwicklungen konzeptionell dargestellt werden. Da IT-Sicherheit integrierter Bestandteil nahezu aller informationstechnischer Anwendungen und Prozesse ist, sind auch Beiträge zu rechtlichen Rahmenbedingungen und wirtschaftlichen Faktoren gewünscht.

Themen dieser Arbeitskonferenz:

- Schutz kritischer Infrastrukturen
- Industriespionage und Geheimdienstaktivitäten
- Aktuelle Angriffstechniken
- Risiko- und Sicherheitsmanagement
- IT-Compliance, Datenschutz und Rechtsfragen
- Incident Handling und Business Continuity
- Identitäts- und Rechtenmanagement
- Biometrische Verfahren und Anwendungen
- Computerkriminalität und Gegenmaßnahmen
- Botnetze, Spam und Phishing
- Electronic Warfare & Cyber Security
- Trusted Computing und DRM
- Sicherheit von Industrie 4.0
- Security Awareness & Usable Security
- Big Data und Analysetools
- Secure Embedded Systems
- WLAN, Mobilfunk und mobile Endgeräte
- Cloud- und Grid-Computing
- eGovernment, eHealth und eCommerce
- Sichere Webservices
- Sicherheit im automotiven Umfeld
- Sichere Steuerung von Industrieprozessen
- Verfügbarkeit und Notfallplanung
- Sicherheitsaspekte mobiler Betriebssysteme
- Intrusion Detection und Computer-Forensik
- Sicherheitsinfrastrukturen und PKI
- Authentifikation und Single-Sign-On
- Protokollierung und Überwachung
- Modellierung von Sicherheit
- Sicherheitstoken, Smartcards und RFID
- Pervasive und Ubiquitous Computing
- Heimautomatisierung und IoT
- Sicherheit & Safety von Drohnen & Robotern
- Netzwerklösungen, VPN und Remote Access
- Bürgerportal und neuer Personalausweis
- Jugendmedienschutz und Altersverifikation
- Netzneutralität, Netzzugang und Netzsperrern
- Elektronische Signatur und Archivierung
- Sicherheit mit/von Open Source
- IT-Bedrohungs- und Schadsoftware-Analyse
- Sichere Softwareentwicklung
- Sichere Migration von Betriebssystemen
- Privacy Enhancing Technologies
- Folgen, Akzeptanz, Trends und Perspektiven

Fachbeiträge und Überblicksarbeiten zu diesen und verwandten Themen sind als Extended Abstract inkl. Related Work und Literaturangaben (anonymisiertes PDF-Dokument in Deutsch, mindestens 4 DIN A4-Seiten), aus dem die Kernaussagen klar ersichtlich sind, unter <https://syssec.at/conf> einzureichen. Der Tagungsband wird zur Konferenz erscheinen.

Termine:	Einreichung des Extended Abstracts:	2. April 2017
	Benachrichtigung über die Annahme:	5. Mai 2017
	Einreichung der Langfassung:	16. Juni 2017

Aktuelle Informationen: <http://www.syssec.at/dachsecurity2017>

Für die **D•A•CH Security 2017** schlage ich folgende Themenschwerpunkte vor:

Ich habe Interesse, die **D•A•CH Security 2017** als Partner zu unterstützen. Bitte informieren Sie mich über die weitere Vorgehensweise.

Ich beabsichtige, die interdisziplinäre Arbeitskonferenz **D•A•CH Security 2017** zu besuchen. Bitte informieren Sie mich über diese Veranstaltung.

Ich beabsichtige, für die Arbeitskonferenz **D•A•CH Security 2017** einen Vortrag einzureichen. Bitte informieren Sie mich über die weitere Vorgehensweise.

Als Arbeitsthema für meinen Beitrag schlage ich vor:

Name:

Tel.-Nr.:

Firma:

Fax-Nr.:

Adresse:

eMail:

Per Fax an: +43 (0)463 2700 993702

Adresse zur Einreichung von Abstracts und Beiträgen im **syssec Konferenzsystem:**
<https://syssec.at/conf>

Assoc.Prof. Dr. Peter Schartner
z.H. Sekretariat Frau Birgit Merl
Alpen-Adria-Universität Klagenfurt
Institute für Informatik – Systemsicherheit
Universitätsstr. 65-67
9020 Klagenfurt
Österreich

Für Rückfragen (Birgit Merl):
Tel.: +43 (0)463 2700 3702
eMail: konferenzen@syssec.at