Workshop der GI-FG SECMGT zur Informatik 2011

Die Fachgruppe Management von Informationssicherheit (SECMGT) möchte folgenden Workshop für die 41. Jahrestagung der GI vom 4. - 7.10.2011 an der TU Berlin anmelden:

Management von Informationssicherheit 2.0 (SECMGT 2.0)

Organisator: Bernhard C. Witt, c/o it.sec GmbH & Co. KG, Einsteinstr. 55, 89077 Ulm, 0731/2058911, bcwitt@it-sec.de, Sprecher der GI-FG SECMGT

Zusammenfassung

Informationssicherheit ist ein Querschnittsthema und bedarf einer zielorientierten Steuerung, damit die Informationen in Unternehmen und Behörden ausreichend geschützt sind. Dies erfolgt nicht nur durch den Betrieb technischer Sicherheitskomponenten, sondern erfordert auch die Übernahme der Verantwortung durch die oberste Managementebene und eines darauf ausgerichteten Handelns im Einklang mit entsprechenden Vorgaben. Neue Technologien und neue Formen des Umgangs mit Informationen erfordern eine Anpassung der Managementstrategien zur Gewährleistung von Informationssicherheit. In diesem Workshop sollen daher typische Themen aus dem Spektrum der Fachgruppe SECMGT im aktuellen Licht neu diskutiert werden. Der Workshop richtet sich an Sicherheitsverantwortliche aus der Praxis und Sicherheitsexperten aus Unternehmen, Behörden und Hochschulen.

Call for Papers

Informationssicherheit ist ein Querschnittsthema und bedarf einer zielorientierten Steuerung, damit die Informationen in Unternehmen und Behörden ausreichend geschützt sind. Dies erfolgt nicht nur durch den Betrieb technischer Sicherheitskomponenten, sondern erfordert auch die Übernahme der Verantwortung durch die oberste Managementebene und eines darauf ausgerichteten Handelns im Einklang mit entsprechenden Vorgaben.

Technische Sicherheitskomponenten entfalten erst ihre Wirkung, wenn ihr Einsatz sich an den tatsächlichen Sicherheitsbedürfnissen der jeweiligen Organisation orientiert und wenn dies auch in den organisationsinternen Abläufen verankert ist. Die Sicherheitsbedürfnisse sind jedoch nicht unabhängig vom technischen Fortschritt und den jeweiligen Gepflogenheiten des Umgangs mit Informationen. Die Konvergenz von in der Vergangenheit sich noch unterscheidenden Informations- und Kommunikationstechniken, die Allgegenwart der Informationsverarbeitung (Ubiquitous Computing) und

die Auflösung des Standortbezugs der Informationsverarbeitung (Cloud Computing) führen zu neuen Herausforderungen. Insofern ist eine ständige Anpassung der Managementstrategien zur Gewährleistung von Informationssicherheit nötig.

Das Management von Informationssicherheit dient der organisationsweiten Koordination und Bündelung aller Aktivitäten zur Gewährleistung ausreichender Informationssicherheit und basiert auf der Grundlage planvollen Handelns. Die zu beachtenden, regulatorischen Anforderungen (Gesetze, Verträge, Standards, interne Vorgaben) an die Gestaltung der eingesetzten Informations- und Kommunikations-Infrastruktur einerseits und die Komplexität der Infrastruktur selbst andererseits sind in den letzten Jahren kontinuierlich gestiegen. Ausschlaggebend für den Erfolg des Managements von Informationssicherheit ist daher ein ganzheitlicher Ansatz und die konsequente Etablierung von Sicherheitsprozessen, die flexibel genug sind, um sich den neuen Herausforderungen stellen zu können.

Das Management von Informationssicherheit fungiert als Schnittstelle zwischen informationstechnischen Schutzmaßnahmen und dem IT-Risikomanagement einer Organisation. Es bildet zugleich eine Brücke zwischen informatischen, juristischen und betriebswirtschaftlichen Sichtweisen des Sicherheitsbegriffs. Die hierbei zur Anwendung kommenden, verschiedenen Ansätze sollen im Rahmen des Workshops zum "Management von Informationssicherheit 2.0" im aktuellen Licht neu diskutiert werden.

Themen, zu denen entsprechende Beiträge eingereicht werden können, sind u.a.:

- Leitbilder der Informationssicherheit
- Etablierung von Informationssicherheit in Organisationsstrukturen
- Beschreibung und Steuerung von Sicherheitsmanagementsystemen mittels formaler Methoden
- Gestaltung eines adäquaten IT Governance, Risk & Compliance Managements bzw. einzelner Teilaspekte hiervon
- Gestaltung eines adäquaten Business Continuity Managements
- Auswahl und Umsetzung von Sicherheitsmaßnahmen
- Schulung, Sensibilisierung und Motivation für Informationssicherheit
- Qualitätssicherung und Revision von Informationssicherheit

Eingereichte Beiträge werden von einem Programmkomitee begutachtet, das sich aus Mitgliedern des Leitungsgremiums der Fachgruppe SECMGT zusammensetzt. Die Beiträge haben zu berücksichtigen, dass jeweils ein 45 minütiger Vortrag mit anschließender Diskussion vorgesehen ist.

Die schriftliche Ausarbeitung (Kurzfassung) zu den Vorträgen soll sechs DIN A4-Seiten nicht übersteigen. Bei Annahme der Beiträge ist eine druckfähige Langfassung im Umfang von bis zu 16 DIN A4-Seiten einzureichen, die im Tagungsband veröffentlicht wird. Es gelten die Terminvorgaben der Organisatoren der Informatik 2011.

Qualität, Originalität, Aktualität und Praxisbezug der Beiträge sind ausschlaggebend bei deren Auswahl. Es wird zudem darauf geachtet, dass durch die angenommenen Beiträge das Themenspektrum der Fachgruppe SECMGT (siehe auch entsprechende Ausführungen unter www.secmgt.de) in ausreichender Breite abgedeckt wird, damit auf den Ergebnissen des Workshops in weiteren Veranstaltungen der Fachgruppe aufgesetzt werden kann. Jeder Beitrag wird von mind. zwei verschiedenen Programmkomitee-Mitgliedern begutachtet.

Der halbtägige Workshop richtet sich an Sicherheitsverantwortliche aus der Praxis und Sicherheitsexperten aus Unternehmen, Behörden und Hochschulen. Die Teilnehmerzahl ist auf 30 beschränkt.