Persönliche Verantwortung und Haftungsrisiken von IT-Verantwortlichen – Zivilrechtliche Aspekte

Jan Pohle

Kanzlei Taylor Wessing
Königsallee 92a, 40212 Düsseldorf
j.pohle@taylorwessing.com

Einleitung

IT-Sicherheit ist ein in vielen privatwirtschaftlichen Unternehmen und sonstigen Einrichtungen viel beachtetes aber kaum bewältigtes Thema.

Jüngst hat die Studie „IT-Security 2004“ von Mummert Consulting ergeben, dass fast jeder zweite Verantwortliche in Unternehmen nicht weiß, wie häufig im vergangenen Kalenderjahr IT-Sicherheitsverstöße in seinem Unternehmen auftraten. Dabei sind es keinesfalls ausschließlich oder auch nur überwiegend externe Angriffe auf die IT-Infrastruktur eines Unternehmens. Die weit überwiegende Anzahl der sicherheitsrelevanten Vorfälle betreffen vorsätzliche oder fahrlässige Angriffe auf die IT-Infrastruktur eines Unternehmens aus dem Unternehmen selbst.

Die Problematik betrifft dabei keineswegs nur privatwirtschaftliche Unternehmen, die öffentliche Verwaltung ist nicht weniger betroffen. Der Bundesrechnungshof kommt nach einer Überprüfung der Computersysteme in Behörden der Bundesverwaltung in 2004 in einem Bericht zu dem Schluss, dass in Computern der Bundesverwaltung die Sicherheit vertraulicher Daten schlicht nicht gewährleistet sei. Nicht nur kann die Kenntnisnahme hochsensibler Daten durch Unbefugte als wahrscheinlich angesehen werden, auch die Datenvernichtung ist ungenügend organisiert.

Diese Befunde spiegeln die technisch-organisatorische Lückenhaftigkeit und Unzuverlässigkeit der in der Privatwirtschaft und der öffentlichen Verwaltung zur Zeit betriebenen IT-Infrastrukturen ebenso anschaulich wie erschreckend. Hinzu tritt in aller Regel noch eine weit verbreitete Unkenntnis der rechtlichen Rahmenbedingungen und der Konsequenzen Ihrer Nichtbeachtung. Auch diese Feststellung ist der jüngst veröffentlichten Studie „IT-Security 2004“ vom Mummert Consulting entnommen. Sie wird in der Praxis täglich bestätigt, das Thema IT-Sicherheit und deren Gewährleistung aus rechtlicher Sicht stößt in aller Regel auf ratlose Gesichter. Dabei existieren quer durch unsere Rechtsordnung zahlreiche Pflichten, die im Einzelnen unmittelbar oder mittelbar bestimmen, welche Anforderungen zur Sicherstellung von IT-Sicherheit zu erfüllen sind. Darüber hinaus beinhaltet unser Rechtssystem ein differenziertes System von Sanktionen, die greifen, wenn eben diese rechtlichen Rahmenbedingungen und Anforderungen an die Gewährleistung von IT-Sicherheit im Einzelfall nicht erfüllt werden. Im Einzelnen handelt es sich – entsprechend der klassischen juristischen Dreiteilung – um öffentlich-rechtliche Sanktionen, beispielsweise im Gewerberecht, strafrechtliche Sanktionen vom Bußgeld hin bis zur Freiheitsstrafe oder aber zivilrechtliche Rechtsfolgen, hier insbesondere Schadenersatzverpflichtungen.

Im folgenden sollen und werden die wesentlichen, insbesondere aus der Sicht des Zivilrechts maßgeblichen Voraussetzungen und Anforderungen an die Gewährleistung von IT-Sicherheit kursorisch dargestellt. Hiervon ausgehend wird die Frage der Haftung des Unternehmens und der persönlichen Verantwortlichkeit, d. h. die Haftung von IT-Verantwortlichen in Unternehmen der Privatwirtschaft, im Grundsatz eingegangen werden.

1 Was ist IT-Sicherheit?

Bevor auf die einzelnen rechtlichen Regelungen zur IT-Sicherheit dargestellt werden, muss der Begriff der IT-Sicherheit aus rechtlicher Sicht beleuchtet werden, um einen Ausgangspunkt dafür zu umreißen, was Gegenstand der rechtlichen Regelung zu diesem Themenkomplex ist.

In rechtlicher Hinsicht lässt sich der Begriff der IT-Sicherheit ausgehend von der Legaldefinition des § 2 Abs. 2 des Gesetzes über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG) begreifen, der wie folgt lautet:

> *Sicherheit in der Informationstechnik bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen*
>
> 1. in informationstechnischen Systemen oder Komponenten oder
> 2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.

Hiervon ausgehend hat sich eine Kategorisierung von Schutzzielen der IT-Sicherheit herausgebildet.

Schutzziel Verfügbarkeit

Verfügbarkeit bezeichnet einen Zustand, in dem die Funktionalität des IT-Systems gewährleistet ist. Informationen und Systeme sollen stets verfügbar sein und bestimmte, fest definierte Antwortzeiten bzw. Reaktionszeiten einhalten. Verfügbarkeit von IT-Systemen meint insbesondere auch den Schutz insbesondere vor Informationsverlust und Informationszerstörung.[1]

Schutzziel Integrität

Das Schutzziel der Unversehrtheit meint den Schutz vor jedweder ungewollter und unautorisierter Informationsveränderung. Ein IT-System sollte so beschaffen sein, dass jede Veränderung offensichtlich wird. Der Schutz bezieht sich jedoch nicht nur auf ein System als solches, sondern auch auf einzelne verarbeitete Daten, d. h. der Vollständigkeit und

[1] Holznagel, Recht der IT-Sicherheit, München 2003, Rz. 6; Heckmann, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, Vortrag anlässlich der 3. Bayerischen IT-Rechtstags 2004, S. 4.

Korrektheit. Der Gewährleistung dieses Schutzziels dient beispielsweise die elektronische Signatur.[2]

Schutzziel Vertraulichkeit

Die Gewährleistung von Vertraulichkeit von Informationen dient dem Schutz vor unbefugter Kenntnisnahme gespeicherter Informationen durch Dritte. IT-Systeme sollen so konstruiert und ausgelegt sein, dass fest definierte Zugangs- und Zugriffsrechte den Zugriff auf Informationen nur durch befugte Personen gewährleisten.

Schutzziel Authentizität

Der Schutzaspekt der Authentizität hat im Wesentlichen die Sicherstellung von Verbindlichkeit elektronischer Kommunikation zum Ziel. Im Rahmen einer Kommunikationsbeziehung muss ferner sichergestellt sein, dass die Identität der Kommunizierenden unverändert erhalten bleibt[3].

Schutzziel Zurechenbarkeit

Ähnlich wie das Schutzziel der Authentizität dient dasjenige der Zurechenbarkeit, der Verbindlichkeit und verlässlicher elektronischer Kommunikation. Daneben dient es jedoch auch der eindeutigen und verlässlichen Identifikation einer bestimmten Stelle oder Einheit, die bestimmte Informationen, insbesondere personenbezogene Daten, verarbeitet und speichert. Sicherzustellen ist, dass eine Information tatsächlich aus der angegebenen Quelle stammt und die Identität eines handelnden Benutzers feststeht. Diesem Ziel dienen u. a. Zutrittskontrollen durch Eingabe von ID oder PIN.[4]

Schutzziel informationelle Selbstbestimmung

Das mit Verfassungsrang ausgestattete Schutzziel informationellen Selbstbestimmung erfordert, dass in IT-Systemen sichergestellt ist, dass jede natürliche Person selbst darüber bestimmen kann, ob, wann, wo und in welchem Umfang Daten über sie erhoben, verarbeitet oder genutzt werden.[5]

Sicherlich ist zu konstantiieren, dass die Legaldefinition des § 2 Abs. 2 BSIG lediglich die Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit ausdrücklich aufführt. Gleichwohl zeigen die praktischen Notwendigkeiten und Bedürfnisse, dass der Begriff der IT-Sicherheit auch im rechtlichen Regelungskontext keinesfalls mit diesen Begrifflichkeiten und ihren Inhalten abschließend definiert ist. Wie die Informationstechnologie selbst ist auch der Begriff der IT-Sicherheit kein statischer, sondern ein sich stets dynamisch wandelnder. Dies hat unmittelbare Konsequenzen auch für die Definition und die inhaltliche Fassung des Begriffs der IT-Sicherheit im rechtlichen Regelungskontext.

[2] Holznagel, Recht der IT-Sicherheit, München 2003, Rz. 7; Heckmann, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, Vortrag anlässlich der 3. Bayerischen IT-Rechtstags 2004, S. 4.

[3] Holznagel, a.a.O., Rz. 9; Heckmann, a.a.O. S. 4f.

[4] Holznagel, a.a.O., Rz. 9; Heckmann, a.a.O., S. 5

[5] Holznagel, a.a.O., Rz. 12.

2 Wen betrifft IT Sicherheit im Unternehmen?

Liegt nun der Begriff der IT-Sicherheit fest, ist damit noch keine Aussage darüber getroffen, an welche Personen in einem Unternehmen diese Schutzziele primär gerichtet sind.

1. Aufsichtsrat

§ 111 Abs. 1 AktG legt fest, dass der Aufsichtsrat die dem Vorstand einer Aktiengesellschaft gem. § 67 ff. AktG obliegende Geschäftsführung der Gesellschaft zu überwachen hat. Zur Überwachungstätigkeit des Aufsichtsrates gehören dabei nicht nur Leitungsmaßnahmen des Vorstands, sondern auch wesentliche Einzelmaßnahmen. Der Pflichtenkreis des Aufsichtsrates in diesem Zusammenhang ist gesetzlich nicht konkret festgelegt, mittelbar folgen dessen Schwerpunkte jedoch aus den in § 90 Abs. 1 AktG geregelten Informationspflichten des Vorstandes gegenüber dem Aufsichtsrat. Schließlich mag man konstatieren, dass sich die Überwachungspflichten des Aufsichtsrates spiegelbildlich an den unmittelbaren Leitungsfunktionen des Vorstands orientieren, mithin der Aufsichtsrat nur insoweit zur Überwachung des Vorstandes hinsichtlich der Maßnahme der IT-Sicherheit verpflichtet ist, wenn und soweit der Vorstand des Unternehmens ebenfalls zur Gewährleistung der IT-Sicherheit verpflichtet ist.[6]

2. Operative Geschäftsführung, sonstige leitende Angestellte und Arbeitnehmer

Der Vorstand einer Aktiengesellschaft bzw. die Geschäftsführer einer GmbH haben als Ausprägung ihrer allgemeinen Leitungsfunktion für das Unternehmen gem. § 76 AktG bzw. § 43 GmbHG die im sonstigen Gesetzesrecht normierten zahlreichen Vorgaben zur IT-Sicherheit zu beachten.

Eine grundsätzliche Verantwortlichkeit von leitenden Angestellten unterhalb der primären Führungsebene und sonstiger Arbeitnehmer ergibt sich bereits aus dem arbeitsvertraglichen Verhältnis zum Unternehmen. Jedoch werden sich Verantwortlichkeiten und Pflichten insoweit nur dann konkretisieren lassen, wenn entsprechende unternehmensinterne bzw. arbeitsvertragliche Anweisungen existieren und darüber hinaus die in Rede stehenden Arbeitnehmer ausreichend fachlich qualifiziert, insbesondere geschult sind.

3. IT-Sicherheitsbeauftragter

Für unternehmensinterne IT-Sicherheitsbeauftragte gilt grundsätzlich nichts anderes als für Arbeitnehmer im Allgemeinen. Sie unterliegen aufgrund der bereits angesprochenen Weisungen, besonderen Qualifikationen und arbeitsvertraglichen Regelungen Besonderheiten nicht nur hinsichtlich ihrer organisatorischen Stellung, sondern auch ihrer rechtlichen Verantwortlichkeit.

Dies gilt im gleichen Maße prinzipiell für externe IT-Sicherheitsbeauftragte. Ihre Verantwortlichkeit folgt grundsätzlich aus dem zugrunde liegenden Vertragsverhältnis mit dem Unternehmen, konkretisiert um die jeweils vertraglich ausgestalteten Pflichten.

[6] Heckmann, a.a.O., S. 6.

4. Betrieblicher Datenschutzbeauftragter

Das zuvor zu Arbeitnehmern im Allgemeinen und zu IT-Sicherheitsbeauftragten im Besonderen gesagte gilt sinngemäß für in- bzw. externe betriebliche Datenschutzbeauftragte.

3 Rechtliche Anforderungen an IT-Verantwortliche

Wie bereits angesprochen findet sich in einer Vielzahl verschiedener Gesetze quer durch unser nationales Rechtssystem eine Vielzahl von Normen, die die rechtlichen Anforderungen an IT-Sicherheit und mithin auch an die IT-Verantwortlichen in Unternehmen näher ausgestalten.

1. Gesellschaftsrechtliche Vorgaben

Die einschlägigen Regelungen des Aktien- bzw. GmbH-Rechts weisen dem Vorstand bzw. der Geschäftsführung die allgemeine Leitungsfunktion für die Gesellschaft zu, §§ 76 AktG, 43 GmbHG. Zu den Pflichten der Unternehmungsleitung gehört die Etablierung eines angemessenen Risikomanagements. Diese zentrale rechtliche Verpflichtung ist mit Einführung des § 91 Abs. 2 AktG im Zuge des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTrag) konkretisiert worden. Diese Norm fordert von den Leitungsorganen der Gesellschaft ausdrücklich geeignete Maßnahmen zur Einrichtung eines Überwachungssystems zu ergreifen, um eine Früherkennung von Entwicklungen zu gewährleisten, die den Fortbestand der Gesellschaft gefährden können. Hierunter fallen die Sicherstellung bzw. Überwachung hinreichender IT-Sicherheit.[7]

Ergänzt werden diese allgemeinen gesetzlichen Vorgaben für das Bankenwesen durch die Regelung des § 25 a Kreditwesengesetz (KWG).

2. Elektronische Buchführung

Sofern ein Unternehmen, wie üblicherweise, auf eine elektronischen Buchführung zurückgreift, sind die Vorgaben der §§ 238 ff. HGB sowie die korrespondierenden Vorschriften der Abgabenordnung, insbesondere § 146 Abs. 5 AO, zu den Grundsätzen ordnungsgemäßen EDV-Buchführungssysteme (GoBS) sowie den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) zu beachten. Auch insofern statuieren die korrespondierenden gesellschaftsrechtlichen Regelungen zur Sicherstellung einer ordnungsgemäßen Buchführung im Unternehmen eine unmittelbare Verantwortung der Unternehmensleitung, § 91 Abs. 1 AktG, § 41 Abs. 1 GmbHG sowie §§ 34, 69, 140 ff. AO.

Hinzu kommt, dass bei börsennotierten Aktiengesellschaften Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses ggf. bei fehlenden Maßnahmen der IT-Sicherheit das Testat verweigern können. Sie sind verpflichtet zu prüfen, ob der Vorstand die erforderlichen Maßnahmen zur Errichtung eines Überwachungssystems getroffen hat und ob dieses tauglich ist.

[7] Roth/Schneider, IT-Sicherheit und Haftung, ITRB 2005, 19; Heckmann, a.a.O., S. 9.

3. Wirtschaftsverwaltungsrechtliche Vorgaben

Die wirtschaftsverwaltungsrechtlichen Vorgaben zur IT-Sicherheit sind mannigfaltiger Natur und sind für privatwirtschaftliche Unternehmen von zentraler Bedeutung..

Zu forderst ist hier an die Richtlinien zur Sicherung einer angemessenen Eigenkapitalausstattung im internationalen Bankenwesen (Basel II) zu denken. Jenseits des unmittelbaren wirtschaftsverwaltungsrechtlichen Hintergrunds hat Basel II einen entscheidenden ökonomischen Aspekt: Die Bonität des Unternehmens drückt sich stärker als bisher als kostenbestimmendes Element aus. Im Rahmen des insoweit durchzuführenden Ratings der Banken sind auch operationelle Risiken von Unternehmen zu berücksichtigen, namentlich die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten[8]. Man wird davon ausgehen können, dass die Nutzung von IT-Infrastrukturen insbesondere dann als ein solches operationelles Risiko eingestuft werden wird, wenn das Unternehmen existentiell auf die Nutzung dieser IT-Infrastrukturen angewiesen ist, was regelmäßig der Fall sein wird.

Weiterhin enthalten spezialgesetzliche Regelungen, wie § 109 des Telekommunikationsgesetzes (TKG), Vorgaben zur Sicherstellung technischer Schutzmaßnahmen. Nach § 109 Abs. 3 TKG haben Betreiber von Telekommunikationsanlagen einen Sicherheitsbeauftragten zu bestellen und ein Sicherheitskonzept zu erarbeiten.

Schließlich wird man die Sicherstellung und Gewährleistung von IT-Sicherheit als Obliegenheit eines Unternehmens auch im Rahmen des öffentlichen Vergaberechts qualifizieren können. Öffentliche Auftraggeber gehen verstärkt dazu über, bei IT-relevanten Aufträgen auch einen Nachweis über die IT-Sicherheit einzufordern. Dies gilt sowohl im Rahmen der Leistungsbeschreibung (§ 8 VOL/A) als auch im Rahmen der Angebotsbewertung (vgl. § 25 Nr. 2 VOL/A „Fachkunde, Leistungsfähigkeit, Zuverlässigkeit“).[9]

4. Datenschutzrecht

Das nationale Datenschutzrecht enthält detaillierte Regelungen, die unmittelbare Anforderungen an die IT-Sicherheit statuieren. Diese sind verteilt über die spezialgesetzlichen Materien des TKG bzw. des Teledienstdatenschutzgesetzes (TDDSG). Sie finden sich jedoch auch in der grundlegenden datenschutzrechtlichen Kodifikation, dem Bundesdatenschutzgesetz (BDSG). Ein wesentlicher Bestandteil des Datenschutzes ist die Datensicherheit im Sinne eines technisch organisatorischen Datenschutzes. Dessen Inhalte sind in der Anlage zu § 9 BDSG im Einzelnen aufgeführt und gesetzlich normiert.

5. Allgemeines Vertrags- und Deliktsrecht

Im unmittelbaren operativen Bereich eines jeden Unternehmens bestehen vertragsrechtlich geschriebene bzw. ungeschriebene Vorgaben zur Gewährleistung von IT-Sicherheit.

[8] Internationale Konvergenz der Kapitalmessung und Eigenkapitalanforderung, Juni 2004, S. 157 (abrufbar im Internet unter http://www.bundesbank.de/download/bankenaufsicht/pdf/eigenkapitalemfehlungen.pdf).

[9] Heckmann, a.a.O., S. 9.

Je nach Ausgestaltung des Vertragsverhältnisses ist es ohne weiteres denkbar, dass IT-Sicherheit und ihre Gewährleistung eine Hauptleistungspflicht einer vertraglichen Sonderverbindung zwischen zwei Parteien einzustufen ist. Hier ist nur an den weiten Bereich des Outsourcings von IT-Infrastrukturen auf konzerninterne, insbesondere aber auch externe Einheiten zu denken. Darüber hinaus kann IT-Sicherheit auch eine ungeschriebene vertragliche Nebenpflicht darstellen, konkret in Gestalt der allgemeinen Rücksichtnahme bzw. Schutzpflicht gegenüber dem jeweils anderen Vertragsteils (§ 241 Abs. 2 BGB). Als Beispiel wäre hier insbesondere an den Bereich des Online-Banking zu denken.[10]

Unabhängig davon wird man jedoch insbesondere auch im vertragsrechtlichen Bereich die Gewährleistung von IT-Sicherheit nicht nur auf der Ebene der unmittelbar IT-sicherheitsbezogenen objektiven Pflichten aus einem Vertragsverhältnis zu berücksichtigen haben. Insbesondere im Bereich der subjektiven Pflichten, gemeinhin des Verschuldens, bei Verletzung sonstiger objektiver vertraglicher Verpflichtungen spielen IT-Sicherheitsstandars eine zentrale Rolle. Zu denken wäre hier insbesondere an den Verschuldensnachweis im Rahmen eines Lieferverzuges, der darin seine Ursache hat, dass im zuliefernden Unternehmen die nach dem Stand der Technik zu fordernden Anforderungen an die Sicherheit der IT-Infrastrukturen nicht gewährleistet sind.

Delitksrechtlich ist die Thematik insbesondere im Zusammenhang mit Fragestellungen der Produkthaftung von Bedeutung.[11] Hier sind insbesondere Softwareunternehmen angesprochen, jedoch auch jeder andere produzierende Betrieb, in dessen Produkten zumindest auch IT-Komponenten (Hard- oder Software) enthalten sind.

6. Versicherungsrechtliche Anforderungen

Schließlich sollte nicht außer Betracht bleiben, dass die Nichtbeachtung der Anforderungen an die Gewährleistung von IT-Sicherheit bzw. die Sicherheit von IT-Infrastrukturen auch im Rahmen des Versicherungsvertragsrechts Bedeutung haben. Nach den versicherungsvertraglichen Regelungen in Verbindung mit den einschlägigen Bestimmungen des Versicherungsvertragsgesetzes (VVG) hat der Versicherungsnehmer, das Unternehmen, regelmäßig Obliegenheiten gegenüber dem Versicherer zu beobachten, um den Versicherungsschutz nicht zu gefährden. Insbesondere bestimmt § 16 VVG die Pflicht des Versicherungsnehmers, den Versicherer vor dem Vertragsschluss über ihm bekannte Umstände, die für den Vertragsschluss von Bedeutung sind, zu informieren.

Wenn man sich nun vor Augen führt, dass Unternehmen regelmäßig Betriebsunterbrechungsversicherungen abschließen liegt es auf der Hand, dass im Rahmen des Vertragsschlusses von Seiten des Unternehmens darauf hinzuweisen ist, dass ggf. der Fortgang der ordnungsgemäßen betrieblichen Tätigkeit zentral von dem Funktionieren von IT-Infrastrukturen abhängig ist. Letzteres wiederum ist alsdann nur gewährleistet, wenn hinreichende Vorkehrungen zur Darstellung von IT-Sicherheit entsprechend dem Stand der Technik gegeben sind. Entsprechend wäre – wiederum nach § 16 VVG – vom Versi-

[10] Roth/Schneider, a.a.O., ITRB 2005, 20.

[11] Spindler, IT Sicherheit und Produkthaftung – Sicherheitslücken Pflichten der Hersteller und Softwarenutzer, NJW 2004, 3145ff.

cherungsnehmer auf Mängel in diesem Bereich bei Vertragsschluss hinzuweisen, sofern solche denn existent sein sollten.[12]

7. Gewerblicher Rechtsschutz

Auch gesetzliche Regelungen des Wettbewerbs- und Urheberrechts beschäftigen sich mit Fragen, die der IT-Sicherheit zuzuordnen sind. Zu denken ist hier an § 7 Abs. 2, Abs. 3 UWG, die u. a. Spamming als wettbewerbswidrige und abmahnfähige Rechtsverletzung behandeln.

Die Regelungen der §§ 69a ff. UrhG wiederum bestimmen, wann und wie Software durch Dritte genutzt werden darf. Insbesondere die Thematik unlauterer Kopien, jedoch auch der Übernutzung bzw. Unterlizensierung von Software ist hier von Relevanz.

8. Maßstab hinreichender IT-Sicherheit

IT-Sicherheit ist auf Grundlage des gegenwärtigen „Stands der Technik“ zu gewährleisten, dies ist der rechtliche Standard, der im Rahmen einer Vielzahl von Bestimmungen den Begriff der IT-Sicherheit konkretisiert. Problematisch und bislang von den Gerichten nicht judiziert ist jedoch die inhaltliche Ausgestaltung dieses Maßstabes. Insofern kann nur empfohlen werden, auf die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik im Rahmen des BSI-Grundschutzhandbuches, auf den britischen Standard BS 7799 oder die ISO 15048 zurückzugreifen und hiervon ausgehend anhand der konkreten Situation und Bedürfnissen des Unternehmens – ggf. unter fachkundiger externer Hilfe – einen IT-Sicherheitsstandard zu entwickeln, der dem jeweiligen „Stand der Technik“ entspricht.

4 Zivilrechtliche Haftung des Unternehmens nach außen

Die Ansatzpunkte für die Haftung eines Unternehmens nach außen im Verhältnis zu Dritten für die Nichtbeachtung der rechtlichen Vorgaben zur IT-Sicherheit sind ebenso, wie die zuvor angesprochenen gesetzlichen Regelungen, die sich mit der Thematik der IT-Sicherheit befassen.

1. Schadenersatzersatzhaftung

Eine allgemeine Schadenersatzhaftung kann sich zu Lasten des Unternehmens infolge vertraglicher Pflichtverletzung, insbesondere Nicht-, Schlecht- und Späterfüllung vertraglicher Hauptleistungs- und Nebenpflichten ergeben. Wie dargestellt brauchen diese Hauptleistungsverpflichtungen nicht zentral die Gewährleistung von IT-Sicherheit zum Gegenstand haben, es genügen insoweit auch schlichte Lieferverpflichtungen, damit Defizite im IT-Sicherheitsbereich haftungsbegründend wirken.

Deliktsrechtlich begründen die Spezialregelung des Produkhaftungsgesetzes, aber auch die allgemein-deliktsrechtlichen Normen der §§ 823 ff. BGB eine Schadenersatzhaftung

[12] Heckmann, a.a.O., S. 10.

zu Lasten des Unternehmens gegenüber Dritten, insbesondere wenn die Nichtbeachtung von IT-Sicherheitsvorgaben zu Eigentumsverletzungen, Eingriffen den eingerichteten und ausgeübten Gewerbebetrieb Dritte oder zur Verwirklichung strafrechtlicher Schutzgesetze führen.

Der Umfang der Schadenersatzverpflichtung bestimmt sich nach §§ 249 ff. BGB. In aller Regel wird Schadenersatz in Geld zu Leisten sein. Insoweit ist die Haftung grundsätzlich dem Inhalt und der Höhe nach unbegrenzt. Sie kann gerade auch mittelbare Schäden und den Ersatz entgangenen Gewinns umfassen. Vertragliche Haftungsbegrenzungen sind grundsätzlich möglich, nicht jedoch im Anwendungsbereich des Produkthaftungsgesetzes.

Mittelbar kann darüber hinaus die Verletzung rechtlicher Vorgaben zur IT-Sicherheit im Rahmen des Mitverschuldens (§ 254 BGB) für ein Unternehmen, das selbst Anspruchsteller gegenüber Dritten ist, von Relevanz werden. Anschaulich belegt dies der jüngst vom OLG Hamm entschiedene Fall, wonach ein Unternehmen ein Mit- oder gar eine Alleinschuld an der Schadensentstehung treffen kann, wenn dessen IT-Verantwortliche nicht dafür Sorge tragen, dass die Unternehmens-IT dem Stand der Technik entspricht. Konkret hatte das Gericht über einen Fall des Datenverlustes zu entscheiden, der jedoch durch ungenügende Datensicherungsmaßnahmen im Unternehmen begünstigt wurde.[13]

2. Urheberrechtsverletzungen

Die Verletzung urheberrechtlicher Normen, insbesondere durch Nutzung nicht oder nicht ausreichend lizensierter Software führt – soweit für die Praxis von Interesse – zu Unterlassungs- und Schadenersatzansprüchen, § 97 UrhG. Wenngleich der Schadenersatzanspruch der Höhe nach in Gestalt der üblicherweise zu zahlenden Lizenzgebühr noch relativ glimpflich erscheint, zumal „Strafzuschläge“ bislang nur in anderen Bereichen zugebilligt worden sind, ist der Unterlassungsanspruch ein scharfes Schwert. Wird er vom Inhaber der Urheberrechte an der in Rede stehenden Software gerichtlich im Wege der einstweiligen Verfügung durchgesetzt, kann dies ebenso kurzfristig wie effektiv den Stillstand ganzer IT-Infrastrukturen und damit ganzer Betriebe nach sich ziehen.

3. Wettbewerbsrechtliche Haftung

Ähnlich wie die urheberrechtlich kodifizierten Rechtsfolgen führen Verstöße gegen geltendes Wettbewerbsrecht zu Unterlassungs- und Schadenersatzansprüchen. Letztere sind in der Praxis vom relativ geringerem Interesse, ist ein materieller Schaden jenseits von Rechtsverfolgungskosten als Folge eines Wettbewerbsverstoßes in aller Regel nur schwer nachweisbar. Der Unterlassungsanspruch, regelmäßig im Wege der einstweiligen Verfügung durchgesetzt, ist demgegenüber der entscheidende Rechtsbehelf. Praktisch relevant wird er Zusammenhang mit Rechtfragen der IT-Sicherheit jenseits der Behandlung unlauterer Werbepraktiken wie Spamming vor dem Hintergrund, dass unter dem Gesichtspunkt der „Vorsprung durch Rechtsbruch“ jedenfalls nach überkommener, jedoch gegenwärtig im Wandel begriffener Rechtsprechung ein jeder Verstoß gegen objektive Rechtsnormen – wie beispielsweise das Datenschutzrecht – einen Wettbewerbsverstoß begründen kann.

[13] OLG Hamm, MMR 2004, 487.

4. Haftung aus § 7 BDSG

Schließlich statuiert § 7 BDSG eine Schadenersatzpflicht von Unternehmen für jedwede From der nicht gesetzeskonformen Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

5 Persönliche Haftung der IT-Verantwortlichen

Unabhängig von der Haftung des Unternehmens nach außen gegenüber Dritten kann im Einzelfall unter bestimmten Voraussetzungen auch eine Ersatzpflicht der IT-Verantwortlichen unmittelbar selbst, d. h. gegebenenfalls auch mit ihrem Privatvermögen, in Betracht kommen. Dabei ist von Fall zu Fall zwischen einer Haftung der IT-Verantwortlichen im Innenverhältnis zum Unternehmen einerseits bzw. im Außenverhältnis zu Dritten andererseits zu differenzieren.

1. Persönliche Haftung der Geschäftsführung

Eine persönliche Haftung des Unternehmensorgans, d. h. des einzelnen Vorstands- bzw. Geschäftsführungsmitglieds, gegenüber der Gesellschaft kann sich dem Grunde nach aus § 93 Abs. 2 Satz 1 AktG bzw. § 43 Abs. 2 GmbHG ergeben. Für Personengesellschaften des Handelsrechts ergibt sich im Ergebnis nichts anderes.

Konkret haftet das jeweilige Unternehmensorgan der Gesellschaft immer dann, wenn eine objektiv, dem Vorstands- bzw. Geschäftsführungsmitglied obliegende Verpflichtung nicht erfüllt worden ist. Der Pflichtenmaßstab, den die Unternehmensorgane zu beachten haben, ist derjenige eines ordentlichen Kaufmanns. Inhaltlich bestimmt sich dieser umfassend und objektiv anhand von Art, Größe und Situation des Unternehmens, den Branchengeflogenheiten sowie der Bedeutung der jeweiligen Aufgabe für das Unternehmen.[14] Dies gilt auch für die Bestimmung der Anforderungen zur IT-Sicherheit.

Risikoerhöhend wirkt dabei für die Unternehmensorgane die für die Aktiengesellschaft ausdrücklich kodifizierte Beweislastumkehr zu Lasten des jeweiligen Vorstandsmitgliedes in § 93 Abs. 2 Satz 2 AktG, wonach ihn die Beweislast dahingehend trifft, ob im Einzelfall die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt worden ist. Diese gilt im Bereich der GmbH entsprechend.[15]

Da jedoch dem Unternehmensorgan selbst faktisch wie rechtlich die Leitungsfunktion hinsichtlich des Unternehmens zukommt, wird das jeweilige Vorstands- bzw. Geschäftsführungsmitglied in aller Regel Pflichten, mithin auch die Pflicht zur Gewährleistung hinreichender IT-Sicherheit auf andere Mitarbeiter des Unternehmens im Rahmen des Zulässigen delegieren. Dies entlastet das jeweilige Unternehmensorgan jedoch nicht vollends,

[14] vgl. Schrey, Persönliche Verantwortung und Haftungsrisiken von IT-Verantwortlichen, RDV 2004, 246, 248 m. w. N.; Roth/Altmeppen, Kommentar zum GmbHG, 4. Auflage, § 43 Rz. 3; vgl. allgemein zur Leitungsfunktion der Geschäftsführung: Baumbach/Hueck, Kommentar zum GmbHG, 17. Auflage, § 35 Rdnr. 16 ff.; Hüffer, Kommentar zum Aktiengesetz, 6. Auflage, § 76 Rz. 7 ff.

[15] Roth/Altmeppen, a.a.O., § 43 Rz. 75.

vielmehr bleibt es für die sorgfältige Auswahl des jeweiligen Mitarbeiters dessen Aufsicht sowie angemessene Unterstützung hinsichtlich Informationsfluss sowie Zurverfügungstellung hinreichender personeller und sachlicher Ressourcen verpflichtet.[16] Die Führungs-, Handlungs- und Ressortverantwortung ist ohnehin nicht delegierbar, sie verbleibt bei dem jeweiligen Unternehmensorgan. Werden solchen Pflichten dennoch delegiert, entsteht eine Haftung aus Organisationsverschulden.[17]

Die Privilegierungen, die Arbeitnehmern in haftungsrechtlicher Hinsicht zukommen und auf die sogleich einzugehen sein wird, gelten für Unternehmensorgane nicht. Es wird jedoch eine Haftungsbeschränkung in den Fällen erwogen, dass Vorstände bzw. Geschäftsführer keine spezifischen Geschäftsführungsaufgaben wahrnehmen bzw. lediglich eine konkrete Ressourzuständigkeit haben.[18]

Von der Haftung des Unternehmensorgans persönlich und unmittelbar gegenüber dem Unternehmen ist eine inhaltsgleiche Haftung gegenüber außen stehenden Dritten im Außenverhältnis zu differenzieren. In aller Regel wird hier ein Haftungspotential wegen vertraglicher Pflichtverletzung unmittelbar nicht in Betracht kommen, da diejenigen Verträge, die infolge Nichtbeachtung der Sicherstellung einer hinreichenden IT-Sicherheit Not leidend werden, in aller Regel im Namen und auf Rechnung des Unternehmens, nicht jedoch des Unternehmensorgans abgeschlossen sind. Eine Ausnahme besteht hier unter dem Gesichtspunkt der Eigenhaftung des Vertreters, wenn der Geschäftsführer bzw. das Vorstandsmitglied besonderes Vertrauen gegenüber dem außenstehenden Dritte in Anspruch genommen hat, §§ 280, 311 BGB.[19] Weiter besteht eine potentielle deliktsrechtliche Haftung aus unerlaubter Handlung gem. § 823 ff. BGB. § 826 BGB statuiert insofern eine Schadensersatzpflicht wegen vorsätzlicher sittenwidriger Schädigung. Wenngleich dieser Tatbestand in der Praxis selten erfüllt sein wird, sanktioniert jedoch die allgemeinere Haftungsnorm des § 823 Abs. 1 BGB bereits jeden unmittelbaren Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb ebenso, wie eine Eigentumsverletzung zu Lasten Dritter. Hinzu kommt eine mögliche Haftung aus § 823 Abs. 2 BGB i.V.m. einem strafrechtlichen Schutzgesetz. Hier sind jedenfalls Konstellationen denkbar, die eine persönliche Haftung denkbar erscheinen lassen.

Daneben wird auch eine Haftung gegenüber den Aktionären einer Aktiengesellschaft bzw. den Gesellschaftern einer GmbH unmittelbar aus allgemeinem Deliktsrecht i.V.m. strafrechtlichen Schutzgesetzes, insbesondere dem der Untreue, diskutiert.[20]

Schließlich ist ein Haftungspotential aus § 97 UrhG tatsächlich gegeben. Hier sind auch praktisch unmittelbar Szenarien wie Übernutzung und Unterlizensierung von Software denkbar, die eine unmittelbare Haftung der Geschäftsführung nach sich zieht. Dieses Potential sollte mit Blick auf das zunehmende Interesse und die verstärkten Maßnahmen der Softwareindustrie zur Eindämmung dieser Phänomene nicht unterschätzt werden.

[16] Roth/Schneider a.a.O., 19, 20f.; Schrey, a.a.O., 247, 248f.
[17] Schrey, a.a.O., 247, 251.
[18] Schrey a.a.O., 247, 248 f.
[19] Hüffer, a.a.O., § 93 Rz. 21; Baumbach/Hueck, a.a.O., § 43 Rz. 54f.
[20] Hüffer, a.a.O., § 93 Rz. 19; Baumbach/Hueck, a.a.O., § 43 Rz. 57f.

Für Aufsichträte gilt über § 116 AktG die Regelung des § 93 Abs. 2 AktG entsprechend. Ob und inwieweit sie für Versäumnisse im Bereich IT-Sicherheit haftbar sind, ist im Rahmen dieser Norm, jedoch auch hinsichtlich einer sonstigen Haftung aus Vertrags- und Deliktsrecht stets eine Frage der Umstände des Einzelfalls.

2. Persönliche Haftung von sonstigen leitenden Angestellten und Arbeitnehmern

Auch Arbeitnehmer, seien es nun leitende Angestellte oder „einfache" Arbeitnehmer, können eine Haftung gegenüber ihrem Unternehmen unmittelbar unterliegen. Haftungsgrund ist die arbeitsvertragliche Pflichtverletzung. Diese konkretisiert sich in aller Regel in der Nichtbeachtung einer arbeitsvertraglichen Weisung bzw. der Verletzung einer arbeitsvertraglichen Nebenpflicht, insbesondere Schutz- und Geheimhaltungspflicht. Einfache Beispiele sind das aufspielen eigener, privater virenverseuchter Software oder das auf dem Desktop-PC mittels aufgeklebten Zettel dokumentierte Passwort

Der Haftungs- bzw. Sorgfaltsmaßstab bestimmt sich grundsätzlich auf Grundlage der gesetzlichen Regelung des § 276 BGB, wonach der einzelne Arbeitnehmer Vorsatz und Fahrlässigkeit zu vertreten hat. Ausgehend hiervon ist der Sorgfaltsmaßstab individuell zu bestimmen. So sind an einen leitenden Mitarbeiter höhere Sorgfaltsanforderungen zu stellen als einen Mitarbeiter in untergeordneter Stellung. Abweichend vom allgemeinbürgerlichrechtlichen Normalfall hat der Arbeitgeber das Verschulden des Arbeitnehmers im Hinblick auf eine arbeitsvertragliche Pflichtverletzung darzulegen und zu beweisen, § 619 a BGB.

Weitergehend hat die Rechtssprechung ausgehend vom allgemeinen Gedanken der Sach- und Betriebsgefahr des Arbeitgebers ein differenziertes System zur Haftungsprivilegierung von Arbeitnehmern entwickelt. Dieses beinhaltet grundsätzlich eine ausschließliche und umfängliche Haftung des Arbeitnehmers in Fällen vorsätzlichen und grob fahrlässigen Verhaltens. Aber auch insoweit greift bereits dann eine Ausnahme, wenn ein grobes Missverhältnis zwischen der Höhe des Einkommens des schädigenden Arbeitnehmers und der Größe des Schadens besteht. Ist ein Fall der so genannten mittleren Fahrlässigkeit gegeben, ist der entstandene Schaden zwischen Arbeitgeber und Arbeitnehmer zu teilen. Handelt der Arbeitnehmer im Einzelfall jedoch nur leicht fahrlässig, greift zu seinen Gunsten ein umfänglicher Haftungsausschluss, der Arbeitgeber hat den Schaden, der aus der Pflichtverletzung des Arbeitnehmers resultiert alleine zu tragen.[21]

Hinsichtlich der Haftung des Arbeitnehmers im Außenverhältnis gegenüber Dritten gilt grundsätzlich nichts anderes, als für Organe des Unternehmens. Eine unmittelbar persönliche Haftung wegen vertraglicher Pflichtverletzungen gegenüber Dritten ist kaum denkbar und in aller Regel nicht praktisch relevant. Dies gilt nicht sofern eine Haftung wegen unerlaubter Handlung aus § 823 ff. BGB in Rede steht sowie in Fällen einer Haftung nach § 97 UrhG. Sofern und Soweit den Arbeitnehmer als Konsequenz aus einer betriebsinternen Nichtgewährleistung hinreichender IT-Sicherheitsstandards und seiner unmittelbar persönlichen Verantwortung hieraus eine Haftung gegenüber außen stehenden Dritten unmittelbar persönlich treffen sollte, steht ihm im Innenverhältnis zu seinem Arbeitgeber

[21] BAG NJW 1994, 856; BAG NJW 1995, 210; BAG NZA 1990, 97ff.; BAG NZA 2003, 37, 39f.

insofern ein Freistellungsanspruch zu, als er – wie soeben im Einzelnen ausgeführt – im Innenverhältnis zum Arbeitgeber haftungsrechtlich privilegiert wäre.[22]

3. Persönliche Haftung von IT-Sicherheitsbeauftragten

Beleuchtet man die Haftung von IT-Sicherheitsbeauftragten, ist zunächst zwischen betriebesinternen und externen IT-Sicherheitsbeauftragten zu differenzieren.

Betriebsinterne IT-Sicherheitsbeauftragten sind in aller Regel Arbeitnehmer, seien es leitende Angestellte oder „einfache" Arbeitnehmer. Entsprechend den obigen Ausführungen haften sie dem Unternehmen gegenüber aus arbeitsvertraglicher Pflichtverletzung. Entscheidend für eine persönliche Haftung ist der konkrete Pflichtenkreis des IT-Sicherheitsbeauftragten entsprechend den Festlegungen seines Arbeitsvertrages. Fehlt es an solchen spezifischen Festlegungen, ist der Pflichtenkreis durch Auslegung des Arbeitsvertrages zu ermitteln. Hier kann auf das BSI-Grundschutzhandbuch, dort konkret das Kapitel „Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit (M 2.193)" zurückgegriffen werden. Im Allgemeinen wird man jedoch unabhängig davon dem Arbeitsvertrag eines IT-Sicherheitsbeauftragten beilegen können, dass der Pflichtenkreis desselben den Aufbau, die Pflege und die Einhaltung eines IT-Sicherheitskonzepts bzw. einer IT-Sicherheitsinfrastruktur ebenso beinhaltet, wie Risiko- und Bedrohungsanalysen. Hieraus wiederum folgt – zumindest in Gestalt einer vertraglichen Nebenpflicht – eine entsprechende Verpflichtung, den Arbeitgeber auf entsprechende Bedrohungen und Risiken hinzuweisen. Dies gilt selbst dann, wenn es dem IT-Sicherheitsbeauftragten an Entscheidungskompetenzen fehlt. Werden diese Pflichten nicht beachtet bzw. erfüllt, steht eine Schadenersatzverpflichtung aus arbeitsvertraglicher Pflichtverletzung gegenüber dem Arbeitgeber im Raum.[23] Gegenüber Dritten wird eine Haftung allenfalls aus deliktischer Haftung praktisch werden. Die Ausführungen soeben unter 2. gelten entsprechend. Die aufgezeigten Haftungsprivilege gelten auch insoweit. Diese können jedoch ein trügersiche Sicherheit bieten, sind doch die individuellen Anforderungen im Rahmen des Verschuldens eines IT-Sicherheitsbeauftragten höher als diejenigen, die an einfache Arbeitnehmer zu stellen sind. So kann gegebenenfalls auch das Verabsäumen einer hinreichenden Vertragsgestaltung und -dokumentation ohne fachkundigen juristischen Rat in komplexen Projekten, jedoch auch in alltäglichen Gestaltungen den Vorwurf mittlerer, im Einzelfall auch grober Fahrlässigkeit mit den entsprechenden persönlichen Haftungsfolgen rechtfertigen.

Externe IT-Sicherheitsbeauftragte sind an sich nicht anders juristisch zu behandeln, als interne IT-Sicherheitsbeauftragte. Auch sie sind gegenüber ihrem Auftraggeber, dem Unternehmen, aufgrund des entsprechenden schuldrechtlichen Vertrages und dem dort niedergelegten Pflichtenkreis zur Beobachtung eben dieses Pflichtenkreises vertraglich verpflichtet. Dessen Inhalt wiederum bestimmt sich entsprechend den Ausführungen soeben zum Pflichtenkreis des internen IT-Sicherheitsbeauftragten. Haftungstechnisch wesentlich ist jedoch der Unterschied, dass in Ermangelung einer spezifischen vertraglichen Regelung dem externen IT-Sicherheitsbeauftragten das von der Rechtsprechung entwickelte Haftungsprivileg eines Arbeitnehmers nicht zugute kommt. Gleichwohl bleibt es externen

[22] Palandt/Putzo, Kommentar zum Bürgerlichen Gesetzbuch, 63. Auflage, § 611 Rz. 159 m. w. N.
[23] Roth/Schneider, a.a.O., 19, 21.

IT-Sicherheitsbeauftragten in der Praxis sicherlich unbenommen, zumindest den Versuch zu starten, ihre vertragliche Haftung durch entsprechende Abreden auszuschließen oder zu beschränken. Dies ist grundsätzlich rechtlich möglich und in Individualvereinbarungen auch weitestgehend zulässig. Hinsichtlich haftungseinschränkender Normen in Standardverträgen und -klauseln gelten die Einschränkungen des AGB-Rechts, §§ 307 ff. BGB. Entsprechendes gilt für die jedenfalls theoretisch auch denkbare Haftung aus unerlaubter Handlung gem. § 823 ff. BGB.

4. Persönliche Haftung von Datenschutzbeauftragten

Die persönliche Haftung von betrieblichen Datenschutzbeauftragten bestimmt sich entsprechend der Ausführungen soeben zur Haftung von Arbeitnehmern gegenüber ihren Arbeitgebern. Handelt es sich bei betrieblichen Datenschutzbeauftragten um interne Datenschutzbeauftragte, d. h. leitende Angestellte oder „einfache“ Arbeitnehmer, gelten auch hier die Haftungsprivilegierungen entsprechen denjenigen eines Arbeitnehmers, wie sie zuvor dargestellt wurden. Sofern externe betriebliche Datenschutzbeauftragte tätig werden, gelten hier diejenigen Ausführungen entsprechend, die zuvor zu externen IT-Sicherheitsbeauftragten getätigt worden sind.

Relevant kann bezüglich der betrieblichen Datenschutzbeauftragten – ob nun innerbetrieblich oder außerbetrieblich – eine Haftung gegenüber außen stehenden Dritten werden. Zwar ist mangels vertraglicher Sonderverbindung zwischen dem internen oder externen betrieblichen Datenschutzbeauftragten einerseits und dem außen stehenden Dritten andererseits eine Haftung aus vertraglicher Pflichtverletzung in aller Regel nicht einmal theoretisch denkbar. Eine unmittelbare persönliche Haftung aus Delikt im Rahmen des Spezialdatentatbestands des § 7 BDSG ist denkbar, wenngleich in der juristischen Fachliteratur umstritten. Teilweise wird vertreten, dass die starke, unabhängige Stellung des betrieblichen Datenschutzbeauftragten eine unmittelbare Zurechnung von Verstößen auf diesen unmittelbar persönlich mit der Folge einer Schadensersatzverpflichtung gegenüber außen stehenden Dritten rechtfertigt. Teilweise wird in der einschlägigen Fachliteratur eine solche unmittelbar persönliche Haftung verneint mit dem Hinweis darauf, dass dem betrieblichen Datenschutzbeauftragten lediglich beratende und unterstützende jedoch keine entscheidende Position im Unternehmen beizumessen ist.[24]

6 Schutzmöglichkeiten der IT-Verantwortlichen vor persönlicher Haftung

Als prinzipielle Schutzmöglichkeiten von IT-Verantwortlichen hinsichtlich einer drohenden persönlichen Haftung kommen – gleich auf welcher Hierarchieebene – eine vertragsrechtliche oder eine versicherungsrechtliche Lösung in Betracht.

Für Geschäftsführer einer GmbH besteht die Möglichkeit, mögliche Haftungsrisiken bereits in ihrem Anstellungsvertrag auszuschließen bzw. einzuschränken. Die Haftung aus § 43 GmbHG ist disponibel.[25] Dies ist jedenfalls rechtstheoretisch nach überwiegender

[24] Schrey, a.a.O., 247, 249 m. w. N.

[25] Roth/Altmeppen, a.a.o., § 43 Rz. 84 m. w. N.

Auffassung möglich, wenngleich praktisch wenig verbreitet und dementsprechend schwierig durchzusetzen. Für Vorstände einer AG besteht die Möglichkeit einer vertraglichen Haftungsbegrenzung oder eines -ausschlusses vor dem Hintergrund der gesetzlichen Regelung des § 93 Abs. 4 GmbHG ohnehin nicht.

Alternativ verbleibt für die Organe der GmbH wie der AG die versicherungstechnische Lösung, konkret eine D&O-Versicherung mit ausreichender Deckungssumme und bestenfalls auf Kosten des Unternehmens. Eine Delegation ihrer Verpflichtungen wird sie demgegenüber eine möglichen Haftung keinesfalls freistellen. Selbst wenn Verpflichtungen tatsächlich wie rechtlich delegierbar sind, was im Rahmen der Führungs-, Handlungs- und Ressortverantwortung schon nicht möglich ist, bleibt ohne weiteres eine Auswahl- und Überwachungsverantwortung beim Leitungsorgan vorhanden.

Für Arbeitnehmer selbst ist das Haftungspotential gegenüber dem Unternehmen und erst recht gegenüber außen stehenden Dritten ohnehin aufgrund der dargestellten Grundsätze zur gefahrgeneigten Arbeit bzw. zur allgemeinen Haftungsprivilegierung abgemildert, wenngleich auch keinesfalls verlässlich ausgeschlossen. In Ermangelung versicherungstechnischer Lösungen, kann hier an sich nur auf die Möglichkeit ergänzender vertragsrechtlicher Haftungsbegrenzungen verwiesen werden. Für diese gilt jedoch gleiches, wie für vertragliche Haftungsbegrenzungen von Unternehmensorganen. Sie sind wenig verbreitet, unüblich und dementsprechend schwer durchzusetzen.

Externen Datenschutzbeauftragten und IT-Sicherheitsbeauftragten stehen wiederum beide Lösungen offen, die vertragsrechtliche und die versicherungsrechtliche. Sie werden in aller Regel zunächst versuchen, ggf. auch unter Hinweis auf ihre standardvertragsrechtlichen Regelungen, eine Haftungsbegrenzung oder, sofern rechtlich möglich und wirksam darstellbar, auch einen Haftungsausschluss zu verhandeln. Dies wird jedoch aus nahe liegenden Gründen ähnlich schwierig erfolgreich darzustellen sein, wie eine Haftungsbegrenzung bzw. ein Haftungsausschluss von Unternehmensorganen. Es bleibt alsdann die versicherungsrechtliche Lösung.

Für sämtliche Beteiligten gilt selbstverständlich, dass Vorbeugung besser ist als Schadensminimierung. Dementsprechend sind in allererster Linie die bestehenden Verpflichtungen zu erfüllen und die innerbetrieblichen Abläufe hinreichend zu qualifizieren und zu dokumentieren, ggf. ist externer Rat und externe Expertise hinzuzuziehen. Sollten IT-sicherheitsrelevante Hinweise oder vorgeschlagene Lösungen nebst angemessener Budgets von Unternehmensführung oder ggf. gar von Gesellschafterebene ignoriert oder abgelehnt werden, sollte auch dies dokumentiert, gleichwohl aber die aus der jeweiligen Entscheidung folgenden Risiken (erneut) aufgezeigt werden.