Cybersicherheitsrecht (Textsammlung)

NIS-2-Richtlinie
CER-Richtlinie
Digital Operational Resilience Act
eIDAS-Verordnung
BSI Gesetz
und viele weitere Texte

Stephan Schmidt (Hrsg.)

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

ISBN 978-3-8005-1893-7

dfv Mediengruppe

www.ruw.de

Druck: WIRmachenDRUCK GmbH, Backnang

Printed in Germany

Inhaltsverzeichnis

I. Einleitung des Herausgebers

A. Einführung

Nur wenige Rechtsgebiete haben in den letzten Jahren eine so dynamische Entwicklung erlebt wie das Cybersicherheitsrecht. Die Geschichte der Gesetze und Regelungen zur Cybersicherheit ist eng mit dem Aufstieg der digitalen Ära verbunden. In den Anfangsjahren des Internets und der digitalen Kommunikation war die Bedrohungslage noch vergleichsweise gering. Es dauerte jedoch nicht lange, bis Cyberkriminelle und andere Akteure die Schwachstellen in digitalen Systemen ausnutzten. Dies führte zur Entstehung der ersten Cybersicherheitsgesetze – das erste deutsche IT-Sicherheitsgesetz (IT-SiG) stammt aus dem Jahr 2015. In den letzten Jahren hat sich das Cybersicherheitsrecht rasant weiterentwickelt. Getrieben von einer stetig steigenden Zahl von Cyberangriffen und den daraus resultierenden Schäden in Wirtschaft und öffentlicher Verwaltung, haben der nationale Gesetzgeber und auch die Europäische Union mittlerweile eine Vielzahl an Normen und Regelungen geschaffen. Cybersicherheit, etwas internationaler auch Cybersecurity genannt, bildet dabei den Oberbegriff für eine Vielzahl von Themen und damit auch gesetzlichen Regelungen. Cybersicherheit umfasst die IT-Sicherheit, die Informationssicherheit und auch die Datensicherheit, wobei man unter Cybersicherheit aus technischer Sicht die Technologien, Dienste, Strategien, Praktiken und Richtlinien versteht, die geeignet sind, Computersysteme, Netzwerke, Softwareanwendungen und digitale Daten und damit auch Menschen vor Cyberangriffen zu schützen. Die Gewährleistung dieses Schutzes stellt die moderne Informationsgesellschaft vor immer neue Herausforderungen.

Unter IT-Sicherheit versteht man die Sicherheit eines IT-Systems, unabhängig davon, ob es sich um ein vernetztes System handelt oder nicht. Der Begriff beinhaltet nicht nur eine infrastrukturell-technische Perspektive, sondern insbesondere auch eine organisatorisch-personelle Komponente. IT-Sicherheit findet sich als Begriff z. B. im BSI Gesetz, in § 5 Onlinezugangsgesetz (OZG) oder im IT-Justizgesetz. Unter Informationssicherheit versteht man die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen und nicht-personenbezogenen Daten und Informationen (Schutzziele der IT-Sicherheit).

Vertraulichkeit ist die Anforderung, dass nur berechtigte Personen auf ein System und die darin gespeicherten Informationen zugreifen können. Integrität bezeichnet die Korrektheit der Daten und die Sicherstellung der Funktionsfähigkeit. Verfügbarkeit bezeichnet die jederzeitige Zugriffsmöglichkeit auf Systeme und deren Daten. Ergänzend wird häufig das Schutzziel der Verbindlichkeit betrachtet, dass die Authentizität, also die Sicherstellung der Identität von Personen, IT-Komponenten oder Anwendungen, sowie die Nichtabstreitbarkeit umfasst.

Unter Datensicherheit werden allgemein die technischen und organisatorischen Maßnahmen, also Sicherheitsmaßnahmen, verstanden, die zum Schutz von personenbezogenen Daten zum Beispiel nach Art. 32 DSGVO erforderlich sind und getroffen werden. Zudem finden sich bereichsspezifische Vorschriften zur Datensicherheit z. B. für den Bereich der Telekommunikation in §§ 165, 167, 169 TKG.

Die Pflicht zur Ergreifung von Cybersicherheitsmaßnahmen, ergibt sich heute sowohl aus nationalem als auch aus europäischem Recht, aus dem sich Rahmenvorschriften und spezialgesetzliche bereichsspezifische Regelungen ergeben können. Die bereichsspezifischen Cybersicherheits-Regelungen sind heute, je nach Sektor und Branche in dem ein Unternehmen tätig ist, sehr vielfältig.

Grundsätzlich gilt, dass sich aus allen Regelungen, die Maßnahmen der Qualitätssicherung, Organisations- oder Verarbeitungsvorgängen von Daten oder zur Nutzung informationstechnischer Systeme enthalten auch Verpflichtungen zur Cybersicherheit ergeben können.

Beginnend mit dem deutschen IT-SiG (2015) haben nationaler und europäischer Gesetzgeber eine Vielzahl an Cybersicherheitsgesetzen geschaffen, zu denen insbesondere die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV – 2016/17), die EU-Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (NIS-RL, 2016) auf europäischer Ebene inklusive des dazugehörigen nationalen Umsetzungsgesetzes (2017), der EU Cybersecurity Act (CSA – 2019), der Vorschlag einer Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen („Cyber Resilience Act") sowie die NIS-2-Richtlinie und die Richtlinie über die Resilienz kritischer Einrichtungen („CER-Richtlinie") (Dezember 2022) gehören. CER-Richtlinie und NIS-2-Richtlinie wurden beide Ende 2022 verabschiedet und müssen bis zum 17. 10.2024 in den Mitgliedstaaten umgesetzt sein. Die CER-Richtlinie wird voraussichtlich durch das Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz), die NIS-2-Richtlinie durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht umgesetzt. Beide Gesetze liegen noch nicht in finalen Fassungen vor, und sind daher in dieser Auflage der Textsammlung noch nicht enthalten.

Die Textsammlung Cybersicherheit bietet einen vertieften Einblick in die Gesetzeslage zu einem Thema, das für Unternehmen und die Gesellschaft als Ganzes zunehmend von entscheidender Bedeutung ist. Die Zukunft der Cybersicherheit-Gesetzgebung wird eng mit der Entwicklung der Technologie und der Bedrohungslage verknüpft sein, und Unternehmen müssen sich auf eine ständige Anpassung einstellen. Die vorliegende Textsammlung soll den Anwendern helfen, ein umfassendes Verständnis für die Bedeutung der Gesetze zur Cybersicherheit zu entwickeln.

B. Inhalt

Ziel der **NIS-2-Richtline** ist, ausweislich ErwG 5, die großen Unterschiede zwischen den Mitgliedstaaten hinsichtlich der auferlegten Anforderungen an die Cybersicherheit von solchen Einrichtungen, die Dienste erbringen oder wirtschaftlich signifikante Tätigkeiten ausüben, zu beseitigen. Dies soll insbesondere durch Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen und Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten erreicht werden. Die Liste der Sektoren und Tätigkeiten, für welche Pflichten im Hinblick auf die Cybersicherheit gelten, wird im Vergleich zur NIS-RL aktualisiert und es werden Abhilfe- und Durchsetzungsmaßnahmen eingeführt. Neben den inzwischen üblichen Bußgeldern bei Verstößen, ist insbesondere auch eine direkte Haftung der Geschäftsleitung vorgesehen.

Die **CER-Richtlinie** (Critical Entities Resilience) zielt darauf ab, die Widerstandsfähigkeit kritischer Einrichtungen zu stärken. Sie verpflichtet die Mitgliedstaaten, solche Einrichtungen zu identifizieren und Maßnahmen zu ergreifen, um ihre physische Widerstandsfähigkeit gegenüber verschiedenen Bedrohungen wie Naturgefahren, Terroranschlägen oder Sabotage zu verbessern. Die Richtlinie legt den Rahmen für den Schutz kritischer Infrastrukturen auf EU-Ebene fest. Es liegt jedoch in der Verantwortung der einzelnen Mitgliedstaaten, spezifische nationale Maßnahmen zur Umsetzung dieser Richtlinie zu erarbeiten und durchzuführen.

Der **Digital Operational Resilience Act (DORA)** ist eine Verordnung, die am 17. Januar 2023 in Kraft getreten ist und darauf abzielt, die IT-Sicherheit von Finanzinstituten wie

Banken, Versicherungsunternehmen und Investmentfirmen zu stärken und sicherzustellen, dass der Finanzsektor in Europa im Falle einer schweren betrieblichen Störung widerstandsfähig bleibt. DORA schafft einen verbindlichen, umfassenden Rahmen für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT) und soll die die digitale operationale Resilienz des gesamten europäischen Finanzsektors stärken.

Der **Rechtsakt zur Cybersicherheit** hat als Verordnung zwei Hauptziele. Zum einen die Stärkung des Mandats der zum 27. Juni 2019 errichteten Agentur der Europäischen Union für Cybersicherheit (ENISA) und zum anderen die Einführung eines EU-Rahmens für die freiwillige IT-Sicherheitszertifizierung. Aufgabe der ENISA ist es, die Cybersicherheitskapazitäten in der EU zu erhöhen und die Abwehrbereitschaft zu fördern. Sie fungiert auch als unabhängiges Kompetenzzentrum, das EU-Organe und Mitgliedstaaten bei der Entwicklung und Umsetzung von politischen Rahmenbedingungen im Bereich der Cybersicherheit unterstützt. Sie erhält durch die Verordnung ein dauerhaftes Mandat und wird mit den erforderlichen Ressourcen ausgestattet. Der Rechtsakt zur Cybersicherheit etabliert zudem einen EU-weiten Rahmen für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen zur Verwirklichung verschiedener Sicherheitsziele, wie z. B. den Schutz gespeicherter, übermittelter und verarbeiteter Daten. Die Schemata für die freiwillige Cybersicherheitszertifizierung können dabei Produkte, Dienste und Prozesse die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ angeben und müssen bestimmte Elemente wie z. B. eine eindeutige Beschreibung des Zwecks des Schemas, den Gegenstand und Umfang des Schemas sowie die Bewertungskriterien und -methoden enthalten.

Die **eIDAS-Verordnung** enthält verbindliche Regelungen in den Bereichen “Elektronische Identifizierung” und „Elektronische Vertrauensdienste“. Sie schafft einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste.

Die **Funkanlagenrichtlinie**, auch bekannt als Radio Equipment Directive (RED), ist ein wichtiges Regelungsinstrument für das Inverkehrbringen elektronischer Produkte in der Europäischen Union. Sie hat das Ziel, ein hohes Maß an Schutz in den Bereichen Gesundheit und Sicherheit zu gewährleisten, sowie ein angemessenes Niveau an elektromagnetischer Verträglichkeit und eine effiziente Nutzung von Funkfrequenzen zur Vermeidung von Störungen sicherzustellen. Sie gilt, mit Ausnahme von Amateurfunkanlagen, Schiffsanlagen, Anlagen an Bord von Luftfahrzeugen und zu reinen Forschungs- oder Entwicklungszwecken betriebenen Erprobungsmodulen, für alle Funkanlagen. Sie soll dabei auch den freien Warenverkehr zu ermöglichen. In Deutschland wurde die Richtlinie durch das Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (Funkanlagengesetz) vom 27. Juni 2017 umgesetzt.

Die **Richtlinie über Angriffe auf Informationssysteme** hat das Ziel eine Angleichung des Strafrechts der Mitgliedstaaten im Bereich Angriffe auf Informationssysteme zu erreichen, indem Mindestvorschriften zur Festlegung von Straftaten und einschlägigen Strafen festgelegt werden. Zudem soll die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten sowie der zuständigen Agenturen und Einrichtungen der Union wie Eurojust, Europol und dessen Europäisches Zentrum zur Bekämpfung der Cyberkriminalität und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) erreicht werden.

Auch die weiteren in der Testsammlung auszugsweise enthaltenen Verordnungen und Richtlinien enthalten für die Cybersicherheit relevante Vorschriften.

Der nationale Gesetzgeber hat sich im europäischen Vergleich bereits sehr früh, und nicht erst im Jahr 2015 mit dem ersten deutschen IT-Sicherheitsgesetz, mit den Bedrohungen aus dem Cyberraum befasst. Seit der 2011 beschlossenen nationalen Cyber-Sicherheitsstrategie hat der Gesetzgeber diverse Gesetze angepasst und um Cybersicherheitsvorschriften ergänzt. Dies passierte nicht zuletzt durch das IT-Sicherheitsgesetz, welches als Artikelgesetz verschiedene Einzelgesetzte betrifft. Zu den geänderten Einzelgesetzen gehören unter anderem das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telekommunikationsgesetz (TKG) sowie das Bundeskriminalamtgesetz (BKAG). Auch das das Telemediengesetz (TMG) wurde durch das IT-Sicherheitsgesetz geändert, die Regelungen sind durch die TMG-Novelle jedoch inzwischen nicht mehr im TMG enthalten. Mit der BSI-Kritisverordnung wurden ergänzend zum IT-Sicherheitsgesetz bzw. dem BSI-Gesetz dann Sektoren festgelegt, die als kritische Infrastruktur gelten. Zuletzt wurden die Sektoren Anfang 2023 um LNG-Anlagen und Seekabelanlandestationen ergänzt.

Die übrigen in der Textsammlung auszugsweise enthalten Gesetze enthalte jeweils spezifische Regelungen zur Cybersicherheit.

November 2023 Stephan Schmidt