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

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.

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

Eingereichte Beiträge sollten sich an folgenden Themen orientieren:

IT-Incident Management

- → Aufgaben des IT-Incident Management
- → Trends, neue Verfahren und Methoden im Bereich IT-Incident Management
- → Nomenklatur(en)
- → Werkzeuge für das IT-Incident Management
- → Aus- und Weiterbildung im Bereich des IT-Incident Management
- → Bewußtseinsbildung
- → Einbettung des IT-Incident Management in Organisationsprozesse
- → Erkennung und Bewertung von Ereignissen
- → Vorgehensmodelle bei der Bearbeitung von Vorfällen
- → Problemstellungen und Herausforderungen beim Aufbau von CERTs/CSIRTs
- → Alltagsprobleme und -lösungen in CERTs/CSIRTs
- → Informationsquellen
- → neue Geschäftsmodelle und ihre Auswirkungen
- → Communities und Infrastrukturen zum Austausch von Informationen
- → Umgang mit Schwachstellen (vulnerability response)
- → Advisories - Aktivitäten zur Standardisierung

IT-Forensics

- → Trends und Herausforderungen im Bereich IT-Forensics
- → Methoden, Verfahren und Einsatzgebiete der IT-Forensics
- → Beweissicherung in IT-Umgebungen
- → Standardisierung von Beweissicherungsprozessen
- → Datenschutz- und andere rechtliche Fragen bei IT-forensischen Untersuchungen
- → Juristische Relevanz IT-forensicher Untersuchungen
- → Bedarf an Kooperation im Vorfeld (z.B. organisationsintern, mit CERTs oder mit Strafverfolgungsbehörden) und Anforderungen

Programmkomitee

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	▪ Landeskriminalamt Baden-Württemberg
Hans-Peter Herrmann	▪ Anwaltskanzlei Herrmann, Hübler und Partner
Stefan Kelm	▪ Secorvo Security Consulting GmbH
Reinhold Kern	▪ Kroll Ontrack
Klaus-Peter Kossakowski	▪ PRESECURE Consulting GmbH
Volker Kozok	▪ Bundeswehr-Streitkräfteamt
Franz-Josef Lang	▪ KoSiB eG
Ralf Moll	▪ Kriminalpolizei Heilbronn
Hans-Joachim Mück	▪ FB-RZ Informatik, Universität Hamburg
Jens Nedon	▪ ConSecur GmbH
Rolf von Rössing	▪ Ernst & Young
Wolfgang Schreiber	▪ Bundeskriminalamt
Uwe Schundelmeier	▪ Polizeiakademie Freiburg
Rolf Schulz	▪ Global Network Security GmbH
Morton Swimmer	▪ IBM Global Security Analysis Lab
Matthias Stoffel	▪ SIZ – Informatikzentrum der Sparkassenorganisation
Marco Thorbrügge	▪ DFN-CERT GmbH
Martin Woitke	▪ secunet Security Networks AG

www.gi-fg-sidar.de/imf2003

Call for Papers

Mit diesem Call for Papers rufen wir zur Einreichung von Beiträgen zu den genannten Themen auf:

- **Wissenschaftliche Beiträge**
- **Praxisbeiträge**

Alle Einreichungen sollen als vollständige Beiträge („Full Papers“) eingereicht werden und einen Umfang von ca. 8-12 Druckseiten haben.

Termine & Formalia

30.06.2003 Elektronische Abgabe der Einreichungen an: **imf2003@gi-fg-sidar.de**
Formatvorlage (Word, LaTeX) erhältlich unter: *www.gi-fg-sidar.de/imf2003*

01.09.2003 Zu-/Absage an Autoren per E-Mail

06.10.2003 Elektronische Abgabe druckfertiger Beiträge, mögliche Formate: Word, LaTeX

Das Einreichen der Beiträge soll via E-Mail erfolgen.

Die Beiträge selbst sollen keine Autorennamen oder sonstige personen- oder organisationsbezogene Hinweise enthalten, da eine anonyme Begutachtung vorgesehen ist. Dafür sind diese Daten (Namen und E-Mailadressen der Autoren sowie bei mehreren Autoren eine Kontaktperson) in der begleitenden E-Mail anzugeben.

Alle eingereichten Beiträge werden durch das Programmkomitee begutachtet. Die angenommenen Beiträge sollen auf der Tagung präsentiert werden. Es ist darüber hinaus vorgesehen, alle angenommenen Beiträge in einem Tagungsband der Reihe Lecture Notes in Informatics (LNI) zu veröffentlichen.

Organisation

Tagungsleitung:

Jens Nedon, ConSecur GmbH (Vorsitz)
Schulze-Delitzsch-Strasse 2, 49716 Meppen
Tel. +49-5931-9224-0, *nedon@consecur.de*

Sandra Frings, Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstrasse 12, D-70569 Stuttgart
Tel: +49-711-9702460, *sandra.frings@iao.fhg.de*

Oliver Göbel, RUS-CERT (Universität Stuttgart),
Allmandring 30e, D-70550 Stuttgart
Tel. +49-711-685-5963, *goebel@cert.uni-stuttgart.de*

Lokale Organisation:

Sandra Frings, Fraunhofer IAO
Tel: +49-711-9702460, *sandra.frings@iao.fhg.de*

Veranstalter

Fachgruppe SIDAR der
Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum, Ahrstraße 45; D-53175 Bonn
Tel.: +49-228-302-145; Fax: +49-228-302-167
http://www.gi-ev.de

Mitveranstalter:

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstrasse 12, D-70569 Stuttgart
http://www.iao.fhg.de

RUS-CERT (Universität Stuttgart)
Allmandring 30e, D-70550 Stuttgart
http://cert.uni-stuttgart.de

Gesellschaft für Informatik e.V.
Fachgruppe SIDAR

Call for Papers

IT-Incident Management & IT-Forensics

24. – 25. November 2003

Institutszentrum der Fraunhofer-Gesellschaft (IZS)
in Stuttgart

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

in Zusammenarbeit mit:

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

RUS-CERT
RUS-CERT (Universität Stuttgart)

www.gi-fg-sidar.de/imf2003