Ausspioniert?!?

Im Rahmen der Enthüllungen von Edward Snowden sind gleich eine ganze Reihe von Sachverhalten zu diskutieren. Neben den Schreckensszenarien einer totalen Überwachung spielen dabei die Fragen zur Sicherheit der aktuell eingesetzten kryptographischen Verfahren eine entscheidende Rolle. Dies gilt gerade auch deshalb, weil der Einsatz von Kryptographie -bspw. im Bundesdatenschutzgesetz- als wesentliches Element zur Sicherstellung von Vertraulichkeit und Integrität angesehen wird.

Vor dem Hintergrund einer umfassenden (und ggf. langfristigen) weltweiten Speicherung von Kommunikationsdaten muss allerdings völlig neu bewertet werden, ob sich Kryptographie auch zukünftig als sinnvolle Schutzmaßnahme einsetzen lässt. Vor allem die Möglichkeit, mittels Quantencomputern heutige kryptographische Protokolle brechen zu können, zwingt zu einer neuen Risikobewertung.

Aber liegt das eigentliche Problem für die Sicherheit durch Kryptographie in der möglichen Existenz eines Quantencomputers? Oder gibt es vielleicht deutlich wichtigere Aspekte, die die Sicherheit, insbesondere die Vertrauenswürdigkeit, unserer Infrastrukturen nachhaltig bedrohen? Dieser Frage gehen die Autoren dieses Schwerpunktheftes anhand von konkreten Beispielen nach, zeigen Problemfelder der Praxis auf und stellen zudem mögliche Lösungsansätze vor:

- Der erste Beitrag **Datenschutz nach dem Summer of Snowden** von Marit Hansen gibt einen chronologischen Überblick über die bisherigen Snowden-Enthüllungen und stellt Schlussfolgerungen für Politik und (Datenschutz-)Praxis vor.
- Tibor Jager erläutert in seinem Beitrag **Die Zukunft der Kryptographie,** ob und wie lange heutige Algorithmen als sicher erachtet werden können. Er betrachtet Quantencomputer und generelle Aspekte zum sicheren Einsatz von Kryptographie.
- Im Beitrag **Zukunft der Web-PKI?** widmet sich Jürgen Brauckmann den Fragen zur Vertrauenswürdigkeit heutiger Web-PKI-Konzepte. Anhand konkreter Problemsituationen zeigt er aktuell ungelöste Fragen und Lösungsansätze auf.
- Peter Koch geht im Beitrag **Vertraulichkeit für den Auskunftsdienst im Internet** auf den Aspekt ein, ob und ggf. wann DNS-Daten als vertraulich betrachtet werden müssen, und diskutiert den aktuellen Stand der Entwicklungen.
- **Authentification and Identification - Taking the User into Account** titelt der erste von zwei Beiträgen zum Themenblock **Identifizierung und Authentifizierung**. Kim Nguyen beleuchtet hierbei das FIDO-Projekt, das dem Nutzer z.B. Wahlmöglichkeiten für die Authentifizierungsmethode einräumt.
- Marc Fischlin zeigt im Beitrag **Abstreitbarkeit bei eID-Lösungen** anhand konkreter Umsetzungen (bspw. beim ePass und nPA), wie sich das Merkmal der Abstreitbarkeit als Mechanismus zum Schutz der Privatsphäre einsetzen lässt.
- Annika Selzer beleuchtet dann die rechtlichen Fragen zum **Datenschutz bei internationalen Cloud Computing Services**. Hierbei wird deutlich, dass es erhebliche Hürden gibt und diese Dienste schon aus rechtlichen Überlegungen nur nach einer gründlichen Risikoanalyse genutzt werden sollten.

Ergänzt wird der Schwerpunkt des Heftes diesmal durch zwei Aufsätze:

- Christoph Busch zeigt in seinem Beitrag **Biometrische Zugangskontrolle mit Smartphones**, wie Biometrie auch Einzug in den Alltag der Normalanwender halten könnten, etwa durch Nutzung biometrischer Sensoren an Smartphones.
- Der Beitrag **Überschussdaten in Retinabildern** vom Team um Michael Friedewald beschäftigt sich mit der Frage, ob und ggf. welche Informationen zum Gesundheitszustand des Betroffenen in biometrischen Daten enthalten sind und wie hier vorbeugende Maßnahmen helfen können, die Privatsphäre zu wahren.

Zusammen mit dem gesamten Herausgeberteam wünsche ich Ihnen als Gastherausgeber eine informative und spannende Lektüre. Wir hoffen, dass auch diese Ausgabe Ihnen, verehrte Leserinnen und Leser, viele Anregungen für Ihre tägliche Praxis gibt.

Christoph Wegener