Call for Papers für 14. Deutschen IT-Sicherheitskongress gestartet

Unter dem Motto „Risiken kennen, Herausforderungen annehmen, Lösungen gestalten" findet vom 19. bis 21. Mai 2015 in Bonn der 14. Deutsche IT-Sicherheitskongress statt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sucht ab sofort aktuelle, kreative und praxisnahe Kongressbeiträge, die sich beispielsweise mit einem der folgenden Themenbereiche der IT-Sicherheit auseinandersetzen:

- Industrie 4.0 / Sicherheit industrieller Prozesse
- Sicheres Cloud Computing
- Sichere mobile Kommunikation
- Sicherheit in der digitalen Gesellschaft
- Sicherheit von Plattformen und Netzen
- IT-Sicherheit und Recht
- Standards und Prüfverfahren
- Sichere Identitäten
- Cyber-Sicherheit
- Management von Informationssicherheit

Diese Liste ist nicht abschließend. Auch zu anderen Themen der IT-Sicherheit können interessierte Autoren aus Unternehmen, Forschungseinrichtungen, Verwaltung und anderen Institutionen per E-Mail unter *papers2015@bsi.bund.de* Beiträge einreichen. Einsendeschluss ist der 31. August 2014. Die Vorschläge werden von einem hochkarätig besetzten Programmbeirat anonym begutachtet und bewertet. Die besten Einreichungen werden für den Kongress ausgewählt. Die Kriterien für die Vortragseinreichung stehen zusammen mit weiteren Informationen zum Kongress, zu den Themenkategorien und zum Programmbeirat auf der Webseite des BSI unter *https://www.bsi.bund.de/DE/Aktuelles/Veranstaltungen/IT-Sicherheitskongress/IT-Sicherheitskongress_node.html* zur Verfügung.

Mit über 600 Fachbesuchern ist der Deutsche IT-Sicherheitskongress, den das Bundesamt für Sicherheit in der Informationstechnik alle zwei Jahre ausrichtet, eine feste Größe im Veranstaltungskalender der nationalen und internationalen IT-Sicherheitsbranche. Ziel des Kongresses ist es, aktuelle Trends und Technologien im Bereich der IT-Sicherheit aus unterschiedlichen Perspektiven zu beleuchten und zu diskutieren sowie Lösungsansätze vorzustellen und weiterzuentwickeln.

Der Hamburgische BfDI: Konsequenzen der EuGH-Grundsatzentscheidung

Die heutige Entscheidung des EuGH vom 13.05.2014 zum Rechtsstreit zwischen Google Spanien und der Spanischen Datenschutzbehörde stärkt in historischer Weise die Rechte von Betroffenen gegenüber Betreibern von Suchmaschinen, die deren persönliche Daten im Netz verbreiten. Zudem enthält das Urteil weitreichende Konsequenzen für die Anwendung des nationalen Datenschutzrechts auf verantwortliche Stellen mit unterschiedlichen Niederlassungen innerhalb der EU.

Danach ist nationales Datenschutzrecht auch dann anwendbar, wenn zwar die Verarbeitung der Nutzerdaten nicht unmittelbar durch die Muttergesellschaft mit Sitz in einem Drittstaat ausgeführt wird, eine Tochtergesellschaft im nationalen Bereich jedoch das Werbegeschäft zur Finanzierung des angebotenen Dienstes betreibt. Internetdiensten ist es künftig nicht mehr möglich, den Verpflichtungen des nationalen Datenschutzrechts dadurch zu entgehen, dass sie die Verantwortlichkeit für die Verarbeitung der Daten der Betroffenen auf eine Niederlassung in der EU verengen. Insoweit erscheinen auch die Datenschutzfragen, die in der Vergangenheit gegenüber dem Sozialen Netzwerkbetreiber Facebook aufgeworfen wurden, in einem neuen Licht.

Außerdem stärkt das Urteil die Rechte der Betroffenen gegenüber Suchmaschinenbetreibern. Diese haben nach der EuGH-Entscheidung eine rechtliche Verantwortung zur Einhaltung der Vorgaben der EU-Datenschutzrichtlinie. Betreiber werden verpflichtet, auf Antrag der Betroffenen Links zu den Internetseiten zu löschen, soweit diese in das Persönlichkeitsrecht der Betroffenen unverhältnismäßig eingreifen. Das gilt insbesondere auch für solche Daten, deren ursprüngliche Verarbeitung rechtmäßig gewesen ist. Suchmaschinenbetreiber können nunmehr Betroffene nicht allein an die ursprünglich für die Veröffentlichung verantwortlichen Stellen verweisen.

Auch ohne dass der EuGH ausdrücklich auf ein Recht auf Vergessenwerden rekurriert, haben Nutzer künftig ein Recht zu verlangen, dass Suchmaschinenbetreiber in den Ergebnislisten vermittelte Daten löschen, soweit diese etwa infolge der seither verstrichenen Zeit nicht mehr mit ihnen in Verbindung gebracht werden sollen. Diese sind künftig auch nicht mehr auf den Zivilrechtsweg verwiesen, sondern können sich zur Durchsetzung ihrer Rechte unmittelbar an die Datenschutzbehörden wenden.

Hessischer LfD: Kernpunkte des 42. Tätigkeitsberichtes für 2013

Die datenschutzrechtliche Debatte des Berichtsjahres war vor allem geprägt durch das massenhafte Ausspähen der Kommunikation durch ausländische Nachrichtendienste.

Abhöraktivitäten ausländischer Nachrichtendienste

Nach den bisher vorliegenden Erkenntnissen muss davon ausgegangen werden, dass us-amerikanische und britische Nachrichtendienste ohne konkreten Anlass massenhaft Telekommunikationsverkehre auch in Hessen überwacht haben. Dies ist nach deutschem Recht unzulässig. Selbstverständlich ist auch bei der Telekommunikationsüberwachung befreundeter Dienste in Deutschland deutsches Recht anwendbar. Der Hessische Datenschutzbeauftragte hat für den Fall eklatanter Verstöße gegen deutsches Recht auf die Möglichkeit hingewiesen, bei den seiner Kontrolle unterliegenden Datentransfers in die USA die erleichterte Datenübermittlung nach dem Safe Harbor Abkommen auszusetzen.

Datenschutzgrundverordnung

Bereits im letzten Tätigkeitsbericht hatte Prof. Dr. Ronellenfitsch über die geplanten Neuregelungen im Datenschutzrecht auf europäischer Ebene berichtet. Obwohl er eine Fortentwicklung des europäischen Datenschutzrechts für dringend erforderlich hält, rechtfertigt die unionsrechtliche Vereinheitlichung aus seiner Sicht keine Beschneidung der Fortentwicklungsmöglichkeiten des deutschen Datenschutzrechts. Er hält deshalb seine schon wiederholt geäußerten verfassungsrechtlichen Bedenken ausdrücklich aufrecht.