Der allgemeine Rechtsrahmen für Cyber-Security in Deutschland und Europa

12. November 2020

Cyber-Security gewinnt in Deutschland und in Europa zunehmend an Bedeutung. Das Bedürfnis, den digitalen Markt und die IT Systeme der dort handelnden Unternehmen vor Angriffen zu schützen, wächst stetig. In den vergangenen zwei Jahren haben 68% der Unternehmen Cyber-Angriffe registriert. Laut Aussage des BSI-Präsidenten kommen täglich 390.000 neue Varianten zu den bekannten 800 Millionen Schadprogrammen hinzu. Der europäische und der deutsche Gesetzgeber haben unter dem Regelungsziel „Cyber-Sicherheit" daher eine Reihe von Rechtsnormen erlassen und den Mitgliedstaaten bzw. Unternehmen weitgehende Pflichten auferlegt. Dieses Briefing soll einen Überblick geben über die prominentesten Gesetzesakte im Bereich Cyber-Security und die darin verankerten Pflichten der Adressaten.

Die bestehenden Rechtsvorschriften zur Cyber-Security lassen sich grob in zwei Gruppen unterteilen: Einige Regelwerke haben Cyber-Security zum unmittelbaren Regelungsgegenstand. Hervorzuheben ist hierbei die im Sommer 2019 in Kraft getretene EU-Cyber-Security-Verordnung (*Cyber-Security-Verordnung*). Es existieren jedoch auch Gesetze mit Regelungen zur Cyber-Security, deren Fokus eigentlich auf anderen Regelungen liegt. Hierunter fällt beispielsweise die Verordnung (EU) 2016/679 (*DSGVO*).

Gesetzesakte zur Cyber-Security

Mit der Richtlinie 2009/140/EG (*Rahmen-Richtlinie*) und der Richtlinie 2002/58/EG (*ePrivacy-Richtlinie*), die in Deutschland durch das Telekommunikationsgesetz (*TKG*) umgesetzt wurden, werden Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher elektronischer Telekommunikationsdienste adressiert. In Umsetzung der Richtlinie (EU) 2016/1148 (*NIS-Richtlinie*) wurden hierzulande u.a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (*BSIG*) und das **Energiewirtschaftsgesetz** (*EnWG*) geändert. Die Vorschriften zur IT-Sicherheit in diesen Regelungswerken richten sich an das BSI selbst, an Betreiber Kritischer Infrastrukturen (Organisationen und Einrichtungen mit hoher Bedeutung für das staatliche Gemeinwesen, deren Ausfall oder Beeinträchtigung erhebliche Folgen hätte) und an Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste). Kleinstunternehmen sind vom Anwendungsbereich des BSIG ausgenommen und die Pflichten der Anbieter digitaler Dienste richten sich auch nicht an kleine Unternehmen.

Die Gesetze zur Cyber-Security legen insbesondere Mindestsicherheitsanforderungen und Meldepflichten fest:

Mindestsicherheitsanforderungen

Die genannten Regelungen schreiben den jeweils adressierten Unternehmen technische und organisatorische Maßnahmen zur Bewältigung der Risiken für die Sicherheit ihrer Netze und IT-Systeme vor. Auswirkungen von Sicherheitsverletzungen sollen vermieden bzw. so gering wie möglich gehalten werden. Die Sicherheitsanforderungen werden in der Regel durch Verweise auf Verordnungen oder „soft law" weiter konkretisiert. Sie legen besondere Vorgaben für einzelne Branchen fest.

So müssen Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher elektronischer Telekommunikationsdienste einen Sicherheitsbeauftragten benennen und auf Grundlage des Sicherheitskatalogs der Bundesnetzagentur ein Sicherheitskonzept erstellen. Erstere müssen dieses Sicherheitskonzept unverzüglich nach Aufnahme des Netzbetriebs bei der Bundesnetzagentur einreichen. Für Anbieter digitaler Dienste werden die Sicherheitsstandards durch die Durchführungsverordnung (EU) 2018/151 der EU-Kommission konkretisiert. Betreiber von Energieversorgungsnetzen müssen sich an einen von der Bundesnetzagentur erstellten Katalog von Sicherheitsanforderungen halten. Für Betreiber von Energieanlagen, die als Kritische Infrastruktur zu qualifizieren sind, gibt es einen entsprechenden Katalog. Alle sonstigen Betreiber Kritischer Infrastrukturen können dem BSI branchenspezifische Sicherheitsstandards vorschlagen und sich diese bestätigen lassen. Sie müssen die Erfüllung der Sicherheitsanforderungen mindestens alle zwei Jahre nachweisen.

Meldepflichten

Von großer praktischer Bedeutung sind ferner die Meldepflichten, die in den genannten Gesetzesakten vorgeschrieben werden. Betreiber öffentlicher Kommunikationsnetze und Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste müssen erhebliche Beeinträchtigungen ihrer Netze und Dienste unverzüglich der Bundesnetzagentur und dem BSI mitteilen (§ 109 Abs. 5 TKG). Betreiber Kritischer Infrastrukturen haben in solchen Fällen gemäß § 8b Abs. 4 BSIG bei Störungen, die zu Ausfällen geführt haben, sowie erheblichen Störungen, die zu Ausfällen führen können, über ihre Kontaktstelle das BSI unverzüglich zu unterrichten. Anbieter digitaler Dienste müssen Vorfälle, die gemäß § 8c Abs. 3 BSIG erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes haben, unverzüglich dem BSI melden. Vorfälle mit erheblichen Auswirkungen sind durch die Parameter der Vorschrift wie beispielsweise die Anzahl der betroffenen

Nutzer, die Dauer, das betroffenen geographische Gebiet sowie das Ausmaß der Unterbrechung näher definiert.

Das BSI wiederum hat die zuständigen Landesaufsichtsbehörden und die Betreiber Kritischer Infrastrukturen unverzüglich über bekannte Sicherheitslücken sowie erfolgte und versuchte Cyber-Angriffe zu unterrichten.

Bußgelder

Legen Betreiber öffentlicher Telekommunikationsnetze das zu erstellende Sicherheitskonzept nicht unverzüglich nach Aufnahme des Netzbetriebs der Bundesnetzagentur vor, droht ihnen nach dem TKG ein Bußgeld bis zu 100.000 Euro. Der Verstoß gegen die Meldepflicht wird nach dem TKG mit bis zu 50.000 Euro geahndet. Für Non-Compliance und bei Missachtung der Meldepflichten sehen das EnWG Bußgelder bis zu 100.000 Euro und das BSIG Bußgelder bis zu 50.000 Euro vor.

Regelungen zur Cyber-Security in anderen Gesetzen

Auch Regelungen anderer Gesetze enthalten Vorschriften zur Cyber-Security. Die DSGVO sowie das **Bundesdatenschutzgesetz** sehen konkrete Maßnahmen vor, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten, so etwa deren Pseudonymisierung und Verschlüsselung. Die Verantwortlichen müssen eine Datenschutzverletzung unverzüglich und möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde melden. Bei einem hohen Risiko für die Rechte des Betroffenen ist auch dieser zu benachrichtigen. Die Datenschutz-Grundverordnung sieht für Non-Compliance und bei Missachtung der Meldepflicht Bußgelder bis zu 10 Mio. Euro vor.

Das **Kreditwesengesetz** verlangt von Kreditinstituten und der BaFin ebenfalls Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit. Nach dem **Netzwerkdurchsetzungsgesetz** müssen Anbieter sozialer Netzwerke, die im Kalenderjahr mehr als 100 Beschwerden über rechtswidrige Inhalte erhalten, einen Bericht über den Umgang mit diesen Beschwerden erstellen und im Bundesanzeiger sowie auf der eigenen Homepage veröffentlichen. Bei Missachtung dieser Pflicht drohen den Betroffenen Bußgelder bis zu 5 Mio. Euro.

Cyber-Security-Verordnung

Am 27. Juni 2019 trat die Cyber-Security-Verordnung in Kraft. Mit diesem Rechtsakt wird der personell und finanziell gestärkten Agentur der Europäischen Union für Netz- und Informationssicherheit (*ENISA*) ein dauerhaftes Mandat geschaffen. Zusätzlich führt die Verordnung einen europäischen Rahmen für die Cyber-Sicherheitszertifizierung von informationstechnischen Produkten, Prozessen und Dienstleistungen ein. Sicherheitsmerkmale in IT-Produkten und -Diensten werden durch eine unabhängige Stelle verifiziert, wodurch Nutzer feststellen können, wie vertrauenswürdig die von

ihnen gekauften IT-Produkte und -Dienste sind. Ferner sieht die Verordnung vor, dass Sicherheitsmerkmale bei IT-Produkten und -Diensten bereits in der Frühphase ihrer technischen Konzeption und Entwicklung eingebaut werden, um spätere Sicherheitslücken zu verhindern („security by design").

Regulatorischer Ausblick

Das breite Spektrum an geltendem Recht schließt viele Sicherheitslücken im Cyber-Raum. Doch die hohe Anzahl an Cyber-Angriffen verdeutlicht, dass die Sicherheitsstandards fortlaufend an die sich verändernden Risiken angepasst werden müssen. Ein weiteres Problem ist die dargestellte Zersplitterung der Regeln zur Cyber-Security auf viele verschiedene Gesetze. Es stellt Unternehmen vor hohe Herausforderungen, den für sie geltenden Rechtsrahmen herauszufinden.

Der Koalitionsvertrag zwischen CDU und SPD sieht ein IT-Sicherheitsgesetz 2.0 vor. Am 7. Mai 2020 hat das Bundesinnenministerium (*BMI*) dieses Gesetzesvorhaben im Wege eines zweiten Referentenentwurfs konkretisiert. Eine entscheidende vorgesehene Neuerung betrifft die Ausweitung der bisher für kritische Infrastrukturen geltenden besonderen Pflichten auf „Unternehmen im besonderen öffentlichen Interesse" (§ 2 Abs. 14 BSIG-E). Hierunter fallen neben Rüstungs-, Raumfahrt-, Chemie- und IT-Sicherheitsunternehmen auch Unternehmen von „besonderer volkswirtschaftlicher Bedeutung". Eine genauere Konkretisierung dieser Kategorien soll im Wege einer Rechtsverordnung erfolgen.

Zudem soll das BMI zukünftig berechtigt sein, den Einsatz kritischer Komponenten nicht vertrauenswürdiger Hersteller durch Betreiber kritischer Infrastrukturen zu untersagen (§ 9b BSIG-E). Durch diese Vertrauenswürdigkeitsprüfung soll insbesondere eine missbräuchliche Zugriffsmöglichkeit auf Hard- und Software zu Sabotage- und Spionagezwecken im Rahmen des Aufbaus der 5G-Netze verhindert werden. Auch die Mitwirkungspflichten von Telekommunikations- und Telemedienanbietern bei der Cyberabwehr sollen verschärft werden. So räumt der Referentenentwurf dem BSI die Befugnis ein, künftig Cyberabwehrmaßnahmen gegenüber Telekommunikations-anbietern anzuordnen (§ 109a Abs. 8 TKG-E). Für Non-Compliance und für die Verletzung von Meldepflichten sieht der aktuelle Referentenentwurf eine drastische Erhöhung der Bußgelder vor, die wie zu erwarten an die Regelungen der DSGVO angeglichen werden sollen. Die Entwicklung des regulatorischen Rahmens zur Verbesserung der Cyber-Security im öffentlichen und privaten Bereich ist also noch lange nicht abgeschlossen.

Wenn Sie Fragen zu den jetzigen beziehungsweise zukünftigen Auswirkungen der Cyber-Security auf Ihr Unternehmen oder Ihre Branche haben, stehen Ihnen Dr. Roland M. Stein und Dr. Christopher Wolters jederzeit gern zur Verfügung.