Dennis-Kenji Kipker

IT-Sicherheitsrecht 2.0

Spätestens mit dem IT-Sicherheitsgesetz von 2015 hat die IT-Sicherheit auch ihren festen Platz im deutschen Recht. Seit Inkrafttreten des Gesetzes im Juli 2015 ist jedoch bereits wieder einige Zeit ins Land gegangen – und da auch die technische Entwicklung seitdem nicht Halt gemacht hat, wurden sowohl auf deutscher wie auch auf europäischer Ebene einige weitere Gesetze auf den Weg gebracht, darunter auch das „IT-Sicherheitsgesetz 2.0" (IT-SiG 2.0 – „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme"). Nachdem es um das Gesetz und dessen Regelungsumfang im Vorfeld viele Spekulationen gab, wurde Anfang April dieses Jahres schließlich der auf den 27. März 2019 datierte Referentenentwurf aus dem BMI veröffentlicht. Der Entwurf zeigt auf, welchen neuen Herausforderungen sich ein künftiges IT-Sicherheitsrecht 2.0 stellen muss und welche neuen Lösungsansätze hierfür in Betracht kommen.

Hauptintention des IT-SiG 2.0 ist es, die IT-Sicherheit für Gesellschaft, Wirtschaft und Staat in der Form eines ganzheitlichen Konzepts weiterzuentwickeln. Das macht auch Sinn, da die Informationstechnologie mehr und mehr alle denkbaren Lebensbereiche durchdringt und bei einer Betrachtung damit einhergehender Gefahrenlagen nicht mehr nur im Wesentlichen auf Kritische Infrastrukturen abgestellt werden kann, wie es das IT-SiG aus 2015 noch tat. Und dass der deutsche Gesetzgeber vorgreift und maßgeblich auch die europäische Rechtsetzung zur IT-Sicherheit beeinflusst, wird beispielsweise am neuen „IT-Sicherheitskennzeichen" deutlich, das durch das Gesetz eingeführt werden soll. Dieses Kennzeichen soll es Verbrauchern ermöglichen, die IT-Sicherheit von Handelswaren selbst besser beurteilen zu können, indem ihnen online auslesbar verschiedene, für diesen Zusammenhang relevante Informationen zur Verfügung gestellt werden. Eine entsprechende Maßgabe findet sich für Produkte mit einer EU-Konformitätserklärung auch in Art. 55 des ebenfalls kurz vor der Verabschiedung stehenden EU Cybersecurity Act – und zwar infolge der deutschen Intervention innerhalb der europäischen Gesetzgebung.

Eine weitere, zentrale Neuerung des IT-SiG 2.0 wird voraussichtlich den Kreis derjenigen Unternehmen und Einrichtungen betreffen, die verpflichtet sind, technisch-organisatorische Mindestsicherheitsstandards in der IT-Sicherheit vorzuhalten und entsprechende Meldepflichten zu implementieren – hier findet eine Erweiterung sowohl für Zulieferer als auch für Branchen von „besonderem öffentlichen Interesse" statt. So gilt für Zulieferer, wozu die Hersteller der Hard- und Software von Kernkomponenten Kritischer Infrastrukturen gehören (sog. KRITIS-Kernkomponenten), die Verpflichtung zur Abgabe einer Vertrauenswürdigkeitserklärung gegenüber dem Betreiber der Kritischen Infrastruktur noch vor dem erstmaligen Einsatz. Diese Verpflichtung erstreckt sich auf die gesamte Lieferkette des Herstellers. Die an eine solche Vertrauenswürdigkeitserklärung zu stellenden Anforderungen bestimmt das BMI durch Allgemeinverfügung. Im klassischen KRITIS-Bereich ergänzt der Gesetzentwurf den bisherigen Rahmen um den Entsorgungssektor mit der Begründung, dass ein Ausfall u.a. den Anstieg der Seuchengefahr zur Folge hätte. Dass das IT-SiG im Gegensatz zu seiner Vorläuferregelung gerade die ganzheitliche Verbesserung der IT-Sicherheit bezweckt, wird besonders durch die vorgeschlagene Neuerung in § 2 Abs. 14 BSIG-E deutlich: Hier wird eine neue Kategorie der „Infrastrukturen in besonderem öffentlichen Interesse" vorgeschlagen. Hierunter fallen grds. Anlagen oder Teile davon, die dem Bereich Rüstung, Kultur und Medien angehören, und solche Einrichtungen, deren Ausfall die Beeinträchtigung bestimmter börsennotierter Unternehmen zur Folge hätte. In der Gesetzesbegründung werden in diesem Zusammenhang auch Infrastrukturen aus den Bereichen Chemie und Automobilherstellung genannt.

Nicht zuletzt enthält das IT-SiG 2.0 auch eine datenschutzrelevante Komponente; denn mit dem umfassenden Ausbau behördlicher Befugnisse zu Zwecken der IT-Sicherheit geht auch die verstärkte Möglichkeit zur Verarbeitung personenbezogener Daten einher. So wird dem BSI zu Zwecken des Schutzes der Regierungsnetze ermöglicht, künftig länger als bisher Daten zu speichern und ohne Pseudonymisierung zu verarbeiten. Darüber hinaus sieht der Entwurf zu § 5 BSIG (laut Entwurfsbegründung) den unverschlüsselten Zugriff des BSI auf Schnittstellen- und Protokolldaten verschlüsselter Kommunikation vor. Weitere datenschutzrechtliche Relevanz besitzen die in den §§ 109 ff. TKG für Provider vorgeschlagenen Änderungen sowie die Bestandsdatenauskunft gem. § 5d BSIG-E.

Im Einzelnen werden durch das IT-SiG 2.0 die folgenden Vorschriften geändert: das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG), das Strafgesetzbuch, die Strafprozessordnung, das Gesetz über die internationale Rechtshilfe in Strafsachen, das Justizvergütungs- und -entschädigungsgesetz, das Artikel 10-Gesetz, das Bundeskriminalamtsgesetz und die Außenwirtschaftsverordnung.