INFORMATIK 2014 – Workshop RiskKom – 26.9.2014

Risikokommunikation im Kontext von IT-Sicherheit und Safety

Workshop der GI-FGn SECMGT & ECOM – http://fg-secmgt.gi.de/riskkom2014

Call for Papers

Thema und Schwerpunkte

Die IT-Sicherheit einer Organisation hängt nicht nur von den technischen Kenntnissen des IT-Sicherheitspersonals ab, sondern auch ganz entscheidend von der **Kommunikation zwischen diesen Sicherheitsexperten, dem Management und den Benutzern bzw. Betroffenen**. Dies betrifft sowohl die Kommunikation nach innen (also innerhalb einer Einrichtung, z.B. hinsichtlich des Schaffens von Sicherheitsbewusstsein (Awareness), als auch nach außen (z.B. bei Eintritt einer ggf. meldepflichtigen Datenpanne oder eines Krisenfalles).

Welches Sicherheitsniveau eine Institution tatsächlich umsetzt, ist zudem eng verbunden mit der persönlichen (subjektiven) Kosten-Nutzen-Einschätzung der vorhandenen Sicherheitsmaßnahmen. Dabei spielen sowohl die Einsicht in Notwendigkeiten als auch die Praktikabilität zu beachtender Regelungen eine Rolle.

Je komplexer eine Infrastruktur ist, je mehr Daten darüber abgewickelt werden, je mehr Personen betroffen sind und je stärker auf Daten oder Infrastrukturen vernetzt aus unterschiedlichen Kontexten zugegriffen wird, desto wichtiger ist es, einen angemessenen Schutz gewährleisten zu können. Allerdings werden dadurch auch die Zusammenhänge der Risiken komplexer und schwieriger zu kommunizieren.

Auf diesem Workshop steht daher der Aspekt „Kommunikation von Sicherheit und Risiken“ im Vordergrund. Es sollen aktuelle Forschungsergebnisse und Erfahrungsberichte aus der Praxis im Bereich der Risikokommunikation diskutiert werden. Dabei soll die Situation sowohl in Behörden und Unternehmen, als auch im Kontext von Anwendern und allgemein in der Gesellschaft betrachtet werden.

Mögliche Themen der Beiträge für den diesjährigen Workshop sind insbesondere:

- Zusammenwirken der Risikokommunikation in den Bereichen Safety und IT-Security
- Untersuchungen zur Risikokommunikation in Unternehmen, Case Studies, Evaluierungen
- Durchführung und Evaluation von Awareness Kampagnen in Unternehmen und in der Bevölkerung als Basis zur Verbesserung der Risikokommunikation
- Berücksichtigung des Faktors „Mensch“ bei der Konzeption und der Kommunikationsstrategie von Sicherheitsmaßnahmen (IT-Sicherheit bzw. Safety)
- Kommunikation von Sicherheits-Risiken aus IT-Quellen wie umfangreichen Event-Protokolldaten gegenüber unterschiedlichen Stellen (sowohl im Rahmen der Vorfallsbearbeitung als auch der anschließenden Krisenbewältigung)
- Spannungsfelder des IT-Sicherheitsmanagements in Unternehmen: Management, IT-Sicherheitsexperten, Stellen innerhalb der Supply Chain außerhalb des Unternehmens, Benutzer bzw. Betroffene
- Spannungsfelder des IT-Sicherheitsmanagements in kritischen Infrastrukturen: gesellschaftliche Auswirkungen fehlender Funktionstüchtigkeit, Betrieb durch nicht-staatliche Eigner, hoher Vernetzungs- und Abhängigkeitsgrad gegenüber anderen kritischen Infrastrukturen, hohe Anzahl an Betroffenen im Krisenfall
- Spannungsfelder des IT-Sicherheitsmanagements im Kontext von Industrie 4.0 (insbesondere hinsichtlich Internet der Dinge und Dienste, Cyber-Physical Systems oder Smart Factories): Funktionalität smarter Infrastruktur, Vernetzungsgrad zwischen verbundener bzw. verbindbarer Infrastruktur, Grad der Fehleranfälligkeit durch verdeckte Kanäle oder aufgrund einer Kaskadierungswirkung von Vorfällen zur IT-Sicherheit oder Safety

INFORMATIK 2014 – Workshop RiskKom – 26.9.2014

- Usability von Sicherheitsmanagement-/Risikomanagement-Tools
- Effektivität von Risikokommunikation in Warnungen, z.B. Kommunikation von Wahrscheinlichkeiten, Unsicherheiten, Schadenshöhe oder der Sicherheitslage
- Methodenentwicklung und Modellbildungen im Bereich der Risikokommunikation

Zielgruppe sind Forscher und Praktiker, die sich für Verfahren zur erfolgreichen Kommunikation der IT-Sicherheitsrisiken, ihrer Evaluation und damit verbundenen Problemen interessieren.

Einreichung der Beiträge

Willkommen sind aktuelle Forschungsergebnisse und Erfahrungsberichte aus der Praxis. Daneben sind auch Work-in-Progress- und Position-Papers erwünscht, sofern sie das Potential für interessante Diskussionen haben.

Beiträge sollen **bis zu 12 Seiten** umfassen (inklusive Literatur und Anhängen) und in **deutscher oder englischer Sprache** verfasst sein. Angenommene Beiträge werden in der GI-Edition *Lecture Notes in Informatics* (LNI) veröffentlicht. Die Beiträge müssen sich also an das **LNI-Format** halten.

Einreichung von Beiträgen:	bis **22.4.2014**
Entscheidung über die Annahme:	bis 20.5.2014
Einreichung der druckfähigen Fassung:	bis 23.6.2014
Workshop in Stuttgart:	26.9.2014

Organisation (Co-Chairs)

Bernhard C. Witt, it.sec GmbH & Co. KG
Steffen Bartsch, TU Darmstadt

Programmkomitee

Zinaida Benenson, Universität Erlangen-Nürnberg
Rainer Böhme, Universität Münster
Marian Harbach, Universität Bonn
Andreas Heinemann, Hochschule Darmstadt
Birgit Henhapl, usd AG
Luigi Lo Iacono, Fachhochschule Köln
Michaela Kauer, TU Darmstadt
Dirk Koschützki, Hochschule Furtwangen
Gerhard Kron, kronsoft
Alexander De Luca, LMU München
Marian Margraf, Hochschule Darmstadt
Kirsten Messer-Schmidt, excepture
Isabel Münch, BSI
Peer Reymann, ITQS
Joachim Vogt, TU Darmstadt
Melanie Volkamer, TU Darmstadt
Bernhard C. Witt, it.sec GmbH & Co. KG