Vorstandswechsel bei der GDD

Anlässlich der Mitgliederversammlung am 21.11.2012 wählten die Mitglieder Prof. Dr. Rolf Schwartmann, Leiter der Kölner Forschungsstelle für Medienrecht an der Fachhochschule Köln, zum neuen Vorstandsvorsitzenden der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD). Als habilitierter Jurist liegt sein Forschungsschwerpunkt im Recht der neuen Medien mit deutlichen Schwerpunkten auf den Datenschutz und das Urheberrecht. Als Vorstandsvorsitzender ist es sein Ziel, die strategische Positionierung der GDD im Internetzeitalter fortzuentwickeln und Datenschutz und Datensicherheit weiter zu verzahnen. Prof. Schwartmann tritt die Nachfolge von Herrn Prof. Peter Gola an, der zunächst als stellvertretender Vorstandsvorsitzender und seit 2004 als Vorstandsvorsitzender für die GDD tätig war. Die Mitglieder wählten Herrn Prof. Gola wegen seiner herausragenden Verdienste um den Datenschutz und die GDD einstimmig zu ihrem Ehrenvorsitzenden.

Als neuer stellvertretender Vorstandsvorsitzender wurde Prof. Dr. Rainer W. Gerling, Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule in München gewählt. Neues Mitglied des Vorstandes als Beisitzer ist Prof. Dr. Gregor Thüsing, Direktor des Instituts für Arbeitsrecht und Recht der sozialen Sicherheit an der Universität in Bonn. Er wird im Vorstand der GDD vornehmlich den Bereich des Beschäftigtendatenschutzrechts betreuen.

Neu in das Amt eines Beisitzers wurde Heiko Kern gewählt, der im Vorstand den Bereich IT-Sicherheit und Informations- und Kommunikationstechnik bearbeiten soll.

In ihren Ämtern bestätigt wurden Dr. Astrid Breinlinger als stellvertretende Vorstandsvorsitzende sowie die Beisitzer Gabriela Krader, Harald Eul und Dr. Martin Zilkens. Als Repräsentant der Erfa-Kreise im Vorstand der GDD wurde Gerhard Stampe bestätigt.

Report des Information Security Forums: "You Could Be Next"

Das Information Security Forum, eine große unabhängige Non-Profit-Organisation für Informationssicherheit, Cybersicherheit und Risikomanagement, hat am 10.12.2012 einen Report für den Umgang mit IT-Sicherheitsvorfällen und Cyberattacken veröffentlicht. „You could be Next" gibt Unternehmen Handlungsempfehlungen für die Bestandaufnahme sowie die Ursachenanalyse bei einem Sicherheitsvorfall. Ein besonderes Augenmerk liegt auf den langfristigen Kosten und der Risikoprävention. Der Report basiert auf den Erfahrungen und Best Practices der ISF-Mitgliedsunternehmen weltweit. Eine kostenlose Kurzfassung ist auf der Website des ISF unter *www.securityforum.org* erhältlich.

Kaspersky Lab: IT-Sicherheitsprognosen für 2013

Am 05.12.2012 hat Kaspersky Lab mit einem Security Bulletin über die IT-Security-Trends für 2013 informiert. Dabei erwartet der IT-Sicherheitsexperte mehr zielgerichtete Angriffe gegen Unternehmen, Cyberspionage und -attacken gegen Unternehmen und Staaten, weitere Hacktivismus-Aktionen sowie Cyberattacken, die gegen Cloud-basierte Dienste gerichtet sind.

In den vergangenen beiden Jahren haben zielgerichtete Attacken gegen Unternehmen stark zugenommen. Kaspersky Lab erwartet für 2013 einen weiteren Anstieg dieser „Targeted Attacks". Unternehmen werden in diesem Zusammenhang vor allem mit Cyberspionage zu kämpfen haben. Darüber hinaus werden sich Firmen und Regierungsorganisationen mit Hacktivismus und politisch motivierten Cyberattacken auseinandersetzen müssen.

Neue Cyberwaffen für Spionage und Sabotage

Mit Flame, Gauss und miniFlame hat Kaspersky Lab in diesem Jahr drei Schadprogramme entdeckt, die im Zusammenhang mit Cyberkriegsoperationen standen. Staatlich unterstützte Cyberwaffen werden nach Meinung des IT-Sicherheitsspezialisten auch im Jahr 2013 auftauchen. Flame war das größte und anspruchsvollste Cyberspionageprogramm, dessen langandauernde Aktivität besonders charakteristisch war. Das Projekt Flame gab es seit mindestens fünf Jahren. Dabei wurden mit einem komplexen Schadprogramm über lange Zeit unbemerkt massive Datenmengen und sensible Informationen der attackierten Opfer gesammelt. Die Experten von Kaspersky Lab gehen davon aus, dass weitere Länder ihre eigenen Programme für Cyberspionage und Cybersabotage entwickeln werden. Deren Attacken werden nicht nur Regierungsorganisationen, sondern auch Unternehmen und kritische Infrastrukturumgebungen betreffen.

Derzeit wird debattiert, ob Regierungen spezielle Überwachungssoftware für ihre Kriminalermittlungen entwickeln und nutzen sollten. Diese Diskussion wird sich im kommenden Jahr fortsetzen. Denn Regierungsorganisationen schaffen und erwerben zusätzliche Überwachungswerkzeuge – neben herkömmlichen Technologien zum Abhören von Telefonen – mit denen sie Personen über einen heimlichen Zugang auf anvisierte mobile Geräte überwachen können. Sobald die Strafermittlungsbehörden versuchen, den Cyberkriminellen einen Schritt voraus zu sein, werden voraussichtlich auch regierungsgestützte Überwachungswerkzeuge weiterentwickelt werden. Gleichzeitig werden in diesem Kontext Themen rund um Zivilrechte und Privatsphäre der Anwender kontrovers diskutiert werden.

Großer Wert sensibler Daten bei Cloud-Diensten

Sowohl Privatanwender als auch Unternehmen haben durch die Entwicklung Sozialer Netzwerke und auch den damit einhergehenden Gefahren mittlerweile eine andere Wahrnehmung hinsichtlich der Online-Privatsphäre und des Vertrauens in bestimmte Dienste. Nutzer wissen, dass sie einen Großteil ihrer persönlichen Daten an Online-Dienstleister weitergeben. Die Frage ist, ob sie diesen Diensten auch vertrauen. Große Passwort-Lecks, wie bei den beliebten Webservices Dropbox oder LinkedIn, sind nicht gerade förderlich für die Vertrauensbildung zwischen Nutzer und Anbieter. Der Wert persönlicher Daten wird – für Cyberkriminelle und Unternehmen – in naher Zukunft signifikant steigen.

Mobile Drive-by-Downloads

In 2012 fand eine regelrechte Explosion im Bereich mobiler Malware statt. Dabei haben sich die Cyberkriminellen vor allem auf Android als populärstes Betriebssystem konzentriert. Für das kommende Jahr geht Kaspersky Lab davon aus, dass sich die Qualität der mobilen Attacken verschärfen wird und Schwachstellen mobiler Geräte für Drive-by-Download-Angriffe missbraucht wer-