GESETZLICHE VERPFLICHTUNGEN ZUR IT-SICHERHEIT FÜR UNTERNEHMEN IN DEUTSCHLAND

Stefan Hessel / Andreas Rebmann

Rechtsanwalt und Associate, reuschlaw Legal Consultants, Team Datenschutz & Cybersecurity
Stengelstraße 1, 66117 Saarbrücken, DE
stefan.hessel@reuschlaw.de; https://www.reuschlaw.de

Wissenschaftlicher Mitarbeiter, Universität des Saarlandes, Lehrstuhl für Rechtsinformatik
Campus C3.1, Postfach 15 11 50, 66041 Saarbrücken, DE
andreas.rebmann@uni-saarland.de, https://legalinf.de/rebmann

Schlagworte: ***IT-Sicherheit, Regulierung, Unternehmen, Compliance***

Abstract: *Unternehmen sind wegen der voranschreitenden Digitalisierung in zunehmendem Maße von IT-Systemen abhängig. Gleichzeitig können Cyberangriffe für Unternehmen gravierende negative Folgen haben. Trotz dieser Risiken gibt es in Deutschland jedoch kein Gesetz, das Unternehmen allgemein zur IT-Sicherheit verpflichtet. Unternehmen werden jedoch durch eine Vielzahl von einzelnen Gesetzen mit unterschiedlicher Zielrichtung zu IT-Sicherheitsmaßnahmen verpflichtet. Eine Umsetzung der gesetzlichen Vorgaben sollte mit Hilfe eines Managementsystems, das im Beitrag skizziert wird, erfolgen.*

1. Einführung

Die Digitalisierung ist in allen Lebensbereichen – und gerade auch in Unternehmen – seit Jahren auf dem Vormarsch. Diese Entwicklung wird mit zunehmender Vernetzung und Automatisierung fortschreiten. Mit steigendem Grad an Digitalisierung wächst auch die Zahl potenzieller Angriffsziele. Hatte vor einigen Jahren jeder Büromitarbeiter noch einen Desktop-PC an seinem Arbeitsplatz so wächst mit Laptops, Tablets und Smartphones die Zahl der Dienstgeräte pro Mitarbeiter immer weiter. Ebenso sind auch fast alle Arbeitsplätze, die nicht vom Schreibtisch ausgeführt werden – von der Produktionsstraße bis zum Seniorenheim –, von der zunehmenden Digitalisierung betroffen. Je mehr vernetzte Geräte genutzt werden, desto mehr potenzielle Einfallstore für Angriffe müssen geschützt werden.

Mit Aufkommen der Covid-19-Pandemie kam ein weiterer Faktor für die IT-Sicherheit von Unternehmen hinzu: Durch den sprunghaften Anstieg von Mitarbeitern im Home Office wurden nun massenweise Unternehmensdaten in IT-Umgebungen verarbeitet, die sich zumindest in Teilen der Kontrolle des Unternehmens entziehen. Gleichzeitig zeigen sich hier die enormen Vorteile der Digitalisierung. Die Möglichkeit zur Aufrechterhaltung von Unternehmensabläufen – auch in Ausnahmesituationen – sichert vielen Unternehmen die Existenz. Daneben erlauben digitalisierte Prozesse unabhängig von der Pandemie häufig enorme Zeit- und Kostenersparnisse für Unternehmen. Digitalisierung hat enorme Potenziale für die gesamte Gesellschaft.

Diese Potenziale einerseits sowie die Unternehmen an sich andererseits gilt es zu schützen. Obwohl IT-Sicherheit von den meisten Unternehmen als wichtig angesehen wird, fordern viele Unternehmen gleichzeitig eine stärkere Regulierung der IT-Sicherheit durch den Gesetzgeber.[1] Denn aktuelle Haftungs- und Präventionsmöglichkeiten scheinen nicht ausreichend bzw. nicht wirksam.

[1] Vgl. VdTÜV, Unternehmen fordern strengere gesetzliche Vorgaben für IT-Sicherheit. https://www.vdtuev.de/news/cybersecurity-studie (aufgerufen am 12. November 2020), 05.11.2019.

2. Aktuelle Bedrohungslage für Unternehmen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) diagnostiziert für 2020 eine weiterhin angespannte Gefährdungslage der IT-Sicherheit.[2] Eine Gefährdung – gerade für Unternehmen – geht vor allem durch Schadsoftware, Identitätsdiebstahl, z.B. durch Social Engineering, und Advanced Persistent Threats, oftmals zum Zwecke der gezielten Informationsgewinnung,[3] aus. Gerade die Zahl von Angriffen mit Schadsoftware ist zum Ende des Jahres 2019 und Beginn 2020 stark angestiegen. Ransomware, also Software die Unternehmensdaten verschlüsselt und gegen Lösegeld wieder frei gibt, ist hierbei nur eine von einer Vielzahl von verschiedenen Arten von Schadsoftware, welche aber seit einigen Jahren eine der größten Bedrohungen von IT-Systemen darstellt.[4]

Große Bekanntheit erlangten 2019 Angriffe durch Emotet, eine Software, die selbst keine Ransomware darstellt, aber wie ein Taschenmesser eine Vielzahl von Schadsoftwarekomponenten, u.a. Ransomware nachladen kann. Besonders betroffen war hiervon das Berliner Kammergericht seit September 2019. Über mehrere Monate war die Nutzung der gesamten IT gar nicht oder nur sehr eingeschränkt möglich, nachdem sich Emotet im Netzwerk verbreitet hatte. Richter und Angestellte des höchsten Berliner Gerichts konnten ihre PCs nur noch als Schreibmaschine nutzen.[5] Erst im August 2020 kam es zu einem Angriff mit Emotet auf die BwFuhrparkService GmbH, den Fahrdienstleister der Bundeswehr und des Deutschen Bundestags.[6] Bereits jedes achte Unternehmen in Deutschland war 2019 mindestens einmal von einem schweren IT-Sicherheitsvorfall betroffen. Besonders häufig traten hier Phishing, Ransomware-Angriffe und andere Schadsoftware in Erscheinung.[7]

Bei den meisten Cyberangriffen handelt es sich nach wie vor nicht um gezielte Angriffe, sondern um sogenannte Massenangriffe, welche mit finanziellen Motiven durchgeführt werden. Jedoch sollte die Gefahr von gezielten Angriffen auf Unternehmensdaten nicht unterschätzt werden. Häufige Beute solcher Angriffe sind etwa Zahlungsinformationen von Kunden von Banken, Zahlungsdienstleistern oder auch des Einzelhandels, bei welchen dann direkt im Kassensystem Kreditkarteninformationen abgegriffen werden. Die erbeuteten Daten werden dann entweder direkt zum Abbuchen von Geldbeträgen genutzt oder es wird mit der Veröffentlichung und damit einhergehender Geschäftsschädigung gedroht.

In anderen Fällen gezielter Cyberangriffe handelt es sich oft um Wirtschaftsspionage. Technologie, Patente und Know-How sind für viele Firmen das wichtigste Kapital, müssen daher besonders geschützt werden, sind gleichzeitig aber auch besonders begehrt, um sie zu kopieren. In anderen Fällen verschaffen sich Unternehmen einen Vorteil, indem sie bei Ausschreibungen oder Unternehmensübernahmen Angebote der Konkurrenz erbeuten und die eigenen entsprechend anpassen können.[8] Opfer solcher gezielten Angriffe wurden bisher auch namhafte Unternehmen wie Bayer, Thyssen Krupp und BASF.[9] Gleichzeitig sind vor allem kleinere Unternehmen, die hoch-spezialisierte Produkte anbieten, gefährdet, da diese nicht über die gleichen Kapazitäten zur Abwehr solcher Angriffe verfügen, wie dies bei den vorgenannten Unternehmen der Fall ist.

---

2 Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2020, S.9. https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/bsi-lagebericht-cybersicherheit-2020.pdf (aufgerufen am 12. November 2020), 2020.

3 Ebenda, S. 28.

4 Ebenda, S. 11.

5 Vgl. Krempl, Emotet: Berliner Kammergericht bleibt bis 2020 weitgehend offline. https://www.heise.de/newsticker/meldung/Emotet-Berliner-Kammergericht-bleibt-bis-2020-weitgehend-offline-4569544.html (aufgerufen am 12. November 2020), 25.10.2019.

6 Vgl. Spiegel.de, Chauffeurdienst des Bundestags wurde mit Erpressersoftware angegriffen. https://www.spiegel.de/netzwelt/netzpolitik/bundestag-chauffeurdienst-wurde-mit-erpressersoftware-angegriffen-a-f374b025-9a19-4434-bef5-78c520163450 (aufgerufen am 12. November 2020), 20.08.2019.

7 VdTÜV, TÜV Cybersecurity-Studie, S. 25. https://www.vdtuev.de/dok_view?oid=769635 (aufgerufen am 12. November 2020), 20.08.2019.

8 Vgl. Kuhn, Cyberattacken und Spionage verursachen Milliardenschaden. https://www.deutschlandfunk.de/angriffe-auf-unternehmen-cyberattacken-und-spionage.766.de.html (aufgerufen am 12. November 2020), 06.11.2019.

9 Vgl. Heide/Kerkmann, Berlin verdächtigt Chinas Regierung der Industriespionage im großen Stil. https://www.handelsblatt.com/politik/deutschland/cyberattacken-berlin-verdaechtigt-chinas-regierung-der-industriespionage-im-grossen-stil/24911728.html (aufgerufen am 12. November 2020), 19.08.2019.

3. Bestehende gesetzliche Verpflichtungen zur IT-Sicherheit in Deutschland

Unabhängig von der Möglichkeit, IT-Sicherheit individuell vertraglich zu vereinbaren, existiert bisher weder in Deutschland noch in der Europäischen Union ein Gesetz, das allgemeine IT-Sicherheitsanforderungen definiert und diese gegenüber Unternehmen verpflichtend macht. Stattdessen gibt es eine Vielzahl von Einzelregelungen, die verschiedene Aspekte der IT-Sicherheit regulieren. Diese lassen sich trennen in Verpflichtungen, die weitestgehend für alle Unternehmen gelten (Allgemeine Anforderungen) und solche, die nur für bestimmte Unternehmen bzw. Branchen gelten (Spezialgesetzliche Anforderungen).

Abbildung 1: Verpflichtungen zur IT-Sicherheit können in allgemeine (hier dargestellt) und spezialgesetzliche Anforderungen getrennt werden. Wegen der vielen Einzelgesetze ist zu einem Managementsystem zu raten (Quelle: eigene Darstellung).

3.1. Überblick zu allgemeinen Anforderungen

Allgemeine Anforderungen zur IT-Sicherheit verfolgen aus gesetzgeberischer Sicht verschiedene Ziele, die sehr unterschiedlich sein und sich teils sogar widersprechen können. Bemerkenswert ist insoweit, dass Verpflichtungen zur IT-Sicherheit bisher nicht zum Selbstzweck, d.h. zur Schaffung von IT-Sicherheit als abstrakt zu schützendes Gewährleistungsziel, erlassen wurden. IT-Sicherheit dient, wie die folgenden Beispiele zei-

gen, vielmehr dazu, andere Rechtsgüter oder Gewährleistungsziele, wie z.B. das Eigentum, die Privatsphäre oder auch die Funktionsfähigkeit von Wirtschaft und Gesellschaft, zu schützen.

3.1.1. Verhütung von unternehmerischen Risiken

Unzureichende IT-Sicherheit kann dramatische wirtschaftliche Auswirkungen auf Unternehmen haben. Beispiele hierfür sind die eingangs dargestellten Angriffe mit Verschlüsselungstrojanern, die Unternehmen tagelang lahmlegen können,[10] oder die Entwendung von Geschäftsgeheimnissen und Know-how durch Wirtschaftsspionage.[11] Vor diesem Hintergrund stellen fehlende IT-Sicherheit und die daraus resultierenden Schadensszenarien ein wirtschaftliches Risiko dar und werden insoweit von den gesetzlichen Vorschriften zur Verhütung von unternehmerischen Risiken erfasst. Ein Beispiel für derartige Regelungen sind die §§ 91, 93 des deutschen Aktiengesetzes (AktG). Vom Vorstand wird dabei einerseits die Einführung eines Überwachungssystems für „den Fortbestand der Gesellschaft gefährdende Entwicklungen" (§ 91 Abs. 2 AktG) verlangt sowie andererseits eine Pflicht zum Schutz von Betriebs- und Geschäftsgeheimnissen konstituiert (§ 93 Abs. 1 AktG). Die nach dem AktG erforderlichen Maßnahmen sind im Rahmen einer Prognose abhängig den möglichen Schadensszenarien und den Kosten der Schadensbeseitigung (sofern möglich) zu treffen.[12] Darüber hinaus sind IT-Sicherheit[13] und – spätestens seit der Einführung der DSGVO – Datenschutzrisiken[14] in das unternehmensweite Früherkennungssystem für Risiken aufzunehmen. Vergleichbare Vorschriften existieren auch für andere Gesellschaftsformen, beispielsweise in § 43 Abs. 1 des Gesetzes betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) für den GmbH-Geschäftsführer.[15]

3.1.2. Schutz natürlicher Personen bei der Verarbeitung ihrer Daten

Datenschutzrechtliche Vorgaben zur IT-Sicherheit sind im Unternehmenskontext relevant, soweit personenbezogene Daten verarbeitet und dadurch beispielsweise die Voraussetzungen von Art. 2 Abs. 1 DSGVO erfüllt werden. Neben der Verarbeitung von Kundendaten ist hierbei insbesondere auch an die Verarbeitung von Mitarbeiterdaten zu denken. Es dürfte daher kaum ein Unternehmen geben, das sich gänzlich dem Anwendungsbereich der DSGVO entziehen kann. Gleichzeitig sind die IT-Sicherheitsvorgaben der DSGVO auf die Verarbeitung personenbezogener Daten beschränkt.

Art. 24 Abs. 1 i.V.m. Art. 32 Abs. 1 DSGVO verpflichtet das verantwortliche Unternehmen, bei der Verarbeitung für einen angemessenen Schutz der personenbezogenen Daten zu sorgen. Vorgaben zu konkreten Maßnahmen enthält die DSGVO jedoch über die in Art. 32 Abs. 1 a) DSGVO genannten Beispiele nicht.[16] Es ist daher eine Konkretisierung der genannten Maßnahmen erforderlich.[17] Diese kann, wie z.B. bei möglichen Maßnahmen zur Pseudonymisierung und Verschlüsselung, insbesondere durch die Aufsichtsbehörden erfolgen.[18] Darüber hinaus verlangt Art. 32 Abs. 1 b) DSGVO eine dauerhafte Gewährleistung der Schutz-

[10] Vgl. Spiegel.de, Honda muss Produktion nach Cyberangriff stoppen. https://www.spiegel.de/netzwelt/web/honda-muss-produktion-nach-cyberangriff-stoppen-a-69f59803-216c-43c7-9ee9-59d3926d6314 (aufgerufen am 12. November 2020), 10.06.2020.

[11] Vgl. Nuri, Wirtschaftsspionage: Mittelstand im Visier von Wirtschaftsspionen. https://www.handelsblatt.com/unternehmen/mittelstand/wirtschaftsspionage-mittelstand-im-visier-von-wirtschaftsspionen/3127338-all.html (aufgerufen am 12. November 2020), 04.03.2009.

[12] Conrad/Streitz, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 50.

[13] Ebenda, Rn. 41 f.

[14] Keppeler/Berning, Auswirkungen der DS-GVO auf Jahresabschluss und Lagebericht von Unternehmen, ZD 2018, S. 157 (S. 160).

[15] Habbe/Gergen, Compliance vor und bei Cyberangriffen – Pflichten der Geschäftsleitung und deren konkrete Umsetzung in der Praxis, CCZ 2020, S. 281 (S. 282).

[16] Paulus, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 30. Editon, Stand 01.11.2019, Art. 32 DSGVO, Rn. 4.

[17] Piltz, in: Gola (Hrsg.), DS-GVO, 2. Auflage 2018, Art. 32 DSGVO, Rn. 27.

[18] Hladjk, in: Ehmann/Selmayr (Hrsg.), 2. Auflage 2018, Art. 32 DSGVO, Rn. 7 f.

ziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).[19] Außerdem enthält Art. 32 Abs. 1 DSGVO funktionale Anforderungen für eine Resilienz der Verarbeitung,[20] die einerseits durch eine Belastbarkeit der Systeme und andererseits durch die rasche Wiederherstellbarkeit bei Vorfällen gewährleistet werden soll.[21] Aus Art. 32 Abs. 1 d) DSGVO ergibt sich auch die Verpflichtung, die getroffenen Maßnahmen einer regelmäßigen Kontrolle, Bewertung und Evaluierung zu unterziehen. Art. 25 Abs. 1 DSGVO enthält darüber hinaus eine vergleichsweise vage Verpflichtung zu datenschutzfreundlicher Technikgestaltung (privacy by design).[22] Um dieser nachzukommen, soll der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel der Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene Maßnahmen zur IT-Sicherheit, aber auch zum Datenschutz allgemein treffen.[23]

3.1.3. Schutz des Wettbewerbs

Verpflichtungen zur IT-Sicherheit können auch dem Schutz des wirtschaftlichen Wettbewerbs und der Integrität des Marktes dienen. Ein Beispiel hierfür ist die in Art. 18 Marktmissbrauchsverordnung (MAR) enthaltene Verpflichtung zur Führung von Insiderlisten bei Aktienunternehmen. Die Vorschrift zielt im Kern darauf ab, Manipulationen im Wertpapierhandel zu verhindern, indem Emittenten und von ihnen Beauftragte den Fluss von Insiderinformationen überwachen können.[24] Eine sinnvolle Überwachung des Informationsflusses ist jedoch nur möglich, wenn zugleich Maßnahmen vorhanden sind, die sicherstellen, dass der Zugriff auf die Informationen unternehmensintern beschränkt ist. Ohne, dass es ausdrücklich angeordnet wird, erfordert Art. 18 MAR folglich die Umsetzung von zugriffsbeschränkenden technischen Maßnahmen, wie z.B. Datenverschlüsselung, innerhalb des Unternehmens. [25]

Ein weiteres Beispiel für Verpflichtungen zur IT-Sicherheit im Kontext des unternehmerischen Wettbewerbs ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Dieses setzt für den rechtlichen Schutz einer Information nach § 2 Nr. 1 b) GeschGehG als Geschäftsgeheimnis angemessene Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber voraus. Zu denken ist hier zunächst an die Kennzeichnung der Information als vertraulich,[26] aber auch vertragliche Vereinbarungen zum Geheimnisschutz, etwa mit Arbeitnehmern oder Dritten.[27] Abhängig von einer Risikobewertung, der Unternehmensgröße und der Anzahl von Geheimnissen können aber auch technische Maßnahmen, wie z.B. ein Passwortschutz oder Verschlüsselung, erforderlich sein.[28] Letztlich erfordert das GeschGehG die Etablierung eines Managementsystems, das geeignet ist, eine Klassifikation und Risikobewertung für Geschäftsgeheimnisse abzubilden sowie die entsprechenden Maßnahmen zu dokumentieren.[29]

3.1.4. Sicherstellung ordnungsgemäßer Besteuerung

Allgemeine Anforderungen an IT-Sicherheit können sich auch aus steuerrechtlichen Vorschriften ergeben. Ziel ist in diesem Fall, wie § 145 Abs. 2 Abgabenordnung (AO) andeutet, Aufzeichnungen so vorzunehmen, dass „der Zweck, den sie für die Besteuerung erfüllen sollen“, erreicht wird. Eine nähere Präzisierung erfahren

---

19 Ebenda.
20 Kühling, in: Buchner/Jandt (Hrsg.), 2. Auflage 2018, Art. 32 DSGVO, Rn. 26.
21 Hladjk, in: Ehmann/Selmayr (Hrsg.), 2. Auflage 2018, Art. 32 DSGVO, Rn. 7 f.
22 Hartung, in: Kühling/Buchner (Hrsg.), 2. Auflage 2018, Art. 25 DSGVO, Rn. 11.
23 Baumgartner, in: Ehmann/Selmayr (Hrsg.), 2. Auflage 2018, Art. 25 DSGVO, Rn. 3.
24 Kumpan/Grübler, in: Schwark/Zimmer (Hrsg.), Kapitalmarktrechts-Kommentar, 5. Auflage 2020, Art. 18 VO (EU) 596/2014, Rn. 5.
25 Conrad, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 232.
26 Ohly, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, S. 441 (S. 444).
27 Ebenda.
28 Ebenda.
29 Hessel/Leffer, Rechtlicher Schutz maschinengenerierter Daten, MMR 2020, S. 647 (S. 650).

die steuerrechtlichen Vorschriften durch § 146 Abs. 1 S. 1 AO[30] und die damit in Zusammenhang stehenden Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung (GoBD) der Finanzverwaltung.[31] Die GoBD verlangt wörtlich, dass Datenverarbeitungssysteme gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) und gegen unberechtigte Eingaben und Veränderungen (z. B. durch Zugangs- und Zugriffskontrollen) geschützt sind. Die Umsetzung dieser Vorgaben verlangt nicht nur ein Datensicherheitskonzept, sondern auch eine umfassende Dokumentation und Kontrolle. [32] Beim Einsatz von elektronischen Kassensystemen ergeben sich weitere IT-Sicherheitsvorgaben aus § 146a Abs. 1 AO. Elektronische Kassensysteme müssen demnach eine technische Zertifizierung aufweisen.

3.2. Spezialgesetzliche Vorgaben bei erhöhten Risiken

Über die bei wirtschaftlichen Tätigkeiten allgemein zu beachtenden gesetzlichen Vorgaben hinaus gibt es gesetzliche Vorschriften zur IT-Sicherheit, die an ein erhöhtes Risiko anknüpfen. Aufgrund dieses erhöhten Risikos hält der Gesetzgeber eine im Rahmen der allgemeinen Vorschriften vorgenommene Risikoanalyse und -bewertung für nicht mehr ausreichend und präzisiert daher die Anforderungen an die IT-Sicherheit durch weitere Vorgaben. Hinsichtlich der gesetzlichen Regelungstechnik knüpfen die Vorgaben in der Regel an branchen- oder tätigkeitsspezifische Risiken und verlangen von den Verantwortlichen die Erfüllung bestimmter Mindestvorgaben. Teilweise werden dabei, wie die folgenden Beispiele zeigen, völlig neue Anforderungen aufgestellt, teilweise erfolgt jedoch auch eine Präzisierung gesetzlicher Vorschriften bzw. deren verstärkte Kontrolle.

3.2.1. Beispiel I: Kritische Infrastrukturen und digitale Dienste

Wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall bestimmter IT-Systeme haben kann, hat der Gesetzgeber bereits 2015 mit dem IT-Sicherheitsgesetz § 8a BSIG eingeführt und erstmals Mindestvorgaben für die Betreiber sog. kritischer Infrastrukturen erlassen.[33] Eine kritische Infrastruktur liegt nach § 2 Abs. 10 S. 1 BSIG vor, wenn eine Einrichtung, Anlagen oder Teile von ihr „den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen“ angehören und „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden”. Eine nähere Bestimmung der kritischen Infrastrukturen erfolgt gemäß § 2 Abs. 10 S. 2 BSIG im Rahmen einer Rechtsverordnung (sog. BSI-KritisV), durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Für die Betreiber kritischer Infrastrukturen gelten strengere Vorgaben zur IT-Sicherheit als für Unternehmen im Allgemeinen. So verlangt § 8a Abs. 1 S. 1 BSIG, dass die Betreiber „angemessene organisatorische und technische Vorkehrungen“ zur IT-Sicherheit ihrer Systeme, Komponenten oder Prozesse treffen, soweit diese funktionskritisch sind. Hierbei sollen die Betreiber nach § 8a Abs. 2 BSIG insbesondere branchenspezifische Sicherheitsstandards erarbeiten und deren Geeignetheit durch das BSI feststellen lassen. Neben strengeren inhaltlichen Vorgaben unterliegen Betreiber kritischer Infrastrukturen aber auch einem engeren Kontrollsystem. Sie müssen beispielsweise nach § 8a Abs. 3 BSIG einen Nachweis zur Erfüllung der Anforderungen erbringen und an das BSI übermitteln sowie nach § 8b Abs. 4 BSIG bestimmte Störungen unverzüglich an das BSI melden. Ein etwas abgeschwächtes Anfor-

30 Rätke, in: Klein (Hrsg.), AO, 15. Auflage 2020, § 146 AO, Rn. 17.

31 Bundesministerium der Finanzen, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD), 28.11.2019, Rn. 103 ff.

32 Conrad, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, Rn. 404.

33 Buchberger, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, § 8a BSIG, Rn. 1.

derungskonzept gilt nach § 8c, der im Jahr 2017 zur Umsetzung der NIS-Richtlinie[34] geschaffen wurde, auch für die Anbieter von digitalen Diensten. [35]

3.2.2. Beispiel II: Digitale Gesundheitsanwendungen

Die gesetzlichen Vorgaben für IT-Sicherheit bei digitalen Gesundheitsanwendungen sind ein Musterbeispiel für die in vielen Branchen entstehenden stark fokussierten gesetzlichen Vorgaben. Der enge Regelungsbereich derartiger Vorschriften zielt, was auch bei den Vorgaben für digitale Gesundheitsanwendungen deutlich wird, auf die Verhinderung ganz spezifischer Risikofaktoren beim Einsatz von IT-Systemen im jeweiligen Kontext. Rechtsgrundlage für die IT-Sicherheitsregulierung bei digitalen Gesundheitsanwendungen ist das am 19.12.2019 in Kraft getretene Digitale-Versorgung-Gesetz (DVG). Es handelt sich dabei um ein Mantelgesetz mit dem der Gesetzgeber eine Vielzahl bestehender Gesetze geändert bzw. ergänzt hat, um die Digitalisierung der Medizin in Deutschland voranzutreiben.[36] In einem Teil der Regelungen wurden auch gesetzliche Rahmenbedingungen für digitale Gesundheitsanwendungen geschaffen. Zu diesen zählt auch § 33a Abs 1 S. 1 SGB V, der eine Legaldefinition für digitale Gesundheitsanwendungen enthält. Eine digitale Gesundheitsanwendung ist demnach ein Medizinprodukt niedriger Risikoklasse, dessen Hauptfunktion wesentlich auf digitalen Technologien beruht und das dazu bestimmt ist, bei den Versicherten oder in der Versorgung durch Leistungserbringer bestimmte medizinische Tätigkeiten zu übernehmen. Zu Letzteren zählt die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Kompensierung von Verletzungen oder Behinderungen. Aus § 33a Abs 1 S. 1 SGB V ergibt sich zugleich auch ein grundsätzlicher Anspruch der Versicherten auf Kostenübernahme durch die Krankenkasse, wenn die Gesundheitsanwendung im Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen aufgenommen ist. Eine Aufnahme in das vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) geführte Verzeichnis bedarf einer Genehmigung, in der gemäß § 139e Abs. 2 Nr. 2 SGB V nachzuweisen ist, dass die digitale Gesundheitsanwendung „Datensicherheit nach dem Stand der Technik gewährleistet". Eine nähere Bestimmung der Anforderungen kann das Bundesministerium für Gesundheit (BMG) gemäß § 139e Abs. 9 SGB V durch Rechtsverordnung vornehmen. Dies ist Anfang April 2020 durch den Erlass der Digitale Gesundheitsanwendungen Verordnung (DiGAV) erfolgt. In der DiGAV hat das BMG nicht nur erhebliche Verschärfungen der DSGVO vorgenommen,[37] sondern über § 4 Abs. 1 DiGAV in Verbindung mit der zugehörigen Anlage 1 sehr detaillierte Vorgaben zur IT-Sicherheit gemacht.

4. Rechtliche Herausforderungen bei der praktischen Umsetzung

Aufgrund der dargestellten gesetzlichen Anforderungen ergibt sich für Unternehmen – neben der tatsächlichen Notwendigkeit zu IT-Sicherheitsmaßnahmen – in zunehmendem Maße auch eine rechtliche Verpflichtung zur IT-Sicherheit. Ausgangspunkte dieser sind dabei sowohl sich weiter verdichtende allgemeine gesetzliche Vorgaben, beispielsweise durch die Auslegung und Präzisierung der DSGVO, als auch der zunehmende Erlass von spezialgesetzlichen Vorgaben bei erhöhten Risiken. Neben Vorgaben für digitale Gesundheitsanwendungen ist hierbei beispielsweise an die Vorgaben der UNECE zu Cybersecurity und Software Updates

[34] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148 (aufgerufen am 12. November 2020).

[35] Ebenda.

[36] Vgl. Bundesministerium für Gesundheit, Ärzte sollen Apps verschreiben können. https://www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html (aufgerufen am 12. November 2020).

[37] Piltz/Hessel, Verbot von Datentransfers in die USA? – Der aktuelle DiGA-Leitfaden ist eine Herausforderung für Anbieter von Gesundheits-Apps & Co. https://www.reuschlaw.de/news/verbot-von-datentransfers-in-die-usa (aufgerufen am 12. November 2020).

bei Fahrzeugen[38] oder die aktuellen Evaluierungen der EU-Kommission zur IT-Sicherheit im Bereich des Internet of Things (IoT)[39] zu denken. Aus unternehmerischer Sicht ist für eine Umsetzung der gesetzlichen Verpflichtungen und Gewährleistung der unterschiedlichen Ziele dieser ein umfassendes Managementsystem notwendig. In einem ersten Schritt sollten hierfür die auf das jeweilige Unternehmen anwendbaren IT-Sicherheitsvorgaben identifiziert werden. Hierbei sind neben den Gesetzen, mit unternehmensbezogener Ausrichtung, auch produktbezogene IT-Sicherheitsanforderungen zu berücksichtigten. In einem zweiten Schritt sollten dann die einzelnen gesetzlichen Vorgaben für die IT-Sicherheit definiert und die notwendigen Risikoabwägungen durchgeführt werden. In einem dritten Schritt sollte sodann auf Basis der identifizierten Maßnahmen ein einheitliches IT-Sicherheitskonzept erstellt bzw. angepasst und, insbesondere zum Nachweis der Compliance, dokumentiert werden. Im Rahmen der Ausgestaltung des IT-Sicherheitskonzepts sind neben technischen Prozessen auch rechtliche Prozesse, wie z.B. Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO, zu berücksichtigten. Ebenso sollten bestimmte IT-Sicherheitsmaßnahmen rechtlich abgesichert werden. Ein klassisches Beispiel hierfür ist die Verpflichtung von Mitarbeitern zur Vertraulichkeit. Die steigenden gesetzlichen Vorgaben sollten Unternehmen aber animieren, auch in anderen Bereichen, etwa bei der Inanspruchnahme von Dienstleistern, detaillierte Regelungen zu treffen und beispielsweise Maßnahmen zum unternehmensübergreifenden Incident Response in vertraglicher Form zu regeln sowie für den Fall von Verstößen Vertragsstrafen und Haftungsregeln zu vereinbaren.

5. Fazit

IT-Sicherheit ist und bleibt ein wesentlicher Schlüsselfaktor für eine erfolgreiche Digitalisierung der deutschen Wirtschaft und die Ausschöpfung der damit verbundenen Potentiale. In der Praxis zeigt jedoch eine Vielzahl von teils folgenschweren Cyberangriffen, dass längst nicht alle Unternehmen ausreichende Schutzmaßnahmen getroffen haben. Dieser Situation versucht der Gesetzgeber bisher mit einem risikobasierten Ansatz zu begegnen. Gesetzliche Vorgaben zur IT-Sicherheit werden folglich stets zur Gewährleistung eines bestimmten Zwecks erlassen. Können aus dem Einsatz eines IT-Systems erhöhte Risiken resultieren, werden die gesetzlichen Vorgaben enger. Dies bedeutet einerseits eine strengere Maßgabe hinsichtlich der erforderlichen Maßnahmen und eine engmaschigere Kontrolle dieser. Aus der risikobasierten Regulierung folgt zugleich eine nur schwer überschaubare Anzahl gesetzlicher Vorgaben, die aus unternehmerischer Sicht die Etablierung eines Managementsystems nach den hier dargestellten Grundsätzen verlangt. Geht man davon aus, dass sich der Trend einer zunehmenden Regulierung fortsetzt, könnte sich aus den vielen Einzelvorschriften zukünftig – zumindest auf faktischer Ebene – eine umfassende Verpflichtung zur IT-Sicherheit für Unternehmen ergeben. Wie effizient diese bei der Verbesserung der IT-Sicherheit sein wird, dürfte maßgeblich auch von der Durchsetzung der gesetzlichen Vorgaben abhängen.

[38] UNECE, UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles. https://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html (aufgerufen am 12. November 2020), 25.06.2020.

[39] Hessel/Rebmann, Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children, International Cybersecurity Law Review 01/2020, S. 27–37. https://link.springer.com/article/10.1365/s43439-020-00006-3 (aufgerufen am 12. November 2020).