## Die Idee der Tagung

Die Fachgruppe SIDAR (Security – Intrusion Detection and Response) der Gesellschaft für Informatik e.V., die sich mit der Erkennung und Beherrschung von Vorfällen der Informationssicherheit beschäftigt, das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO sowie das RUS-CERT (Universität Stuttgart) veranstalten vom 24.-25. November 2003 eine Tagung zum Thema IT-Incident Management und IT-Forensics.

Die Tagung richtet sich an Personen und Organisationen, die in diesem Arbeitsgebiet tätig sind und soll den Erfahrungsaustausch sowie die vertiefende Diskussion unter den Teilnehmern fördern.

## Themenüberblick

Montag, 24.11.2003: IT-Incident Management

Das IT-Incident Management umfasst typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. Das Spektrum möglicher Vorfälle reicht dabei von technischen Problemen und Schwachstellen bis hin zu konkreten Angriffen auf die IT-Infrastruktur. IT-Incident Management im engeren Sinne muss dabei sowohl organisatorische, als auch rechtliche sowie technische Detailfragen berücksichtigen.

Dienstag, 25.11.2003: IT-Forensics

Die IT-Forensik als ein Teilaspekt des IT-Incident Management behandelt technische Verfahren und deren organisatorische Einbettung, die geeignet sind, Sicherheitsverletzungen und deren Ursachen bzw. Urheber zu identifizieren, die Vorgänge zu bewerten sowie juristische Beweisbarkeit zu schaffen.

**www.gi-fg-sidar.de/imf2003**

## Montag, 24. November 2003 (Programm)

| | |
|---|---|
| **10:00** | **Begrüßung** |
| **10:15-10:55** | **Effiziente Bearbeitung von Abuse-Beschwerden** (W. Hommel, LRZ München) |
| **10:55-11:35** | **IT-Incident Management durch externe Dienstleistung - Die Lösung aller IT-Incident Management Probleme?** (R. Wagner, DATEVeG) |
| **11:35-12:15** | **Eine Informationsbasis für zeitoptimiertes Incident Management** (P. Scholz, FH Landshut, R. Mörl, SIOS) |
| | **Mittagessen** |
| **13:45-14:25** | **Informationslogistische Ansätze für CERTs** (Dr. C. Thiel, Fraunhofer ISST) |
| **14:25-15:05** | **Problem-Solving Support for Centralized Network Security Monitoring: Challenges, Tools and Benefits** (M. Stolze, IBM Research Zurich Laboratory) |
| **15:05-15:45** | **Aufbau und Organisation des Computer Emergency Response Teams** (V. Kozok, Bundeswehr Streitkräfteamt) |
| | **Pause** |
| **16:15-17:00** | **Keynote - The challenge of electronic evidence: The European response** (Neil Mitchison, Institute for the Protection and the Security of the Citizen - Joint Research Centre (IPSC/JRC), European Commission) |
| **17:05-18:15** | **FG-Treffen der GI-Fachgruppe SIDAR** |
| **20:00** | **Gemeinsames Abendessen** |

## Dienstag, 25. November 2003 (Programm)

| | |
|---|---|
| **10:00** | **Begrüßung** |
| **10:15-10:55** | **Einführung in die IT-Forensik** (D. Mauersberger, LKA München) |
| **10:55-11:35** | **Post-Mortem-Analysen mit Open Source Software** (M. Hofherr, GeNUA) |
| **11:35-12:15** | **Elektronische Beweise** (R. Kern, Kroll Ontrack GmbH) |
| | **Mittagessen** |
| **13:45-14:25** | **Integrationsplattform zur systemübergreifenden Erfassung und forensischen Analyse von Spurenträgern** (C. Fischer, BFK edv-consulting GmbH) |
| **14:25-15:05** | **Forensik: Einbettung in präventive und reaktive Unternehmensprozesse** (N. Magnus, secunet Security Networks AG) |
| **15:05-15:45** | Kurzbeiträge und Ausblick auf weitere Themen und Aktivitäten |
| **15:45-16:00** | **Verabschiedung** |

## Sponsoren

## Teilnahmegebühren

| Teilnahmegebühr zur Fachtagung | bei Anmeldung nach 1.11.2003 |
|---|---|
| Reguläre Gebühr (Normalzahler) | 250 € |
| Hochschulangehörige | 200 € |
| GI-Mitglieder *) | 175 € |
| Studierende/ Auszubildende | 75 € |
| student./auszub. GI-Mitglieder | 50 € |

*) sowie Mitglieder einer der folgenden wissenschaftlichen Gesellschaften: ACM, IEEE Comp. Society, CEPIS-Gesellschaften, CCF (RC), EUROGRAPHICS, DMV, GIL und GOR.

Die Tagungsgebühr enthält einen Tagungsband sowie die Teilnahme für eine Person am gemeinsamen Abendessen am 24.11.2003. Begleitpersonen zum gemeinsamen Abendessen zahlen je 25 €.

Ein **Anmeldeformular** (sofern es diesem Heft nicht beilag) finden Sie im Internet unter *www.gi-fg-sidar.de/imf2003*

## Organisation

**Tagungsleitung:**

Jens Nedon (Vorsitz)
ConSecur GmbH
Schulze-Delitzsch-Strasse 2, 49716 Meppen,
Tel. 05931-92240, *nedon@consecur.de*

Sandra Frings
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstrasse 12, D-70569 Stuttgart
Tel. 0711-970 2460, *sandra.frings@iao.fhg.de*

Oliver Göbel
RUS-CERT (Universität Stuttgart),
Allmandring 30e, D-70550 Stuttgart
Tel. 0711-6855963, *goebel@cert.uni-stuttgart.de*

**Lokale Organisation und Tagungsbüro:**

Sandra Frings
Fraunhofer IAO, Nobelstraße 12, D-70569 Stuttgart
Tel. 0711-970 2460, *sandra.frings@iao.fhg.de*
Fax 0711-970 2401

## Tagungsort

Institutszentrum Stuttgart der Fraunhofer-Gesellschaft (IZS)
Nobelstraße 12, D-70569 Stuttgart
Tel. 0711-970 01

## Programmkomitee

Die Beiträge der Tagung sind durch das Programmkomitee nach wissenschaftlichen Kriterien begutachtet worden.

| | |
|---|---|
| Günther Ennen | CERT-Bund |
| Christoph Fischer | BFK edv-consulting GmbH |
| Ulrich Flegel | Universität Dortmund |
| Sandra Frings | Fraunhofer IAO |
| Oliver Göbel | RUS-CERT |
| Guido Gluschke | Viccon GmbH |
| Jens Gruhl | Justizministerium Stuttgart |
| Jürgen Hauber | LKA Baden-Württemberg |
| Hans-Peter Herrmann | Anwaltskanzlei Herrmann, Hübler und Partner |
| Stefan Kelm | Secorvo Security Consulting GmbH |
| Reinhold Kern | Kroll Ontrack |
| Dr. Klaus-Peter Kossakowski | PRESECURE Consulting GmbH |
| Volker Kozok | Bundeswehr-Streitkräfteamt |
| Franz-Josef Lang | KoSiB eG |
| Ralf Moll | Kriminalpolizei Heilbronn |
| Dr. Hans-Joachim Mück | FB-RZ Informatik, Univ. Hamburg |
| Jens Nedon | ConSecur GmbH |
| Rolf von Rössing | Ernst & Young |
| Wolfgang Schreiber | Bundeskriminalamt |
| Rolf Schulz | Global Network Security GmbH |
| Matthias Stoffel | SIZ – Informatikzentrum der Sparkassenorganisation |
| Morton Swimmer | IBM Global Security Analysis Lab |
| Marco Thorbrügge | DFN-CERT GmbH |
| Martin Woitke | secunet Security Networks AG |

## Veranstalter

Fachgruppe SIDAR der Gesellschaft für Informatik e.V.
Wissenschaftszentrum, Ahrstraße 45; D-53175 Bonn
Tel. 0228-302145; Fax: 0228-302167, *http://www.gi-ev.de/*

**Mitveranstalter:**

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
*http://www.iao.fhg.de/*

RUS-CERT (Universität Stuttgart)
*http://cert.uni-stuttgart.de/*

**Gesellschaft für Informatik e.V.**
**Fachgruppe SIDAR**

# Einladung und Programm

# IT-Incident Management & IT-Forensics 2003

24. – 25. November 2003

Institutszentrum Stuttgart der Fraunhofer-Gesellschaft (IZS)

Tagung der Fachgruppe SIDAR der Gesellschaft für Informatik e.V. (GI)

in Zusammenarbeit mit:

Fraunhofer Institut Arbeitswirtschaft und Organisation
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

RUS-CERT
RUS-CERT (Universität Stuttgart)

**www.gi-fg-sidar.de/imf2003**