IT-Sicherheitsgesetz 2.0 – Das Warten hat ein Ende

Steve Ritter

Am 23. 4. 2021 hat das IT-Sicherheitsgesetz 2.0 endlich den Bundestag passiert. Da sich der Bundesrat am 7. 5. – trotz entsprechender Ausschussempfehlungen – nicht noch in den Weg gestellt hat, kann es im Sommer in Kraft treten. Angesichts der bis zuletzt wechselvollen Entstehungsgeschichte des Gesetzes war dies nicht selbstverständlich. Bereits im Koalitionsvertrag hatten sich die Regierungsparteien 2018 darauf verständigt, das IT-Sicherheitsgesetz fortzuentwickeln. Bis jedoch ein offizieller Referentenentwurf veröffentlicht wurde, musste sich die interessierte Öffentlichkeit recht lange gedulden. Zwar tauchten seit 2019 immer wieder inoffizielle Entwürfe auf, die begierig von der Rechtswissenschaft aufgegriffen wurden – welche der enthaltenen Regelungen aber tatsächlich als Gesetzentwurf das Licht der Welt erblicken würden, blieb bis Ende 2020 unklar. Erst dann wurde der offizielle Entwurf des Innenministeriums an die Verbände verteilt.

Noch im Dezember wurde der Kabinettsentwurf verabschiedet und in den Bundestag eingebracht. Dort erntete er teilweise unerwartet harte Kritik von allen Sachverständigen. Bei deren mündlicher Anhörung konnte man den Eindruck gewinnen, es gäbe wenig Gutes an dem Entwurf. Einige schlechte Regelungen verdeckten den Blick auf viele gute. So ist es z. B. gut, dass künftig auch Unternehmen der Siedlungsabfallentsorgung zum Kreis der Betreiber Kritischer Infrastrukturen (KRITIS) gehören, die ihre versorgungsrelevante IT absichern müssen. Mit den ebenfalls neuen IT-Sicherheitspflichten für Unternehmen im besonderen staatlichen Interesse wird eine Lücke geschlossen, die das IT-Sicherheitsgesetz 1.0 durch die enge KRITIS-Definition offenließ. Sie sollte Versorgungsausfälle verhindern, aber nicht die Gefährdungen, die von Einrichtungen selbst ausgehen, sollte deren IT angegriffen werden. Mit der Einbeziehung von Unternehmen i. S. d. Störfall-Verordnung wird die Lücke geschlossen. Auch die Erhöhung der Bußgelder war durchaus zu begrüßen.

Der Innenausschuss ist dafür zu loben, dass er die Kritik der Sachverständigen aufgriff und sich ernsthaft um die Überarbeitung des Entwurfes bemühte. So wurde die Stellung des BSI als IT-Sicherheits-Aufsicht gegenüber der Bundesverwaltung gestärkt. Dies war überfällig, da es kaum vermittelbar ist, wenn die gesetzliche Kontrolldichte gegenüber Unternehmen kontinuierlich erhöht wird, während sie in der Bundesverwaltung niedrig bleibt. Auf vereinzelte Kritik wurde auch die Unabhängigkeit des BSI durch punktuelle Änderungen gestärkt. Das Gesetz stellt nun klar, dass das BSI sich an wissenschaftlichen Erkenntnissen orientiert und nicht an Interessen anderer Sicherheitsbehörden. Auch die in der Breite kritisierten Regelungen zu den kritischen Komponenten („lex Huawei“) wurden noch einmal komplett überarbeitet. Ob sich damit die geäußerte Kritik wirklich erledigt hat, werden Wissenschaft und Jurisprudenz noch klären.

Doch kein Licht ohne Schatten. Den werfen Änderungen des Ausschusses, die das Gesetz ohne rechtlichen Mehrwert verkomplizieren. Die in § 2 Abs. 2 BSIG enthaltene gesetzliche Definition des Begriffs „Sicherheit in der Informationstechnik“ wurde um einen bloßen Programmsatz ergänzt, der die Wichtigkeit von sicherer Informationstechnik betont. Zur – ohnehin unnötigen – rechtlichen Begriffsschärfung trägt er nicht bei. Eine ähnlich unnötige Ergänzung findet sich in der Aufgabennorm des § 3 Abs. 1 S. 1 BSIG, die dem BSI bisher die Förderung der Sicherheit in der Informationstechnik auferlegte. Dort wurde ein Verweis auf die IT-Sicherheitsgrundwerte Integrität, Verfügbarkeit und Vertraulichkeit ergänzt, die – Überraschung – bereits Inhalt der Legaldefinition von „Sicherheit in der Informationstechnik“ sind. Die Gesetzessystematik wurde geopfert, um rein politisch motivierte Programmsätze zu ergänzen.

Es tröstet wenig, dass rechtlich unnötige Gesetzesänderungen in den letzten Jahren häufiger aufzutreten scheinen. Einmal mehr fühlt man sich an das Plädoyer von Daniel Zimmer für „Weniger Politik“ in der Gesetzgebung erinnert. Das IT-Sicherheitsrecht ist bereits unsystematisch und kaum überschaubar. Eine verantwortungsvolle Legislative sollte die Gesetze klarer statt unübersichtlicher machen. Die Gelegenheit dazu wird der Gesetzgeber noch zur Genüge erhalten. Die im Gesetz vorgesehene Evaluierung und eine kontinuierliche Berichterstattung des BMI gegenüber dem Bundestag werden sicher Anpassungsbedarf aufzeigen. Zudem wird auf EU-Ebene bereits die NIS-RL 2.0 erarbeitet, die vermutlich fundamentalen Änderungsbedarf im deutschen Recht mit sich bringen wird. Bis dahin wird aber auch das IT-SiG 2.0 bereits für mehr IT-Sicherheit sorgen.