Rahmen des Kongresses stattfindende Postersession ausgewählt. Die Kriterien für die Vortragseinreichung stehen zusammen mit weiteren Informationen zum Kongress, zu den Themenkategorien und zum Programmbeirat auf der Webseite des BSI *https://www.bsi.bund.de/ContentBSI/Aktuelles/Veranstaltungen/IT-SiKongress/13_IT-SiKongress/13_ITSiKongress.html;jsessionid=EDE61071144DDB242B-23CA7A39F27850.2_cid294* zur Verfügung.

TeleTrusT-Innovationspreis für IT-Sicherheitslösungen ausgeschrieben

Seit 1999 verleiht TeleTrusT einen „TeleTrusT-Innovationspreis". Traditionell wird dieser Preis im Rahmen der von TeleTrusT und EEMA ausgerichteten IT-Sicherheitskonferenz „Information Security Solutions Europe" (ISSE; *www.teletrust.de/veranstaltungen/isse/*) – in diesem Jahr am 23./24.10.2012 in Brüssel – überreicht.
Die Bewerbungsfrist endet am 31.08.2012.
Die Auswahlkriterien für den TeleTrusT-Innovationspreis sind in der Reihenfolge ihrer Gewichtung:

- Grad an Innovation
- Nutzen für die Anwender
- die Konformität mit Standards
- Vorbildcharakter des eingereichten Vorschlages auf nationaler, europäischer und weltweiter Ebene.

Bewertung und Auswahl der Preisträger erfolgt durch eine Jury aus IT-Sicherheitsexperten. Die Jury steht stellvertretend für den Anspruch von TeleTrusT, IT-Sicherheit interdisziplinär zu betrachten. Die Jury entscheidet unabhängig von kommerziellen Erwägungen. Das Bewerbungsformular ist unter *http://www.teletrust.de/innovationspreis/teletrust-innovationspreis/*
abrufbar.

Hochschulen entwickeln innovatives und datenschutzkonformes IT-Frühwarnsystem

Das Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen hat als Konsortialführer gemeinsam mit fünf Kooperationspartnern das Forschungsprojekt „innovative Anomaly and Intrusion-Detection" (kurz: iAID) erfolgreich gestartet. Ziel des Projekts ist es, effektive Schutzmaßnahmen gegen neue Angriffsmechanismen im sogenannten „Cyberwar" zu entwickeln.

Die Zusammenarbeit von vier deutschen Hochschulen (Westfälische Hochschule Gelsenkirchen, Hochschule Darmstadt, Fachhochschule Frankfurt am Main und Ruhr-Universität Bochum) sowie zwei Industriepartnern (Vodafone D2 GmbH und Dr. Bülow & Masiak GmbH) im Projekt iAID ist eine Antwort auf die aktuelle Bedrohungslage der IT-Sicherheit in der Bundesrepublik. Laut eines aktuellen Lageberichts des Bundesamtes für Sicherheit in der Informationstechnik (BSI) nimmt derzeit die Anzahl der Angriffe auf IT-Systeme stetig zu. Aufgrund der zunehmenden Vernetzung, beispielsweise durch Cloud-Computing-Technologien, steigt gleichzeitig auch die Gefährdungslage. Daten und Dienste werden zunehmend über Computernetzwerke miteinander verknüpft und werden schnell zur Zielscheibe krimineller Attacken. Die Angreifer versuchen hierbei die Verfügbarkeit von Diensten (Denial of Service Attacken) einzuschränken, Kundendaten zu stehlen oder Industriespionage zu betreiben. Bei erfolgreichen Angriffen entstehen enorme Schäden – nicht nur finanzieller Art. Die monetären Schäden können durchaus in die Milliarden gehen, dazu kommen noch die signifikanten negativen Auswirkungen auf das Firmenimage.

Ziel von iAID ist die Entwicklung von innovativen Lösungen und Verfahren zur Vorbeugung, Erkennung und Reaktion auf solche Angriffe über Netzwerke. Während klassische Erkennungssysteme nur bekannte Angriffsmuster erkennen können, werden im Rahmen von iAID innovative Methoden der Anomalie-Detektion entwickelt, um auch unbekannte Angriffe zu erkennen. Hierdurch wird die Erkennungsleistung signifikant gesteigert und es können auch bisher unbekannte, neue Angriffe erkannt und bekämpft werden. Zur Vorbeugung und Reaktion werden Prozesse und (teil-)automatisierte Verfahren entwickelt, die einen zeitnahen und effizienten Schutz vor Angriffen ermöglichen und die eine stetige Optimierung der Sicherheitsmaßnahmen einschließen. Weiteres zentrales Ziel von iAID ist die Einhaltung der Vorgaben und Bestimmungen des Datenschutzes. Das innovative IT-Frühwarnsystem wird in der Lage sein, große Datenmengen gleichzeitig zu analysieren und die Fehlererkennungsrate gegenüber den auf dem Markt befindlichen Erkennungssystemen zu verbessern. Dadurch kann es sowohl flexibel in Unternehmensnetzwerken als auch im Bereich der Internet-Service-Provider eingesetzt werden.

Schon jetzt sind die beiden beteiligten Industriepartner hoch motiviert. Die Kooperation zwischen Hochschulen und Industrie ermöglicht Synergien in der Entwicklung und Integration. Durch die Einbindung des IT-Frühwarnsystems in die Netzwerkinfrastruktur und die stetige Begleitung können bereits früh Anpassungen vorgenommen und richtungweisende Entscheidungen getroffen werden, um iAID für den Realbetrieb vorzubereiten. Neben technischen Aspekten bringen die Unternehmen zudem ihre erfahrenen Netzwerkadministratoren in das Projekt ein, um an der Interaktion zwischen IT-Frühwarnsystem und Administrator mitzuwirken und insbesondere die Reaktionen und Strategien unter realen Gesichtspunkten mitzugestalten. Die hier entwickelten IT-Frühwarnlösungen werden die Partner dann in ihr Portfolio integrieren, um neben dem Schutz des IT-Netzes ihres eigenen Unternehmens und dem ihrer Kunden auch auf dem wachsenden Markt ihre Chancen gegenüber Mitbewerbern zu verbessern. Zudem werden neue Geschäftsfelder für Managed-Security entstehen.

Website des Projekts: *http://www.internet-sicherheit.de/institut/forschung/aktuelle-forschungsprojekte/internet-fruehwarnsysteme/iaid/*

ENISA: Übersicht zu Europas 173 CERTs

Die neueste Karte zu Europas „digitaler Feuerwehr", den Computer Emergency Response Teams, CERTs in Europe (map, v.2.7), ist nun online. Die „CERTs in Europe map" verzeichnet 173 CERT Teams. CERTs werden von EU-Mitgliedsstaaten und anderen öffentlichen und privaten Einrichtungen gebildet, um eine schnelle Reaktion auf Notfälle zu ermöglichen, die vitale Computernetzwerke oder Informationssysteme bedrohen. Mit der Veröffentlichung der Karte ist gleichzeitig auch eine aktualisierte Version des Verzeichnisses von CERT-Aktivitäten in Europa verfügbar. Sie bietet eine Übersicht von Response Teams nach Land und enthält eine Auflistung von Kooperations-, Support- und Standardisierungsangeboten.