BLOMSTEIN

# Der allgemeine Rechtsrahmen für Cyber-Security in Deutschland und Europa

6. Juni 2019

Cyber-Security in Deutschland und in Europa wird immer wichtiger. 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 vor Kurzem beschlossene 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 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 Störungen, die zu Ausfällen geführt haben, sowie erhebliche 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**

Nach der politischen Einigung zwischen Vertretern des Europäischen Parlaments, des Rates und der EU-Kommission wurde die Cyber Security Verordnung am 12. März 2019 im Europäischen Parlament verabschiedet. Die Verordnung muss vom Rat noch förmlich angenommen werden und tritt 20 Tage nach ihrer Veröffentlichung in Kraft.

Mit diesem Rechtsakt soll die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) personell und finanziell gestärkt sowie ein dauerhaftes

Mandat für sie geschaffen werden. Zusätzlich sieht die geplante Verordnung die Einführung eines europäischen Rahmens für die Cyber-Sicherheitszertifizierung von informationstechnischen Produkten, Prozessen und Dienstleistungen vor. Sicherheitsmerkmale in IT-Produkten und -Diensten sollen durch eine unabhängige Stelle verifiziert werden, 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. Dieses soll neben den bislang verpflichteten Branchen auch Hersteller und Anbieter von IT-Produkten in die Pflicht nehmen. Weniger konkret geblieben sind bisher andere Ansatzpunkte: So wird auf politischer Ebene diskutiert, den Begriff der Kritischen Infrastruktur zu erweitern und damit auch Branchen zu adressieren, deren Versorgungsdienstleistungen nicht die höchste, aber eine hohe Stufe an Wichtigkeit für die Gesellschaft haben. Derzeit fallen nämlich nur etwa 2.000 der rund 3,5 Mio. Unternehmen in Deutschland unter diese Kategorie. Das geltende IT-Sicherheitsgesetz umfasst nur wenige Branchen und die Verordnung zur Bestimmung Kritischer Infrastrukturen sieht einen Regelschwellenwert von 500.000 versorgten Personen vor. Auch der Verbraucherschutz im Cyber-Raum könnte gestärkt werden. So könnte neben einem Zertifizierungssystem, das die Cyber Security Verordnung bereits vorsieht, eine Produkthaftung für digitale Produkte mit einer Beweislastumkehr-Regelung eingeführt werden. Zudem ist nicht auszuschließen, dass die vorgesehenen Bußgelder für Non-Compliance und für die Verletzung von Meldepflichten – beispielsweise auf das Niveau der DSGVO – erhöhen werden.

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.