Leseprobe zu

Voigt

IT-Sicherheitsrecht

Pflichten und Haftung im Unternehmen

2018, rd. 350 Seiten, broschiert, Monographie / Praxisbuch / Ratgeber, 17 x 24cm

ISBN 978-3-504-56107-9

79,80 €

2. IT-Sicherheit als Nebenpflicht

108 IT-Sicherheit kann nicht nur zum Gegenstand der vertraglichen (Haupt-)Leistungspflichten werden, sondern kann auch aus Vertrauensgesichtspunkten im Rahmen von Verträgen relevant werden. Dabei muss es sich nicht notwendigerweise um Verträge handeln, die einen offensichtlichen IT-Sicherheitsbezug aufweisen. § 241 Abs. 2 BGB verpflichtet Vertragsparteien zur gegenseitigen Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen der jeweils anderen Partei. Verträge begründen eine Sonderbeziehung zwischen den Parteien, die nicht nur die Erbringung der geschuldeten Leistungen, sondern auch gegenseitige Rücksichtnahme als **Nebenpflicht** erforderlich machen.[1] Die **Einhaltung der eigenen IT-Sicherheitspflichten durch das Unternehmen** kann daher auch eine vertragliche Pflicht sein, da den Vertragspartnern durch Zwischenfälle materielle oder immaterielle Schäden entstehen können.

109 **Umfang und Inhalt** der Nebenpflichten gibt § 241 Abs. 2 BGB nicht vor. Wichtige Fallgruppen bilden jedoch Schutz- und Aufklärungspflichten.[2] Während **Schutzpflichten** die Vertragsparteien zu einem Verhalten verpflichten, durch das die Rechte, Rechtsgüter und Interessen des anderen Teils nicht verletzt werden, verpflichten **Aufklärungspflichten** zur unaufgeforderten Information der anderen Partei über erkennbar entscheidungserhebliche Umstände.[3] Umfang und Inhalt der Nebenpflichten sind vom konkreten Fall und daher vom vereinbarten Vertragszweck, der Verkehrssitte, den beiderseitigen Interessen und den Anforderungen des Geschäftsverkehrs abhängig.[4] **Je mehr eine Partei** auf die Zusammenarbeit angewiesen ist oder auf die **IT-Sicherheitsvorkehrungen** der anderen Partei **vertrauen muss** und je größer die Sicherheitsrisiken sind, denen sie durch die vertragliche Beziehung ausgesetzt wird, **desto mehr** erlangen die Nebenpflichten im konkreten Fall an **Gewicht**.[5] Ein generelles Pflichtenprogramm lässt sich allerdings nicht ablesen.

110 Sind die gesetzlichen IT-Sicherheitsverpflichtungen des Unternehmens besonders intensiv ausgeprägt, stellt deren Einhaltung regelmäßig eine Nebenpflicht im Rahmen der vom Unternehmen mit Dritten abgeschlossenen Verträge dar. Dies ist z.B. beim **Online-Banking** (s. insbesondere Rz. 290 ff., Rz. 471 ff.) der Fall.[6] Das Bestehen umfassender IT-Sicherheitspflichten ist auf ein **hohes Risikopotential** zurückzuführen, so dass IT-Sicherheitsvorfälle nicht nur ein hohes Risiko für die Interessen des Unternehmens, sondern auch für diejenigen der Vertragspartner bergen. Die IT-Sicherheitspflichten sind dann zugleich **Schutzpflichten**. Unternehmen sollten prüfen, wann und wie sich die unternehmensinterne **Verletzung eigener IT-Sicherheitspflichten auf Vertragspartner nachteilig auswirken kann**. Wird deren vermögens- und persönlichkeitsrechtlicher *status quo* durch Sicherheitsvorfälle im Unternehmen potentiell beeinträchtigt, bildet dies ein starkes Indiz dafür, dass die IT-Sicherheit eine Schutzpflicht zum Vertrag ist.

---

1 *Grüneberg* in Palandt, BGB, § 241 Rz. 6; *Sutschet* in Bamberger/Roth/Hau/Poseck, BeckOK/BGB, § 241 Rz. 15.

2 *Grüneberg* in Palandt, BGB, § 241 Rz. 7.

3 *Grüneberg* in Palandt, BGB, § 241 Rz. 7 und § 280 Rz. 30; *Bachmann* in MünchKomm/BGB, § 241 Rz. 110.

4 *Grüneberg* in Palandt, BGB, § 241 Rz. 6; *Bachmann* in MünchKomm/BGB, § 241 Rz. 52; BGH, Urt. v. 30.9.2009 – VIII ZR 238/08, NJW 2010, 1135, 1137 = MDR 2010, 18.

5 *Sutschet* in Bamberger/Roth/Hau/Poseck, BeckOK/BGB, § 241 Rz. 44; *Bachmann* in MünchKomm/BGB, § 241 Rz. 52.

6 *Roth/Schneider*, ITRB 2005, 19, 20; *Beucher/Utzerath*, MMR 2013, 362, 367.

Beispiel für IT-Sicherheit als vertragliche Nebenpflicht: Eine Bank wird zum Opfer eines Cyber-Angriffs, wodurch zahlreiche Überweisungen von Kundenkonten an Dritte veranlasst werden, die nicht alle rückgängig gemacht werden können. Auch Kunde X ist davon betroffen und erleidet einen Schaden i.H.v. 400 Euro. Der Angriff ist auf eine Schwachstelle im IT-System der Bank zurückzuführen, die von Hackern ausgenutzt wurde.

Die Sicherheitsrisiken beim Online-Banking sind besonders hoch. Die Nutzung von Zahlungsdiensten ist für Kunden zur Abwicklung alltäglicher Geschäfte besonders wichtig, macht eine Verarbeitung vertraulicher Zahlungsdaten erforderlich und Banken unterliegen dementsprechend strengen IT-Sicherheitspflichten. Aus den vorgenannten Gründen ist die Einhaltung der IT-Sicherheitspflichten für Banken und Kunden gleichermaßen von besonderer Bedeutung. Sicherheitsvorfälle können leicht zu Schäden beim Kunden führen. So hat Kunde X durch den Cyber-Angriff 400 Euro verloren. Durch den Vorfall ist es damit zu einer Verletzung der Rechtsgüter des X gekommen. Die Einhaltung der IT-Sicherheitspflichten ist eine Nebenpflicht der Bank bzgl. ihres Vertrags mit X.

Gesetzliche IT-Sicherheitspflichten überschneiden sich insofern **mit** entsprechenden **vertraglichen Nebenpflichten**, als dass sie auch einen Hinweis auf über den Umfang gesetzlicher Pflichten hinausgehende Schutzpflichten liefern können. Vor allem im Datenschutzrecht sind (teilweise bereichsspezifische) **Benachrichtigungspflichten** vorgesehen, die Unternehmen zur Meldung von Datenschutzverletzungen an betroffene Personen verpflichten, etwa in Art. 34 DSGVO, § 15a TMG, § 109a TKG. Dabei geht es häufig um IT-Zwischenfälle im Unternehmen, durch die Daten von Kunden oder Vertragspartnern an unberechtigte Dritte gelangen. Die gesetzlichen Benachrichtigungspflichten wurden zum Schutz der Betroffenen geschaffen, um diesen das Ergreifen von Gegenmaßnahmen zu ermöglichen, und dienen somit deren **Integritätsinteresse**.[1] Es handelt sich dabei gewissermaßen um die Verrechtlichung von **Aufklärungspflichten**. Diese Benachrichtigungspflichten sind jedoch durch ihren Anwendungsbereich und etwaige Ausnahmeregelungen beschränkt. Wenn die gesetzliche Benachrichtigungspflicht nicht zur Anwendung gelangt, kann daher unter Umständen eine vertragliche Benachrichtigungspflicht entstehen[2], da die Aufklärung über Datenschutzverletzungen für Vertragspartner zumeist eine erhebliche Information darstellen sollte. Damit liefern normierte IT-Sicherheitspflichten mit Bezug auf betroffene Personen außerhalb des Unternehmens einen wertvollen Hinweis auf den Mindestumfang vertraglicher Nebenpflichten, die je nach Umständen des Einzelfalls auch darüber hinausgehen können.[3] 111

3. Hinweise zur Vertragsgestaltung

Da IT-Sicherheitspflichten im Rahmen von Verträgen nicht nur als Leistungs-, sondern auch als Nebenpflichten relevant werden, ist ein **gänzlicher Ausschluss** der IT-Sicherheit als Vertragspflicht **kaum denkbar**. Zumindest aus der Pflicht zur gegenseitigen Rücksichtnahme müssen Unternehmen ihre IT-Sicherheitspflichten auch zum Schutz der Interessen, Rechte und Rechtsgüter ihrer Vertragspartner wahren. 112

Werden beim Vertragsschluss ausdrücklich Leistungspflichten mit IT-Sicherheitsbezug vereinbart, sollte die Vertragsgestaltung besonders sorgfältig erfolgen. Auch aus Haftungsgründen (s. Rz. 221 ff.) sollte ein Anbieter im Vertrag eine möglichst genaue Beschreibung des eigenen Pflichtenprogramms vornehmen, also die internen IT-Sicherheitsmaßnahmen präzise darle- 113

1 Siehe dazu etwa ErwGr. 85 f. DSGVO.
2 *Mehrbrey/Schreibauer*, MMR 2016, 75, 81 m.w.N.
3 *Spindler*, CR 2016, 297, 308.

gen.[1] Aus Anbietersicht gilt es, soweit möglich, zu **vermeiden**, für einen **bestimmten Sicherheitserfolg als Hauptleistungspflicht einstehen zu müssen**. Aus diesem Grund wären für Anbieter bspw. dienstvertragliche Regelungen vorzugswürdig, da dann zwar eine **bestimmte Leistung**, wie z.B. das Bemühen um einen vereinbarten Sicherheitszustand, aber **kein bestimmter IT-Sicherheitszustand als Erfolg geschuldet** wird.[2] Ist das Unternehmen Abnehmer oder Nutzer von IT-Produkten oder -Leistungen, wären dahingegen entsprechend Werkverträge günstiger, da sie dann von ihrem Vertragspartner einen vereinbarten IT-Sicherheitserfolg verlangen können.

114 Lagert ein Unternehmen eigene IT-Prozesse auf **externe Dienstleister** aus, sollte auch hier darauf geachtet werden, dass das Pflichtenprogramm des Dienstleisters in Bezug auf anzustrebende Sicherheitsstandards klar umrissen wird. Das Unternehmen sollte außerdem entsprechende **Kontroll- und Berichtspflichten** im Vertrag vorsehen, um die Einhaltung der Vorgabe überprüfen zu können.[3]

4. Übersicht zu typischen Fallgruppen

IT-Sicherheit als Leistungspflicht		
= wird ausgehend von den vertraglichen Vereinbarungen als Leistung geschuldet → Bestimmung des Pflichtenprogramms im Einzelfall		
Vertrag	**IT-Sicherheitspflichten**	**Mögliche Verletzungsfolgen**
IT-Outsourcing-Verträge Beispiele: Cloud Computing, Beauftragung externer IT-Sicherheitsbeauftragter, …	Auftraggeber gibt die eigenen IT-Sicherheitspflichten im Rahmen des Vertrags an den Outsourcing-Anbieter weiter – als **Dienstvertrag**: Leistungserbringung unter Berücksichtigung der IT-Sicherheitsvorgaben wird geschuldet – als **Werkvertrag**: vereinbarter IT-Sicherheitsstandard wird als Erfolg geschuldet	– **Dienstvertrag**: keine umfassenden Gewährleistungsansprüche, daher insb. Schadensersatzansprüche des Auftraggebers (statt der Leistung oder neben der Leistung bei unzureichender oder nicht rechtzeitiger Leistungserbringung) und ggf. Recht zur Kündigung des Vertrags – **Werkvertrag**: umfassende Gewährleistungsansprüche (Behebung von Mängeln, Rücktrittsrecht, Minderung der Vergütung, …) einschließlich Schadensersatzansprüche (statt oder neben der Leistung), Recht zur Kündigung bis zur Vollendung des Werks

1 *Conrad* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 255.
2 *Conrad* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 255 f.; s. zum Leistungsmaßstab des Dienstrechts *Müller-Glöge* in MünchKomm/BGB, § 611 Rz. 19 ff.
3 *Conrad* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 256.

IT-Sicherheit als Leistungspflicht		
= wird ausgehend von den vertraglichen Vereinbarungen als Leistung geschuldet → Bestimmung des Pflichtenprogramms im Einzelfall		
Vertrag	**IT-Sicherheitspflichten**	**Mögliche Verletzungsfolgen**
Auftragsdaten-verarbeitung	– Auftraggeber (= für die Verarbeitung personenbezogener Daten Verantwortlicher) verpflichtet den Auftragnehmer (= Auftragsverarbeiter) zu IT-Sicherheitsmaßnahmen – eigene datenschutzrechtliche IT-Sicherheitspflichten des Auftragsverarbeiters	– Schadensersatzansprüche des Verantwortlichen – Bußgelder auf Grundlage des allg. Datenschutzrechts – bei **Werkvertrag**: umfassende Gewährleistungsansprüche
Kaufverträge über IT-Produkte	– Produkt muss bestimmte IT-Sicherheitseigenschaften aufweisen (vereinbarte/gewöhnliche Beschaffenheit) – **Pflicht zum Bereitstellen von Erhaltungs-Updates** zur Sicherung der Funktionsfähigkeit des Produkts (zumindest während der Gewährleistungsfrist auf Kosten des Verkäufers)	– umfassende Gewährleistungsansprüche (Nacherfüllung bei Mängeln, Rücktrittsrecht, …) sowie Schadensersatzansprüche (statt oder neben der Leistung bei unzureichender oder nicht rechtzeitiger Vertragserfüllung)
Verträge über die zeitweise Überlassung von IT-Produkten Beispiele: ASP, SaaS, …	– Produkt muss vereinbarte IT-Sicherheitsbeschaffenheit während der Laufzeit des Vertrags aufweisen → Herstellung des vertraglich vereinbarten Zustands des Produkts – **mietvertragliche Erhaltungspflicht**: begrenzte Update-Pflicht zur Erhaltung des vereinbarten Sicherheitsstandards, keine Pflicht zur umfassenden Anpassung an geänderte Sicherheitsrisiken	– Schadensersatzansprüche (statt oder neben der Leistung bei unzureichender oder nicht rechtzeitiger Leistungserbringung) – Minderungsrecht bzgl. vereinbarter Vergütung – Recht zur Selbstvornahme bei Mängeln des Produkts
Verträge über die Wartung und Pflege von IT-Produkten	– Erhalt der Gebrauchsfähigkeit und Sicherheit der IT-Produkte wird geschuldet – **häufig dienst- und werkvertragliche Elemente**	– s. Anmerkungen zu möglichen Verletzungsfolgen bei IT-Outsourcing-Verträgen

IT-Sicherheit als Nebenpflicht (§ 241 Abs. 2 BGB) = Verpflichtung zur Einhaltung eigener IT-Sicherheitspflichten zur gegenseitigen Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen der Vertragspartner		
Pflicht	**Umfang**	**Verletzungsfolge**
Schutzpflichten	= Unternehmen schuldet IT-Sicherheit, damit die Rechte, Rechtsgüter und Interessen der Vertragspartner nicht verletzt werden – je intensiver die IT-Sicherheitspflichten des Unternehmens, desto weitreichender seine Schutzpflichten	– Schadensersatzansprüche des Vertragspartners – kann Recht zum Rücktritt oder zur Kündigung des Vertrags auslösen (§§ 314, 324 BGB)
Aufklärungspflichten	= Unternehmen schuldet seinen Vertragspartnern unaufgeforderte Information über IT-Sicherheitsvorfälle, die diese schädigen könnten – Aufklärungspflichten in Form spezialgesetzlicher Benachrichtigungspflichten (z.B. Art. 33 DSGVO, § 8b Abs. 4 BSIG) weitgehend verrechtlicht	

VIII. IT-Sicherheit als wettbewerbsrechtliche Pflicht

115 Die Einhaltung der **IT-Sicherheitspflichten** ist für Unternehmen, wie bereits gezeigt (s. Rz. 27 ff.), nicht nur aus rechtlicher, sondern auch aus **unternehmerischer Sicht bedeutsam**. Ein unzureichender IT-Sicherheitsstandard kann zum Reputationsverlust und damit zu empfindlichen Umsatzeinbußen führen. Investitionen in die unternehmenseigene IT-Sicherheit sind daher Investitionen in die Zukunfts- und Wettbewerbsfähigkeit am Markt.[1] Die Wettbewerbsfreiheit wird durch die Vorgaben des UWG sichergestellt. Das Gesetz dient dem Schutz der Interessen von Mitbewerbern und Verbrauchern vor einer **Beeinträchtigung durch unlautere geschäftliche Handlungen**, § 1 UWG. Auch unzureichende IT-Sicherheit kann einen Einfluss auf die Wettbewerbsfreiheit haben: mangelnde Sicherheitsstandards bieten nicht nur Dritten eine Angriffsfläche auf die Betriebsgeheimnisse des Unternehmens, sondern können zugleich einen Wettbewerbsverstoß darstellen.

1. IT-Sicherheit zum Schutz von Betriebsgeheimnissen

116 Die wettbewerbliche Entfaltungsfreiheit kann insbesondere durch IT-gestützte Industriespionage verletzt werden. Wirtschaftsgeheimnisse bestimmen regelmäßig den geschäftlichen Erfolg zahlloser Unternehmen und stehen daher immer mehr im Zentrum vielfältiger konkurrierender Interessen.[2] **Betriebs- und Geschäftsgeheimnisse** sind häufig ein wesentlicher Vermögensbestandteil des Unternehmens; mit ihrem **Geheimbleiben steht und fällt deren Wert**.[3] Mit der zunehmenden Digitalisierung **wächst** auch die **Wirtschaftsspionage exponentiell**, wobei sich das genaue Ausmaß von Industriespionage und Geheimnisverrat man-

1 *Byok*, BB 2017, 451, 453.
2 *Brammsen*, ZIP 2016, 2193, 2193.
3 *Köhler* in Köhler/Bornkamm, UWG, Vorbem. §§ 17-19 Rz. 1 m.w.N.

gels verlässlicher Daten, hoher Dunkelziffern und geringer Aufklärungsquoten kaum verlässlich abschätzen lässt.[1] Die Offenlegung von Geschäftsgeheimnissen birgt ein **gewichtiges Schadenspotential** und kann für Unternehmen zum existenzbedrohenden Risiko werden.[2] **Unzureichende IT-Sicherheit bietet erfolgreicher Industriespionage** regelmäßig erst einen **Nährboden**. Mit der zunehmenden Vernetzung der Unternehmensdaten innerhalb der eigenen IT-Systeme und der allgegenwärtigen Nutzung von Internet und Telekommunikationsnetzen werden Daten- und Wirtschaftsspionage erheblich begünstigt.[3]

117 Werden Betriebs- oder Geschäftsgeheimnisse das Ziel externer Angriffe auf die IT eines Unternehmens, so können **Straftaten nach §§ 17–19 UWG** vorliegen. Diese Vorschriften schützen sowohl Unternehmensinhaber vor einer Verletzung ihrer Geschäfts- und Betriebsgeheimnisse als auch den Wettbewerb vor Verfälschung.[4] § 17 UWG enthält drei Straftatbestände: den **Geheimnisverrat** durch einen Beschäftigten (Abs. 1), die **Betriebsspionage**, also das Ausspähen eines Geheimnisses mit bestimmten Mitteln und Methoden (Abs. 2 Nr. 1), und die **Geheimnisverwertung**, also die unbefugte Verwertung eines durch Verrat oder Ausspähung erlangten Geheimnisses (Abs. 2 Nr. 2).[5] § 18 UWG stellt die unbefugte Nutzung anvertrauter Geheimnisse durch Selbstständige unter Strafe. § 19 UWG dient einer Erweiterung des strafrechtlichen Schutzes vor Geheimnisverrat durch §§ 17, 18 UWG, indem er bestimmte Vorbereitungshandlungen unter Strafe stellt.[6] Entsprechende Taten sind mit **Freiheits- oder Geldstrafe** bedroht. Neben den strafrechtlichen Folgen von Industriespionage kommen auch **Schadenersatzansprüche des betroffenen Unternehmens** in Betracht, deren Grundlage überwiegend das Deliktsrecht bildet (s. Rz. 253 ff.). So sind die **§§ 17–19 UWG Schutzgesetze** i.S.d. § 823 Abs. 2 BGB.[7] Die in der Theorie bestehenden Ansprüche können in der Praxis dem betroffenen Unternehmen aufgrund **mangelnder Erfolge in der Strafverfolgung** jedoch häufig kaum finanzielle Abhilfe verschaffen.

118 Da ein **rechtlicher Schutz** von Betriebsgeheimnissen lediglich **repressiv** gewährleistet wird, müssen Unternehmen deren präventiven Schutz selbst herbeiführen. Industriespionage kann von Unternehmen durch die **Einhaltung eigener IT-Sicherheitspflichten** zwar nicht immer verhindert, ein **Angriffsrisiko** aber zumindest gesteuert bzw. **minimiert** werden. Wollen Unternehmen den Wert der eigenen Geschäftsgeheimnisse erhalten, sollten sie alle zumutbaren Mittel daran setzen, deren Offenlegung zu vermeiden. Dazu bieten umfangreiche inner- wie außerbetriebliche IT-Sicherheitskonzepte, ergänzt durch klassischere Hilfsmittel wie etwa vertragliche Geheimhaltungsvereinbarungen, den bestmöglichen Weg.[8] Eine etwa durch fehlende IT-Sicherheit ermöglichte Offenlegung und **Verbreitung von Betriebs- und Geschäftsgeheimnissen** kann auch dazu führen, dass diese **keinem Geheimnisschutz** über die §§ 17 UWG **unterfallen**. Taugliche Tatobjekte dieser Straftaten sind nur solche Geheimnisse, die nicht offenkundig – d.h. weder allgemein bekannt noch leicht zugänglich – sind.[9] So liegt ein schutzfähiges Geheimnis zumindest dann nicht (mehr) vor, wenn dessen Veröffentlichung in

1 *Brammsen*, ZIP 2016, 2193, 2193 f. m.w.N.
2 Siehe etwa die Beispiele bei *Brammsen*, ZIP 2016, 2193, 2194 f.
3 *Brammsen*, ZIP 2016, 2193, 2197.
4 *Köhler* in Köhler/Bornkamm, UWG, § 17 Rz. 2.
5 *Köhler* in Köhler/Bornkamm, UWG, Vorbem. §§ 17-19 Rz. 7.
6 *Köhler* in Köhler/Bornkamm, UWG, Vorbem. §§ 17-19 Rz. 7.
7 *Köhler* in Köhler/Bornkamm, UWG, § 17 Rz. 53.
8 So auch *Brammsen*, ZIP 2016, 2193, 2201 m.w.N.
9 Dazu eingehend *Köhler* in Köhler/Bornkamm, UWG, § 17 Rz. 6 ff.

allgemein zugänglichen Medien stattgefunden hat, wie etwa in (Fach-)Zeitschriften und Büchern, im Internet oder in Datenbanken.[1]

119 Unternehmen sollten sich in diesem Bereich auf **künftige Rechtsänderungen** einstellen. Bis zum 9.6.2018 müssen die Mitgliedstaaten der EU die **Geheimnisschutz-Richtlinie**[2] in nationales Recht umsetzen. Diese führt in der EU nicht nur einen einheitlichen Geheimnisbegriff ein, der die Problematik um die Bestimmung tauglicher Straftatgegenstände grundsätzlich hinfällig machen wird, sondern wird auch zu einer Anpassung der Sanktions- und Ausgleichsansprüche von Unternehmen führen, die zum Opfer einer Betriebsspionage geworden sind.[3] **Geschützte Informationen** sind nach Art. 2 Abs. 1 Geheimnisschutz-Richtlinie solche, die angemessenen **Geheimhaltungsmaßnahmen unterliegen**, innerhalb des Betriebs weder allgemein bekannt noch ohne weiteres zugänglich sind und aufgrund ihrer Geheimhaltung eine kommerziellen Wert besitzen.

2. IT-Sicherheitsdefizite als Rechtsbruch

120 Die **Verletzung eigener IT-Sicherheitspflichten** kann für das Unternehmen selbst **wettbewerbsrechtliche Relevanz** entfalten. Dafür bietet insbesondere § 3a UWG die Grundlage.

§ 3a UWG – Rechtsbruch

Unlauter handelt, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.

121 § 3a UWG ist eine Transformationsnorm, welche die Voraussetzungen normiert, unter denen der **Verstoß** gegen eine **gesetzliche Vorschrift außerhalb des Wettbewerbsrechts** als unlautere geschäftliche Handlung zu beurteilen ist.[4] Dies ist nicht bei jedem Gesetzesverstoß der Fall, der Auswirkungen auf den Wettbewerb haben kann.[5] Vielmehr muss die verletzte Rechtsvorschrift **zumindest auch dazu bestimmt** sein, **im Interesse der Verbraucher, Mitbewerber und sonstigen Marktteilnehmer** das **Marktverhalten zu regeln**.[6] Ob Vorschriften des Rechts der IT-Sicherheit als interessenschützende Markverhaltensregelungen anzusehen sind, lässt sich nur anhand des konkreten Charakters der relevanten Verpflichtungen bestimmen. Die pauschalisierende Aussage, dass IT-Sicherheitsrecht marktverhaltensregelnd ist, lässt sich nicht treffen.

a) IT-sicherheitsrechtliche Vorschriften als Marktverhaltensregelungen

122 Eine Vorschrift regelt das Marktverhalten, sofern sie das Anbieten und Nachfragen von Waren und Dienstleistungen, die Geschäftsanbahnung oder den Abschluss und die Durchführung

1 *Köhler* in Köhler/Bornkamm, UWG, § 17 Rz. 7 m.w.N.
2 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8.6.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.
3 Siehe dazu etwa *Ann*, GRUR-Prax. 2016, 465, 465 ff.
4 *Ohly* in Ohly/Sosnitza, UWG, § 3a Rz. 1.
5 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.6.
6 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.6, 1.61.

von Verträgen Handlungs- oder Unterlassungspflichten unterwirft.[1] Den Gegensatz dazu bilden Vorschriften über Verhaltensweisen, die der Betätigung auf dem Markt vorangehen oder nachfolgen, wie z.B. die Produktion, Forschung und Entwicklung.[2] Von hoher Praxisrelevanz sind dabei **Marktzutrittsregelungen**, bei denen Verstöße **keine wettbewerbsrechtlichen Folgen** nach sich ziehen. Dabei handelt es sich um solche Normen, die Personen den Marktzutritt aus Gründen verwehren oder bestimmten Bedingungen unterwerfen, die nichts mit deren **Art und Weise des Agierens am Markt** zu tun haben, sondern z.B. dem Schutz bestimmter Personen oder der Festlegung von Rahmenbedingungen des Wettbewerbs dienen.[3] Die Abgrenzung von Marktverhaltens- und -zutrittsregelungen wird allerdings dadurch erschwert, dass **Normen häufig** einen **Doppelcharakter** besitzen. Regeln die Vorschriften zumindest auch das Marktverhalten, kann ein Verstoß nach § 3a UWG wettbewerbsrechtliche Konsequenzen nach sich ziehen.[4]

Von einer Doppelfunktion kann nach der Rechtsprechung in der Regel ausgegangen werden, 123
wenn eine Betätigung am Markt einer öffentlich-rechtlichen Erlaubnis unterliegt bzw. die betreffende Norm gleichzeitig im Interesse der Marktteilnehmer – insbesondere der Verbraucher – eine **bestimmte Qualität, Sicherheit oder Unbedenklichkeit der angebotenen Waren** oder Dienstleistungen sicherstellen will.[5] IT-Sicherheitsverstöße eines Unternehmens können, wie bereits gezeigt (s. Rz. 12 ff.), nicht nur negative Folgen für das Unternehmen selbst, sondern auch für dessen Kunden und Geschäftspartner – also andere Marktteilnehmer – haben. Damit liegt es auf den ersten Blick nahe, dass das IT-Sicherheitsrecht bestimmte Standards schafft, die zumindest auch die Marktteilnehmer vor IT-Risiken schützen sollen. Wie bereits gezeigt (s. Rz. 87 ff.), können Kunden bspw. beim Erwerb von IT-Produkten oder der Inanspruchnahme IT-basierter Dienste einen bestimmten Sicherheitsstandard und damit eine bestimmte Qualität erwarten. Eine **pauschalisierende Klassifizierung** von IT-Sicherheitsvorschriften als Marktverhaltensregelungen ist dennoch **nicht möglich**, sondern muss immer anhand der verletzten Einzelnorm bestimmt werden. Es ist entscheidend, ob die IT-Sicherheitspflicht (auch) der Förderung des Unternehmensabsatzes dient, auf die Marktteilnehmer einwirkt und deren Schutz bezweckt.[6] Nicht immer kann zweifelsfrei vom Vorliegen aller drei Voraussetzungen ausgegangen werden.

aa) Datenschutzrecht

Als Marktverhaltensregelungen kommen insbesondere datenschutzrechtliche Vorgaben in Be- 124
tracht. In den ErwGr. 2, 7 der im Mai 2018 in Kraft tretenden Datenschutz-Grundverordnung heißt es, dass das Regelungswerk nicht nur dem Schutz der Rechte und Freiheiten natürlicher Personen, deren Daten verarbeitet werden, dient, sondern auch der Förderung der digitalen Wirtschaft. Damit weist das Datenschutzrecht grundsätzlich sowohl einen Marktbezug als auch einen Schutzcharakter auf. Daher kann es sich im Bereich des **Datenschutzrecht**s teil-

1 *Ohly* in Ohly/Sosnitza, UWG, § 3a Rz. 15; *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.62.
2 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.62.
3 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.76.
4 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.82 f.
5 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.83; BGH, Urt. v. 25.4.2002 – I ZR 250/00, GRUR 2002, 825, 826 = ZIP 2002, 1645; BGH, Urt. v. 2.6.2005 – I ZR 215/02, GRUR 2005, 875, 876; BGH, Urt. v. 15.1.2009 – I ZR 141/06, GRUR 2009, 881, 882 f.
6 *Byok*, BB 2017, 451, 453.

weise um Marktverhaltensregelungen handeln.[1] Beziehen sich datenschutzrechtliche Regelungen (auch) auf Unternehmenshandlungen, die personenbezogene Daten von Verbrauchern betreffen und kommerziellen Zwecken dienen, liegt die Annahme einer Marktverhaltensregel nahe.[2]

bb) Vorgaben des IT-Sicherheitsgesetzes und des NIS-Richtlinien-Umsetzungsgesetzes

125 Die Bestimmung des Vorliegens von sonstigen Marktverhaltensregelungen im Bereich der IT-Sicherheit fällt schwer, da bisher **Rechtsprechung** dazu **fehlt**, ob Verstöße gegen das Schutzgut der IT-Sicherheit einen Rechtsbruch gem. § 3a UWG darstellen können.[3] Die wettbewerbsrechtliche Relevanz von Verstößen gegen IT-Sicherheitsrecht unterliegt damit einer **großen Rechtsunsicherheit**. In Anbetracht der weitreichenden Folgen von IT-Sicherheitsverstößen für Unternehmen und ihre Kunden wird jedoch bereits **teilweise befürwortet**, dass zumindest **Teilbereiche des IT-Sicherheitsrechts als Marktverhaltensregelungen** zu qualifizieren sind. So wird ein Zusammenhang zwischen Informationssicherheit und Absatzförderung im Anwendungsbereich der **NIS-Richtlinie** (s. Rz. 346 f.) diskutiert, da die von den Regelungen betroffenen Betreiber wesentlicher Dienste, die der Bevölkerung Energie-, Finanz- oder andere Versorgungsleistungen erbringen, diese Dienste nur mit Hilfe sicherer IT-Systeme fortlaufend bereitstellen können und damit sowohl der Absatz als auch der Schutz der Nutzer vom IT-Sicherheitsstandard abhängen.[4] In Anbetracht dieser Diskussion sollten Unternehmen in jedem Fall künftige Rechtsentwicklungen beobachten. Die bestehende Tendenz der Verschärfung des IT-Sicherheitsrechts unterstreicht den Bedeutungsgewinn des Schutzguts IT-Sicherheit, so dass dessen Rolle für den Absatz am Markt im Wandel befindlich ist.

b) Wettbewerbsrechtliche Verletzungsfolgen

126 Künftige Rechtsentwicklungen, insbesondere auf Grundlage der Rechtsprechung, können zur Annahme eines Rechtsbruchs gem. § 3a UWG führen. In solchen Fällen führt die Verletzung von IT-Sicherheitsrecht potentiell zu empfindlichen wettbewerbsrechtlichen Konsequenzen. Dabei spielt das Risiko von auf Beseitigung und/oder Unterlassung gerichteten **Abmahnungen** für Wettbewerbsverstöße nach § 8 UWG eine eher untergeordnete Rolle, da mangelnde IT-Sicherheit im Unternehmen von außen kaum erkennbar oder gar nachweisbar ist.[5] Angesichts des hohen Schadenspotentials von IT-Sicherheitsmängeln (s. Rz. 12 ff.) dürften vor allem die übrigen Rechtsfolgen des UWG, insbesondere **Schadensersatz und Gewinnabschöpfung** gem. §§ 9, 10 UWG, von Relevanz sein.[6] Von noch höherer Relevanz dürften **nicht-materielle Folgen am Markt** sein, insbesondere der Reputationsverlust des Unternehmens gegenüber Kunden und Geschäftspartnern (s. Rz. 27 ff.).

1 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.74; *Ohly* in Ohly/Sosnitza, UWG, § 3a Rz. 79; *v. Jagow* in Harte-Bavendamm/Henning-Bodewig, UWG, § 3a Rz. 33 jeweils m.w.N.; s. zum Telemediendatenschutz *Gerlach*, CR 2015, 581, 581 ff.
2 *Köhler* in Köhler/Bornkamm, UWG, § 3a Rz. 1.74 m.w.N.
3 *Byok*, BB 2017, 451, 453.
4 *Byok*, BB 2017, 451, 453.
5 *Gerlach*, CR 2015, 581, 589; *Byok*, BB 2017, 451, 454.
6 *Byok*, BB 2017, 451, 454.

■ **Das Wesentliche in Kürze:**

– IT-Sicherheitsvorkehrungen sind zum präventiven Schutz eigener Betriebsgeheimnisse unerlässlich, da der wettbewerbsrechtliche Schutz lediglich repressiv wirkt, also wenn die Geheimnisse durch Offenlegung bereits ihren wirtschaftlichen Wert verloren haben.

– Die Verletzung der eigenen IT-Sicherheitspflichten durch Unternehmen stellt ggf. einen sanktionsfähigen Rechtsbruch gem. § 3a UWG dar. Diesbezüglich besteht aufgrund fehlender Kasuistik zu dieser Thematik allerdings ein hohes Maß an Rechtsunsicherheit.

IX. Praktische Umsetzung: IT-Sicherheitskonzept des Unternehmens

Während die Verantwortlichkeit der Unternehmensleitung für IT-Sicherheit grundsätzlich nicht vollständig delegiert werden kann, ist bei der **praktischen Umsetzung** der IT-Sicherheitspflichten die **Beteiligung verschiedener Akteure im Unternehmen** unerlässlich. Zur effektiven Risikoerkennung und -behandlung bieten sich in der Praxis verschiedene Instrumente an, wobei drei Möglichkeiten in diesem Abschnitt eine Darstellung erfahren werden. Zur Implementierung eines möglichst umfassenden IT-Sicherheitsstandards ist insbesondere eine **Kombination dieser Instrumente** in der Praxis angezeigt, die mittlerweile durchaus als marktüblich anzusehen ist.[1] 127

Unabhängig davon, welche Maßnahmen im Unternehmen zur Schaffung eines hinreichenden IT-Sicherheitsstandards zum Einsatz kommen, sind vor allem zwei Dinge unerlässlich: ein **klares IT-Sicherheitskonzept** und dessen **konsequente Umsetzung**. Unternehmen sollten daher zunächst prüfen, welche Sicherheitsmaßnahmen ihrer Gesellschafts- bzw. Konzernstruktur und vor allem ihren personellen und finanziellen Ressourcen am besten entsprechen und auf dieser Grundlage ein entsprechendes IT-Sicherheitskonzept ausarbeiten. Dabei müssen insbesondere der Umfang und die inhaltliche Ausprägung der auf das Unternehmen anwendbaren Rechtspflichten zur IT-Sicherheit (s. dazu insbesondere Rz. 290 ff.) Berücksichtigung finden. Über eine dauerhafte und effektive Umsetzung des entwickelten Konzepts muss die Einhaltung der IT-Sicherheitspflichten fortlaufend sichergestellt werden. 128

1. Benennung betrieblicher Beauftragter für IT-Sicherheit

Unternehmen sollten die Ernennung eines betrieblichen Beauftragten für IT-Sicherheit erwägen. Dieser soll im Wesentlichen die **Geschäftsleitung** bei der Wahrnehmung ihrer IT-Sicherheitspflichten **beraten und unterstützen**.[2] Die dabei anfallenden Verpflichtungen in Bezug auf die Informations-, Daten- und IT-Sicherheit werden auf verschiedene Rollen im Unternehmen verteilt, so dass grundsätzlich die Benennung **verschiedener betrieblicher Beauftragter mit Bezug zur IT-Sicherheit** in Betracht kommt. 129

Unter den verschiedenen betrieblichen Beauftragten **spielt der IT-Sicherheitsbeauftragte die wesentliche Rolle hinsichtlich der technischen Sicherheit** der IT-Infrastruktur des Unter- 130

1 *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rz. 217.

2 Vgl. dazu BSI, IT-Sicherheitsbeauftragter, S. 1, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/07itsibe_pdf.pdf?__blob=publicationFile, zuletzt aufgerufen am 12.1.2018.

nehmens.[1] Grundsätzlich existieren jedoch weder eine gesetzliche Pflicht noch gesetzliche Vorgaben zur Einrichtung und Stellung von IT-Sicherheitsbeauftragten.[2]

Ausnahme: Gesetzliche Pflicht zur Benennung eines IT-Sicherheitsbeauftragten

In folgenden Fällen ist die Benennung eines IT-Sicherheitsbeauftragten gesetzlich vorgeschrieben:

- gem. § 109 TKG für Telekommunikationsanbieter (s. Rz. 429);
- gem. § 11 Abs. 1a EnWG für Betreiber von Energieversorgungsnetzen (s. Rz. 452).

131 Am Fehlen einer allgemeinen Rechtspflicht zur Benennung des IT-Sicherheitsbeauftragten wird ein besonders starker Unterschied zum Datenschutzrecht deutlich (s. zu Einzelheiten Rz. 290 ff.), durch welches Unternehmen gem. Art. 37 ff. DSGVO sowie § 38 BDSG-neu zur Benennung eines Datenschutzbeauftragten, der eine vergleichbare Funktion erfüllt, verpflichtet werden. Allerdings lässt sich ggf. **mittelbar** aus der Pflicht der Gesellschaftsorgane zur Erkennung und Abwehr von IT-Risiken (s. Rz. 32 ff.) eine **Pflicht zur Ernennung** des IT-Sicherheitsbeauftragten und anderer Beauftragter, deren Aufgaben Bezug zur IT-Sicherheit aufweisen, ablesen: Fie „übliche Sorgfalt", die die Geschäftsleitung bei der Erfüllung ihrer Aufgaben walten lassen muss, wird von der Rechtsprechung regelmäßig anhand von etablierten Marktstandards beurteilt, wobei sich die Benennung von IT-Sicherheitsbeauftragten bereits als marktüblich bezeichnen lässt.[3] Zumindest von Unternehmen ab einer gewissen Größe kann damit die Benennung eines IT-Sicherheitsbeauftragten regelmäßig erwartet werden. Aufgaben, Funktion und Stellung eines IT-Sicherheitsbeauftragten können bspw. mehr oder weniger stark an diejenigen eines Datenschutzbeauftragten i.S.d. Art. 37 ff. DSGVO (s. Rz. 329 ff.) angelehnt werden.[4] Ob die Aufgaben von einer Einzelperson, einer Abteilung im Unternehmen oder nur in Teilzeit ausgeübt werden, ist von der Größe des Unternehmens, den vorhandenen Ressourcen und dem angestrebten IT-Sicherheitsniveau abhängig. Die **konkrete Ausgestaltung** dieser Position – wie auch anderer Positionen mit IT-Sicherheitsbezug – liegt damit im **Ermessen des Unternehmens**.[5]

a) Abgrenzung verschiedener betrieblicher Beauftragter

132 Während der **IT-Sicherheitsbeauftragte** maßgeblich Funktionen bzgl. der **technischen Sicherung der IT-Infrastruktur** des Unternehmens erfüllt, kann es zu einer **Überschneidung mit anderen unternehmensinternen Rollen** kommen. Damit wird eine Abgrenzung der verschiedenen betrieblichen Beauftragten erforderlich, deren **Aufgaben einen Bezug zur IT-Sicherheit aufweisen**. Nicht alle dieser Positionen werden stets im Unternehmen vorgesehen sein. So ist deren **Schaffung teilweise rechtlich vorgeschrieben** und teilweise zur Abwehr von Risiken vom Unternehmen (s. Rz. 32 ff.) angezeigt:[6]

1 *Müller* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. (im Erscheinen), E. I. 3.
2 *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rz. 251.
3 Zu Einzelheiten *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rz. 252.
4 Siehe dazu ausführlich *Voigt/von dem Bussche*, Handbuch DSGVO, 1. Aufl. (im Erscheinen), Teil 3.6; sowie mit einer Gegenüberstellung möglicher Aufgaben *Müller* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. (im Erscheinen), E. I.4.
5 *Schmidl* in Hauschka/Moosmayer/Lösler, Corporate Compliance, § 28 Rz. 253.
6 Siehe dazu ausführlich *Müller* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. (im Erscheinen), E. I.3.

Position	**Rechtspflicht zur Benennung**	**Funktionen**
IT-Sicherheitsbeauftragter	Grds. nein, Ausnahmen: § 109 TKG, § 11 Abs. 1a EnWG	– Gewährleistet v.a. technische Sicherheit der IT-Infrastruktur – Unterstützung der Geschäftsleitung bei der Einhaltung der IT-Sicherheitspflichten – Erstellung, Integration und Pflege von IT-Sicherheitskonzept und Betriebsrichtlinien, Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb
Datenschutzbeauftragter	Art. 37 ff. DSGVO, § 38 BDSG-neu	– Gesetzlich geregelte Funktionen (s. Rz. 329 ff.) – Wichtige Rolle zur Gewährleistung des Datenschutzes im Unternehmen, einschließlich Datensicherheit
Zentrales Risikomanagement	Ggf. §§ 76, 93 AktG	– Zentrale Stelle zur Entgegennahme von Risikomeldungen aus den verschiedenen Unternehmensteilen (auch: IT-Risiken) – Steuerung unternehmerischer Risiken
IT-Risikobeauftragter	Ggf. §§ 76, 93 AktG	– Erkennung, Bewertung und Management von IT-Risiken – Durchführung entsprechender Risikoanalysen in Zusammenarbeit mit IT-Sicherheits- und/oder Datenschutzbeauftragtem – Beteiligung an Konzeption und Umsetzung des IT-Risikomanagementsystems
Informationssicherheitsbeauftragter (Chief Information Security Officer, CISO)	Ggf. §§ 76, 93 AktG	– Definiert IT-Sicherheitspolitik des Unternehmens anhand der Unternehmensstrategie – Für IT-Sicherheitsrahmen im Unternehmen strategisch verantwortlich – Ausschließlich auditive Tätigkeiten: Überwachung der verantwortlichen Abteilungen und Beauftragten
Compliance-Officer	Ggf. §§ 76, 93 AktG	– Überwacht die Einhaltung aller Compliance-Vorgaben im Unternehmen (Gesetze, Organisationsgrundsätze, Unternehmensrichtlinien …)

Einleitung

I. Einführung

Informationstechnologie ist aus dem Unternehmensalltag nicht mehr wegzudenken und **dominiert alle Unternehmensbereiche** – von der Kommunikation bis hin zur Produktherstellung oder Buchhaltung. IT-Systeme ermöglichen aber nicht nur eine effizientere Organisation und Geschäftsabwicklung, sondern eröffnen gleichzeitig ein hohes Risikopotential. So ist die IT-Infrastruktur eines Unternehmens nicht nur Bedrohungen von außen, z.B. durch Viren oder gezielte Cyber-Angriffe ausgesetzt, sondern auch solchen von innen durch die Mitarbeiter des Unternehmens, z.B. durch Fehler im Umgang mit der Technik oder gar durch eine Mitnahme vertraulicher Dateien aus dem Unternehmen.[1] Mit der zunehmenden Vernetzung von Gegenständen steigt auch im Machine-to-Machine-Bereich das Risikopotential. Schon heute kommen in Unternehmen viele Geräte zum Einsatz, die über Schnittstellen an das Internet oder Firmennetzwerk angeschlossen sind und automatisch kommunizieren. Diese übernehmen Bereiche, welche in der Vergangenheit weitestgehend der menschlichen Kommunikation vorbehalten waren.[2] Die **Sicherheit der eigenen IT-Systeme** bildet aus diesen Gründen ein **zentrales Thema** für Unternehmen. 1

IT-Sicherheit beschreibt den **Zustand der Sicherheit** vor Gefahren oder Schäden aller Art im Hinblick auf die IT-Infrastruktur.[3] Zur Umsetzung kommen verschiedene technische, organisatorische oder rechtliche Maßnahmen in Betracht. Dabei besteht nicht nur ein praktisches Bedürfnis nach IT-Sicherheit: ein möglichst hohes Sicherheitsniveau liegt im **Eigeninteresse des Unternehmens**, um die eigenen Geschäftsabläufe und Betriebsgeheimnisse zu schützen. Unternehmen, gleich welcher Branche, trifft überdies eine diesbezügliche Rechtspflicht. Der Umfang dieser Pflicht ist jedoch schwer zu erfassen. Ein **„Recht der IT-Sicherheit"** im eigentlichen Sinn gibt es nicht.[4] IT-Sicherheitspflichten ergeben sich aus Gesetzen diverser Rechtsgebiete. Dabei handelt es sich teilweise um branchenspezifische oder auf bestimmte Technologien bezogene Normen, so dass sich ein genereller Sicherheitsstandard nicht ohne weiteres identifizieren lässt. 2

Der Gesetzgeber hat die Bedeutung hinreichender Sicherheitsstandards erkannt und wird auf diesem Gebiet zunehmend tätig. Besonders die **Rechtsetzung durch die Europäische Union** spielt dabei eine wichtige Rolle. Teils durch neue Gesetze geschaffene **Haftungsansprüche** nehmen Unternehmen immer stärker in die Pflicht – ein Ende dieser gegenwärtigen Rechtsentwicklung ist nicht absehbar.[5] So veröffentlichte die **Europäische Kommission** gemeinsam mit dem Hohen Vertreter der EU für Außen- und Sicherheitspolitik im September 2017 eine Mitteilung bzgl. der nächsten Schritte zur **Stärkung der Maßnahmen gegen Cyber-Angriffe**.[6] Neben einer beabsichtigten Reform zur Stärkung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und der Unterstützung der Mitgliedstaaten bei der vollständi- 3

1 *Conrad*/*Huppertz* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 1.
2 *Grünwald*/*Nüßing*, MMR 2015, 378, 378.
3 *Roth*/*Schneider*, ITRB 2005, 19, 19; *Conrad*/*Huppertz* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 8.
4 *Conrad*/*Huppertz* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 9.
5 *Conrad*/*Huppertz* in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, § 33 Rz. 3, 7.
6 Europäische Kommission, Joint Communication JOIN(2017) 450 final, abrufbar in englischer Sprache unter: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:52017JC0450, zuletzt aufgerufen am 12.1.2018.

gen und effektiven Umsetzung der NIS-Richtlinie (s. Rz. 342 ff.) möchte die EU auch Unternehmen mit präventiven Hilfestellungen zur proaktiven Umsetzung und Aufrechterhaltung von IT-Sicherheit anhalten.[1] IT-Sicherheit bildet damit aus wirtschaftlicher wie rechtlicher Sicht ein zentrales Thema für Unternehmen.

II. Checkliste der wichtigsten IT-sicherheitsrechtlichen Pflichten

4 Dieses Handbuch schafft einen Überblick zum bestehenden Rechtsrahmen und legt das sich daraus ergebende **Pflichtenprogramm aus Unternehmenssicht** dar. Zu diesem Zweck umfasst dieses Werk als Abschluss der verschiedenen Kapitel kurze übersichtsartige Zusammenfassungen („Das Wesentliche in Kürze"). Die **wesentlichen IT-Sicherheitspflichten** lassen sich **im Rahmen einer „Checkliste" wie folgt systematisieren**:

5 ☐ Jedes Unternehmen treffen nach allgemeinen Rechtsvorschriften (überwiegend aus dem Handels- und Gesellschaftsrecht) **grundlegende IT-Sicherheitspflichten**, die insofern gewissermaßen den **branchen- und sektorübergreifenden „IT-Sicherheits-Mindeststandard"** bilden (s. Rz. 9 ff.). Die **Umsetzung** der IT-Sicherheit im Unternehmen fällt dabei **in den Verantwortungsbereich der Geschäftsleitung** (s. Rz. 32 ff.). Es bestehen folgende grundlegende IT-Sicherheitspflichten:

- Pflicht zur Einhaltung der anwendbaren IT-sicherheitsrechtlichen Vorschriften, die insbesondere branchen- oder sektorspezifischer Natur sein können, sog. **IT-Compliance** (s. Rz. 50 ff.);
- Pflicht zur Einrichtung eines Systems zur Früherkennung und Überwachung bestandsgefährdender IT-Sicherheitsrisiken (s. Rz. 40 ff.);
- Pflicht zur **Überwachung und Steuerung aller IT-Sicherheitsrisiken** (s. Rz. 50 ff.); zur praktischen Umsetzung empfiehlt sich in vielen Fällen die Einrichtung eines **IT-Risikomanagementsystems** (s. Rz. 149 ff.);
- eine EDV-gestützte **Buchführung** macht die **Einrichtung eines Internen Kontrollsystems** mit Steuerungs- und Überwachungselementen erforderlich, um eine ordnungsgemäße Buchführung zu gewährleisten (s. Rz. 61 ff.);
- zum präventiven **Schutz eigener Geschäftsgeheimnisse** müssen Unternehmen **IT-Sicherheitsvorkehrungen** treffen, da der wettbewerbsrechtliche Schutz letztlich nur repressiv nach Offenlegung der Geheimnisse wirkt (s. Rz. 115 ff.);
- die unternehmerischen IT-Sicherheitspflichten bilden bei Verträgen mit Dritten regelmäßig einen Bestandteil des vertraglichen Pflichtenprogramms (s. Rz. 87 ff.).

6 ☐ Nahezu alle Unternehmen verarbeiten auf irgendeine Weise personenbezogene Daten (z.B. von Mitarbeitern und Kunden), so dass **bei der Verarbeitung dieser Daten datenschutzrechtliche IT-Sicherheitsvorgaben** einzuhalten sind (s. Rz. 290 ff.):

- Das Ergreifen **technischer und organisatorischer Maßnahmen** zum Schutz der personenbezogenen Daten während ihrer Verarbeitung (s. Rz. 313 ff.);

1 Vgl. auch Hunton & Williams, https://www.huntonprivacyblog.com/2017/09/13/eu-publishes-measures-strengthen-eu-cybersecurity-structures-capabilities/, zuletzt aufgerufen am 12.1.2018.

- das **Umsetzen präventiver Datenschutzmaßnahmen** im Vorfeld der Verarbeitung, indem neue Produkte und Dienste möglichst datenschutzfreundlich eingestellt werden (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), (s. Rz. 321 ff.);
- die Benennung eines **Datenschutzbeauftragten** (s. Rz. 329 ff.);
- das Führen eines **Verzeichnisses der Datenverarbeitungstätigkeiten** zu Dokumentationszwecken (s. Rz. 326 f.);
- die **Durchführung einer Datenschutz-Folgenabschätzung** zur Ermittlung des Schutzbedarfs bei risikoreichen Verarbeitungsvorgängen (s. Rz. 328);
- kommt es zu **Datenschutzverletzungen**, werden regelmäßig **Meldepflichten** des Unternehmens ausgelöst (s. Rz. 332 ff.).

☐ Ergänzend dazu müssen Unternehmen **zur Erreichung einer IT-Compliance auf sie anwendbare branchen- und sektorspezifische IT-Sicherheitsvorgaben erfüllen**. Diese erfordern regelmäßig die Erreichung eines erhöhten IT-Sicherheitsstandards: 7

- Unternehmen, die als **Versorgungsdienstleister** in bestimmten Sektoren regelmäßig mehr als 500.000 Personen versorgen, unterfallen als KRITIS-Betreiber dem Pflichtenprogramm des BSIG (s. Rz. 352 ff.). Sie müssen:
  - angemessene technische und organisatorische Sicherheitsvorkehrungen zum Schutz der KRITIS-Anlagen treffen und dies regelmäßig nachweisen;
  - eine Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik einrichten;
  - erhebliche Störungen der IT-Systeme an das Bundesamt melden.
- Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Cloud-Computing-Diensten treffen als **„Anbieter digitaler Dienste"** mit den vorbeschriebenen Pflichten vergleichbare, eigene Pflichten aus dem BSIG (s. Rz. 386 ff.).
- **Telemediendiensteanbieter** müssen gem. § 13 Abs. 7 TMG technische und organisatorische Vorkehrungen treffen, um ihre Dienste gegen Datenschutzverletzungen, Störungen und unerlaubten Zugriff durch Dritte zu schützen (s. Rz. 409 ff.).
- Unternehmen, die ganz oder teilweise geschäftsmäßig **öffentlich zugängliche Telekommunikationsdienste** erbringen, müssen die im TKG vorgesehenen IT-Sicherheitspflichten erfüllen (s. Rz. 422 ff.):
  - Ergreifen technischer und organisatorischer Vorkehrungen zur Verhinderung erheblicher störungsbedingter Beeinträchtigungen der Dienste;
  - Benennung eines Telekommunikationssicherheitsbeauftragten;
  - Erstellung eines Sicherheitskonzepts;
  - Meldung von Beeinträchtigungen der Dienste und über Datenschutzverletzungen.
- Unternehmen, die **Gas-, Elektrizitäts-, Übertragungsnetze oder Energieanlagen betreiben**, müssen auf Grundlage des EnWG einen Katalog mit Sicherheitsanforderungen einhalten sowie erhebliche Störungen melden (s. Rz. 449 ff.).

- **Unternehmen, die Kernbrennstoffe aufbewahren oder verwenden**, unterliegen IT-Sicherheitspflichten auf Grundlage des AtG. Eine Genehmigung zur Verfolgung entsprechender Wirtschaftstätigkeiten erfordert den Nachweis angemessener IT-Sicherheitsvorkehrungen. Genehmigungsinhaber müssen IT-Störungen unverzüglich melden (s. Rz. 460 ff.).
- **Unternehmen, die zum Betrieb oder zur Nutzung der Telematikinfrastruktur** nach dem SGB V zugelassen werden möchten, müssen den Nachweis eines angemessenen IT-Sicherheitsstandards erbringen. Wurden sie zugelassen, müssen sie auftretende Störungen unverzüglich melden (s. Rz. 466 ff.).
- **Versicherungsdienstleister** sind zur Einführung eines allgemeinen Risikomanagementsystems auf Grundlage des VAG verpflichtet (s. Rz. 472 ff.).
- **Kredit- und Finanzdienstleistungsinstitute** müssen hohe IT-Sicherheitsvorkehrungen treffen. Dies umfasst (s. Rz. 478 ff.):
  - die Gewährleistung eines wirksamen Risikomanagements;
  - die Einführung eines angemessenen Notfallkonzepts für IT-Systeme;
  - das Vorhandensein einer angemessenen technisch-organisatorischen Ausstattung.
  - Hinzu kommen tätigkeitsbezogene IT-Sicherheitspflichten im Onlinezahlungsverkehr und bei der Erbringung von Wertpapierdienstleistungen.

8 ☐ Kommt es im Unternehmen zu **IT-Sicherheitsdefiziten, droht stets ein erhebliches Haftungsrisiko**, wobei die Haftungsverhältnisse alle für entsprechende Defizite verantwortlichen Akteure und betroffenen Personen umfassen. Eine entsprechende Darstellung der Haftungsgrundlagen erfolgt in Rz. 197 ff. Während die Haftung innerhalb des Unternehmens letztlich die Geschäftsleitung trifft, droht **bei Schäden Dritter durch IT-Sicherheitsdefizite überwiegend eine Inanspruchnahme des Unternehmens** selbst. Die Verletzung auf das Unternehmen anwendbarer spezialgesetzlicher IT-Sicherheitsvorgaben führt regelmäßig zur **Verwirklichung spezialgesetzlicher Ordnungswidrigkeiten** mit entsprechenden Haftungsfolgen.