

Wo liegen nun die Gründe dafür, dass Außenstehende die Datenschutzbeauftragten als „wichtig, aber mit relativ geringem Einfluss“ wahrnehmen? „Das, was wir in der Praxis mitunter mühsam erreichen, müssen wir besser kommunizieren“, zieht Biewald Bilanz. „Zugleich ist zu klären, ob Datenschützer überhaupt gerüstet sind, alle Aufgaben umfassend wahrzunehmen“. Die Politik müsse sich fragen, warum sie regelmäßig nur über die Bestellung von Datenschutzbeauftragten statt über deren Ausstattung mit Kompetenzen diskutiere. „Wirksamer Datenschutz ist eine Frage von wirksamen Instrumenten“, betont Spaeing.

Die Studie kann über den Berufsverband bezogen werden:

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., Budapester Straße 31, 10787 Berlin, E-Mail: bvd-gs@bvdnet.de, Tel.: 030/2196 4397

(a-I3): 7. Interdisziplinäres Symposium, Bochum, 16./17.04.2012

Am 16. und 17. April 2012 findet in Bochum das 7. Interdisziplinäre Symposium der Arbeitsgruppe Identitätsschutz im Internet (a-i3) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) statt.

In diesem Jahr sollen unter dem Oberthema „Perspektiven und Risiken der digitalen Gesellschaft – ID-Management und Datenschutz für Cloud Computing & IPv6“ aktuelle Themen aus den Bereichen Infrastruktursicherheit, Identitätsmanagement und Datenschutz umfassend aus rechtlicher und technischer Perspektive beleuchtet werden.

Die Veranstaltung richtet sich an Entscheidungsträger von Verwaltungsbehörden, an Leiter, Mitarbeiter und Datenschutzbeauftragte in Organisationen und Unternehmen aus den Gebieten IT-Sicherheit, Softwareentwicklung und E-Commerce. Weiterhin an Juristen in Justiz, Unternehmen und Verbänden, spezialisierte Rechtsanwälte sowie Leiter und Mitarbeiter in Aufsichts- und Datenschutzbehörden.

Aktualisierte Informationen zur Veranstaltung finden Sie unter www.a-i3.org.

App „Permission Watcher“ für Android-Smartphones

Die App entstand im Rahmen der Master-Arbeit von Eric Struse sowie eines gemeinsamen Forschungsprojekts der Mobile Human-Computer-Interaction Group an der Universität Duisburg-Essen (Enrico Rukzio) und der Arbeitsgruppe Langzeitsicherheit der Ruhr-Universität Bochum (Christopher Wolf).

Die App hilft Nutzern, die Berechtigungen der auf ihren Smartphones installierten Apps zu überwachen. Sie warnt vor verdächtigen Berechtigungs-Kombinationen, die benutzt werden können, um Datenschutz und Privatsphäre des Nutzers zu beeinträchtigen oder unerwünschte Kosten zu verursachen.

Wenn Sie die App installieren helfen Sie uns, Sicherheitsaspekte im Bereich Nutzerinteraktion besser zu verstehen. Sie steht im Android Market unter:

<https://market.android.com/details?id=de.struse.apewatch> oder auf

<http://www.apewatch.de> und ist in deutscher und englischer Sprache verfügbar.

Rückfragen bitte an Eric Struse <Eric@Struse.de>

McAfee: Jahresprognose zur Cybersicherheit 2012

Der IT-Sicherheitsspezialist McAfee hat am 29.12.2011 seine Jahresprognose der Risiken und Gefahren für die Computersicherheit vorgelegt („2012 Threat Predictions“). Die firmeneigene Forschungsabteilung McAfee Labs, die für den Bericht verantwortlich zeichnet, erwartet, dass die 2011 notorisch gewordenen Eingriffe in mobile Banktransaktionen, pseudolegaler Spam und Betrug im Zusammenhang mit Cybergeld im Jahr 2012 weiter an Bedeutung gewinnen. Des Weiteren geht McAfee Labs davon aus, dass die Zahl der im weitesten Sinn politisch motivierten Angriffe zunehmen wird, etwa in Form der Kompromittierung von Industrieunternehmen und Personen des öffentlichen Lebens oder durch Zurschaustellung von Fähigkeiten zur Cyberkriegsführung durch Nationalstaaten.

Folgende Trends prognostiziert McAfee Labs für das Jahr 2012:

Angriffe auf Infrastrukturunternehmen

Die Versorgung mit Wasser, Strom, Öl und Gas dient der Erfüllung von Grundbedürfnissen der Bevölkerung. Dennoch sind die entsprechenden Dienstleister nur unzulänglich vor Cyberangriffen geschützt. Oft fehlt es an grundlegenden Sicherheitsmechanismen. Es ist davon auszugehen, dass Angreifer diesen Mangel an Sicherheitsvorkehrungen in Zukunft verstärkt zum Beispiel zur Erpressung dieser Unternehmen ausnutzen werden.

„Legalisierung“ von Spam durch die werbetreibende Industrie

Das weltweite Aufkommen an klassischem Spam ist laut McAfee Labs in den vergangenen zwei Jahren zwar zurückgegangen, doch inzwischen setzt die ganz normale Werbeindustrie zunehmend auf Methoden, die sie sich bei Spammern abgeguckt hat. So übernehmen beispielsweise Werbetreibende Adressbestände von in Konkurs gegangenen Unternehmen oder kaufen auf anderen Wegen E-Mail-Adressen, deren Inhaber angeblich dem Empfang von Werbetexten zugestimmt haben. McAfee Labs geht davon aus, dass dieser pseudolegale Spam nach dem „Gießkannenprinzip“ schneller zunimmt als beispielsweise Phishing (Abgreifen von Zugangsdaten) und „Confidence-Scams“ (zum Beispiel Vorschussbetrug nach dem „Nigeria“-Muster).

Angriffe auf Mobilgeräte unter Umgehung des PCs

Noch nie gab es so viel Schadsoftware für Mobilgeräte wie 2011. Für das kommende Jahr erwartet McAfee Labs, dass vor allem der Betrug im Zusammenhang mit unterwegs getätigten Bankgeschäften zunimmt. Dabei ist davon auszugehen, dass Methoden, die einst auf das klassische Online-Banking gemünzt waren – wie die Vorspiegelung einer rechtmäßigen Transaktion zum Zweck der Geldentwendung, während der Nutzer bei seiner Bank angemeldet ist –, nun beim mobilen Banking Anwendung finden. Da immer mehr Menschen ihre Geldgeschäfte mit Hilfe von Mobilgeräten tätigen, werden die Angreifer nach der Prognose von McAfee Labs in Zukunft die PCs ihrer Opfer links liegen lassen und sich auf deren Mobile-Banking-Apps konzentrieren.