Ein neues Grundrecht

Wir brauchen ein neues „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" – so bewertete das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 die Fragen rund um die Online-Durchsuchung und weckte damit bei Beteiligten und Beobachtern hohe Erwartungen.

Bei genauerer Betrachtung kehrt jedoch schnell Ernüchterung ein: Mehr als vier Jahre nach dem besagten Urteil ist die Frage in den Mittelpunkt gerückt, ob und ggf. wie das neue Grundrecht in der Praxis in Erscheinung tritt und umgesetzt werden könnte. Gerade die durch die Analyse des Chaos Computer Clubs ausgelösten Diskussionen rund um den Bundestrojaner im vergangenen Jahr haben gezeigt, wie fragil die Sicherheitsqualitäten von IT-Systemen sind.

Dieses Schwerpunktheft befasst sich daher mit den Fragen rund um die Themen Vertraulichkeit und Integrität. Aufbauend auf dem Urteil des BVerfG untersuchen die Autoren, ob und ggf. wie sich diese Schutzziele in einer Welt der modernen IT-Prozesse umsetzen lassen.

Die einzelnen Beiträge im Überblick

- Im Beitrag **Das neue Computergrundrecht – eine Erfolgsgeschichte?** beschreibt Martin Kutscha zunächst die Umstände des Urteils und vor allem die anschließenden Entwicklungen sowohl auf staatlicher als auch privater Ebene.
- Gabriel Schulz greift das Thema nochmals auf. **Das neue IT-Grundrecht – staatliche Schutzpflicht und Infrastrukturverantwortung** beleuchtet den Umgang des Staates mit dem Grundrecht – etwa im Rahmen der Bereiche Quellen-TKÜ, der De-Mail und eID und dem Entwurf zum neuen E-Government-Gesetz.
- **„Der Bau" von Kafka oder die (Staats)Trojaner-Architektur** heißt der Beitrag von Wolfgang Schmale und Marie-Theres Tinnefeld. Sie diskutieren das Scheitern einer Sicherheitsarchitektur, die zur Abwehr von potentiellen Feinden errichtet wurde – sich dabei aber in technischen Überlegungen verliert.
- Marit Hansen beleuchtet das Thema **Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter**. Der Beitrag zeigt klar auf, dass sich das Grundrecht zwar auf eine moderne IT ausdehnen lässt, eine Umsetzung in der Praxis aber auf große Schwierigkeiten stößt.
- In **Software-Integrität – geht das?** widmet sich Sachar Paulus der Frage, ob und wie sichere Software gebaut werden kann. Insbesondere der Aspekt der Integrität ist im Rahmen von regelmäßigen Updates und Patches kritisch zu betrachten und nicht zuletzt muss auch das zugrunde liegende System vertrauenswürdig sein.
- Das Thema **Informationssicherheit in der Arztpraxis: Aktuelle Herausforderungen und Lösungsansätze** wird im Anschluss von Marcel Winandy diskutiert. Er stellt in seinem Beitrag klar, dass Wunsch und aktuelle Realität noch weit auseinander liegen – und dass den Beteiligten oft Wissen und Erfahrungen fehlen, um dies zu erkennen.

Drei weitere Beiträge widmen sich dem Thema „Neue Datenschutz-Schutzziele":

- **Datenschutz-Schutzziele im Recht** stellen Kirsten Bock und Sebastian Meissner dar. Sie zeigen auf, ob und ggf. wie die neuen Schutzziele im Bereich Datenschutz im Gesetz verankert sind. Martin Rost stellt in seinem Beitrag ein Konzept für eine **Standardisierte Datenschutzmodellierung** vor, das es ermöglichen soll, jedes Verfahren mit Personenbezug systematisch und vollständig zu prüfen. Der Fragestellung adäquater Schutzmaßnahmen widmet sich schließlich Thomas Probst im Beitrag **Generische Schutzmaßnahmen für Datenschutz-Schutzziele**.

Ein weiterer Beitrag geht auf das aktuelle Thema „Smart Meter / Smart Grid" ein:

- **Informationssicherheit im zukünftigen Smart Grid** von Stephan Gerhager beschreibt die Risiken der „smarten" Stromversorgung, insbesondere im Hinblick auf Aspekte, die über das Thema Datenschutz für den Kunden hinaus gehen.

Zusammen mit dem gesamten Herausgeberteam wünsche ich Ihnen als Gastherausgeber auch diesmal wieder eine spannende Lektüre und hoffe, dass sie viele Anregungen für Ihre aktuellen Projekte bekommen.

Christoph Wegener