Zerto

WHITEPAPER

Juli 2016

1.

# Das neue IT-Sicherheitsgesetz: Erweiterte Rechtspflichten und potenzielle Haftungsfallen des modernen IT-Sicherheitsmanagements

## Die Bedeutung von Disaster Recovery/Business Continuity im virtuellen Zeitalter

*Von Rechtsanwalt und Fachanwalt für IT-Recht*
*Dr. Jens Bücking**

# Das neue IT-Sicherheitsgesetz: Erweiterte Rechtspflichten und potenzielle Haftungsfallen des modernen IT-Sicherheitsmanagements

*- Die Bedeutung von Disaster Recovery/Business Continuity im virtuellen Zeitalter -*

*Von Rechtsanwalt und Fachanwalt für IT-Recht Dr. Jens Bücking**

Management Summary ..... 2
I. Problemaufriss ..... 3
II. Risiken der IT-Sicherheit ..... 3
1. Technische und wirtschaftliche Risiken ..... 4
2. Rechtliche Risiken ..... 4
a) Keine Delegierung durch Fremdvergabe des IT-Managements (insbes. „Outsourcing“) ..... 4
b) Handels- und Steuerrecht; Personendatenschutz ..... 5
c) Strafrecht ..... 5
3. Datensicherheit im Desasterfall ..... 6
4. Gewährleistung von Verfügbarkeit ..... 6
III. Haupthaftungsrisiko: Nichtverfügbarkeit unternehmenskritischer Informationen ..... 7
1. Zulässige Aufbewahrungsformen ..... 7
2. Aufbewahrung und Prüfung nach den „GoBD“ ..... 7
2. Aufbewahrungsfristen ..... 8
3. Haftungsfalle E-Mail: Sichere Kommunikation, Aufbewahrung, Beweismittel ..... 8
4. Haftungsfolgen ..... 9
IV. Gesetzgebung und Rechtsprechung zur IT-Sicherheit ..... 10
1. Gesetzgebung ..... 10
2. Rechtsprechung ..... 12
3. Ausgewählte Praxisbeispiele ..... 13
V. Das IT-Sicherheitsgesetz ..... 14
1. KRITIS-Betreiber und das BSIG ..... 14
2. Erweiterte technische Sicherungspflichten für Internetanbieter ..... 16
VI. Besonderheiten bei Cloud-Nutzung und Outsourcing ..... 18
VII. Haftungsvermeidung durch Risiko-Management ..... 20
VIII. Versicherbarkeit von IT-Sicherheitsrisiken ..... 20
Rechtssicherheit durch technische Sicherheit: Das ganzheitliche DR/BC-Lösungskonzept von ZERTO ..... 21

## MANAGEMENT SUMMARY

Die „rechtssichere“ Aufbewahrung und Verfügbarhaltung von unternehmenskritischen Informationen und IT-Systemen gehört im Informationszeitalter zu den rechtlichen Selbstverständlichkeiten, entsprechende Backup- und Archivierungsprozesse sind zur Einhaltung der jeweils einschlägigen Compliance-Standards unabdingbar. Welche konkreten - auch persönlichen - Haftungsrisiken sich allerdings dahinter verbergen, ist selbst auf Managementebene oft nicht bekannt. Eine „Noncompliance“ kann jedoch fatale Folgen haben. Dies betrifft insbesondere Schäden infolge von Versäumnissen beim IT-Risikomanagement. Aus der Rechtsprechung sind Fälle bekannt, die von der Anfechtbarkeit des Beschlusses über die Entlastung des Managements bis zur außerordentlichen Kündigung der Anstellungsverträge und Abberufung aus der Funktion des CEO reichen. Auch kann der Versicherungsschutz für derlei „Cyberrisiken“ unzureichend sein oder gar insgesamt ausfallen. Dies gilt umso mehr vor dem Hintergrund neuer - und erweiterter -

Sicherheitspflichten durch das IT-Sicherheitsgesetz von 2015, das unterschiedlichen Kategorien von Unternehmen mannigfaltige Verpflichtungen in Bezug auf die Sicherheit ihrer Systeme und Daten auferlegt. Den Betreibern kritischer Infrastrukturen (KRITIS) droht bei Versäumung oder Schlechterfüllung der Pflichtenkataloge des neuen Gesetzes neben empfindlichen Ordnungsmitteln, die über die bloßen Bußgelder hinaus bis zur Untersagung bzw. Sperrung ihrer Dienste reichen können, insbesondere auch die Schadenshaftung: Es kommen Schadensersatzansprüche sowohl von Vertragspartnern wie auch von geschädigten Dritten in Betracht (etwa gegenüber anderen KRITIS-Betreibern im Falle der Verletzung von Meldepflichten) und - im Bereich der geschäftlichen Internet-Angebote - aus dem allgemeinen Kreis der Nutzer dieser Angebote. Das neue Gesetz eröffnet jedoch zugleich die Chance und gibt entsprechende Hinweise, durch Beachtung seiner technischen und organisatorischen Anforderungen Betriebsausfälle und Haftungsrisiken weitgehend zu beschränken.

## I. Problemaufriss

Das Thema IT-Sicherheit ist aus dem Wirtschafts- und Verwaltungsleben nicht mehr wegzudenken. Seit den Ereignissen der Jahre 2013 ff. mit den diversen Abhör- und Spionageaffären ist die besondere Bedeutung des Schutzes von Geschäfts- und Personendaten in das allgemeine Bewusstsein gerückt. Die Einhaltung von entsprechenden Schutz- und Sicherheitsstandards ist als Teil der „Corporate Governance“ zu recht Chefsache – auch unter Haftungsgesichtspunkten: Aus der Rechtsprechung sind Fälle bekannt, die von der Anfechtbarkeit des Beschlusses über die Entlastung des Managements bis zur außerordentlichen Kündigung der Anstellungsverträge und Abberufung aus der Funktion des CEO reichen. Auch die Mitglieder von Aufsichtsgremien und die Sonderbeauftragten (insbesondere für Compliance, IT-Sicherheit und Datenschutz) stehen potenziell in der Haftung. Andererseits kann der Versicherungsschutz für „Cyberrisiken“ unzureichend sein oder gar insgesamt ausfallen.

Es liegt daher nicht nur unter betriebswirtschaftlichen Aspekten nahe, das Hosting von Daten, Systemen und Applikationen, insbesondere aber auch deren Sicherheit und unterbrechungsfreien Betrieb im Desaster-Fall an spezialisierte IT-Dienstleister und Anbieter von Security-Lösungen zu vergeben. Dieser Leitfaden bietet einen Überblick darüber, welche Haftungsrisiken, aber auch Chancen sich aus einem solchen „Fremdmanagement“ betriebswichtiger IT-Systeme ergeben und erklärt, wie man Risiken steuern und durch ein geeignetes IT-Sicherheitsmanagement begrenzen kann. Der Fokus gilt dabei den Themen „Disaster Recovery“ (DR) und „Business Continuity“ (BC) im aktuellen Kontext mit dem neuen IT-Sicherheitsgesetz.

## II. Risiken der IT-Sicherheit

Unternehmen sehen sich im globalen Wettbewerb gesteigerten Anforderungen in Bezug auf den Schutz und die Vorhaltung ihres geistigen Eigentums ausgesetzt angesichts steigender Risiken von Datenverlust und dem Diebstahl von Daten, für den sich inzwischen ein grauer Markt entwickelt hat.

Im Unterschied zu früher, als das (auch geistige) Eigentum, Rohstoffe, Auftragslage etc. über des Schicksal eines Unternehmens entschieden, stellt die Verfügbarkeit und der Schutz von Informationen heute die betriebswichtigste Ressource im unternehmerischen Organismus dar.

Es liegt unter fachlichen und wirtschaftlichen Gesichtspunkten nahe, diese Aufgabe an spezialisierte Anbieter und deren IT-Produkte zu delegieren. Hierbei können insbesondere externe Rechenzentren neue Wertschöpfungsketten und erhebliche Einsparungspotenziale erschließen. Jedoch sind die Erstellung transparenter und detaillierter Anforderungskataloge an deren IT sowie die Prüfung, ob die angebotenen Lösungen technisch und rechtlich sicher umgesetzt werden können, für jeden Auftraggeber unabdingbar.

## 1. Technische und wirtschaftliche Risiken

Vor diesem Hintergrund arbeiten heutzutage die Abteilungen IT und Recht zusammen an der Schaffung und Implementierung neuer Policies und technisch-organisatorisch abgesicherter Geschäftsprozesse. Hier geht es vornehmlich um die Vermeidung von Betriebsausfallzeiten, Auftragsverluste, Reputationsschäden und weitere finanzielle Einbußen, wenn vertrauliche Daten verloren gehen, gestohlen werden oder kompromittiert werden.

Denn wie Statistiken belegen, müssen 70% der Unternehmen, bei denen es zu katastrophalen Datenverlusten kommt, innerhalb von 18 Monaten aufgeben. Berichten zuverlässiger Quellen wie *Europol*, dem *Bundeswirtschaftsministerium* und dem IT-Branchenverband *Bitkom* zufolge werden täglich in Deutschland Daten von 20 Mio. Telefonaten und 10 Mio. Internetverbindungen allein durch die NSA gespeichert. Dabei geht es auch um Wirtschaftsinteressen. Deutschland ist dabei das wichtigste Wirtschaftsspionageziel in der EU. Laut *Bitkom* ist die Hälfte aller Unternehmen betroffen. Die Schäden belaufen sich auf jährlich 51 Mrd. Euro, weltweit werden diese laut Europol auf 290 Mrd. Euro geschätzt. Angegriffen wird meist nicht, um an bestimmte Informationen zu gelangen - die Mehrzahl der Fälle zielt auf reine Sabotage (DoS-Attacken, Viren etc.).

Konjunktur haben bei der neuen Cyberkriminalität insbesondere Methoden, die Schadcode über das Internet durch Webseiten und Dienste unbeteiligter Dritter verbreiten. Bei diesen Attacken wird der Computer des Nutzers infiziert, während er Webseiten oder Dienste eines unbescholtenen Drittanbieters nutzt. Gefahren lauern sowohl auf großen Webseiten mit hoher Nutzerzahl, wie bspw. auf Internetportalen oder Nachrichtenseiten, aber auch auf weniger aufwendigen und weniger frequentierten Webseiten wie Blogs. Schadcode wird dabei auch auf Werbeflächen oder nutzergenerierten Inhalten platziert. Diese Verbreitungsformen gehören zu den größten Bedrohungen der Netzsicherheit. Nach dem *Lagebericht des BSI* resultiert aus solchen Attacken eine erhebliche Gefahr für Nutzer und Systeme, zumal 75 % der im Internet erreichbaren Webseiten grundsätzlich als verwundbar eingestuft wurden, und hierbei 20 % aller Webseiten als kritisch verwundbar. Beim ungewollten Hosten von Malware auf Webseiten wird Deutschland derzeit an zweiter Stelle gesehen. Dies wirkt sich naturgemäß auch wirtschaftlich entsprechend aus: Schätzungen zufolge belaufen sich die Schäden, die allgemein durch Cybercrime eintreten, auf 400 Milliarden Dollar. Im Verhältnis zum Bruttoinlandsprodukt sind diese Schäden nirgends so hoch wie in Deutschland.

## 2. Rechtliche Risiken

Aus der Erkenntnis heraus, dass der Schutz und die Verfügbarkeit von Daten mithin ein „do-or-die“-Kriterium in Wirtschaft und Verwaltung ist, besteht von Gesetzes wegen die Verpflichtung zu einem effektiven Risiko- und Informationsmanagement. Deren Einhaltung gehört zu den unternehmerischen Lenkungs- und Leitungsaufgaben. Spiegelbildlich bestehen entsprechende Kontroll- und Hinweispflichten der Sonderbeauftragten für Compliance, IT-Sicherheit und Datenschutz.

### a) Keine Delegierung durch Fremdvergabe des IT-Managements (insbes. „Outsourcing“)

Ein Outsourcing der Verantwortungsbereiche an IT-Dienstleister und in externe Rechenzentren über moderne Modelle wie ASP, SaaS und Cloud kann auf der einen Seite Investitions- und Betriebskosten erheblich senken und zugleich auf Ebene der Geschäftsprozesse deutliche Verbesserungen in puncto Datensicherheit, Performance, Verfügbarkeit und Skalierbarkeit von IT-Services bewirken.

Outsourcing führt jedoch im Grundsatz nicht zu einer Entlassung aus der Haftung. Über ein zeitgemäßes Risikomanagement IT-Sicherheit zu gewährleisten, gehört zu den allgemeinen Sorgfalts- und Vorsorgepflichten des Managements. Über diese allgemeine Anforderung hinaus verlangt das Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr (KonTraG) im Bereich der Privatwirtschaft ein effizientes Risikomanagementsystem, das nach einhelliger Ansicht eine Überwachung und Früherkennung sowie entsprechende Reaktionsszenarien im Schadensfall

umfasst. Zu beachten ist in diesem Kontext auch die Beweislastumkehr, wonach in Fällen, in denen streitig ist, ob die zuständigen Mitglieder des Managements die Sorgfalt eines ordentlichen Geschäftsleiters angewandt haben, diese zu ihrer Entlastung die alleinige Beweislast trifft. Auf der Ebene der Haftungsentlastung kommt daher der Auswahl des geeigneten IT-Anbieters erhebliche Bedeutung zu.

Das Recht sieht es als Selbstverständlichkeit an, dass unternehmenskritische - und insbesondere auch beweiserhebliche - Dokumente bei den Unternehmen vorgehalten werden. Von ihnen wird erwartet, dass sie die Verfügbarkeit elektronischer Dokumente in geordneter Weise gewährleisten können - oder aber entsprechende Sanktionen zu erwarten haben. Oft genug entscheiden derlei Dokumente einen Rechtsstreit, indem sie eine Anspruchsposition belegen oder eine Gegenposition beweisrechtlich widerlegen.

**b) Handels- und Steuerrecht; Personendatenschutz**

Die Pflicht zur Gewährleistung von Datenschutz und Datensicherheit betrifft regelmäßig unternehmenssteuernde (ERP-, CRM etc.) Daten (wie z.B. SAP), personenbezogene und steuerrelevante Daten, Berufs- und Geschäftsgeheimnisse (wie etwa Forschungs- und Entwicklungsdaten), Kundendaten, Mitarbeiterdaten etc.

Verletzungen des Personendatenschutzes können hohe direkte Strafsanktionen von in Deutschland bis zu 300 TEUR für jeden Einzelfall zur Folge haben. In schweren Fällen, etwa planmäßigen Datenschutzverletzungen aus kommerziellem Interesse, besteht die Möglichkeit des Abschöpfens eines etwaigen finanziellen Vorteils des Datenschutzverstoßes durch die Strafe (zusätzlich zum Geldstrafen- bzw. Bußgeldsanktionsmittel).

Mit bis zu 250 TEUR kann jeder Einzelverstoß gegen das in der Abgabenordnung verankerte Recht der Außenprüfung auf Datenzugriff geahndet werden. Mit dieser Geldbuße können beispielsweise Fälle einer unzulässigen Auslandsverlagerung der elektronischen Buchhaltung sanktioniert werden. Damit, dass der Steuergesetzgeber dem Steuerpflichtigen unter bestimmten Voraussetzungen das Recht einräumt, elektronische Bücher in einem anderen Mitgliedstaat der EU zu führen und zu verwahren, trägt er einerseits dem unternehmerischen Bedürfnis der Arbeitsteiligkeit in internationalen Konzernen Rechnung, verbindet dies andererseits jedoch für den Fall der Unzulässigkeit mit einer scharfen Sanktion, unabhängig davon, ob es sich um einen In- oder Auslandssachverhalt handelt.

**c) Strafrecht**

Die Verletzung von IT-Sicherheitspflichten kann aber auch strafrechtliche Folgen haben, die über den Personendatenschutz, die Besteuerung und den Schutz von geschäftskritischen Daten noch hinausgehen. Wenn beispielsweise der Verlust oder die Unauffindbarkeit von Finanzdaten eine vollständige Übersicht über die Vermögensverhältnisse des Unternehmens erschwert, ist eine Haftung des Unternehmens und seiner Organe nicht ausgeschlossen.

Ebenso kann dies der Fall sein bei der Gefährdung von Geschäftsgeheimnissen. So hat der Bundesgerichtshof die Haftung von Vorstand und Compliance-Officer erweitert in Bezug auf eine sog. „Garantenpflicht“, die zum Inhalt hat, im Zusammenhang mit der Tätigkeit des Unternehmens stehende Rechtsverletzungen von Unternehmensangehörigen durch geeignete unternehmensinternen Prozesse aufzudecken und zu verhindern. Neben dem Compliance-Beauftragten gilt dies grundsätzlich auch für andere Sonderbeauftragte in deren jeweiligen Pflichtenkreisen - wie etwa für den IT-Sicherheitsbeauftragten und gegebenenfalls auch den Datenschutzbeauftragten.

Der Bundesgerichtshof sieht die Sicherheit der Kommunikation als Compliance-relevante Verpflichtung an und hat ferner entschieden, dass Geschäftsinterna wegen der etwaigen Vorwerfbarkeit eines strafbaren Geheimnisverrats nicht ungesichert via E-Mail zur Verfügung gestellt werden dürfen.

## 3. Datensicherheit im Desasterfall

Der Schutz und die Sicherheit personenbezogener, steuerrelevanter oder sonst betriebskritischer Daten (wie insbesondere Daten des geistigen Eigentums) werden durch verschiedene nationale und internationale Regelwerke geschützt. In Deutschland finden sich derlei Regelungen verteilt über diverse Spezialgesetze, aber auch an zentraler Stelle im Bundesdatenschutzgesetz (BDSG): Gemäß § 9 BDSG sind alle Stellen, die personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und/oder organisatorische Maßnahmen zu treffen um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind. Die Spezifizierung dieser Anforderungen ergibt sich aus der Anlage zu § 9 (den sog. „8 Geboten der Datensicherheit"). Dort ist unter dem Punkt „Verfügbarkeitskontrolle" geregelt: „*Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden*." Als Maßnahme dafür ist u.a. das Vorhandensein eines Desaster- bzw. Backup-Konzepts („Disaster Recovery"/DR) vorgesehen um sicherzustellen, dass Daten nicht verloren gehen, selbst wenn sie versehentlich gelöscht oder zerstört werden. Auch die Rechtsprechung unterstreicht, dass eine zuverlässige IT-Sicherheit in Bezug auf Unternehmensdaten zu den Selbstverständlichkeiten im Zeitalter digitaler Datenverarbeitungen gehört (dazu unten IV)

## 4. Gewährleistung von Verfügbarkeit

Zwingender Bestandteil des demnach gebotenen IT-Risikomanagements (dazu unten VI) ist daher zugleich die jederzeitige Gewährleistung eines effizienten Kontinuitätsmanagements („Business Continuity"/BC), das - abgestuft nach der Unternehmensrelevanz der jeweiligen Daten - die Szenarien eines Desasters abbilden muss. Schlüsselsysteme wie das ERP beispielsweise sollten umgehend mit aktuellen Daten, die die Produktivsetzung ohne wesentlichen Zeitversatz erlauben, geladen werden können. Nur die nicht zeitkritischen Daten, die beispielsweise für externe oder interne Audits oder für ein Gerichtsverfahren als beweisrelevante Dokumente benötigt werden, sollten innerhalb von einer bis maximal zwei Wochen verfügbar sein.

Das Vorhandensein eines geeigneten, zeitgemäßen Notfallplans wird folgerichtig ebenfalls als organisatorische Selbstverständlichkeit der „Corporate Governance" vorausgesetzt. Dieser ist in regelmäßigen Abständen durch geeignete „scharfe" Tests auf seine Belastbarkeit zu überprüfen. Auch in den Maßnahmenkatalogen zu den spezielleren Regelungen des BDSG zur Verfügbarkeitskontrolle (s.o.) sind ein zeitgemäßes DR/BC-Konzept und die Dokumentation der regelmäßigen Überprüfung auf Schlüssigkeit, Angemessenheit und Funktionalität unverzichtbar.

Über zeitgemäße Backup- und Continuity-Systeme, deren Funktionalität durch regelmäßige Überprüfungen zu gewährleisten und gegebenenfalls an veränderte Bedrohungsszenarien anzupassen ist, ist gegen Verluste oder Kompromittierungen von Daten Vorsorge zu treffen. Solche Systeme müssen gleichzeitig aber auch den Bedürfnissen des Datenschutzes gerecht werden. Die Aufgabe des Managements ist es mithin, technisch-organisatorisch und rechtlich durch effiziente Maßnahmen der IT-Sicherheit, insbesondere durch DR/BC-Strategien, „beweissichere" Archivierung und flankierende IT-Richtlinien den Schutz unternehmenskritischer und personenbezogener Daten gegen Verlust, Störung der Verfügbarkeit oder ungewollte Offenlegung zu gewährleisten.

Die wichtigsten Vorschriften und Richtlinien für die Aufbewahrung und Sicherung bestimmter Kategorien von Daten - und damit zugleich die rechtlichen Grundlagen für eine revisionssichere Archivierung - sind geregelt im Bundesdatenschutzgesetz (Anlage 1 zu § 9 BDSG, Handelsgesetzbuch (§§ 257, 239 Abs. 4 HGB) und Abgabenordnung (§§ 146 Abs. 5, 147 AO) in Verbindung mit den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD

von 2014), die von allen Buchungspflichtigen zu beachten sind. Da für andere Rechtsgebiete keine vergleichbaren, branchenspezifischen Vorschriften bestehen, ist den handels- und steuerrechtlichen Anforderungen gleichsam eine Vorbildfunktion immanent für die interdisziplinär zu bestimmenden Aufbewahrungskriterien der Sicherheit, Vertraulichkeit, Integrität, jederzeitige Auffindbarkeit und Verfügbarkeit.

## III. Haupthaftungsrisiko: Nichtverfügbarkeit unternehmenskritischer Informationen

Unbeschadet der Vermögens-, Image- und sonstigen direkten oder indirekten Nachteile durch staatliche Sanktionen wie Bußgeldverfahren stellt die Information und ihre Verfügbarkeit einen Wert an sich und als solche die vitale Ressource jedes Unternehmens dar. Ihre Nichtverfügbarkeit erweist sich daher als besonders schadensträchtige Haftungsquelle. Den immanenten Risiken ist zu begegnen durch die „Compliance“ des Informationsmanagements mit den einschlägigen Bestimmungen – insbesondere zur Aufbewahrung:

### 1. Zulässige Aufbewahrungsformen

Jeder Kaufmann hat die Pflicht zur geordneten Aufbewahrung von geschäftlichen Unterlagen. Hierzu gehören unter anderem die „empfangenen und versandten Handelsbriefe“. Dies betrifft - oft übersehen - auch E-Mails. Ein Gutteil aller dienstlichen E-Mails dürfte die weite Definition des „Handelsbriefes“ erfüllen und damit aufbewahrungspflichtig sein.

Nach den Bestimmungen des Handels- und Steuerrechts (§§ 257, 239 HGB, §§ 146, 147 AO) können die empfangenen und abgesandten Handelsbriefe und die Buchungsbelege auch als Wiedergabe auf einem Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsgemäßer Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden, sie während der Dauer der Aufbewahrungsfrist verfügbar sind sie jederzeit innerhalb angemessener Frist, die Frage des Einzelfalls ist, lesbar gemacht und für die Besteuerung maschinell ausgewertet werden können.

Handels- und Steuerrecht verlangen mithin Transparenz sowie Revisions- und Datensicherheit. Die GoBD geben dabei den Regelungsrahmen vor. Neben geeigneten technisch-organisatorischen Sicherheitsvorkehrungen stellen sie insbesondere Vorschriften für die Archivierung digitaler Dokumente und für den Zugriff auf diese Dokumente im Rahmen von Betriebsprüfungen auf. Diese Vorschriften können gerade am Beispiel von E-Mails, die häufig „Handelsbrief“, gelegentlich auch „Beleg“ oder „Rechnung“ im Rechtssinne sein können, mannigfaltige Probleme aufwerfen:

### 2. Aufbewahrung und Prüfung nach den „GoBD“

Hiernach hat der Steuerpflichtige sein IT-System gegen Verlust (z.B. Unauffindbarkeit, Vernichtung, Kompromittierung und Diebstahl) zu sichern und gegen unberechtigte Eingaben und Veränderungen zu schützen. Werden die elektronischen Dokumente nicht ausreichend geschützt und können deswegen nicht mehr vorgelegt werden, ist die Buchführung formell nicht mehr ordnungsgemäß. Das zum Einsatz kommende Verfahren muss die Gewähr der Integrität bieten. Alle Informationen (Programme und Datenbestände), die einmal in den Verarbeitungsprozess eingeführt wurden, dürfen nicht mehr unterdrückt oder ohne Kenntlichmachung überschrieben, gelöscht, geändert oder verfälscht werden können. Es ist ein internes Kontrollsystem (IKS) einzurichten, auszuüben und zu protokollieren. Notwendig ist ferner eine umfassende Verfahrensdokumentation, die nachvollziehbar beschreibt, wie die relevanten Informationen angelegt, geordnet, gespeichert, indiziert und geschützt wurden und später wieder gefunden und verlustfrei reproduziert werden können. Es besteht demnach eine Indexierungspflicht. Der Erhalt der Verknüpfung zwischen Index, digitalem Dokument und Datenträger muss während der gesamten Aufbewahrungsfrist gewährleistet sein. Die archivierten Daten müssen in wiedergabefähiger, maschinell lesbarer und auswertbarer Form

zur Verfügung gestellt werden können. Ihre periodengerechte Auswertung durch die jeweils aktuelle Prüfsoftware der Finanzverwaltung muss gewährleistet sein.

Neben den außersteuerlichen und steuerlichen Informationen zu Geschäftsvorfällen sind alle Unterlagen aufzubewahren, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind. Betroffen sind zum einen alle steuerrelevanten Unterlagen, also sämtliche Informationen, die für eine steuerliche Veranlagung im Sinne von Entstehen, Entfallen oder Minderung einer Steuerlast Bedeutung erlangen können. Andererseits geht es bei den Aufbewahrungspflichten nicht allein um die im engeren Sinne steuerrelevanten Unterlagen. Gemeint sind darüber hinaus die nach Handelsrecht aufbewahrungspflichtige „bloße“ Geschäftskorrespondenz und die einschlägigen Organisationsunterlagen des Unternehmens (beispielsweise Gründungsprotokolle, Prüfberichte, Aufsichtsratsbeschlüsse, ferner aber auch die Arbeitsverträge, Lohn- und Sozialversicherungsunterlagen der Arbeitnehmer oder die im laufenden Geschäftsbetrieb abgeschlossenen Verträge mit der in diesem Zusammenhang angefallenen Korrespondenz, gleichgültig in welcher Form).

**2. Aufbewahrungsfristen**

Das öffentliche Recht kennt eine Vielzahl unterschiedlicher, über die verschiedensten Regelwerke verstreute Aufbewahrungsfristen, die von einem Jahr bis zu 30 Jahren (und in Ausnahmefällen darüber) liegen können. Die Aufbewahrungsfrist knüpft in der Regel an den jeweiligen Aktenvorgang an und beginnt mit dem Ablauf des betreffenden Haushaltsjahres.

Im Bereich des Privatrechts sind Rechnungen und andere Buchungsbelege, bestimmte Zollunterlagen und Handelsbücher nebst allen Aufzeichnungen (so auch Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zum Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen) 10 Jahre, die sonstigen handels- und steuerrechtlich relevanten Unterlagen (Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind) 6 Jahre aufzubewahren.

Wichtig bei der Berechnung der Aufbewahrungsfrist ist, dass der Fristenlauf erst mit dem Ende des Kalenderjahres beginnt, in welches der betreffende „Geschäftsvorfall“ fällt. Es ist also danach zu fragen, wann der Buchungsbeleg entstanden ist bzw. wann die geschäftsrelevante E-Mail gesendet oder empfangen wurde. Eine Verlängerung durch offene Veranlagungszeiträume, für die noch kein bestandskräftiger Steuerbescheid vorliegt, ist möglich und daher vom Unternehmen bei der Berechnung seiner Aufbewahrungsfristen gleichfalls zu berücksichtigen. Daraus kann sich im Einzelfall eine deutliche Erstreckung der Aufbewahrungsfristen um mehrere Jahre ergeben.

In der Praxis gestaltet sich die Abgrenzung der Handels- oder Geschäftsbriefe und sonstigen steuerrelevanten Unterlagen (Archivierung über mindestens 6 Jahre) schwierig, insbesondere von den Buchungsbelegen, für die eine wenigstens zehnjährige Aufbewahrungsfrist besteht. Gerade bei E-Mails kann die Grenze zu den steuerrelevanten Buchhaltungsunterlagen fließend sein, dies insbesondere in den Fällen, in denen der E-Mail zugleich Belegfunktion zukommt, weil sie nicht nur als Informationsträger, sondern beispielsweise auch zur Fakturierung oder zur Auftragsabwicklung eingesetzt wird (dazu sogleich unten Ziff. 3). Deshalb sollten im Zweifel auch alle elektronisch archivierten E-Mails in revisionssicherer Form über die Zehnjahresfrist verfügbar gehalten werden. Diese Organisationsentscheidung ist allerdings gegen das Gebot der Datensparsamkeit aus dem BDSG abzuwägen und das Ergebnis dieses Abwägungsvorgangs zu dokumentieren.

**3. Haftungsfalle E-Mail: Sichere Kommunikation, Aufbewahrung, Beweismittel**

Ein Paradebeispiel unzureichenden Informationsmanagements ist nach wie vor das Thema E-Mail. Hier ist immer noch anzutreffen, dass Mail-Accounts durch Mitarbeiter in regelmäßigen Abständen „auf eigene Faust“ analysiert,

Altbestände in Archivordner verschoben und E-Mails, die für nicht mehr geschäftsrelevant gehalten werden, gelöscht werden. Eine solche Praxis steht regelmäßig im Widerspruch zu den Bestimmungen des Fernmeldegeheimnisses, des Datenschutzrechts und zu den gesetzlichen Aufbewahrungsvorschriften. Wie bereits dargelegt, sieht der Bundesgerichtshof die Sicherheit der Kommunikation zudem als Compliance-relevante Verpflichtung an und bestätigt, dass geschäftliche Interna im Grundsatz nicht ungesichert per E-Mail zur Verfügung gestellt werden dürfen. Die im Rahmen der IT-Sicherheit geforderte Integrität, Vertraulichkeit und Verfügbarkeit kritischer Daten betrifft mithin gerade auch E-Mails.

Die E-Mail-Verfügbarkeit im Rechtsstreit, bei der Innenrevision oder der Steuerprüfung ist das häufigste Praxisbeispiel, aus dem sich juristische Fallstricke ergeben können. Gerade am Beispiel der E-Mail zeigt sich besonders deutlich das Interesse des Unternehmens, zu seiner eigenen Rechtssicherheit und beweisrechtlichen Positionierung so viele Informationen wie möglich zu sammeln, abzuspeichern, auszuwerten und für die Zukunft verfügbar zu halten. Denn in einem Prozess muss jede Partei die ihr günstigen Tatsachen darlegen und beweisen. Der Erfolg der Beweisführung wird dabei maßgeblich durch die Beweisqualität der vorzulegenden Dokumente beeinflusst. Dies betrifft namentlich Fragen der „Compliance“ mit den Ordnungs- und Aufbewahrungskriterien der GoBD und - im Bereich der personenbezogenen Daten - „den 8 Geboten der Datensicherheit“.

E-Mail-Accounts können steuerrelevante Informationen enthalten, und zwar sowohl hinsichtlich der Anhänge wie auch hinsichtlich des E-Mail-Textes selbst. Steuerrelevanz ist gegeben, wenn eine Rechnung als oder per E-Mail gesendet wird. Zu denken ist jedoch nicht allein an die Fälle der elektronischen Fakturierung. Vielmehr betrifft die Steuerrelevanz von E-Mails auch die elektronische Belegeverwaltung, Spesenabrechnungen, Preiskalkulationen und steuerrelevante Vertragsgestaltungen. Schon Kommentierungen zu Mail-Attachments mit Berechnungen, Vertragsklauseln etc. machen eine E-Mail steuerrelevant und führen zum Erfordernis der zehnjährigen steuersicheren Aufbewahrung. In diesen Fällen sind neben der Abgabenordnung die GoBD mit dem dortigen Erfordernis der wahlfreien maschinellen Auswertbarkeit - gemeint ist ein Lesevollzugriff - einschlägig. Demnach ist die elektronische Post durch Übertragung der Inhalts- und Formatierungsdaten auf einem Datenträger zu archivieren und mit einem unveränderbaren Index zu versehen. Im Rahmen der digitalen Außenprüfung geht es also bei der Aufbewahrungspflicht von E-Mails darum, mittels Recherche auf solche E-Mails lesend zuzugreifen, die einen steuerrelevanten Inhalt besitzen und die gegebenenfalls diesen E-Mails beigefügten Anhänge lesen bzw. auswerten zu können. Bei der Archivierung von E-Mails ist außerdem darauf zu achten, dass auch die Anlagen und - im Falle der Signierung und Verschlüsselung - auch die verschlüsselten und entschlüsselten Dokumente nebst Schlüsseln mit aufbewahrt werden. Für die elektronische Aufbewahrung unter GoBD-Gesichtspunkten ist dabei entscheidend, ob die E-Mail selbst steuerrelevante Informationen beinhaltet oder ob sie nur als Trägermedium für eine steuerrelevante Information fungiert.

**4. Haftungsfolgen**

Eine in jeder Hinsicht rechtskonforme, geordnete und jederzeit verfügbare Aufbewahrung ist auch prozessrechtlich aus Gründen der strategischen Rechtssicherheit unabdingbar, insbesondere um sich gegebenenfalls für eine künftige juristische Auseinandersetzung beispielsweise mit Vertragspartnern, Belegschaft oder auch den Steuerbehörden und der Datenschutzaufsicht beweisrechtlich positionieren zu können. Denn das Hauptrisiko stellen in wirtschaftlicher Hinsicht die Haftungsfolgen infolge von Versäumnissen beim IT-Risikomanagement dar. Das Schadenspotenzial, das sich beispielsweise aus der Nichtverfügbarkeit beweiserheblicher Daten oder betriebswichtiger Systeme ergeben kann, ist beträchtlich. Neben der persönlichen Haftung des Managements ist hier die volle Bandbreite der Schadenshaftung, von der Anfechtbarkeit des Beschlusses über die Vorstandsentlastung bis zur außerordentlichen Kündigung des Anstellungsvertrages (nebst Abberufung aus der Funktion des CEO), eröffnet. Für Berufsgeheimnisträger wie Anwälte, Steuerberater und Wirtschaftsprüfer bedeuten IT-Schäden und deren Folgen neben den Umsatzverlusten und Kosten für die Wiederbeschaffung und Wiederherstellung von Daten insbesondere auch Haftung gegenüber

Mandanten, berufsrechtliche Inanspruchnahme, Reputationsverlust - und in der Regel auch das Ende von Mandatsverhältnissen.

Versäumnisse können im IT-Risikomanagement zudem zum Verlust des Versicherungsschutzes führen, denn mangelnde IT-Compliance ist als Erhöhung der versicherten Gefahr z.B. in der *IT-Coverage* und in der *Director's and Officer's* Versicherung anzeigepflichtig. Das Fehlen bzw. die Ungeeignetheit einer dem Stand der Technik entsprechenden IT-Infrastruktur und deren Einbettung in ein ganzheitliches Risikomanagement können im Rechtsstreit als grobe Fahrlässigkeit zum Verlust des Versicherungsschutzes oder zum erfolgreichen Einwand des Mitverschuldens führen. Im Extremfall kann es zu einer Reduzierung der eigenen Schadensansprüche auf Null kommen, wenn Mängel der IT-Compliance den Schaden ermöglicht, mit verursacht oder erhöht haben.

Darüber hinaus kann der Verlust wichtiger bzw. die Offenbarung vertraulicher Daten leicht zu einem über den bezifferbaren Schaden noch deutlich hinausgehenden Imageschaden führen, etwa wenn grobe Versäumnisse im Bereich des Datenschutzes an die Öffentlichkeit gelangen. Hinzuweisen ist ferner auf die „Skandalisierungspflicht" (§ 42a BDSG), wonach ein solches Szenario bei besonders sensiblen Daten (etwa Bankdaten, Kundendaten, Mitarbeiterdaten, Kommunikationsdaten mit Kunden, Mitarbeitern, Behörden, Wirtschaftsprüfern, Anwälten etc.) nicht nur der zuständigen Aufsichtsbehörde und der von der Datenschutzverletzung betroffenen Person anzuzeigen sondern dieser Umstand gegebenenfalls zudem in mindestens halbseitigen Anzeigen in zwei bundesweit erscheinenden Tageszeitungen zu veröffentlichen ist. Eine solche Benachrichtigung ist jedoch nicht erforderlich bei einem entsprechenden Sicherheitskonzept und einer verschlüsselten Speicherung. Auch hier zeigt sich, dass nur ein hoher Standard bei der IT-Sicherheit gewährleisten kann, dass Folgeschäden für das Image des Unternehmens verhindert werden.

## IV. Gesetzgebung und Rechtsprechung zur IT-Sicherheit

### 1. Gesetzgebung

Der Schutz und die Sicherheit von Informationen werden durch verschiedene nationale und internationale Regelwerke geschützt. In Deutschland finden sich derlei Regelungen verteilt über diverse Spezialgesetze, aber auch an zentraler Stelle im BDSG (dazu schon oben II 2-4).

Ein Blick ins Ausland belegt dort ähnliche, teilweise noch schärfere Kriterien: So unterliegen alle amerikanischen Unternehmen und Prüfungsgesellschaften, auch ausländische Prüfungsgesellschaften und Unternehmen mit einer amerikanischen Börsennotierung, dem Sarbanes-Oxley-Act von 2002, der strenge Anforderungen bezüglich Aufbewahrung, Änderung und Zerstörung von Unterlagen bzw. Daten aufstellt. Die Sicherung der Finanz- und Geschäftsdaten ist ein wesentlicher Bestandteil, um diese zu erfüllen. Durch die extraterritoriale Wirkung des Gesetzes sind inzwischen in den meisten Ländern entsprechende nationale Vorschriften entstanden, wie z.B. die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates. Und neben zahlreichen anderen Anforderungen der IT-Compliance verlangen Basel II und III, dass Finanzinstitute ihre Daten stets vertraulich, integer und verfügbar haben und Backup-Pläne für die Systeme vorhanden sein müssen.

Auf europäischer Ebene wird sich die EU-Datenschutz-Grundverordnung (DS-GVO) des Themas annehmen. Ab dem 25.05.2018 wird sie auf Unternehmen und Behörden anwendbar. Die DS-GVO wird sich auf alle Unternehmen auswirken, die geschäftlich von der EU aus tätig sind bzw. Geschäftsbeziehungen zu Unternehmen und Organisationen mit Sitz in der EU unterhalten oder ihre Daten in EU-Mitgliedsstaaten sammeln, verarbeiten und speichern (lassen). Damit erstreckt sich die Verordnung auch auf Verarbeiter mit Sitz außerhalb der EU. Die DS-GVO wird demnach erhebliche Konsequenzen auch für nicht-europäische Unternehmen haben, die in der EU tätig sind, da Anknüpfungspunkt die Geschäftstätigkeit bzw. das Handeltreiben in den Mitgliedsstaaten der EU ist. Die Regelungen der DS-GVO über die Datensicherheit sind zum Gutteil den inländischen Regelungen des BDSG nachempfunden.

Insgesamt wird sich die Verordnung in datensicherheitsrechtlicher Hinsicht an der Maxime „Datenschutz durch Technik“ („Privacy by Design“) und durch „datenschutzfreundliche Voreinstellungen“ („Privacy by Default“) orientieren. Die EU-Kommission kann die Kriterien und Anforderungen in Bezug auf die Maßnahmen und Verfahren festlegen, speziell was die Anforderungen an den Datenschutz durch Technik und die datenschutzfreundlichen Voreinstellungen für ganze Sektoren und bestimmte Erzeugnisse und Dienstleistungen betrifft sowie die technischen Standards hierfür definieren.

Der Grundsatz des Datenschutzes durch Technik verlangt, dass der Datenschutz während des gesamten Lebenszyklus der Technologie „eingebaut“ sein muss, von der frühesten Entwicklungsphase über ihre Einführung und Verwendung bis zur endgültigen Außerbetriebnahme. Die Ermittlung der Risiken und die hieraus abzuleitenden Maßnahmen zu deren Eindämmung sind also bereits im Vorfeld des Einsatzes der Technik konzeptionell zu entwickeln. Sie müssen ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Die technischen und organisatorischen Maßnahmen für die Datensicherheit sollen grundsätzlich auf Basis einer Risikobewertung erfolgen. Ähnlich wie im bereits aus dem Aktien- und Handelsrecht bekannten Teilbereich der „Corporate Governance“ mit den dortigen Rechtspflichten für ein effizientes Risikomanagement (und ein hierauf bezogenes internes Kontrollsystem mit entsprechender Dokumentationspflicht, dazu noch unten VI) soll diese Risikobewertung dokumentiert sein. Gleiches gilt für die hieraus abgeleiteten Maßnahmen in Bezug auf die IT-Sicherheit und insbesondere für von der IT ausgehende unternehmensgefährdende Risiken durch Datenverlust oder Verletzungen des Datengeheimnisses und des geschäftlichen Geheimnisschutzes. Die Maßnahmen sollen dabei den aktuellen Stand der Technik „für bestimmte Sektoren und Datenverarbeitungssituationen“ sowie die technologische Entwicklung berücksichtigen. Eine frühzeitige und regelmäßige Soll-/ Ist-Analyse mit Risikobewertung und mit einer entsprechenden Datenschutz-/ Datensicherheits-Folgeabschätzung ist aus diesem Grunde dringend anzuraten.

Etwaige Sicherheitsverletzungen sind zwingend zu dokumentieren, dies unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der einschlägigen Verordnungsbestimmungen ermöglichen. Die Sicherheit der Verarbeitung obliegt allen hieran Beteiligten, also sowohl dem verantwortlichen Unternehmen wie auch dem Auftragsdatenverarbeiter oder - beispielsweise in Konzernstrukturen - beiden oder allen Unternehmen, die wechselseitig für sich oder für Dritte oder auch gemeinsam verordnungsrelevante Daten verarbeiten.

Ähnlich dem deutschen Vorbild in § 109a TKG sind Verlautbarungspflichten, sog. „Data Breach-Notifications“, vorgesehen, insbesondere in Fällen von Sicherheitslecks. Hier hat entsprechend dem TKG eine Meldung an die Aufsichtsbehörde zu erfolgen. Die Aufsichtsbehörde kann das verantwortliche Unternehmen zur Benachrichtigung der Betroffenen nach Prüfung der negativen Auswirkungen verpflichten. Eine Benachrichtigung entfällt, wenn der Aufsichtsbehörde nachgewiesen wird, dass geeignete technische Sicherheitsvorkehrungen getroffen wurden. (Nach Maßgabe dieser technischen Sicherheitsvorkehrungen sind insbesondere die betreffenden Daten für alle Personen zu verschlüsseln, die nicht zum Zugriff auf Daten befugt sind.)

Der Sanktionskatalog der DS-GVO sieht bei erstmaligen, unvorsätzlichen Verstößen die Verwarnung und bei lediglich leichten Verstößen Strafen bis zu 250 TEUR bzw. im Falle von Unternehmen von bis zu 0,5 % des weltweiten Jahresumsatzes vor. Bei schweren Verstößen sind Strafen von bis zu 500 TEUR bzw. von bis zu 1 % des weltweiten Jahresumsatzes vorgesehen. Schwerste Verstöße können sanktioniert werden mit Strafen bis zu 1 Mio. bzw. bis zu 2 % des weltweiten Jahresumsatzes, wobei ein solcher gravierender Verstoß etwa darin gesehen wird, dass Datenverarbeitungen ohne hinreichende Rechtsgrundlage oder mit unzureichenden Sicherheitsmaßnahmen oder unter anschließender Verletzung der Notifikationspflichten durchgeführt werden.

## 2. Rechtsprechung

Auch die Rechtsprechung unterstreicht, dass eine zuverlässige IT-Sicherheit in Bezug auf Unternehmensdaten zu den unternehmerischen Selbstverständlichkeiten im Zeitalter digitaler Datenverarbeitungen gehört. Die Arbeitsgerichtsbarkeit wertet das betriebliche Interesse an Datensicherheit als Rechtsgut, das höher zu werten ist als das der unternehmerischen Mitbestimmung. Nicht zuletzt das höchste deutsche Zivilgericht, der Bundesgerichtshof, sieht die Sicherheit der Kommunikation als Compliance-relevante Verpflichtung an. Unternehmenskritische - und insbesondere auch beweiserhebliche - Dokumente müssen aus Gründen der Rechtssicherheit und Beweisführung vorgehalten werden. Wird dies nicht ermöglicht, kann ein Prozess bereits unter bloßen Beweislastgesichtspunkten wegen „Beweisfälligkeit“ verloren gehen.

Ein Outsourcing der IT-Sicherheit genügt grundsätzlich nicht, das delegierende Unternehmen und dessen Management zu Lasten beauftragter IT-Unternehmen (wie z.B. Cloud-Provider oder IT-Wartungsfirmen) zu „exkulpieren“, also aus der haftungsrechtlichen Verantwortung für den Schutz und die Sicherheit seiner Daten und Systeme zu nehmen. Dies kann sogar gelten bei einem Verschulden des externen IT-Dienstleisters bei einem Datenverlust, wenn das den Auftrag erteilende Unternehmen die Konsequenzen dieses Verlusts durch unzuverlässige Desaster- und Backup-Strategien mit verursacht hat. Der Mitverschuldensanteil kann hier bis zu 100 %, also bis zur Vollhaftung des Unternehmens für den entstandenen Datenverlust und damit den hierdurch verursachten finanziellen Schaden, führen. Zu beachten ist in diesem Kontext auch die Beweislastumkehr, wonach in Fällen, in denen streitig ist, ob die zuständigen Mitglieder des Managements die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, diese zu ihrer Exkulpation die alleinige Beweislast trifft.

Was das Desaster-Management anbelangt, verlangt die Rechtsprechung als allgemeine Schutz- und Sorgfaltspflicht, dass regelmäßig und zuverlässig geeignete, lückenlose Datensicherungsroutinen eingesetzt werden. Dies dürfen auch externe Fachpersonen - wie etwa mit Wartung und Support beauftragte IT-Firmen oder Rechenzentrumsbetreiber, die im Wege der Auftragsdatenverarbeitung mit den Daten des Unternehmens arbeiten - ohne besondere Erkundigungspflicht als Selbstverständlichkeit voraussetzen. Es bestehen insoweit grundsätzlich keine zusätzlichen Überprüfungs- und Hinweispflichten solcher externer Dritter. Umgekehrt sind aber diese Dritten wiederum im Zweifel auch ohne ausdrückliche Vereinbarung zu Datensicherungsmaßnahmen wie insbesondere Backups verpflichtet, wenn die Verarbeitung von Unternehmensdaten zu ihrem Vertragspflichtenkreis gehört.

Konkret verlangt die Rechtsprechung die Implementierung und Überprüfung zuverlässiger Sicherheitsroutinen im Bereich Produktivsystem, Archivsystem und Backup. Datensicherungsroutinen, die nicht täglich die Unternehmensdaten sichern und eine Vollsicherung mindestens einmal wöchentlich gewährleisten, sind hiernach ungeeignet. Weiter werden zum unternehmerischen IT-Schutzpflichtenkreis revisionssichere Archivierungsprozesse gezählt, Firewalls, Filter- und Überwachungssysteme, eine Verschlüsselung jedenfalls bei besonders sensitiven Daten sowie eben auch ein Kontinuitätsmanagement, das einen Wiederanlauf nach Wiederherstellung von System und Daten im Schadensfall gewährleistet. Organisatorisch sind geeignete IT-Unternehmens- und Datenschutzrichtlinien sowie eine entsprechende Einweisung und Schulung der Mitarbeiter erforderlich.

Gerade auch Unternehmen mit effektiver Geschäftstätigkeit in UK und den USA sehen sich der besonderen Bedeutung (und erheblichen Sanktionsfolgen) eines lückenlosen und beweissicheren Dokumentmanagement ausgesetzt. Dementsprechend wurden die Zivilprozessordnungen beispielsweise im UK in 2010 ergänzt um Regelungen zur elektronischen Bereitstellung. Dasselbe gilt für Ergänzungen im US-Zivilprozessrecht im Jahre 2006. Im Zuge dieser Entwicklungen wurden zugleich neue Sanktionen für Vertraulichkeits- und Datenschutzverletzungen implementiert.

Zusammengefasst etabliert die Rechtsprechung zunehmend - und vor dem Hintergrund von Regelwerken mit Ausstrahlungswirkung in andere Wirtschaftsbereiche (wie etwa den SEC-Regeln, dem Sarbanes-Oxley-Act oder den

Baseler Eigenkapitalübereinkünften) - allgemeine Sorgfaltspflichten für eine effektive, zeitgemäße IT-Sicherheit. Es lässt sich die Tendenz ersehen, eine Vorlage von Daten, auch wenn diese bereits vor langer Zeit in großen, gegebenenfalls auch externen oder auch internationalen (Backup-) Speichern abgelegt wurden und entsprechend schwer verfügbar gemacht werden können, für ein laufendes Gerichtsverfahren in einer „beweisfesten" Form zu verlangen, wobei diese Verpflichtung besteht unabhängig von gegebenenfalls höherer Gewalt oder etwaigem Fremdverschulden. Dies bedingt ggf. den Einsatz zeitgemäßer IT-Systeme, die starke Indizien für Beweissicherheit - und damit letztlich Rechtssicherheit - liefern.

**3. Ausgewählte Praxisbeispiele**

An prominenten Rechtsfällen ist zunächst Daten-Desaster im Cloudservice „Amazon EC 2" aus dem April 2011 zu nennen, bei dem eine unbekannte Datenmenge unwiederbringlich verloren ging. Amazon musste seinerzeit einräumen, dass sämtliche Versuche zur manuellen Wiederherstellung der Kundendateien gescheitert waren. Ähnliches war bei einem anderen Cloudservice schon im Oktober 2009 geschehen: Ein Serverfehler hatte zu Datenverlust bei Nutzern des Dienstes „Sidekick", den T-Mobile gemeinsam mit der Microsoft-Tochter Danger anbot, geführt. Die US-Telekom-Tochter „T-Mobile USA" teilte mit, dass es bei einem Rücksetzen der Mobilgeräte zu einem Verlust von in der Cloud gespeicherten Daten wie Kontakten, Terminen, Aufgaben und Bildern gekommen sei. Abermals die Telekom stand in der Kritik für Datenverluste in ihrem E-Mail-Center aus dem September 2010. Dem Vernehmen nach waren Einstellungen in den Posteingangsordnern, die mit „Nie löschen" hinterlegt waren, in Folge eines Updates mit einer Standard-Vorhaltedauer von 90 Tagen überschrieben worden. Businessmails, die älter als 90 Tage waren, gingen Nutzerangaben zufolge unwiederbringlich verloren.

Auch das vermeintliche Qualitätsmerkmal „Cloud made in Germany" konnte sich daher bislang nicht mit überzeugendem Erfolg an den technischen Herausforderungen einer durchgängigen IT-Sicherheit und Verfügbarkeit betriebskritischer Daten im Falle von Angriffen und Desaster-Szenarien beweisen.

Auf verwaltungsrechtlicher Ebene begannen im März 2016 erste Landesdatenschutzbehörden damit, Bußgeldverfahren gegen Unternehmen einzuleiten, die - nach dem Wegfall der Rechtsgrundlage für Datentransfers in die USA („Safe Harbor") durch Urteil des Gerichtshofs der Europäischen Union (EuGH) vom 06.10.2015 - weiterhin personenbezogene Daten in die USA transferierten, um sie dort zu speichern oder zu verarbeiten. Derlei Fälle unzulässiger Datenübertragungen in datenschutzrechtlich „unsichere Drittstaaten" können über die Verhängung empfindlicher Bußgelder bis hin zur Untersagung der Datenverarbeitung und Betriebsstilllegung führen. Die besagten Bußgeldverfahren betrafen ursprünglich die Bundesländer Hamburg, Rheinland-Pfalz und Bayern, sind inzwischen allerdings dem Vernehmen nach auch auf weitere Bundesländer ausgeweitet worden.

Aus der inländischen zivilrechtlichen Judikatur, bei der zumeist Haftungstatbestände im Zusammenhang mit dem Verlust betriebswichtiger oder dem fahrlässigen Bruch der Vertraulichkeit geheimhaltungsbedürftiger Daten Anlass für - auch persönliche (Managerhaftung) - Schadensersatzansprüche waren, erscheinen insbesondere die folgenden Aussagen praxisrelevant:

- Das Fehlen eines IT-Sicherheitskonzepts berechtigt ein Unternehmen dazu, den mit einem Vorstandsmitglied geschlossenen Anstellungsvertrag außerordentlich und mit sofortiger Wirkung zu kündigen (Landgericht Berlin) bzw. bei Mängeln in der Dokumentation eines Früherkennungssystems in Bezug auf dem Unternehmen drohende Risiken einen wichtigen Grund zu sehen, der zur Anfechtbarkeit des Beschlusses über die Haftungsentlastung des gesamten Vorstands führt (Landgericht München I).

- Das Landesarbeitsgericht Rheinland-Pfalz sieht in dem betrieblichen Interesse an Datenschutz und Datensicherheit ein überragendes Rechtsgut, das in der Abwägung gewichtiger ist als die betriebliche

Mitbestimmung, weshalb kollektiv-arbeitsrechtliche Aspekte im Zweifel gegenüber Aspekten der Datensicherheit zurücktreten.

- Die Oberlandesgerichte Hamm, Karlsruhe und Köln beurteilen eine zuverlässige IT-Sicherheit in Bezug auf Unternehmensdaten als unternehmerische Selbstverständlichkeit, die hinsichtlich ihrer haftungsrechtlichen Aspekte auch nicht durch Maßnahmen des Outsourcings auf Dritte delegiert werden können.

- In Fällen, in denen kein aktuelles Backup vorliegt, wird darüber hinaus sogar bei solchen Datenverlusten, die infolge fehlerhafter Wartungsarbeiten eines beauftragten IT-Fachdienstleisters eintreten, ein *Allein*verschulden des beauftragenden Unternehmens angenommen (Oberlandesgericht Hamm).

- Der Bundesgerichtshof sieht in der Sicherheit der elektronischen Kommunikation eine Compliance-relevante Verpflichtung, wenn er ausführt, dass geschäftliche Interna wegen des immanenten Risikos eines Geschäftsgeheimnisverrats nicht ungesichert per E-Mail zur Verfügung zu stellen sind.

- Ebenfalls laut Bundesgerichtshof steht der Compliance-Beauftragte in der persönlichen Haftung für Informationsschutzpflichtenverstöße, aus denen sich die Gefahr ergibt, dass aus dem Unternehmen heraus Rechtsgüter verletzt und Straftaten begangen werden. (Wegen vergleichbarer Interessenlage dürfte viel dafür sprechen, dass diese Rechtsprechung auch für weitere Sonderbeauftragte wie den Datenschutzbeauftragten sowie für leitende Ressortverantwortliche wie den IT-Sicherheitsbeauftragten einschlägig ist.)

## V. Das IT-Sicherheitsgesetz

Durch das seit dem 25.07.2015 in Kraft stehende Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz“) werden bestimmten Branchen und Kategorien von Unternehmen mannigfaltige Verpflichtungen in Bezug auf die Sicherheit ihrer Systeme und Daten auferlegt. Darüber hinausgehend werden allgemein alle geschäftsmäßigen Anbieter von Telemediendiensten zur Umsetzung von Sicherheitsmaßnahmen nach dem Stand der Technik verpflichtet; dies betrifft nahezu sämtliche nicht dem rein privaten Bereich zuzurechnenden Internet-Angebote wie Webshops, Online-Auktionshäuser, Suchmaschinen, Webmailer, Informationsdienste, Podcasts, Chatrooms, Social Communities, Webportale und Blogs. Zentraler Gesetzeszweck ist die Fortsetzung der nationalen und - beispielsweise auf EU-Ebene - internationalen Bestrebungen, Betriebsausfälle und Haftungsrisiken gesetzgeberisch bestmöglich zu beschränken.

Angriffe auf Daten und Systeme gehören inzwischen zum unternehmerischen Alltag. In Ländern mit zahlreichen Technologieführern wie Deutschland ist dies in besonderem Maße - und rasant zunehmend - zu beobachten (dazu bereits oben II 1). Vor dem Hintergrund dieser Gefahren ist das neue Gesetz entstanden; die wichtigsten Regelungen bestehen in der Formulierung von neuen bzw. erweiterten

- technischen Sicherungspflichten für Telemediendiensteanbieter im reformierten Telemediengesetz (TMG; dazu unten 2.) und

- technischen Mindestanforderungen und Meldepflichten zu IT-Sicherheitsvorfällen für die Betreiber kritischer Infrastruktureinrichtungen (KRITIS) im neuen Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz /BSIG; dazu sogleich 1.).

### 1. KRITIS-Betreiber und das BSIG

Der KRITIS-Adressatenkreis ist in der am 03.05.2016 in Kraft getretenen „Rechtsverordnung zur Bestimmung kritischer Infrastrukturen“ (im Sinne des BSIG) festgelegt. Es handelt sich hierbei um Unternehmen aus den Sektoren

- Energie,
- Informationstechnik und Telekommunikation,
- Transport und Verkehr,
- Gesundheit,
- Wasser,
- Ernährung sowie
- Finanz- und Versicherungswesen,

wenn diese Infrastrukturen von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil ihr Ausfall oder ihre Beeinträchtigung zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentlichen Sicherheit führen würde.

KRITIS-Betreiber werden verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen vor dem Hintergrund der Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen und Prozessen maßgeblich sind. Die Maßnahmen müssen dabei sowohl präventive Ziele verfolgen wie auch Maßnahmen zur Entdeckung und Behebung von Störungen enthalten.

Anforderungsmaßstab ist der aus anderen Gesetzen bekannte „Stand der Technik“, d.h. der „Einsatz fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, die den Schutz der Funktionsfähigkeit [der IT] gegen Beeinträchtigungen gesichert erscheinen lassen“. Über die Anforderung des (jeweiligen) „Stand(es) der Technik“ wird sichergestellt, dass die Unternehmen hinsichtlich ihrer Sicherheitsstandards Flexibilität und Aktualität gewährleisten. Die Unternehmen stehen daher beispielsweise in der Pflicht, ihre Sicherheitstechnik fortlaufend zu überprüfen und zu aktualisieren, insbesondere also für zeitnahe Sicherheits-Updates zu sorgen. Gleichzeitig müssen die Auswirkungen der Maßnahmen beherrschbar bleiben. KRITIS-Betreibern wird mithin eine Technikfolgenabschätzung auferlegt. Die Betreiber und ihre Branchenverbände haben jedoch auch die Möglichkeit, selbst für Rechtssicherheit zu sorgen, indem branchenspezifische Sicherheitsstandards zur Einhaltung der Anforderungen erarbeitet und dem BSI vorgeschlagen werden. Auf Antrag stellt das BSI sodann fest, ob diese Standards geeignet sind, die Einhaltung der Anforderungen zu gewährleisten. Die Umsetzungen von Maßnahmen zur Einhaltung der Anforderungen können durch Auditierungen, Prüfungen oder Zertifizierungen erfolgen; das BSI kann hier Konkretisierungen treffen.

IT-Sicherheitsvorfälle sind dem BSI zu melden, um die Erstellung eines IT-Sicherheitslagebildes zu ermöglichen und sämtliche Betreiber frühzeitig warnen zu können. Die Meldepflicht differenziert zwischen solchen Vorfällen, die zu einem Ausfall führen können (z.B. bei entdeckten Sicherheitslücken, Schadprogrammen und ähnliche schädliche Einwirkungsmöglichkeiten) und solchen, die tatsächlich bereits zu einem Ausfall geführt haben. Eine namentliche Meldung des Betreibers ist nur bei tatsächlichen Ausfällen oder Beeinträchtigungen der Funktionsfähigkeit erforderlich. Gemeint sind hier unmittelbare Auswirkungen auf die KRITIS.

Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse sind unverzüglich - maximal binnen 14 Tagen - zu melden, wenn sie erheblich sind, d.h. die Funktionsfähigkeit der KRITIS zumindest bedroht ist und sie nicht automatisiert oder mit geringem Aufwand abgewehrt werden kann. Eine Störung in diesem Sinne liegt vor, wenn die eingesetzte Technik ihre Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, auf sie einzuwirken. Als Störung gelten auch externe Angriffe wie Cyberattacken zu Sabotage- oder Spionagezwecken. In funktionaler Hinsicht liegt eine Störung vor, wenn außergewöhnliche und unerwartete technische Defekte mit IT-Bezug vorliegen. Erfasst werden erfolgte, versuchte oder auch erfolgreich abgewehrte Angriffe.

Da das BDSG unbeschadet dessen gilt, besteht gegebenenfalls die Verpflichtung zu Mehrfachmeldungen – neben der Meldung an das BSI eine solche nach § 42a BDSG an die zuständige Datenschutzaufsichtsbehörde; auch die „Skandalisierungspflicht“ nach § 109a TKG bleibt bestehen (vgl. oben III 4). Das BSI kann die Öffentlichkeit von dem Störfall benachrichtigen.

Bei Auftreten von Sicherheitsmängeln kann das BSI die Übermittlung der gesamten Kontrollergebnisse und (natürlich) die Beseitigung der Mängel verlangen. Darüber hinausgehend kann das BSI auch die Hersteller betroffener IT-Produkte oder IT-Systeme für eine Mitwirkung an der Beseitigung eines Mangels in die Pflicht neben.

Auf die Unternehmen kommt demnach - neben der Einrichtung einer jederzeit für das BSI erreichbaren Kontaktstelle - die risikobehaftete Aufgabe abzuwägen, ob die gesetzlichen Voraussetzungen der Meldepflicht gegeben sind. Mehr Rechtssicherheit dürfte hier der angekündigte BSI-Kriterienkatalog - nach dem Vorbild der Anlage zu § 9 BDSG mit den dortigen 8 Geboten der Datensicherheit (dazu oben II 3) - schaffen.

Bei (auch fahrlässigen) Verstößen gegen die vorstehenden Verpflichtungen kann das BSI Bußgelder (je nach Verstoß bis 50 bzw. 100 TEUR) verhängen. Der Sanktionskatalog sieht Bußgelder bereits vor für die nicht erfolgte, nicht richtige, nicht vollständige oder nicht rechtzeitige Meldung bereits eingetretener Sicherheitsverletzungen.

Haftungsrechtlich erlangt die Einhaltung der Mindestanforderungen Bedeutung bei der Bestimmung des Fahrlässigkeitsmaßstabes bzw. der einschlägigen Verkehrssicherungspflichten (als Voraussetzungen für Schadensersatzansprüche von Vertragspartnern und geschädigten Dritten). Auch die - besonders schadensträchtige - Haftung gegenüber anderen KRITIS-Betreibern kommt in Betracht, so etwa wenn diese infolge einer Verletzung von Meldefristen nicht mehr rechtzeitig vom BSI gewarnt werden konnten, wenn Angreifer Systeme hacken und auf Komponenten zugreifen können, von deren Funktionsfähigkeit mehrere Betreiber abhängig sind, oder wenn mangelhafte IT-Sicherheit es Unbefugten ermöglicht, Daten auszulesen und mit diesen Daten die Systeme anderer Betreiber missbräuchlich zu nutzen.

**2. Erweiterte technische Sicherungspflichten für Internetanbieter**

Für geschäftsmäßig angebotene Internetdienste wurde die Rechtslage ebenfalls unter IT-sicherheitsspezifischen Aspekten verschärft. § 13 Abs. 7 TMG soll die Verbreitung von Schadsoftware über Webseiten - die zu den wirtschaftlich bedeutsamsten Bedrohungen der Netzsicherheit zählt (vgl. oben II 1) - eindämmen, indem den Anbietern technische und organisatorische Vorkehrungen zum Schutz des Zugriffs auf ihre Angebote nach dem „Stand der Technik“ auferlegt werden. Anknüpfungspunkt sind hier (abermals) die „8 Gebote der Datensicherheit“ (vgl. oben II 3 und V 1).

Als Maßnahme wird exemplarisch der Einsatz von Verschlüsselungstechniken genannt. Weitere Maßnahmen, die den „Stand der Technik“ berücksichtigen, können beispielsweise das Scannen gehosteter Daten oder die Installation von Firewalls sein. Die Sicherungspflichten werden zwar auf solche Maßnahmen beschränkt, die technisch möglich und wirtschaftlich zumutbar sind. Derlei verbreitete und anerkannte Basissicherheitstechnik wird freilich stets zumutbar

sein, zumal der Gesetzgeber die Anwendung von Verschlüsselungsverfahren explizit benennt. In organisatorischer Hinsicht sind geeignete Berechtigungskonzepte für Zugangs- und Administrationsrechte zu fordern, ferner Schulungen und die Einräumung vertraglicher Kontrollmechanismen. Auch ein Outsourcing der Sicherheitsmaßnahmen an spezialisierte Dienstleister sowie deren Überwachung und Kontrolle beispielsweise durch Audits oder die Vorlage von Zertifikaten unabhängiger Prüforganisationen sind in diesem Kontext zu nennen.

Der (jeweilige) „Stand der Technik" muss sich orientieren am „Entwicklungsstand fortschrittlicher Verfahren", der zur Erreichung eines „allgemein hohen Schutzniveaus geeignet ist". Der Stand der Technik stellt damit auf Maßnahmen ab, die evident praxistauglich sind und den Schutz am Besten verwirklichen. Dies impliziert eine fortlaufende Aktualisierungspflicht für die eingesetzte Internet- und Sicherheitssoftware. Auch muss sichergestellt werden, dass eingebundene Inhalte von Drittanbietern denselben Schutzanforderungen entsprechen. Die Erhebung und Verwendung von Nutzungsdaten zum Zweck der Störungsbeseitigung bleibt jedoch unbeschadet dessen unzulässig. Die vom *Bundesgerichtshof* in 2014 im Rahmen des § 100 TKG bestätigte Zulässigkeit einer Speicherdauer von 7 Tagen von IP-Adressen zur Gewährleistung einer effektiven Störungsbeseitigung bleibt daher die einzige rechtliche Legitimation für eine solche Vorratsspeicherung.

Ferner haben die Anbieter Störungen bei der Nutzung ihrer Telemediendienste zu verhindern. Eine Störung liegt immer dann vor, wenn Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit des Telemediendienstes beeinträchtigt sind. Für die Verfügbarkeit der technischen Einrichtungen ist sicherzustellen, dass sowohl die Systeme selbst als auch der Zugangspunkt von außen entsprechend gesichert sind. Der Baustein „B5.4 Webserver" des BSI IT-Grundschutzes kann hier einen Hinweis auf geeignete Maßnahmen bieten. Weitere Anhaltspunkte für „als sicher anerkannte Verschlüsselungsverfahren" gibt das BSI in seiner technischen Richtlinie „BSI TR-02102 Kryptografische Verfahren". Werden die Telemedien über externe Dienstleister wie Serviceprovider verfügbar gemacht, so ist sicher zu stellen, dass auf Seiten des Providers dieselben grundlegenden Sicherheitsmaßnahmen eingehalten werden müssen - einschließlich der Verpflichtung zur Datensicherung (die nach der Rechtsprechung wenn nicht als Haupt- so jedenfalls als vertragliche Nebenpflicht - selbst für den Fall, dass sie im Verhältnis zwischen Provider und Kunde nicht ausdrücklich in das Vertragsverhältnis einbezogen wurde - anzusehen ist, vgl. oben IV 2)

Verstöße sind mit bis zu 50 TEUR bußgeldbewehrt. Weitere hoheitliche Sanktionen reichen bis zur Untersagung und Sperrung der Dienste. Einer drohenden Sicherheitsverletzung kann ferner als Gefahr für die öffentliche Sicherheit präventiv durch die zuständigen Behörden mit geeigneten und angemessenen Mitteln begegnet werden.

Haftungsrechtlich bestehen gegenüber den Nutzern Schadensersatzpflichten aus Vertragsverletzung und - außerhalb einer vertraglichen Beziehung - aus unerlaubter Handlung (§§ 823 Abs. 2 BGB i.V. mit 13 Abs. 7 TMG als deliktisches Schutzgesetz, § 823 Abs. 1 BGB aufgrund Verkehrssicherungspflichtverletzung, wobei § 13 Abs. 7 TMG die Mindestanforderungen an die Verkehrssicherungspflichten konkretisiert). Der Dienstanbieter kann sich jedoch „exkulpieren", d.h. hinsichtlich seiner Haftung entlasten, wenn er eine geeignete, für seinen Dienst etablierte „Best Practise"-Policy umgesetzt hat. Eine Haftung für Rechtsverletzungen kommt ferner in Betracht im Urheber-, Marken- und Wettbewerbsrecht, wo die Rechtsprechung eine Täterhaftung bejaht, wenn Webseitenbetreiber ihre Webseiten nicht ausreichend technisch und organisatorisch absichern und hierdurch ein Dritter im Namen des Täters auftreten kann. Daneben können Host- und Content-Provider strafrechtliche Garantenpflichten treffen, die abermals durch § 13 Abs. 7 TMG konkretisiert werden.

Als allgemein geeignete technische Maßnahmen und zugleich Mindeststandards, die vom Anbieter - neben gegebenenfalls weiteren einschlägigern Pflichten im jeweiligen - beachtet werden müssen, dürften der Einsatz konfigurationsfehlerfreier Internet- und spezieller Sicherheitssoftware (Firewall, Malware-Scanner, Intrusion Detection- und Data Loss Prevention-Systeme etc.) anzusehen sein, die Einspielung regelmäßiger Sicherheitssoftware-Updates für die im Rahmen der Erstellung und Aktualisierung von Webseiten verwendeten Programme (z.B. CMS)

und nach dem Stand der Technik sichere Administrationszugänge nebst geeigneten Sicherheits-Policies. Auf Administratorenseite besteht eine Recherche- und Fortbildungspflicht in Bezug auf neue Bedrohungsszenarien und Sicherheitsupdates. Bei Hinweisen auf eine Kompromittierung ist der Schadcode mit Hilfe spezieller Software - und gegebenenfalls auch unter Einbindung externer Fachdienstleister - zu untersuchen und zu bereinigen.

Bei Webshop-Funktionalität sind des Weiteren die Anforderungen des § 9 BDSG und des § 13 Abs. 4 TMG zu beachten. Es ist ein Sicherheitskonzept auszuarbeiten, das die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle gewährleistet und das datenschutzrechtliche Trennungsgebot berücksichtigt. In diesem sensiblen Bereich ist spezielle Software zu verwenden, die die Verwundbarkeit des Systems in kurzen Abständen scannt. Aus Sicherheitsgründen sollte der Datenbankserver, mit dem der Webshop verbunden ist, nicht auf demselben Server gehostet werden. Da im Webshop auch sensible Daten wie insbesondere Kreditkartennummern hinterlassen werden, ist eine sichere Nutzerauthentifizierung durchzuführen, wobei Benutzername und Passwort auf dem Server stets nur in verschlüsselter Form hinterlegt werden dürfen. Auch für die Nutzerpasswörter müssen entsprechende Mindestsicherheitsstandards gelten. Bei der Übertragung von Account- oder Zahlungsdaten ist eine Transportverschlüsselung nach fortgeschrittenem Standard zu implementieren. Nutzerdaten, aber auch statistische Daten wie Cookies und die Backups sind stets nach den entsprechenden Standards zu verschlüsseln. Schlüssel und Passwörter sind sowohl gegen innerbetriebliche wie auch gegen Zugriffe von außen zu sichern. In Notfallplänen sind Reaktionen auf Angriffe und Desaster-Szenarien festzulegen und in regelmäßigen Abständen Notfälle testweise zu simulieren. Die getroffenen technischen und organisatorischen Vorkehrungen sind zu dokumentieren und nach dem Maßstab des Standes zu bewerten, damit gegebenenfalls ein sachkundiger Dritter die umgesetzten Maßnahmen substanziell überprüfen und ein Gericht zu einem Urteil hinsichtlich der Verantwortlichkeiten im verkehrssicherungspflichtigen oder nebenvertraglichen Bereich gelangen kann.

## VI. Besonderheiten bei Cloud-Nutzung und Outsourcing

Ein Gutteil der leistungsstarken Cloud-Anbieter hat seinen Sitz oder seine Serverfarmen in den zunehmend in Spionageverdacht geratenen USA. Die Übermittlung von Daten in unsichere „Drittstaaten“, wie die USA von der EU in datenschutzrechtlicher Hinsicht eingestuft wurde, ist - nachdem der Europäische Gerichtshof (EuGH) mit Urteil vom 06.10.2015 zudem das Aus für „Safe Harbor“ (als die prominenteste Rechtsgrundlage für den Datenaustausch mit den USA) verkündet hat - mit riskanten rechtlichen Unwägbarkeiten verbunden.

Dies gilt umso mehr, als auch das rechtliche Schicksal der von der EU-Kommission unter dem Arbeitstitel „Privacy Shield“ vorgestellten Ersatzlösung zu „Safe Harbor“ ist unklar, das erst nach zähem Ringen am 12.07.2016 verabschiedet wurde. Vor allem die Wirtschaft hatte eine solche schnelle politische Einigung zwischen der EU und den USA grundsätzlich herbeigesehnt. Tatsächlich wirft das „Privacy Shield“ jedoch mehr Fragen auf als es beantwortet, weshalb zahlreiche Unternehmen dem Rat namhafter Experten folgend nicht unter den Schutzschild gehen werden. Denn die in der Art. 29-Datenschutzgruppe organisierten EU-Datenschutzbehörden sehen den „Privacy Shield“ auch weiterhin nicht konform mit den Vorgaben des EuGH. Die Verunsicherung hat daher mit dem 12.07.2016 eher noch zugenommen. Sowohl der EU-Datenschutzbeauftragte als auch die der Mitgliedsstaaten hatten das „Privacy Shield“ im Vorfeld zurückgewiesen. Zumindest nach Ansicht der Art. 29-Gruppe schafft auch die Verabschiedung von „Privacy Shield“ keine langfristige Rechtssicherheit. Dazu trägt auch die Art. 29-Gruppe selbst bei, die eine abschließende Aussage erst nach Verabschiedung der neuen EU-Datenschutzgesetze gemäß der EU-Datenschutzgrundverordnung im Jahre 2018 treffen will, da das „Privacy Shield“ auch den darin formulierten neuen – und nochmals höheren – Anforderungen an den Datenschutz genügen muss.

Die Ungewissheit rund um das „Privacy Shield“ hat bereits dazu geführt, dass immer mehr Cloud-Anbieter auf regionale Rechenzentren. In Fachkreisen wird betont, dass der EuGH das Abkommen jederzeit wieder kippen kann.

Viele Experten raten daher Unternehmen, alternative Mechanismen zu verwenden oder „Privacy Shield“ nur als zusätzliche Option zu nutzen.

Rechtlich offen ist die Situation durch das Urteil des EuGH nun aber auch wieder hinsichtlich der für die Praxis ersten Alternative zu „Safe Harbor“, der sog. „ EU-Standardvertragsklauseln“. Denn ob diese den strengen inhaltlichen Vorgaben, die der EuGH in seinem Urteil ebenfalls aufstellte, letztendlich standhalten werden, wird von führenden Datenschützern bezweifelt. Daraus folgt, dass die Aufsichtsbehörden im Einzelfall Datentransfers auf dieser Grundlage untersagen können, sofern die Rechte der Betroffenen nicht ausreichend gewahrt werden. Am 25.05.2016 wurde zudem nun bekannt, dass Irland nach „Safe Harbor“ auch die EU-Standardvertragsklauseln vor dem EuGH überprüfen lassen will. Mangels eines Nachfolgers für „Safe Harbor“ waren Unternehmen wie Facebook und die großen Cloud-Anbieter aus den USA auf diese alternative juristische Grundlage für die gleiche Praxis ausgewichen, ohne dass der Schutz europäischer Daten in den USA rechtlich wie praktisch verbessert worden wäre. Wenn Irlands Datenschützer nun vorpreschen, könnte das darauf hindeuten, dass diese selbst nicht an die rechtskonforme Umsetzung des „Privacy Shield“ glauben. Ein juristischer K.O. droht damit auch den Ausweichoptionen „Privacy Shield“ und „EU-Standardvertragsklauseln“.

Für Zündstoff sorgt in diesem Kontext auch das Microsoft-Verfahren in den USA, von dem grundsätzliche Aussagen zu den Pflichten von Unternehmen in Bezug auf die Herausgabe von Daten an US-Sicherheitsbehörden erwartet werden. Das Microsoft-Urteil dürfte in seinen Wirkungen ähnlich weit reichen wie das Safe Harbor-Urteil des EuGH und damit auch für Zustandekommen und Inhalte des EU-US Privacy Shields von maßgeblicher Bedeutung sein.

All dies macht eine datenschutzkonforme Auslagerung von Datenverarbeitungen mit Personenbezug in globale Clouds derzeit nahezu unmöglich, wenn nicht ausnahmsweise eine zulässige Auftragsdatenverarbeitung (ADV) vorliegt. Eine ADV ist europarechtlich nur zulässig, wenn ein Gesetz sie gestattet oder ein schriftlicher Vertrag die ADV detailliert regelt. Besteht letzteren Falls kein solcher Vertrag, stellt dies einen bußgeldbewehrten Verstoß gegen die Verpflichtung des Auftraggebers dar, die jeweiligen Verantwortlichkeiten und technisch-organisatorischen Maßnahmen in schriftlicher Form detailliert zu dokumentieren und kann weitere Sanktionen nach sich ziehen. Der Auftragsverarbeiter ist sorgfältig nach Kriterien wie Zuverlässigkeit, Leistungsfähigkeit, seinen dem Stand der Technik entsprechend zum Einsatz kommenden technisch-organisatorischen Sicherheitsmaßnahmen etc. auszuwählen. Die Auswahl beinhaltet insbesondere die Kontrolle der technisch-organisatorischen Maßnahmen vor Beginn der Datenverarbeitungen und sodann regelmäßig während der Laufzeit der ADV.

Damit sind europäische und nationale Cloud- und Rechenzentrumslösungen zu Recht wieder massiv in das Interesse der deutschen Wirtschaft gerückt. Aber auch inländische Cloud-Lösungen bieten keine Garantie. So wurden in jüngerer Vergangenheit gleich zwei „Wellen“ des Verlusts von E-Mails der Business-Kunden eines großen deutschen Anbieters bekannt, der mit der besonderen Sicherheit seiner inländischen Standorte geworben hatte. Offenbar nach einem Update war eine Vorhaltefrist von 90 Tagen gesetzt worden; ältere Mails gingen unwiederbringlich verloren.

Benötigt werden daher zuverlässige IT-Anbieter, die die Sicherheit der eingesetzten IT-Systeme und einen EU-rechtskonformen Schutz der an sie übermittelten Daten sicherstellen können. Denn trotz der Flexibilität und der Kostenfaktoren birgt Outsourcing zahlreiche Risiken. Dies betrifft vor allem die Sicherheit, Vertraulichkeit, Unversehrtheit und Verfügbarkeit von unternehmenskritischen Daten von der Wiege (Generierung) über ihren Lebenszyklus (Bearbeitung, Transport) bis zum Grabe (Archivierung, Löschung).

Da es sich bei Cloud in der Regel um ADV handelt, besteht die gesetzliche Verpflichtung zu einer sorgfältigen Anbieterauswahl. Der Auftragsverarbeiter ist nach strengen (und zu dokumentierenden) Kriterien wie Zuverlässigkeit, Leistungsfähigkeit, seinen dem Stand der Technik entsprechend zum Einsatz kommenden technisch-organisatorischen Sicherheitsmaßnahmen etc. auszuwählen und hat insbesondere auch eine „Compliance“ nach Maßgabe des „TOM-

Katalogs“ (Anlage 1 zu § 9 BDSG) - d.h. mit den sog. „8 Geboten der Datensicherheit“ (dazu schon oben II 3, V 1-2) - zu gewährleisten. Mit einschlägigen Audits und Zertifizierungen (z.B. Audit nach § 9a BDSG, Zertifizierung nach ISO 27001) können die Betreiber von Rechenzentren in der EU und dem Europäischen Wirtschaftsraum (EWR) die Einhaltung der gesetzlichen Vorgaben verlässlich und transparent nachweisen und somit Cloud „Made in Germany“ bzw. „Europe“ zu einem überzeugenden Qualitäts- und Abgrenzungsmerkmal machen.

## VII. Haftungsvermeidung durch Risiko-Management

Ist von IT-Haftung die Rede, wird es wie gesehen zumeist um die Sicherheit, Integrität, Vertraulichkeit und Verfügbarkeit von kritischen Daten gehen. Über diese allgemeinen Sorgfalts- und Organisationspflichten hinaus hat das Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr (KonTraG) im Bereich der Privatwirtschaft die Rechtspflicht zu einem effizienten Risikomanagementsystem eingeführt, das eine Überwachung und Früherkennung sowie entsprechende Reaktionsszenarien im Schadensfall umfasst. Die Organe sind verpflichtet, geeignete Schutzmaßnahmen in Bezug auf die IT-Sicherheit, gerade auch für betriebswichtige Systeme und Daten, zu konzipieren, umzusetzen, zu überwachen und zu dokumentieren. Im Falle des Schadenseintritts wird ihr Verschulden vermutet. Das Gesetz sieht als Sanktion die persönliche Haftung der geschäftsführenden Organe zur Kompensation eines durch IT-Missmanagement hervorgerufenen Schadens beim Unternehmen vor. Hierbei ist zu berücksichtigen, dass durch eine besondere gesetzliche Beweislastumkehr die Vorstände nachweisen müssen, dass sie ihren Pflichten in einem ausreichenden Maße nachgekommen sind. Ihr Verschulden wird quasi von Gesetzes wegen vermutet. Die Vorstände haften also persönlich und zusätzlich wird der Aufsichtsrat verpflichtet, Schadensersatzansprüche gegen sie zu verfolgen.

Ein zentraler Bestandteil dieses Risiko-Controllings ist das Informations- und Kommunikationsmanagement, das insbesondere die Betriebs- und Angriffssicherheit der IT-Infrastruktur sowie die in dieser Infrastruktur verwalteten Informationen (wie z.B. die elektronische Post, Entwicklungsdokumentationen, Geschäftsgeheimnisse, sonstige Unterlagen von besonderem Schutzniveau wie Gesundheitsdaten, beweisrelevante oder sonst betriebskritische Unterlagen etc. ) betrifft.

Die Einrichtung eines Risikomanagements war zwar ursprünglich unmittelbar nur für Aktiengesellschaften vorgeschrieben. Das Gesetz hat jedoch inzwischen erhebliche Ausstrahlungswirkung auf andere Gesellschaftsformen und den Inhalt der allgemeinen kaufmännischen und behördlichen Sorgfaltspflichten erlangt. Die Verpflichtung zu einem effektiven Risikomanagement nach dem Vorbild des KonTraG ist infolge dieser Ausstrahlungswirkung nicht (mehr) auf den Bereich der Privatwirtschaft beschränkt. In der öffentlichen Verwaltung gelten diese Grundsätze in weiten Teilen entsprechend.

Es lässt sich sonach festhalten, dass sich das Vorhandensein eines dokumentierten, stets auf aktuellem Stand gehaltenen effektiven Risikomanagementsystems mit internem Kontrollsystem inzwischen zu einem zentralen Grundsatz ordnungsgemäßer Geschäftsführung etabliert hat. Diese Sorgfaltspflichten beinhalten - über die Einhaltung der zwingenden Aufbewahrungsvorschriften hinaus - eine allgemeine organisatorische Obliegenheit, kritische Daten aus Gründen der Rechtssicherheit (Beweissicherung) geordnet und lückenlos dokumentiert aufzubewahren. Die Relevanz bestimmter Daten kann sich unter Umständen erst nach Jahren erweisen, etwa im Bereich der Garantie- und Gewährleistungsfristen und der Forderungs- oder der Haftungsverjährung, die in Deutschland bis zu 30 Jahren beträgt. Der Erfolg der Beweisführung wird dabei maßgeblich beeinflusst durch die Qualität der im Streitfall verfügbaren Beweisdokumente.

## VIII. Versicherbarkeit von IT-Sicherheitsrisiken

Zum IT-Risikomanagement gehört auch die Prüfung der Versicherbarkeit von IT-Sicherheitsrisiken. Denn es stellt sich die Frage nach den Möglichkeiten einer Haftungsentlastung bzw. Schadenskompensation bei Realisierung der zuvor

aufgezeigten Risiken. Umgekehrt können Versäumnisse im IT-Risikomanagement zum Verlust des Versicherungsschutzes führen, denn mangelnde IT-Compliance ist als Erhöhung der versicherten Gefahr z.B. in der IT-Coverage Versicherung und in der „D&O"-Berufshaftpflichtversicherung für Manager (für: „Directors and Officers") anzeigepflichtig. Das Fehlen bzw. die Ungeeignetheit einer dem Stand der Technik entsprechenden IT-Infrastruktur und deren Einbettung in ein ganzheitliches Risikomanagement können im Rechtsstreit als grobe Fahrlässigkeit eine Eintrittspflicht des Versicherers ausschließen oder zum erfolgreichen Einwand des Mitverschuldens der Gegnerversicherung führen. Im Extremfall kann es zu einer Reduzierung der eigenen Schadensansprüche auf Null kommen, wenn Mängel der IT-Compliance den Schaden ermöglicht, mit verursacht oder erhöht haben.

Die Versicherungswirtschaft hat die Bedrohungsszenarien, denen sich die Wirtschaft inzwischen durch den erheblichen Anstieg von IT-Vorfällen wie Sabotage und Spionage ausgesetzt sieht, erkannt und zur Abdeckung von Versicherungslücken neue Produkte für sog. „Cyberrisiken" entwickelt. Hierdurch wird dem Umstand Rechnung getragen, dass Ausfälle der IT-Infrastruktur oder der Verlust wichtiger bzw. die Offenbarung vertraulicher Daten leicht zu einem über den bezifferbaren Schaden deutlich hinausgehenden Imageschaden führen können, insbesondere wenn grobe Versäumnisse im Bereich des Datenschutzes an die Öffentlichkeit gelangen. Hinzu kommt gegebenenfalls die sog. „Skandalisierungspflicht".

## RECHTSSICHERHEIT DURCH TECHNISCHE SICHERHEIT: DAS GANZHEITLICHE DR/BC-LÖSUNGSKONZEPT VON ZERTO

Im Bereich Kontinuitätsmanagement ist die klassische synchrone Spiegelung für einen unterbrechungsfreien Betrieb der unternehmenskritischen Systeme und Rechenoperationen zumeist nicht ausreichend. Unter dem Aspekt der Ausfallsicherheit (DR/BC) ist der aktuelle Stand der Technik nicht mehr in der Synchronisation zu sehen, sondern in einer Kombination von redundanten Rechenzentren und einer Softwaretechnologie, die sich Umgebungs- und Applikations-übergreifend sowie speicherneutral den unmittelbar beim Schadensereignis vorliegenden „Letztstand" des Produktivprozesses „merkt", ihn repliziert und die betroffenen Systeme im Sekundenbereich wieder produktiv an diesen Letztstand ansetzen lassen kann. Eine solche fortschrittliche Technologie muss sich nicht mehr auf das Wiederanlaufen von Systemen beschränken sondern setzt die Betriebsabläufe unmittelbar fort.

Die Nachteile der synchronen Spiegelung sind hinreichend beschrieben: Ein Schutz ist nur gegen physikalische Fehler gegeben. Die überwiegende Anzahl von Störungen liegt jedoch im logischen Bereich und ist daher auf beiden Seiten des Spiegels „synchron" vorhanden. Die Wiederherstellung erfordert dementsprechend den Einsatz kostbarer Zeit bis zur Isolierung und Beseitigung des logischen Fehlers, zum Wiedereinspielen verlorener Daten und Neustart des Produktivsystems. Die Ausfallzeiten liegen üblicherweise im Stunden- wenn nicht Tagebereich. Greifen hier mehrere Sicherheitslösungen ineinander, bringt die Komplexität der Wiederanlaufszenarien zudem einen eigenen Geschäftsprozess mit entsprechendem Administrationsaufwand mit sich, der indes oft an der konsistenten Wiederherstellung der gesamten Unternehmenssteuerungssoftware scheitert.

Der Replikationsansatz sollte daher ganzheitlich sein, unabhängig von Anwendung und umgebender IT-Architektur eine unmittelbare Replikation der Originalbedingungen erlauben und der Zeitversatz sich in engen Grenzen bewegen.

Bei der Lösung „Zerto Virtual Replication (ZVR)" werden losgelöst von der jeweils eingesetzten Applikation die Vorteile einer asynchronen Spiegelung - wie z.B. die Entfernungsunabhängigkeit - mit der Technik der kontinuierlichen Datensicherung verknüpft. Das Produktivsystem, d.h. die die datenverarbeitende Applikation wird durch die asynchrone Sicherung nicht beeinträchtigt. Durch die permanente Replikation sind RPOs (Recovery Point Objectives) im Sekundenbereich möglich. Da die Daten bei der Übertragung komprimiert werden, kann die Netzwerkbelastung gering gehalten werden. Der Recovery Point kann für die gesamte Anwendung für jeden Zeitpunkt

in Sekundenschritten bis zu 14 Tage rückwirkend wiederhergestellt werden. Durch Virtuelle Protection Groups (VPGs) wird gewährleistet, dass die Applikation - beispielsweise ERP-Systeme wie SAP - ebenso wie die umgebenden bzw. ansetzenden Systeme ganzheitlich und in ihrem produktiven Zusammenspiel genau vom selben Zeitpunkt wiederhergestellt werden können. Auf diese Weise wird eine in sich konsistente und funktionsgerechte Wiederherstellung in Sekundenschritten ohne manuelle Nachkonfigurationen ermöglicht. Da keine Abhängigkeit von bestimmten Storage-Systemen besteht, können an verschiedenen Lokationen unterschiedliche Systeme eingesetzt werden. Applikation und Daten können zudem in die verschiedenen Cloud-Typen (Private-, Hybrid- und Public) migriert werden, was dem Unternehmen die ganze Bandbreite zur Verfügung stehender Cloud-Lösungen – je nach Anwendung und Produktivbedarf – außerhalb einer bestimmten Cloud-Technologie und Konfiguration eröffnet. Es werden mithin über Rechenzentren hinweg und bis in die jeweilige Cloud-Lösung hinein im Desaster-Fall Wiederherstellungen beliebiger Dateien aus beliebigen Anwendungen möglich mit einem Zeitversatz des Replikationsstandes von nur Sekunden vor dem Desaster - und so ein produktiver Weiterlauf der im Sekundengedächtnis des Systems replizierbaren Daten binnen eines RTOs (Recovery Time Objective) von wenigen Minuten erlaubt. Zudem ist auch ein Desaster Recovery Testing im laufenden Betrieb mit Reporting möglich, was bei anderen Lösungen oft nur sehr aufwändig am Wochenende und nicht im produktiven Betrieb möglich ist. Das Testing mit dem Reporting ist gerade auch bei Audits ein wichtiges Instrument und dokumentiert die Funktionsfähigkeit und Verfügbarkeit der IT.

* Der Autor ist Rechtsanwalt und Fachanwalt für IT-Recht. Er ist darüber hinaus Gründungspartner der Rechtsanwaltskanzlei e/s/b Rechtsanwälte (http://www.kanzlei.de) sowie zugleich Fachbuchautor im IT-Recht und Lehrbeauftragter an der Hochschule für Technik in Stuttgart und als associate Professor an der E.N.U. in Kerkrade, Niederlande tätig.

** Disclaimer: Dieses Dokument stellt eine generelle rechtliche Bewertung dar. Es ersetzt nicht die verbindliche Rechtsauskunft durch einen spezialisierten Anwalt. Bitte haben Sie Verständnis, dass trotz größtmöglicher Sorgfalt bei der Erstellung eine Garantie oder Haftung für die inhaltliche Richtigkeit, Aktualität und individuelle Brauchbarkeit nicht übernommen wird.