Cybersicherheits-architektur – Großbaustelle ohne Plan

Cybersicherheit hat allumfassenden Charakter. Aus digitalen Angriffen können sich Risiken für jeden Bereich unseres Lebens ergeben. Eine Erweiterung von polizeilicher Cybercrime-Kompetenz, von nachrichtendienstlicher Aufklärung, von Cyber-Know-How in der Bankenaufsicht, technischer Kompetenz der Datenschutzbeauftragen – all das ist unzweifelhaft notwendig. Entsprechend groß ist das Wachstum von Aufgaben und Personal der verschiedenen öffentlichen Einrichtungen, die sich mit Cybersicherheit beschäftigen.

Das Wachstum ist bislang eher organisch erfolgt – einen übergreifenden Plan gibt es nicht. Das erkennbare Wuchern von Cyberaufgaben allüberall im öffentlichen Sektor birgt die Gefahr, dass eine effektive Cybersicherheit durch Behördenrivalitäten, unklare Ansprechpartner, mangelnde Abstimmung und widersprüchliche Regulierung behindert wird. Wesentliche Architekturentscheidungen stehen an, um diese Großbaustelle zu ordnen:

Einheitliche Gefahrenabwehr: In Deutschland sind primär die Länder für die Gefahrenabwehr zuständig, vor allem die Polizeien. Das IT-Sicherheitsgesetz baut hingegen entsprechende BSI-Befugnisse weiter aus. Gleichzeitig gibt es für die Abwehr von Angriffen aus dem Ausland noch keine Lösung.

Einheitliche Regulierung: Die IT-Sicherheit der Systeme wichtiger Unternehmen wird mittlerweile gleich dreifach reguliert: neben dem BSI machen auch sektorale Aufsichtsbehörden wie BAFin und BNetzA sowie Datenschutzbeauftragte IT-Sicherheitsvorgaben. Für Innovation und Wettbewerbsfähigkeit ist das eine schlechte Lösung.

Zusammenarbeitsformen: Eine Vielzahl von Initiativen soll die Zusammenarbeit von Unternehmen und Behörden bei der Cybersicherheit gewährleisten. Gesetzliche Meldepflichten und informelle Zusammenarbeit stehen dabei in Konkurrenz. BSI, Verfassungsschutz und Polizei pflegen allerlei Kooperationen mit Privaten – gleichzeitig sind weite Teile der Wirtschaft in keine dieser Plattformen eingebunden.

In der kommenden Wahlperiode des Deutschen Bundestages wird Deutschland Antworten auf diese Fragen der Cybersicherheitsarchitektur geben müssen. Im Mittelpunkt der Debatte steht die Rolle des BSI: Allumfassender Regulierer, Sonderpolizeibehörde, neutraler Ratgeber oder unabhängiger Gutachter – wo wird das Amt positioniert? Ähnliche Entscheidungen wie in Deutschland stehen auch in Europa an.

Mit dem Schwerpunktthema dieses Heftes leisten erfahrene Autorinnen und Autoren Beiträge zu der anstehenden Debatte. Sie beleuchten die Rolle der Länder (Remy/Stettner), der Datenschutzbeauftragten (Hansen) und der Forschung (Kreutzer/Schneider). Die Zusammenarbeit auf europäischer Ebene (Kowalski/Intemann/Mühlenbruch) wird ebenso untersucht wie die Zusammenarbeit von Staat und Wirtschaft (Lahmann). Die heutige und künftige Rolle von ZITiS (Karl/Hummert) und BSI (Schallbruch) runden die Betrachtung ab.

Eins zeigen alle Beiträge sehr deutlich: wir haben inzwischen genügend belastbare Erfahrungen, um einen großen Wurf zu schaffen: unsere Cybersicherheitsarchitektur aus einem ungeplanten Wuchern in einen geplanten Ausbau zu überführen.

Zusätzlich zu den Schwerpunktbeiträgen enthält das Heft ein Positionspapier – Erfahrbarer Datenschutz und IT-Sicherheit in Smart Home Anwendungen – und den Aufsatz von Arlette Amend ‚Anwaltliche Geheimhaltungspflicht vs. Datenschutzaufsicht'.

Martin Schallbruch