Schwachstellen der Gesellschaft

Wir mussten in den letzten Jahren mit ansehen, wie professionelle Hacker aus der ganzen Welt uns zeigen, dass sie in der Lage sind, alles im IT-Umfeld zu hacken, wenn sie nur genug Energie auf das Ziel setzen. Die Chinesen greifen z.B. Google, NY Times und das US Verteidigungsministerium an, die Russen das, was politisch gerade passt oder finanziell besonders attraktiv ist und die Amerikaner, neben unserer Kanzlerin, alles, um die Welt vor Terrorismus zu retten. Die kriminellen Organisationen haben einen sehr lukrativen Business-Bereich gefunden, usw.

Diese sehr schlechte IT-Sicherheitssituation hat weitreichende Auswirkungen für alle Menschen und Unternehmen: 50 Milliarden Euro Schaden im Jahr im Bereich Wirtschaftsspionage laut den Aussagen des Bundesinnenministeriums, allein in Deutschland. Angriffe auf kritische Infrastrukturen bedeuten eine prinzipiell höhere Angreifbarkeit unserer Gesellschaft. Die vielen Angriffe auf unsere Persönlichkeitsrechte – sogar auf die Privatsphäre – durch die US-Marktführer sind auch ein Angriff auf die Demokratie.

Mit den allgemein verfügbaren IT-Produkten und –Lösungen und Infrastrukturen steht weder den Staaten noch den Anwendungsentwicklern und erst recht nicht den Nutzern ein Potential zu einem angemessenen Schutz gegen die intelligenten Angriffe zur Verfügung. Wer gut oder böse ist, wird in den komplexen und intransparenten Strukturen immer schwerer erkennbar. Der strukturelle Angriff auf das Internet mit all seinen Standards, Technologien und Playern ist uns mit der NSA-Affäre klar geworden. Es macht sich ein Ohnmachtsgefühl breit, was uns leider nicht weiter hilft.

Doch was sind die wichtigsten Herausforderungen und welcher Handlungsspielraum steht uns zur Verfügung, um diese schlechte IT-Sicherheitssituation zu verbessern?

In diesem Heft wollen wir an Beispielen einiger interessanter Ideen aufzeigen, welche Möglichkeiten heute schon bestehen, aber auch welche in der Zukunft die Vertrauenswürdigkeit und die IT-Sicherheit unserer immer wichtigeren Technologien der Informations- und Wissensgesellschaft angemessen verbessern.

Themen sind Vertrauenswürdigkeit und IT-Sicherheit von Software und Hardware sowie moderne IT-Sicherheitskonzepte. Verbesserte Konzepte, wie Mobile ID sowie neue und flexible IT-Sicherheitstechnologien in Mobiltelefone/Smartphones werden aufgezeigt, diskutiert und Anwendungsbeispiele dargestellt. Ideen werden vorgestellt, wie z.B. Zertifizierungsinfrastrukturen vertrauenswürdiger für alle überprüfbar betrieben werden können und welche neuen Trust Service Provider perspektivisch aus der eIDAS-Verordnung entstehen können.

Ein innovatives Konzept zeigt auf, wie eine sichere Authentikation preisgünstig und einfach im e-Mobility-Bereich umgesetzt werden kann. Die rechtliche und ethische Verpflichtung der Verschlüsselung wird diskutiert, aber auch über die informationelle Mündigkeit und informationelle Müdigkeit wird philosophiert. Für den interessierten Laien, neugierigen Experten und Kryptologie-Begeisterten wird die Lernsoftware CrypTool 2.0, Open-Source Kryptologie für Jederman, erläutert und zur Nutzung motiviert.

Wir wünschen Ihnen viel Freude und interessante Erkenntnisse beim Studium der Beiträge dieser DuD-Ausgabe. Auch über ein Feedback würden wir uns sehr freuen.

Norbert Pohlmann