NomosGesetze

Hoeren | Pinelli [Hrsg.]

Cyber-sicherheitsrecht

Textsammlung

Nomos

NomosGesetze

Prof. Dr. Thomas Hoeren | Stefan Pinelli

Cyber-sicherheitsrecht

Textsammlung

Nomos

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

ISBN 978-3-8487-7199-8

1. Auflage 2021

Inhalt

Europäische Gesetzeswerke

Einführung in das Recht der Cybersicherheit

Die sog. **Cybersicherheit** ist gerade in den letzten Jahren zunehmend in den Fokus des öffentlichen Interesses getreten. Unter „Cyber" wird in der Regel der externe digitale Raum von Computern, Programmen und Daten verstanden, über den ein Angriff erfolgen kann. Diese Sicherheit gegen unautorisierte Eingriffe „von außen" zu gewährleisten, ist eine der zentralen Herausforderungen für die Informationsgesellschaft. Und die Zahl der Cyberangriffe ist spürbar gestiegen[1]. Beispiele für Cybersicherheitsrisiken und damit verbundene Schwachstellen sind:

i. Verlust oder unbefugter Zugriff auf Daten, Nichteinhaltung von Vorschriften (z. B. EU-Datenschutzgrundverordnung (EU-DSGVO) und weiterer Gesetze zum Schutz von Daten wie z. B. das Geschäftsgeheimnisgesetz);
ii. Störung von oder unbefugter Zugriff auf Systeme(n) und Anwendungen;
iii. Ausfall oder fehlender Support von (Alt)Systemen;
iv. Verlust von Service/Support durch Drittanbieter; Überlastung von Systemen (Systemabsturz) durch externe Angriffe/übermäßige Nutzung;
vi. unbeabsichtigte Vireninfektion;
vii. unzureichendes Fachwissen im Hinblick auf die Wartung oder Pflege von (Alt)Systemen und in Bezug auf die Entwicklung von angemessenen Maßnahmen für aktuelle/zukünftige Anforderungen;
viii. fehlendes Fachpersonal zum präventiven und reaktiven Umgang mit diesen Risiken sowie fehlende überfachliche Kompetenz zum Erkennen der Bedeutung der Cybersicherheit.

Generell fungiert der Begriff der Cybersicherheit als Oberbegriff für andere Sicherheitskategorien, die mit Informationstechnologien zu tun haben.[2] Die sog. **IT-Sicherheit** befasst sich mit der Sicherheit eines IT-Systems und **enthält für Kritische Infrastrukturen** gemäß § 8a Abs. 1 Satz 1 BSIG die Verpflichtung, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind. Integrität umfasst dabei die unveränderte Unvollständigkeit eines IT-Systems. Die sog. **Informationssicherheit** hingegen konzentriert sich im Wesentlichen auf die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen[3] gerade vor dem Hintergrund der Gefahr von nicht autorisierten Eingriffen. Mit Informationen sind – wie häufig leider nicht beachtet – nicht nur personen-, sondern auch nicht-personenbezogene Daten bzw. Informationen gemeint. Ob die Informationssicherheit per definitionem weitergehender ist als die IT-Sicherheit[4] oder umgekehrt, bedarf im Hinblick auf die nachstehende Sammlung keiner näheren Wertung. Vertraulichkeit bedeutet, dass nur Berechtigte die Möglichkeit haben, auf editierte Systeme und die darin enthaltenen Informationen zuzugreifen. Verfügbarkeit bezieht sich auf den jederzeitigen Zugriff auf IT-Systeme und deren Informationen.

Eine weitere „Sicherheitskategorie", nämlich die sog. **Datensicherheit**, zeichnet sich durch die enge Verbindung mit dem Datenschutz und damit mit dem Schutz personenbezogener Daten aus. Das Datenschutzrecht schützt nicht Informationen an sich, sondern die von einer Datenverarbeitung betroffene Person selbst vor Beeinträchtigungen ihres Rechts auf informationelle Selbstbestimmung. Cybersicherheit als übergeordnete Materie setzt beim Schutz von Daten und Informationen als solchen an, Datensicherheit beschränkt sich insofern auf Sicherheitsmaßnahmen für personenbezogene Daten. Nach Art. 32 DSGVO treffen den Verantwortlichen und auch den Auftragsverarbeiter die Pflicht, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein hinreichendes Schutzniveau für die Verarbeitung personenbezogener Daten zu gewährleisten. Insofern bedarf es einer Risikoabschätzung je nach Kategorie der personenbezogenen Daten im Rahmen einer Datenschutzfolgenabschätzung. Ergänzend gelten bereichsspezifisch §§ 109, 109a TKG sowie §§ 14a, 15 TMG für den Bereich der Telekommunikation.

---

1) Dazu https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Digitalbarometer_090919.html und https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/Sicherheitslage_TK_24062020.pdf?__blob=publicationFile&v=1.

2) Dazu auch das äußerst empfehlenswerte Buch *Kipker, Dennis-Kenji* (Hg.), Cybersecurity, 2020.

3) DIN ISO/IEC 27001:2008-2009, dort Ziffer 3.4; vgl. hierzu weiterhin DIN ISO/IEC 27002:2008-2009, dort Ziffer 0.1.

4) So jedenfalls *Schläger/Thode*, Handbuch Datenschutz und IT-Sicherheit, 2018, S. 503 Rn. 2.

Abzugrenzen ist die Sicherheit im Sinne von **Security**, wie sie in den o. g. Begriffskategorien gemeint ist, von dem Begriff der „**Safety**“, vgl. hierzu auch beispielsweise § 3 ProdHG. Der Terminus „Safety“ ist vereinfacht dargestellt vor allem bei Fehlfunktionen von Produkten ohne Fremdeinwirkung bedeutsam, während Security sich mit Fragestellungen hinsichtlich gezielter und absichtlicher Fremdeingriffe in IT-Systeme befasst.

Der Begriff „Cybersecurity“ bezieht sich im Wesentlichen auf **IT-Systeme**. Unter IT-System versteht man ein „geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen“[1]. Dadurch, dass vernetzte Produkte, Dienste und Systeme im „Internet der Dinge“ künftig noch stärker im Fokus der nationalen Sicherheit stehen werden, wird deutlich, dass fehlende Cybersicherheit nicht nur für den Einzelnen und ein Unternehmen ein gravierendes Problem darstellen kann, sondern auch für Volkswirtschaften. Durch die immer stärkere Vernetzung bzw. Verknüpfung von IT-Systemen ist Cybersicherheit eine Herausforderung bei weltweit zum Einsatz kommenden Technologien (Bsp. weltweiter Cloud-Verbund) und nahezu weltweit fließenden Informationen. Korrespondierend ist das Recht der Cybersicherheit notwendigerweise grenzüberschreitend und interdisziplinär, gilt es doch – sofern nicht durch supranationales Recht harmonisiert – die unterschiedlichen nationalen Rechtsregime miteinander konform zu beraten und bei der technischen Umsetzung zu beachten.

Geregelt sind Tatbestände der Cybersicherheit in einem Mosaik und Wirrwarr von unterschiedlichen Gesetzen und sonstigen Bestimmungen. Versucht man einmal Ordnung hier hinein zu bringen, muss man unterscheiden zwischen EU-Vorgaben und nationalstaatlichen, insbesondere deutschen Regelungen. Unionsrechtliche Normen der EU finden sich in Verordnungen und Richtlinien. Verordnungen sind Bestimmungen der EU, die unmittelbar gelten und nicht durch nationalstaatliche Umsetzungsvorschriften konkretisiert werden. Richtlinien hingegen sind Bestimmungen der EU, die noch einer nationalen Umsetzung bedürfen.

Typischerweise werden Cybersicherheitsfragen in Gesetzen geregelt, die durch verschiedene einzelne Gesetze hindurch Änderungen vornehmen. Diese Änderungen werden in einem Gesetz zusammengefasst (Omnibusgesetz). Typischerweise nimmt der Bund im Rahmen der konkurrierenden Gesetzgebung nach Art. 72, 74 GG für sich in Anspruch, möglichst viele Regelungsbereiche zu normieren; die Bundesländer haben daher nur einen sehr kleinen Regulierungsspielraum für Cybersicherheit. Neben den formellen Gesetzen bestehen noch Rechtsverordnungen, die durch die Verwaltung geschaffen werden. Zu nennen ist hier die BSI- Kritisverordnung. Typischerweise ist Cybersicherheit unter das Besondere Verwaltungsrecht zu subsumieren; das Rechtsgebiet strahlt aber auch in das Strafrecht und das Zivilrecht aus (so z. B. bei der Haftung für Datensicherheit).

Eine zentrale Rolle bei der Cybersicherheit spielt der Begriff des „**Standes der Technik**“. Darunter wird der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen verstanden, der nach Ansicht führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Darunter liegt das Schutzniveau allgemein anerkannter Regeln der Technik. Darüber liegt der Stand von Wissenschaft und Technik, der sich auf die neuesten wissenschaftlich vertretbaren Erkenntnisse bezieht. Inhaltlich wird der Begriff teilweise in Gesetzen legal definiert (so im Wasserhaushaltsgesetz). Auf dem Begriff wird in einzelnen gesetzlichen Vorgaben der Cybersicherheit Bezug genommen (siehe § 8a Abs. 1 BSIG). Im Übrigen gelten branchenspezifische Sicherheitsstandards zur Konkretisierung des Standes der Technik.

Die Grundstrukturen des Sicherheitsrechts finden sich im IT-Sicherheitsgesetz. Dieses Gesetz wird derzeit durch das neue „**IT-Sicherheitsgesetz 2.0**“ aktualisiert. Hiernach haben Unternehmen eine verstärkte Meldepflicht gegenüber dem Bundesamt für Informationssicherheit (BSI), wenn bestimmte, im Gesetz definierte KRITIS-Anlagen betroffen sind. Unter KRITIS versteht man die Betreiber kritischer Infrastrukturen, mit entscheidender Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere wesentliche Folgen für das Gemeinwohl eintreten würden. Die umfangreiche Liste solcher Betreiber wurde jetzt auch auf den Bereich der Entsorgung ausgeweitet. Außerdem wurde die Kategorie „Infrastruktur von besonderem öffentlichen Interesse“ eingeführt, für die die KRITIS-Regeln ebenfalls angewandt werden sollen. Dies betrifft u.a. Bereiche wie Kultur, Medien und Rüstung. Auch Unternehmen „von erheblicher volkswirtschaftlicher Bedeutung“ sollen im Zuge

1) *Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 3.

des IT-Sicherheitsgesetzes 2.0 dem BSI gegenüber erläutern, welche Maßnahmen sie zur Verbesserung ihrer IT-Sicherheit planen. Das Amt soll daraufhin zusätzliche Maßnahmen für die Unternehmen anordnen können. Außerdem sollen Unternehmen verpflichtet sein, dem BSI Cyberangriffe unverzüglich zu melden.

Branchenspezifische Vorgaben gelten insbesondere für Anbieter von Telemediendiensten (TMG), für Telekommunikationsanbieter (TKG) und für Betreiber kritischer Infrastrukturen/KRITIS (BSI Gesetz & NIS Richtlinie)[1]. Auch gelten besondere Rechtsgrundlagen für Betreiber von Energieversorgungsnetzen (§ 11 EnWG), Betreiber von Telematikdiensten (§ 291b SGB V) und den ganzen Bereich der Finanzwirtschaft (§ 25a KWG, Wertpapierhandelsgesetz, § 5 IV Börsengesetz). Ein separates Rechtsgebiet ist weiterhin der ganze Bereich der Medizinsicherheit. Ein Sonderthema ist ebenfalls das Recht der Nachrichtendienste, wie beispielsweise die Zugriffsbefugnisse des BKA.

In der vorliegenden Gesetzessammlung konnten wir nur eine Auswahl von branchenspezifischen Rechtsgrundlagen zusammenstellen und haben uns wegen der besonderen Bedeutung des „Internet der Dinge" auf die telekommunikationsbezogenen Vorschriften beschränkt.[2] Gerade im Bereich der sog. UNECE-Regelungen wird umfangreiche Regulatorik in Bezug auf die Cybersicherheit – beispielsweise mit Relevanz für Kraftfahrzeuge – geschaffen.[3] Dasselbe gilt für den Bereich des Funkanlagenrechts.[4]

Die Gewährleistung der IT-Sicherheit ist ein **allgemeines Prinzip unternehmerischer Sorgfaltspflichten** und von elementarer Bedeutung im Kontext eines technisch-funktional und rechtlich angemessen zu gestaltenden „Internets der Dinge". So gehört die Risikovorsorge zu den allgemeinen Geschäftsleitungspflichten einer Aktiengesellschaft (§ 76 Abs. 1 AktG). Nach § 91 Abs. 2 AktG hat der Vorstand einer Aktiengesellschaft geeignete Maßnahmen vorzusehen, um für die Gesellschaft potenziell bestandsgefährdende Entwicklungen früh zu erkennen. Die Pflicht zur sorgfältigen Unternehmensführung und die sich daraus ergebenden Compliance-Pflichten gebieten die Einführung präventiver IT-Sicherheitsmaßnahmen, bei der die Rechtsprechung dem Vorstand oder der Geschäftsleitung einen weiten Ermessensspielraum über Art und Umfang gibt. Zu den Sorgfaltspflichten gehört auch die Pflicht zur ordnungsgemäßen Buchführung, unter besonderer Berücksichtigung der Revisionssicherheit (§ 239 Abs. 4 S. 2 HGB, § 146 Abs. 5 S. 2 AO). Ferner gehören hierzu angemessene Geheimhaltungsmaßnahmen nach dem Geschäftsgeheimnisgesetz. Die Pflicht zur angemessenen Cybersicherheit ist auch Bestandteil allgemeiner Haftungsgrundlagen nach dem BGB. Ein Datenverlust ist als Eigentumsverletzung im Sinne von § 823 Abs. 1 BGB anzusehen, sofern die Daten in einem Datenträger verkörpert sind. Schwierigkeiten bestehen jedoch immer noch bei der deliktsrechtlichen Einordnung des Verlustes reiner Daten ohne Datenträger; ob dann ein Datenverlust deliktisch nach § 823 Abs. 1 BGB zu einem Schadensersatzanspruch führt, ist umstritten. In der Rechtsprechung ist eine Verantwortlichkeit für Daten im Rahmen der kauf- und werkvertraglichen Gewährleistung anerkannt. Ferner ist die Cybersicherheit verankert in den Vorschriften zum **Computerstrafrecht**. Dies gilt zunächst spezifisch für die auf den Schutz von Daten zugeschnittene Straftatbestände, wie die der Datenveränderung (§ 303 Abs. 1 StGB). Verboten ist danach die Unterdrückung fremder Daten, das Unbrauchbarmachen, Löschen oder Verändern. Eine Hardwaremanipulation fällt direkt unter den Tatbe-

1) Unternehmen, die in besonderen Risikosphären (sog. kritische Infrastrukturen) tätig sind.

2) Dabei gilt es zu beachten, dass auch die sog. Anbieter digitaler Dienste unter KRITIS ähnliche Pflichten fahren.

3) Die Arbeitsgruppe der UNECE für Fahrzeugregularien (WP.29) hat mit den Regularien UN Regulation No. 155 und UN Regulation No. 156 Normen für Cybersicherheit und Software Updates bei Kraftfahrzeugen erstellt. Die UN Regulation No. 155 trat am 22. Januar 2021 in Kraft. Diese Regelungen betreffen die Cybersicherheit und die Cybersicherheit-Managementsysteme. Text von UN Regulation No. 155: https://unece.org/sites/default/files/2021-03/R155e.pdf und die von der WP.29 veröffentlichte vorgeschlagene Interpretationshilfe für UN Regulation No. 155: https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/WP29-182-05e.pdf. Die UN Regulation No. 156 trat ebenfalls am 22. Januar 2021 in Kraft. Diese Regelungen betreffen Software Updates und Software Updatesysteme bei Kraftfahrzeugen. Text der UN Regulation No. 156: https://unece.org/sites/default/files/2021-03/R156e.pdf und die von der WP.29 veröffentlichte vorgeschlagene Interpretationshilfe für UN Regulation No. 156: https://unece.org/sites/default/files/2021-02/ECE-TRANS-WP29-2021-060e.pdf.

4) Richtlinie 2014/53/EU: Diese Richtlinie dient der Harmonisierung der Rechtsvorschriften über die Bereitstellung von Funkanlagen. Die Richtlinie wurde in Deutschland durch das Funkanlagengesetz umgesetzt. (In Österreich durch das Gesetz für Funkanlagen und Marktüberwachung). Der Volltext der Richtlinie ist einsehbar unter: https://eur-lex.europa.eu/eli/dir/2014/53/oj?locale=de. Der Volltext des Funkanlagengesetzes ist einsehbar unter: https://www.gesetze-im-internet.de/fuag/BJNR194710017.html#BJNR194710017BJNG000200000.

stand der Sachbeschädigung (§ 303 StGB). Aus diesen Tatbeständen kann dann eine Straftat mit erheblich gesteigerter Strafandrohung erwachsen, nämlich die Computersabotage (§ 303b Abs. 1 Nr. 1, 3 StGB), soweit durch eine solche Tat eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich gestört wird. Im Computerstrafrecht von besonderer Bedeutung ist auch der Straftatbestand der Fälschung beweiserheblicher Daten (§ 269 StGB). Weiterhin ist auch das Ausspähen von Daten nach § 202a Abs. 1 StGB) verboten, sofern die Daten gegen unberechtigten Zugang besonders gesichert sind. Dazu muss die Programmierung eines informationstechnischen Systems spezifisch darauf gerichtet sein, den Zugriff auf die Daten nicht oder nur nach verlässlicher Authentifikation zu gestatten. § 202a StGB knüpft auch an den Straftatbestand der Datenhehlerei an (§ 202d StGB). Besondere Vorbereitungshandlungen zur Vorbereitung eines Ausspähens und Abfangens von Daten stellt § 202c StGB unter Strafe, insbesondere das Herstellen oder Sichverschaffen von Sicherungscodes mit dem Ziel einer Datenveränderung oder Computersabotage.

In den **USA** gibt es bedauerlicherweise nicht einen einzigen (Bundes-) Cybersecurity Act.[1] Stattdessen existiert eine nicht einfach zu überblickende Vielzahl hunderter bundesstaatlicher und föderaler Gesetze, Verordnungen und bindender Guidelines. Auf föderaler Ebene sind vor allem sektorspezifische Gesetze zu erwähnen, wie den Health Insurance Portability and Accountability Act (HIPAA) für Gesundheitsdaten und den folgenden Finacial Services Modernization Act für den Schutz persönlicher Finanzinformationen. Ergänzend kommen die Entscheidungen der Federal Trade Commision (FTC) besondere, die mangelhafte Sicherheitsstandards als unfaire Marktmethoden ahnden. Für das Problem des Hacking gilt der Computer Fraud and Abuse Act (CFAA).

In der Volksrepublik **China** gilt seit 2017 das Internetsicherheitsgesetz.[2] Es dient der Erhaltung der Souveränität über den Cyberspace und der Gewährleistung der nationalen Sicherheit.[3] Es gilt für die Datenverarbeitung natürlicher und juristischer Personen, die auf chinesischem Territorium Informationen erheben, verarbeiten oder verbreiten. Sofern ausländische Unternehmen an chinesische Kunden gerichtete Websites betreiben oder über Niederlassungen in China verfügen, gilt das Gesetz auch. Das Gesetz gibt dem Staat das Recht, Maßnahmen zum Umgang mit Netzsicherheitsrisiken zu ergreifen und die Netzwerkkommunikation aufgrund wichtiger öffentlicher Interessen zu beschränken (Art. 5 und 58). Das sieht auch vor, dass die Anbieter von kritischer Netzwerkausrüstung und spezifischen Cybersicherheitsprodukten vor deren Vermarktung in China eine behördliche Überprüfung und Zertifizierung ihrer Produkte durchführen müssen (Art. 35). Daten, die im Rahmen des Betriebs von kritischen Informationsinfrastrukturen anfallen, müssen grundsätzlich im chinesischen Inland gespeichert werden (Art. 37), es sei denn, ein Transfer von Daten ins Ausland ist ausnahmsweise aus zwingenden Gründen erforderlich. Verstöße gegen diese Regeln können Geldbußen und weiterer Strafen bis hin zur Suspendierung der Geschäftsaktivitäten nach sich ziehen.

In **Russland** wurde aufgrund der Cybersecurity-Doktrin von Dezember 2016 mit dem Information Technologies and the Protection of Information Act ein neues Cybersecurity Gesetz 2017 geschaffen; dies gilt auch für weite Teile der Wirtschaft, etwa im Finanzmarkt, Bergbau oder Energie. Diese sind insbesondere involviert in die neue Gesetzgebung bei Vorliegen kritischer Informationsinfrastrukturen, d. h. bei Einrichtungen mit herausgehobener sozialer Bedeutung. Solche Unternehmen trifft die Pflicht, Mittel zur Verhütung, Erkennung und Beseitigung der Folgen von Computerangriffen und zur Reaktion auf Computervorfälle vorzuhalten. Außerdem haben sie Maßnahmen zum Schutz der Betriebsfähigkeit des kritischen Informationsinfrastrukturobjekts zu entwickeln. Darüber berichten sie unmittelbar der russischen Behörde für Informationssicherheit und werden alle drei Jahre überprüft.

1) Dazu seit *Jeff Kosseff*, Cybersecurity Law, Hoboken 2017.
2) Englische Fassung abrufbar unter: https://www.newamerica.org/cybersecurity-initiative/di-gichina/blog/translation-cyber security-law-peoples-republic-china/.
3) *Hoeren/Pinelli*, Datenschutz im neuen chinesischen Zivilgesetzbuch, DuD 2020, 678 ff.