Neue Lösungsansätze

Jede Art von vertrauenswürdiger elektronischer Datenverarbeitung erfordert eine Form von Sicherheitsinfrastruktur. Solche Strukturen treten im täglichen Leben zu meist in Gestalt von Public-Key-Infrastrukturen in Erscheinung, welche die Grundlage für sicheres Surfen im Internet und vertrauenswürdige Online-Dienste darstellen. Neben den aus den Webbrowsern wohlbekannten HTTPS-gesicherten Seiten mit den dazu gehörigen SSL-Zertifikaten existiert in der Kryptographie auch noch eine Reihe von weniger bekannten, jedoch nicht weniger nützlichen Sicherheitsmechanismen.

Gerade die in jüngster Zeit zunehmende Nutzung von Cloud-Computing-Diensten stellt Datenschützer vor neue Herausforderungen und erfordert innovative Lösungsansätze, um vertrauenswürdige Datenverarbeitung in zunehmend verteilten und vernetzten Systemen zu ermöglichen. Hierbei sind Konflikte unvermeidbar: Dem Recht auf Datenschutz steht z. B. das Recht auf Auskunftspflicht gegenüber. Gerade bei der Nutzung von Online-Diensten und sozialen Netzwerken zeigt sich das Phänomen einer bereitwilligen und bisweilen unreflektierten Herausgabe von persönlichen Daten. Diese Daten zu schützen ist Aufgabe von geeigneten Sicherheitsinfrastrukturen.

Die Beiträge dieses Heftes geben einen Einblick in laufende Forschungsaktivitäten und beschreiben neue Erkenntnisse im Bereich der IT-Sicherheitsinfrastrukturen. So nehmen Sorge und Krohn-Grimberghe eine erste Einordnung des überraschend erfolgreichen Bitcoin-Verfahrens vor. Der Beitrag von Höhne, Pöhls und Samelin untersucht die Rechtsfolgen digitaler Signaturen, die begrenzte nachträgliche Änderungen zulassen.

Unternehmensinterne Sicherheitsinfrastrukturen sind oft maßgeschneiderte Lösungen und somit häufig nicht zentraler Gegenstand akademischer Betrachtungen. Ein Projekt, welches Infrastrukturen im Hinblick auf das Abhörissiko untersucht und zu optimieren versucht, stellen Schauer, Rainer und Schmid in ihrem Beitrag vor. Die zunehmende Nutzung von Smartphones stellt neue Anforderungen an Sicherheitssysteme. So sind z. B. Passworte und PINs bei der Eingabe häufig leicht auszuspionieren. Der Beitrag von Kollmitzer und Fenzl beschreibt die Erfahrungen mit nicht zeichenbasierten Zugangscodes als Alternative zu herkömmlichen Passwörtern. Braun, Maisch, Seidl, Gemein und Höfling untersuchen Angriffe auf das OpenID-Authentifikationssystem. Anschließend stellen Slamanig und Stingl in ihrem Beitrag technische und kryptographische Möglichkeiten vor, wie Datenschutz im Cloud Computing zumindest teilweise inhärent in Systemen verankert werden kann. Schließlich gibt Wigoutschnigg einen Überblick über Anonymisierungsprotokolle, und Dittmayer zeigt rechtliche Fallstricke für Blogger auf.

Stefan Rass