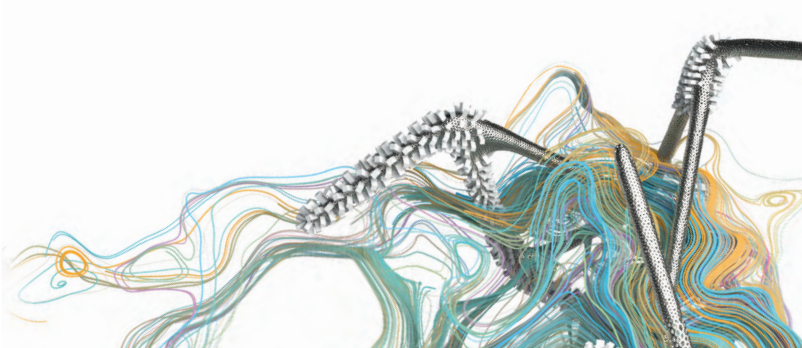
Juristische Informationen
für die Unternehmensleitung

TREND MICRO

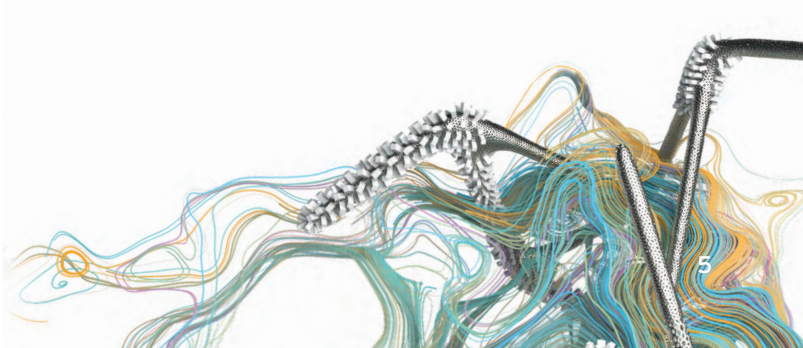
IT-Security und IT-Compliance im Unternehmen

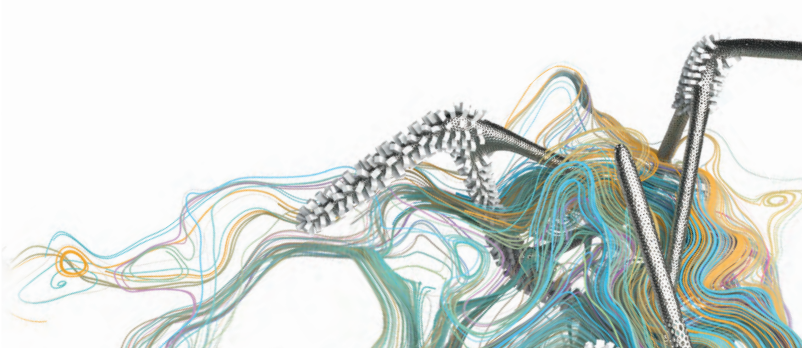
6. Auflage | **Juni 2019**

In Erinnerung an
Günter Untucht
(1948 – 2018)



Inhaltsverzeichnis





IT-Security und IT-Compliance im Unternehmen

Juristische Informationen für die Unternehmensleitung

Ohne den Einsatz von Informationstechnologie ist die Führung eines Unternehmens heute kaum mehr denkbar: Nahezu alle geschäftskritischen Prozesse erfolgen elektronisch, Geschäftsleitung und Mitarbeiter sind online mit der Unternehmens-IT und untereinander verbunden, Daten und Applikationen werden in die „Cloud" ausgelagert. Big Data und IoT (Internet of Things) stellen die nächste Stufe technologischer Innovationen dar, die in Unternehmen zum Einsatz kommen.

Allerdings bietet die Informationstechnologie nicht nur Vorteile: Sicherheitslücken und Datenlecks, Hackerangriffe, Datenschutzverstöße und der Missbrauch von IT-Systemen durch Mitarbeiter kann die Geschäftstätigkeit erheblich beeinträchtigen und unter Umständen sowohl zu **strafrechtlichen Konsequenzen** als auch zu **Schadensersatzforderungen** gegen das Unternehmen und die Unternehmensleitung führen.

Im Rahmen der Corporate Governance sind **IT-Security** und **IT-Compliance** für die Geschäftsleitung von Unternehmen von großer Bedeutung. Sie stellen sicher, dass Geschäftsführer, Vorstand oder Aufsichtsrat den einschlägigen rechtlichen Anforderungen gerecht werden können und ihren Pflichten nachkommen.

Dieser Leitfaden gibt einen Einblick in wichtige juristische Themengebiete, die für den Einsatz von IT-Infrastruktur und Internet in Unternehmen relevant sind. Dabei liegt der Schwerpunkt auf der IT-Security. Die nachfolgenden Kapitel enthalten **juristische Informationen für die Geschäftsleitung**, jedoch keine konkrete Handlungsanweisung oder -anleitung. Diese Hinweise sind lediglich allgemeiner Art und können weder eine Untersuchung des jeweiligen Einzelfalls noch eine Rechtsberatung durch eine interne Rechtsabteilung bzw. einen Rechtsanwalt ersetzen.

Auch wenn der Autor schon seit vielen Jahren im Bereich des IT-, Internet- und Datenschutzrechts sowie der IT-Security tätig ist und sorgfältig recherchiert hat, wird keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität dieses Leitfadens übernommen.

Die Themen im Überblick

Die Sicherstellung der IT-Security ist **originäre Pflicht und Aufgabe der Unternehmensleitung**. Sie umfasst insbesondere:

- **Wirksame Schutzmaßnahmen gegen Angriffe von außen, z.B. durch Hacker, Viren oder sog. Botnets (ferngesteuerte Netzwerke von infizierten Computern) sowie gegen Advanced Persistent Threats**
- **Einhaltung der datenschutzrechtlichen Pflichten**
- **Regelmäßige Erstellung von Backups**
- **Berücksichtigung von Handlungsanleitungen, Best Practice-Vorgaben und Wirtschaftsprüfungsstandards**

Bei Nichtbeachtung drohen als Sanktionen u.a. **zivilrechtliche Schadensersatzansprüche** von Geschädigten gegen das Unternehmen, **Geldbußen, ökonomische Nachteile** wie z.B. ein schlechteres Kreditrating, Verlust des Versicherungsschutzes oder der Ausschluss bei der Vergabe öffentlicher Aufträge.
Geschäftsführer, Vorstände und Aufsichtsräte können zudem persönlich in die Haftung genommen werden.
Der Einsatz internetbasierter Technologien im Unternehmen wie Cloud Computing und Social Media, die gleichzeitige private und dienstliche Nutzung von Smartphones und Tablets („Consumerization") und die seit 2018 geltende **Datenschutz-Grundverordnung** bringen zusätzliche rechtliche Anforderungen mit sich.

Betreiber kritischer Infrastrukturen (KRITIS) müssen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme nach dem Stand der Technik treffen.
Der Missbrauch von IT-Infrastruktur und der Datendiebstahl können nach mehreren Vorschriften **strafbar** sein. Dazu zählen z.B. das Ausspähen von Daten, die Verletzung des Fernmeldegeheimnisses oder die Verletzung von Geschäftsgeheimnissen. Das Cyberstrafrecht soll künftig verschärft werden und u.a. auch die unbefugte Nutzung informationstechnischer Systeme unter Strafe stellen.
Ein heikles Thema für die Beziehungen zwischen der Geschäftsleitung und den Mitarbeitern eines Unternehmens (und ihren Vertretungsorganen) stellt die Nutzung des vom Unternehmen zur Verfügung gestellten E-Mail-Accounts und Internetzugangs für private Zwecke dar. Hierbei kommt es darauf an, die Weichen richtig zu stellen.

I. IT-Security und IT-Compliance im Unternehmen

Im Rahmen der Corporate Governance soll die Unternehmensleitung und überwachung transparent gemacht werden, um das **Vertrauen in die Unternehmensführung** zu stärken. Der Vorstand bzw. die Geschäftsführung hat die Einhaltung der gesetzlichen Bestimmungen zu gewährleisten, auf deren Beachtung durch die Konzernunternehmen hinzuwirken und für ein angemessenes Risikomanagement und -controlling im Unternehmen zu sorgen. IT-Security und IT-Compliance bilden dabei wichtige Bausteine.

1. Bedeutung der IT-Security

Das Schlagwort „IT-Security" umfasst nicht nur technische Schutzmaßnahmen der Unternehmen gegen Angriffe auf ihre IT-Infrastruktur, sondern schließt auch zahlreiche rechtliche Aspekte ein.

Nach dem „Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik" (BSIG) bedeutet **„Sicherheit in der Informationstechnik"** (...) „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen."

a) Verfügbarkeit

Der Schutz vor Informationsverlust, Informationsentzug, Informationsblockade und Informationszerstörung muss gewahrt werden. Wichtige Kunden- oder Geschäftsdaten müssen während der üblichen Arbeitszeiten permanent verfügbar sein, damit der fortlaufende Geschäftsbetrieb nicht beeinträchtigt wird. So können einem Urteil des Bundesgerichtshofs vom 12. Dezember 2000 (Az. XI ZR 138/00) zufolge Kunden von Online-Banking erwarten, dass sie zu dem Online-Service „rund um die Uhr" Zugang haben.

Üblicherweise wird im Unternehmensverkehr die Verfügbarkeit von IT-Anwendungen und Online-Diensten in **Service Level Agreements (SLA)** geregelt. Zur Sicherstellung der Verfügbarkeit muss eine regelmäßige Datensicherung vorgenommen und die IT-Infrastruktur insbesondere gegen Schad-Software („Malware"), Virenausbrüche und Angriffe von Hackern geschützt werden. Die Maßstäbe hierfür werden durch den permanenten technologischen Fortschritt gesetzt. Daher kann es z.B. erforderlich sein, wegen der nahezu ständig verfügbaren mobilen Datenkommunikation und Virtualisierung der IT-Systeme **Echtzeitschutz** im Rahmen von kollektiven Sicherheitsnetzwerken in Anspruch zu nehmen.

b) Unversehrtheit
Unternehmen müssen ihre IT-Infrastruktur gegen **ungewollte Informationsveränderungen** schützen. Unbefugte dürfen unter keinen Umständen Daten verändern können. Besonders sensible Daten – wie Buchhaltungsunterlagen oder elektronisch gespeicherte rechtsverbindliche Erklärungen – müssen ausreichend gegen externe Angriffe geschützt sein. Hinzu kommt der Schutz der Integrität von Dokumenten gegen unbefugte Änderungen, beispielsweise durch Verschlüsselung und den Einsatz einer elektronischen Signatur.

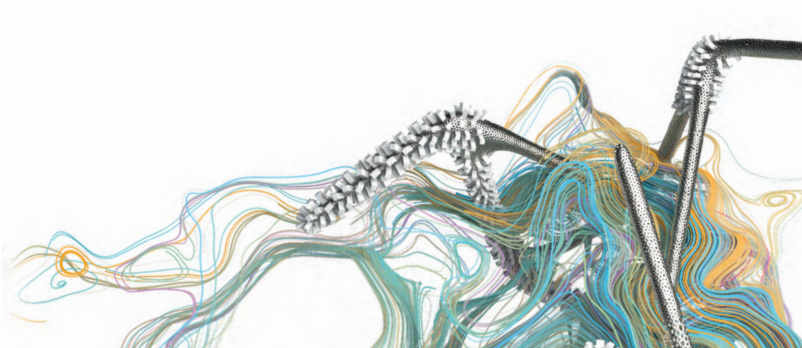
c) Vertraulichkeit
Vertrauliche Unternehmensinformationen müssen gegen das Ausspähen durch Dritte geschützt werden. Dies betrifft insbesondere drei Arten von Daten:

- **personenbezogene Daten, die dem Datenschutz unterliegen,**
- **Inhalte der Telekommunikation und deren nähere Umstände, die durch das Fernmeldegeheimnis geschützt sind, sowie**
- **Geschäfts- und Betriebsgeheimnisse von Unternehmen.**

Der Zugriff auf derartige Daten und Informationen darf nur berechtigten Personen möglich sein. Im Rahmen der IT-Security sind sowohl **Zugriffsbeschränkungen** als auch **Schutzvorrichtungen** gegen das Ausspähen von Daten durch Externe ebenso wie gegen Datenmissbrauch durch eigene Mitarbeiter und gegen Datenlecks einzurichten.

d) Authentizität
Schließlich ist die Authentizität der handelnden Personen sicherzustellen. Insbesondere wenn Geschäftskontakte ausschließlich online erfolgen, kennen sich die Vertragsparteien nicht unbedingt persönlich. E-Mail-Absender können fingiert sein, Webseiten können gar kein oder ein falsches Impressum enthalten.

Mittels der elektronischen Signatur lässt sich sicherstellen, dass es sich bei dem Vertragspartner auch um die Person handelt, für die er sich ausgibt. Zusätzlich sollte elektronische Post aber auch auf ihrem Weg zum Empfänger durch geeignete **Verschlüsselungstechnologie** für Unbefugte unlesbar gemacht werden.



2. Rechtliche Verpflichtung zur IT-Security

IT-Security ist nicht Selbstzweck, sondern **rechtliche Verpflichtung der Unternehmensleitung**.

a) Anforderungen an die Geschäftsführung, IT-Leiter und den Aufsichtsrat
Das Aktiengesetz und das Handelsgesetzbuch regeln die Anforderungen an Vorstände von Aktiengesellschaften und die Geschäftsführung großer Kapitalgesellschaften in Bezug auf Kontrolle und Transparenz:

Der Vorstand bzw. die Geschäftsführung muss geeignete Maßnahmen treffen und insbesondere ein **Überwachungssystem** einrichten, um für den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig zu erkennen.

- Es ist ein unternehmensweites Risikomanagement zu installieren. Teil der Risikoprävention ist dabei der **Schutz der IT-Infrastruktur**, also die Sicherstellung der IT-Security.

- Im Rahmen des Lageberichts von Kapitalgesellschaften (mit Ausnahme sog. „kleiner Kapitalgesellschaften") ist darauf einzugehen – und vom Abschlussprüfer zu kontrollieren –, ob die Chancen und Risiken der künftigen Entwicklung des Unternehmens zutreffend dargestellt sind. Die **IT-Risiken** sind dabei zu benennen.

- Die Unternehmensleitung ist dafür verantwortlich, wirksame Maßnahmen zum Schutz der IT-Infrastruktur zu treffen und ein entsprechendes **Risikomanagement** einzurichten. Sollten **Geschäftsführer bzw. Vorstände** diese Pflicht verletzen und das Unternehmen dadurch Schaden erleiden, **haften** sie gegenüber ihrem Unternehmen **persönlich**. Dies gilt gleichermaßen für den Aufsichtsrat einer Aktiengesellschaft im Falle eines Verstoßes gegen seine Pflicht zur Überwachung der Geschäftsführung.

Aber auch **Unternehmensmitarbeiter** wie der IT-Leiter können bei Verstößen gegen die Anforderungen der IT-Sicherheit gegebenenfalls wegen Verletzung ihrer arbeitsvertraglichen Pflichten in Anspruch genommen werden.
Anforderungen an die IT-Security können Marktverhaltensregeln im Sinne des Gesetzes gegen den unlauteren Wettbewerb (UWG) darstellen, so dass im Falle einer Verletzung möglicherweise Mitbewerber hiergegen mittels **Abmahnung** und einstweiliger Verfügung vorgehen können.
Sofern bei der Umsetzung von IT-Sicherheitsmaßnahmen **externe Unternehmen** beauftragt worden sind, kommt bei entsprechenden Pflichtverletzungen eine Haftung aus Dienst-, Werk- oder Geschäftsbesorgungsvertrag in Betracht.
Der IT-Security muss also von allen Beteiligten – auch in ihrem eigenen Interesse – **höchste Priorität** eingeräumt werden!

b) Vermeidung öffentlich-rechtlicher Konsequenzen und ökonomischer Nachteile
Die Sicherstellung der IT-Security ist auch zur Vermeidung ökonomischer Nachteile für Unternehmen von erheblicher Bedeutung.

Unter dem Stichwort **„Basel III"** hat der Basler Ausschuss für Bankenaufsicht ein umfassendes Reformpaket zur Stärkung der Regulierung, der Aufsicht und des Risikomanagements im Bankensektor verabschiedet. „Basel III" ist seit 1. Januar 2014 in Kraft und hat zum Ziel, die Resistenz des Bankensektors gegenüber Schocks aus Stresssituationen im Finanzsektor und in der Wirtschaft sowie das Risikomanagement zu verbessern und die Transparenz und Offenlegung der Banken zu stärken. Diese Regelungen bringen **erhöhte Sicherheitsanforderungen an IT-Systeme** mit sich. Bei der Finanzierung von Unternehmen sind besonders versteckte organisatorische Risiken zu beachten. Für Unternehmen, die stark von der Funktionsfähigkeit ihrer IT-Infrastruktur abhängig sind, ist die IT-Sicherheit für das Rating und damit auch für die Kreditkonditionen von großer Bedeutung.

Auch der US-amerikanische **Sarbanes-Oxley Act (SOX)** hat auf europäische Unternehmen Einfluss, wenn sie an einer amerikanischen Wertpapierbörse notiert sind oder ein solches Unternehmen als Muttergesellschaft haben. Diese Unternehmen müssen u.a. ein **Kontrollsystem für Finanzdaten** vorhalten, mit dem auch Anforderungen an IT-Systeme impliziert werden, da in aller Regel Finanzdaten elektronisch verarbeitet werden. Die Geschäftsleitung muss über Schwächen des internen Kontrollsystems unaufgefordert informieren. Verstöße gegen SOX können Auswirkungen auf das Börsen-Listing sowie Bußgelder oder sogar Gefängnisstrafen für die verantwortlichen Manager nach sich ziehen.

Wirtschaftsprüfer können bei börsennotierten Aktiengesellschaften das **Testat im Rahmen der Jahresabschlussprüfung** verweigern, wenn die IT-Sicherheitsstandards unzureichend sind. Seit Juni 2016 gelten durch das Abschlussprüferreformgesetz erhöhte Anforderungen der EU an die Abschlussprüfung und die Unabhängigkeit und Integrität der Abschlussprüfer wird gestärkt. Betont wird hierbei die Bedeutung der Prüfungsqualität und die besonders wichtige gesellschaftliche Funktion der Abschlussprüfer mit dem Ziel, dass diese ihre Prüfung börsennotierter Gesellschaften strenger durchführen werden. Zudem ist die Wirksamkeit des internen Kontroll- und Risikomanagementsystems kapitalmarktorientierter Kapitalgesellschaften durch den Aufsichtsrat oder einen von ihm bestellten Prüfungsausschuss besser zu kontrollieren. Im Juli 2017 wurden zusätzliche Straftatbestände im Falle einer Verletzung der Pflichten bei Abschlussprüfungen durch

Mitglieder eines Aufsichtsrats oder eines Prüfungsausschusses eingeführt. Auch wenn die Entscheidung über Einrichtung, Art und Umfang eines **Risikomanagementsystem**s weiter im Aufgabenbereich der Geschäftsführung bzw. des Vorstands liegt, wurden die Anforderungen an die IT-Compliance und IT-Security nochmals erhöht und damit die **Haftung von Vorstand und Aufsichtsrat verschärft**.

Öffentliche Auftraggeber fordern im Rahmen der Leistungsbeschreibung bei IT-relevanten Aufträgen häufig einen Nachweis über die IT-Sicherheit und eine Erklärung, keine vertraulichen Daten an ausländische Geheimdienste und Sicherheitsbehörden weiterzugeben. Anbieter, die dies nicht nachweisen können, laufen Gefahr, dass ihr Angebot wegen eines Ausschlusskriteriums oder der Nichterfüllung besonderer Anforderungen an die Auftragsausführung schon bei der ersten Prüfung ausgeschlossen wird.

Bei besonders schwerwiegenden Verstößen gegen die Grundsätze der IT-Security kann sogar die gewerberechtliche Zuverlässigkeit des Unternehmens in Frage gestellt werden und eine **Gewerbeuntersagung** erfolgen.

3. Anforderungen an Betreiber kritischer Infrastrukturen (KRITIS) / IT-Sicherheitsgesetz

Seit 25. Juli 2015 ist das **IT-Sicherheitsgesetz** in Kraft. Hierdurch soll eine signifikante Verbesserung der IT-Sicherheit in Deutschland erreicht werden. Betreiber sog. „kritischer Infrastrukturen" müssen wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer IT-Infrastrukturen nach sich ziehen kann, ein Mindestniveau an IT-Sicherheit einhalten und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitsvorfälle melden. Unter **„kritischen Infrastrukturen (KRITIS)"** werden Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen verstanden, bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die kritischen Infrastrukturen aus den Bereichen Informationstechnik und Telekommunikation, Wasser und Ernährung sowie Energie werden durch die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) vom 22. April 2016 konkretisiert, die aus den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr durch den zweiten Korb der BSI-KritisV vom 21. Juni 2017. Die BSI-KritisV wird alle zwei Jahre evaluiert, um eine flexible Möglichkeit der Anpassung der kritischen Bereiche, auf die sie Anwendung findet, Anlagenkategorien und Schwellenwerte zu schaffen.

Unter dem Schlagwort **„IT-Sicherheitsgesetz 2.0"** hat das Bundesinnenministerium im März/April 2019 den Referentenentwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme" vorgelegt. Es verweist hierbei auf die immer ausgefeilteren und gefährlicheren Angriffe, etwa durch Ransomware, und eine weitere

Verschärfung der Bedrohungslage durch die zunehmende Verbreitung von IoT-Geräten (zu IoT siehe Kapitel IV).

Die wesentlichen Anforderungen an KRITIS-Betreiber und zusätzliche Verpflichtungen, die durch das IT-Sicherheitsgesetz 2.0 eingeführt werden, sind:

a) Maßnahmen zur IT-Sicherheit
Betreiber kritischer Infrastrukturen müssen angemessene organisatorische und technische Vorkehrungen zur **Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme**, Komponenten oder Prozesse treffen. Dabei soll der Stand der Technik eingehalten werden, so dass fortschrittliche Verfahren und bewährte IT-Sicherheitsprodukte zum Einsatz kommen müssen. Die betroffenen KRITIS-Betreiber – lediglich Kleinstunternehmen mit weniger als zehn Beschäftigten und einem Jahresumsatz bis 2 Millionen Euro sind von den Verpflichtungen ausgenommen – müssen die erforderlichen Schutzmaßnahmen anhand ihrer jeweiligen konkreten Situation bestimmen und u.a. sicherstellen, dass sie branchenspezifische Mindestanforderungen an die IT-Sicherheit erfüllen, wie Maßnahmen zur Detektion und Behebung von Störungen, Einrichten eines **Information Security Management**, Identifizierung kritischer Cyber-Assets, **Maßnahmen zur Angriffsprävention und -erkennung** und Implementierung eines **Business Continuity Managements**. Die Betreiber kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen. Bei Sicherheitsmängeln kann das BSI die Audit-, Prüfungs- oder Zertifizierungsergebnisse anfordern und die **Beseitigung der Sicherheitsmängel** anordnen.

b) Kontaktstelle
Die KRITIS-Betreiber müssen dem BSI eine Kontaktstelle benennen und sicherstellen, dass sie hierüber rund um die Uhr (24/7) erreichbar sind.

c) Meldepflicht
KRITIS-Betreiber werden durch das IT-Sicherheitsgesetz verpflichtet, erhebliche Störungen ihrer IT-Systeme, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit führen können oder geführt haben, an das BSI zu melden. **Gewöhnliche Störungen, die hingegen keine Meldepflicht auslösen, sind beispielsweise Spam und Schadsoftware im üblichen Umfang, die standardmäßig durch Spamfilter und Virenscanner abgefangen werden**, sowie technische Defekte im üblichen Rahmen wie Festplattenfehler.

Auch wenn kein Ausfall oder erhebliche Beeinträchtigung der Funktionsfähigkeit der betriebenen kritischen Infrastrukturen vorliegt, also kein IT-Sicherheitsvorfall gegeben ist, kann eine IT-Störung dennoch meldepflichtig sein. Eine **IT-Störung** liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Das BSI nennt als **Beispiele** den Ausfall der Kühlung eines Rechenzentrums, ein falsch konfiguriertes System oder ein **fehlerhaft eingespieltes Update**. **Um eine Meldepflicht auszulösen, muss eine IT-Störung zudem erheblich sein**. Ob dies der Fall ist, stellt eine Einzelfallentscheidung der Verantwortlichen in KRITIS-Unternehmen dar. **Beispielskriterien für eine erhebliche IT-Störung** sind dem BSI zufolge:

- eine Nicht-Behandlung der IT-Störung würde zu immer weiterführenden negativen Auswirkungen führen
- die Behandlung der IT-Störung muss durch speziell vorgehaltene Incident-Responder oder Störfallteams durchgeführt werden
- es werden zusätzliche Aufwände und Mittel wie z.B. zusätzliche Mitarbeiter eingesetzt oder eingeplant, die über die für den Regelbetrieb hinausgehen
- wichtige IT-Systeme oder Komponenten zur Vermeidung weiterer Auswirkungen müssen abgeschaltet oder isoliert werden
- es müssen für den Bewältigungszeitraum Betriebsprozesse geändert werden
- die IT-Störung verursacht einen hohen finanziellen Schaden
- **es liegt die Vermutung nahe, dass das KRITIS-Unternehmen Ziel eines neuartigen, außergewöhnlichen, zielgerichteten oder aus technischer Sicht bemerkenswerten Angriffs oder Angriffsversuchs ist, wie z.B. ein Advanced Persistent Threat (APT)**
- es bestehen für solche IT-Störungen besondere Berichtspflichten gegenüber der Unternehmensleitung

Die Meldung muss unverzüglich nach Erkennung der IT-Störung erfolgen. **Für die Erstmeldung gilt dem BSI zufolge grundsätzlich Schnelligkeit vor Vollständigkeit**. Für meldepflichtige KRITIS-Betreiber stellt das BSI ein **Online-Melde- und Informationsportal** unter https://mip.bsi.bund.de bereit. Üblicherweise wird der Eingang einer Störungsmeldung vom BSI innerhalb von 30 Minuten quittiert. Zudem betreibt das BSI die Webseite www.allianz-fuer-cybersicherheit.de. Diese umfasst eine **generelle Meldestelle für Cyber-Sicherheit in Deutschland**, über die Unternehmen Sicherheitsvorfälle und Cyber-Angriffe melden können. Die Meldung kann über ein Online-Meldeformular erfolgen und ist auch anonym möglich.

Sofern bei einem KRITS-Betreiber meldepflichtige IT-Störungen auftreten, darf das BSI erforderlichenfalls auch die Hersteller der entsprechenden IT-Produkte und Systeme zur Mitwirkung an der Beseitigung oder Vermeidung einer IT-Störung verpflichten. Nicht nur KRITIS-Betreiber müssen daher dem Stand der Technik entsprechende sichere IT-Sys-

teme, Komponenten und Prozesse einsetzen, sondern auch die **Hersteller sind in der Pflicht, sichere IT-Produkte anzubieten und IT-Störungen zu vermeiden**. Zu diesem Zwecke darf das BSI auch IT-Produkte auf ihre Sicherheit hin untersuchen.

Meldepflichten und Verpflichtungen zur Einhaltung von Mindeststandards, die bislang nur für KRITIS-Betreiber gelten, sollen durch das IT-Sicherheitsgesetz 2.0 **auf weitere Teile der Wirtschaft ausgeweitet** werden, bei denen ein besonderes öffentliches Interesse besteht oder bei deren Beeinträchtigung ein Grundinteresse der Gesellschaft gefährdet ist. Dies betrifft Unternehmen aus den Bereichen Rüstung, Medien und Kultur, sowie näher bestimmte börsennotierte deutsche Aktiengesellschaften, bei deren Beeinträchtigung ihrer Geschäftstätigkeit erheblicher volkswirtschaftlicher Schaden eintreten würde.

Die **Meldepflicht** der KRITIS-Betreiber über erhebliche Störungen wird durch das IT-Sicherheitsgesetz 2.0 zudem auf die **Hersteller von IT-Produkten und von Software von KRITIS-Kernkomponenten ausgeweitet**, deren Anwendung zu einem Ausfall oder einer erheblichen Beeinträchtigung kritischer Infrastrukturen führen kann. Danach müssen künftig auch **Hersteller Sicherheitslücken kurzfristig dem BSI melden**, um rechtzeitig Schutzmaßnahmen ergreifen zu können. Die Meldung muss Angaben zu der Störung des betroffenen IT-Produkts bzw. der betroffenen Software, zu möglichen grenzüberschreitenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache sowie zu den Auswirkungen der Störung enthalten. Wie diese Meldepflicht näher ausgestaltet wird und ob hierfür ebenfalls das Melde- und Informationsportal des BSI zu nutzen ist, bleibt abzuwarten. Allgemeine Newsletter über Software-Patches werden zur Erfüllung der Meldepflicht allerdings kaum ausreichen.

Das BSI kann zudem unter bestimmten engen Voraussetzungen Informationen über Störungen öffentlich machen, so dass hierdurch auch die **Reputation** des betroffenen Unternehmens leiden kann. Dieses **Warnrecht des BSI über Sicherheitslücken** umfasst auch die Nennung konkreter Produkte und Hersteller, so dass auch aus diesen Gründen Hersteller von IT-Produkten und →→ Systemen ein großes Interesse an einer umfassenden IT-Sicherheit haben sollten.

d) Einführung eines IT-Sicherheitskennzeichens

Durch das IT-Sicherheitsgesetz 2.0 sollen die Voraussetzungen für ein einheitliches, freiwilliges IT-Sicherheitskennzeichen geschaffen werden, das die IT-Sicherheit von Produkten sichtbar macht und dem Schutz der Bürger dienen soll. Hersteller können hierdurch die

IT-Sicherheit ihrer Produkte darstellen und sich zu weniger sicheren Konkurrenzprodukten abgrenzen. **Das IT-Sicherheitskennzeichen soll sich aus zwei Komponenten zusammensetzen:**

- einer **Herstellererklärung**, mit dem der Hersteller ausdrückt, dass das konkrete Produkt die IT-Sicherheitsvorgaben erfüllt; diese ergeben sich entweder aus einer Technischen Richtlinie des BSI oder aus geeigneten branchenabgestimmten IT-Sicherheitsvorgaben
- **BSI-Sicherheitsinformationen** zum Produkt

Herstellerinformationen und BSI-Sicherheitsinformationen bilden gemeinsam einen **„elektronischen Beipackzettel"**, der auf der Webseite des BSI abgerufen werden kann. Hersteller können und sollen mit dem IT-Sicherheitskennzeichen werben, um dem Verbraucher eine informierte Kaufentscheidung zu ermöglichen.

e) Vertrauenswürdigkeitserklärung für KRITIS-Kernkomponenten
Das IT-Sicherheitsgesetz 2.0 definiert den neuen Begriff der „KRITIS-Kernkomponenten" als IT-Produkte, die zum Betrieb von kritischen Infrastrukturen dienen und für diesen Zweck besonders entwickelt oder geändert werden, wie z.B. im Sektor Informationstechnik und Telekommunikation IT-Produkte zum Betrieb von Anlagen oder Systemen zur Sprach- und Datenübertragung oder im Sektor Gesundheit IT-Produkte zum Betrieb eines Krankenhausinformationssystems. **KRITIS-Kernkomponenten dürfen künftig nur von solchen Herstellern bezogen werden, die gegenüber dem KRITIS-Betreiber eine Vertrauenswürdigkeitserklärung abgeben haben**. Die Anforderungen an die Vertrauenswürdigkeitserklärung werden vom Bundesinnenministerium näher geregelt und gelten ab deren Bekanntmachung. Die Vertrauenswürdigkeitserklärung muss sich auf die gesamte **Lieferkette des Herstellers** erstrecken, da mit zunehmender Komplexität der eingesetzten KRITIS-Kernkomponenten ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege und der Updates beim Hersteller bzw. bei der Lieferkette verbleibt. Die Vertrauenswürdigkeitserklärung ist zudem Voraussetzung für eine etwaige **Zertifizierung von KRITIS-Kernkomponenten**.

f) Bußgeldvorschriften
Verstöße gegen das IT-Sicherheitsgesetz können derzeit mit **Geldbußen** bis zu 100.000 Euro geahndet werden. Mit dem IT-Sicherheitsgesetz 2.0 werden die Bußgeldvorschriften des BSI-Gesetzes überarbeitet und die Bußgelder erheblich erhöht. Sie sollen sich künftig der Höhe nach an der Datenschutz-Grundverordnung orientieren, so dass einzelne Verstöße mit **Geldbußen bis zu 20 Millionen Euro oder bis zu 4 % des gesamten weltweiten Jahresumsatzes** geahndet werden können.

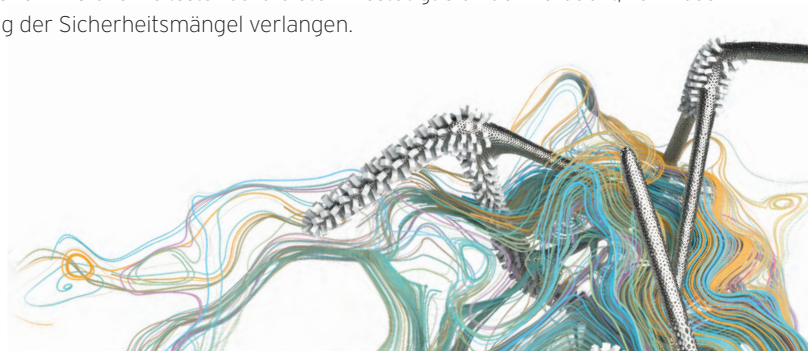
g) Zusätzliche Anforderungen der EU-Richtlinie zur Netz- und Informationssicherheit (NIS)

Auch die EU hat das Thema IT-Sicherheit auf der Agenda. Ziel der **Richtlinie über Netz- und Informationssicherheit (NIS-Richtlinie)**, die am 8. August 2016 in Kraft getreten ist und in Deutschland durch das NIS-Umsetzungsgesetz vom 23. Juni 2017 umgesetzt wurde, ist es, ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU zu gewährleisten. Die EU-Mitgliedstaaten werden hierdurch zu Maßnahmen verpflichtet, ihre Abwehrbereitschaft zu erhöhen und ihre Zusammenarbeit zu verbessern. **Betreiber kritischer Infrastrukturen** in bestimmten Bereichen wie digitale Infrastruktur, Finanzdienste, Verkehr, Energie und Gesundheitswesen sowie **Anbieter digitaler Dienste** müssen hiernach **Risikomanagementmethoden** einführen und **große Sicherheitsvorfälle** in ihren Kerndiensten melden.

In Deutschland sind die Vorgaben der NIS-Richtlinie bereits weitestgehend durch das IT-Sicherheitsgesetz erfüllt, doch durch das NIS-Umsetzungsgesetz wurden zusätzlich **besondere Anforderungen an Anbieter digitaler Dienste** aufgenommen. Hierbei handelt es sich um Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste, die geeignete und verhältnismäßige technische und organisatorische Maßnahmen treffen müssen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung ihrer digitalen Dienste in der EU nutzen, zu bewältigen. Durch solche Maßnahmen soll gegen Auswirkungen von Sicherheitsvorfällen vorgebeugt und diese Auswirkungen so gering wie möglich gehalten werden. Die **Maßnahmen zur Risikobewältigung** sollen angemessen sein und den Stand der Technik berücksichtigen. Das Gesetz nennt hierbei folgende Aspekte:

- **Sicherheit der Systeme und Anlagen**
- **Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen**
- **Betriebskontinuitätsmanagement**
- **Überwachung, Überprüfung und Erprobung**
- **Einhaltung internationaler Normen**

Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Bereitstellung eines digitalen Dienstes haben, hat der Anbieter unverzüglich dem BSI zu melden. Zudem kann das BSI Informationen und Nachweise über ergriffene Sicherheitsmaßnahmen anfordern, um die IT-Sicherheit zu bewerten, wenn Anhaltspunkte vorliegen, dass Anbieter digitaler Dienste keinen angemessenen IT-Sicherheitsstandard bieten. Bestätigt sich der Verdacht, kann das BSI die Beseitigung der Sicherheitsmängel verlangen.



4. Anforderungen an Diensteanbieter von Telemedien

Durch das IT-Sicherheitsgesetz wurde zudem das Telemediengesetz geändert. Hiernach werden Diensteanbieter von Telemedien wie etwa **Betreiber werbefinanzierter Webseiten** verpflichtet, im Rahmen des technisch Möglichen und wirtschaftlich Zumutbaren sicherzustellen, dass kein unerlaubter Zugriff auf ihre technischen Einrichtungen möglich ist und diese gegen Datenschutzverletzungen und äußere Angriffe gesichert sind. Wesentliches Ziel der Regelung ist es, die **Verbreitung von Schadsoftware einzudämmen**, und die Diensteanbieter haben entsprechende organisatorische Vorkehrungen zu treffen, wie etwa den **Einsatz von Virenscannern und das Einspielen regelmäßiger Sicherheitspatches** ihrer Software. Wird etwa wegen einer Sicherheitslücke eine Webseite gehackt und dabei werden Kundendaten wie Log-In-Daten oder Kreditkartendaten gestohlen, stellt dies eine Verletzung dieser Verpflichtung dar und der Diensteanbieter kann hierfür auf Schadensersatz haften und mit einer Geldbuße bis zu 50.000 Euro belegt werden. Das Gesetz sieht ausdrücklich vor, dass eine Maßnahme hierunter insbesondere die Anwendung eines als sicher anerkannten **Verschlüsselungsverfahrens** ist.

5. IT-Sicherheitsbeauftragter

Zwar besteht keine generelle Pflicht für Unternehmen, einen IT-Sicherheitsbeauftragten zu bestellen; dies ist nur für bestimmte Behörden sowie für Telekommunikationsunternehmen zwingend vorgeschrieben. Allerdings empfiehlt das BSI Unternehmen die Ernennung eines IT-Sicherheitsbeauftragten und dies liegt durchaus auch im Interesse der Unternehmensführung, deren Sorgfaltsplicht die Erkennung und Bekämpfung von IT-Risiken umfasst. **Effektive Sicherungsmaßnahmen können demnach auch die Einrichtung eines IT-Sicherheitsbeauftragten umfassen**. Das BSI stellt ein Muster für eine Bestellung eines IT-Sicherheitsbeauftragten zur Verfügung, das u.a. dessen Aufgaben, Verantwortlichkeiten und Befugnisse regelt.

6. Maßnahmen zur IT-Security und IT-Compliance

Nachfolgend werden einige **konkrete Maßnahmen zur Sicherstellung der IT-Security und IT-Compliance** in Unternehmen vorgestellt. Dieser Maßnahmenkatalog basiert primär auf rechtlichen Erwägungen und ist nicht abschließend. Seine Umsetzung sollte zwischen der Unternehmensleitung und hierbei insbesondere dem CIO (Chief Information Officer), dem IT-Sicherheitsbeauftragten und dem Compliance-Beauftragten, der IT-Abteilung, der Rechtsabteilung, dem Datenschutzbeauftragten und gegebenenfalls externen Beratern des Unternehmens (z.B. IT-Systemhäuser, Rechtsanwälte und Wirtschaftsprüfer) abgestimmt werden.

a) Schutz vor Hackern, Viren, Trojanern, Spyware, Botnets etc.
Unternehmen müssen zur Sicherstellung der IT-Security wirksame Maßnahmen gegen Angriffe von außen implementieren. Der Schutz gegen Hacker, also fremde Dritte, die in Computersysteme des Unternehmens eindringen und dabei Daten ausspähen, verändern oder zerstören, ist erforderlich, um die Verfügbarkeit, Unversehrtheit und Vertraulichkeit der IT-Infrastruktur sicherzustellen und personenbezogene Daten zu schützen. Dies gilt auch für Angriffe durch Schadsoftware wie Viren oder Würmer sowie durch Trojaner, welche es einem Dritten ermöglichen, die Kontrolle über ein EDV-System zu übernehmen. Über die Errichtung von sog. **„Botnets"** (Netzwerke von infizierten Computern) gelingt es sog. „Botmasters" mit kriminellen Zielen immer häufiger, fremde Computer für sich zu nutzen, um z.B. Spam oder Denial of Service-Attacken zu initiieren. Ebenso können sie mit Hilfe von Spyware fremde Daten sammeln oder Computer dafür missbrauchen, illegal urheberrechtlich geschützte Werke herunterzuladen.

Die **Abwehr gegen den Befall durch Schadsoftware** ist aus zweierlei Gründen wichtig: Zum einem muss das Unternehmen seine eigene IT-Infrastruktur schützen, zum anderen muss es verhindern, selbst haftbar gemacht zu werden.

Wird ein Unternehmenscomputer z.B. über ein Botnet dafür missbraucht, Viren oder Spam an Dritte zu versenden, eine Denial of Service-Attacke zu initiieren oder Urheberrechtsverletzungen zu begehen, muss das Unternehmen befürchten, für Unterlassung und Schadensersatz einstehen zu müssen. Dieser Fall kann bei **unzureichenden Sicherungsmaßnahmen** (z.B. veralteter Virenschutz oder ungesichertes WLAN) des IT-Systems durchaus eintreten. Besonders brisant ist dies für vom Unternehmen zur Verfügung gestellte **Home Office-Systeme** und im Falle von **BYOD** (siehe hierzu Kapitel VII.4), denn hier können die IT-Systeme des Unternehmens leichter angreifbar sein.

Der **Einsatz** entsprechender **Internet Security-Software** und deren ständige **Aktualisierung** ist also zwingende Voraussetzung, um die Anforderungen bezüglich IT-Compliance zu erfüllen und die Haftung gegenüber Dritten zu minimieren.

b) Schutz gegen Advanced Persistent Threats (APT)
„Advanced Persistent Threats" (APT) sind eine neue Bedrohungsform für Unternehmen, bei der der Angreifer unerkannt in das Unternehmensnetzwerk eindringt, um individuelle Malware zu installieren und so für einen längeren Zeitraum sensible Informationen auszuspähen. Um APTs vorzubeugen, empfiehlt sich der Einsatz von **„Breach Detection Systems" (BDS)**. Dies sind Lösungen für flexiblen Schutz vor individuellen Bedrohungen,

mit der gezielte Angriffe auf Unternehmen erkannt und analysiert sowie Abwehrmechanismen angepasst werden können. Zudem sollte durch die Bereitstellung von **Sicherheitsupdates** die Abwehr weiterer Angriffe ermöglicht werden.

c) Schutz gegen Datenlecks („Data Leak Prevention")

Der Schutz gegen Datenlecks – sog. **„Data Leak Prevention"** – ist erforderlich, um entsprechend den Anforderungen der IT-Security die Vertraulichkeit sensibler Informationen zu wahren, Geschäftsgeheimnisse zu schützen und die datenschutzrechtlichen Anforderungen an die Zugriffskontrolle zu erfüllen. Auch vertraglich ist ein Unternehmen häufig zur Geheimhaltung verpflichtet, sei es aufgrund eines **Non Disclosure Agreements (NDA)** oder einer Geheimhaltungsklausel. Es ist hiernach sicherzustellen, dass elektronisch gespeicherte Daten nicht verloren gehen, gestohlen werden oder zur Kenntnis oder in den Besitz unautorisierter Dritter gelangen. Fehlende Compliance auf diesen Gebieten kann zum **Verlust von Rechtsschutz** für betriebswichtiges Know-How oder geistiges Eigentum führen und **Schadensersatzforderungen**, **Vertragsstrafen** oder **Geldbußen** auslösen. Deshalb liegt der Einsatz einer wirksamen Data Leak Prevention-Technologie eindeutig im Unternehmensinteresse. Ist die Sicherheitspanne nämlich trotz eines umfassenden IT-Sicherheitssystems eingetreten und kann dem betroffenen Unternehmen seine fahrlässige Verursachung auch sonst nicht vorgeworfen werden, so sollten sich Geldbußen oder vertragliche Ansprüche aus einer Vertraulichkeitsvereinbarung jedenfalls insoweit erfolgreich abwehren lassen, wie sie einen schuldhaften Verstoß voraussetzen. Mit Blick auf Vertragsstrafenklauseln ist zu beachten, dass diese häufig eine Beweislastumkehr zulasten des Verpflichteten vorsehen, so dass von einer Sicherheitspanne betroffene Unternehmen ggf. beweisen müssen, dass sie diese nicht fahrlässig verursacht haben. Gerade dann zeigt sich aber, welchen Wert umfassende Maßnahmen zur IT- und Datensicherheit – und der Nachweis darüber – haben.

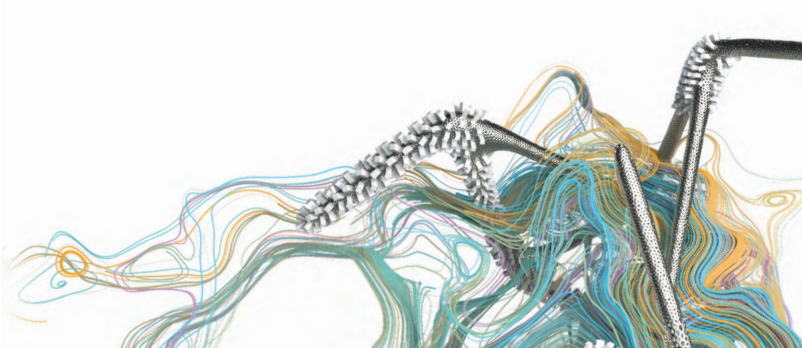
Eine **Sicherheitslücke** in einem in Deutschland befindlichen IT-System löst unter Umständen zusätzliche **Benachrichtigungspflichten nach US-amerikanischem Recht** aus. Es kommt vor, dass in Europa ansässige Unternehmen, bei denen eine Sicherheitspanne eintritt, von Betroffenen (oder deren Anwälten) in den USA benachrichtigt und – unter Vorbehalt der Geltendmachung aller Rechte einschließlich Schadensersatz und Mitteilung an die zuständigen Behörden – zur Einhaltung der anwendbaren „Security Breach Notification Laws" angehalten werden.

Auch die **EU-Datenschutz-Grundverordnung** sieht eine Pflicht zur Unterrichtung über Datenschutzverstöße (Data Breach Notification) vor. Unternehmen müssen die Aufsichtsbehörde und ggf. auch betroffene Bürger unverzüglich, möglichst binnen 72 Stunden über Datenschutzverstöße informieren.

d) Spionageaufklärung und -abwehr von innen („Deep Discovery“)
Zur sorgfältigen Gestaltung der IT-Sicherheitsstruktur eines Unternehmens gehört es auch, Verfahren oder Produkte einzusetzen, die den Abfluss von wertvollen Daten als Folge von gezielten Angriffen auf IT-Ressourcen des Unternehmens verhindern. Dazu müssen aber die sicherheitsrelevanten Ereignisse nicht nur gesammelt und einzeln ausgewertet, sondern für die Analyse miteinander korreliert und in Echtzeit überwacht werden (**„Deep Discovery“**). Denn das Wesen gezielter Angriffe besteht unter anderem in ihrem komplexen, mehrstufigen Aufbau, so dass erst die Summe der Einzelereignisse Hinweise auf Gefahren gibt.

e) Datensicherung
Nach einem Urteil des Oberlandesgerichts Hamm vom 1. Dezember 2003 (Az. 13 U 133/03), das bis heute relevant ist, gehört es „im gewerblichen Anwenderbereich heute zu den vorauszusetzenden Selbstverständlichkeiten, dass eine **zuverlässige, zeitnahe und umfassende Datenroutine** die Sicherung gewährleistet“. Das heißt: Eine Sicherung muss täglich erfolgen, eine Vollsicherung mindestens einmal wöchentlich. Sofern ein Unternehmen kein regelmäßiges Backup seiner Daten und seiner IT-Systeme durchführt, ist ihm im Falle eines durch Datenverlust entstehenden Schadens ein **„haftungsüberdeckendes Mitverschulden“** vorzuwerfen. Etwaige Schadensersatzansprüche gegen Dritte, die an sich für den Datenverlust verantwortlich sind, sind somit nicht oder nur in stark begrenztem Umfang durchsetzbar. Sollte ein Datenverlust erfolgen und die Daten mangels ausreichender Backups nicht wiederhergestellt werden können, droht aufgrund dieses grob fahrlässigen Außerachtlassens von Sicherheitsvorkehrungen auch ein **Verlust des Versicherungsschutzes**.

f) Schutz von Legacy-Betriebssystemen
Betriebssysteme werden nicht unendlich lange vom Hersteller unterstützt. So hat zum Beispiel Microsoft nach mehr als zehn Jahren am 8. April 2014 Support und Updates für Windows XP eingestellt. Wenn ein solches „Legacy Betriebssystem“ nach Ende des Supports weiterhin verwendet wird, sind die entsprechenden Computer anfälliger für Sicherheitsrisiken und Viren. Um solchen Bedrohungen vorzubeugen, bietet sich z.B. das Virtualisieren der entsprechenden Umgebung, der Einsatz eines **Intrusion Prevention Systems** im LAN und ein erweiterter **Schutz der Endpunkte** an.



g) Quellcode-Hinterlegung (Software-Escrow)
Wenn Unternehmen Software für unternehmenskritische Anwendungen nutzen und diese von einem Softwareanbieter lizenzieren, erhalten sie die Software in der Regel nur im ausführbaren Objektcode. Dieser lässt sich – anders als der Quellcode – nicht lesen und bearbeiten. Stellt der Softwareanbieter seine Geschäftstätigkeit – etwa wegen Insolvenz – ein, besteht die Gefahr, dass die Software nicht mehr gewartet wird und Fehler zu Betriebsunterbrechungen und Schäden führen. Aus diesen Gründen wird häufig eine Hinterlegung des Quellcodes der Software bei einer neutralen Hinterlegungsstelle (sog. **„Software-Escrow"**) vereinbart, die den Quellcode bei Eintritt klar definierter Fälle wie etwa der Insolvenz des Softwareanbieters an den Lizenznehmer herausgibt, damit dieser seine weitere Nutzung und Pflege der Software sicherstellen kann. Allerdings ist bei Software, deren Funktionalität von ständigen Aktualisierungen abhängig ist (wie dies etwa im Bereich der Internet Content Security der Fall ist), die Quellcode-Hinterlegung kaum zweckmäßig, denn selbst wenn dem Lizenznehmer der Quellcode bekannt ist, nützt ihm die Software ohne die laufenden Aktualisierungen wenig. Zudem erhöht eine Offenlegung des Quellcodes das Risiko, Schwachstellen der Software ausfindig zu machen und sie Angriffen von Hackern auszusetzen. Das Unternehmen sollte daher sorgfältig abwägen, ob es Software einsetzt, deren Quellcode offengelegt ist, für die ein Software-Escrow besteht oder bei der der Quellcode geheim ist und weder offengelegt noch hinterlegt wird.

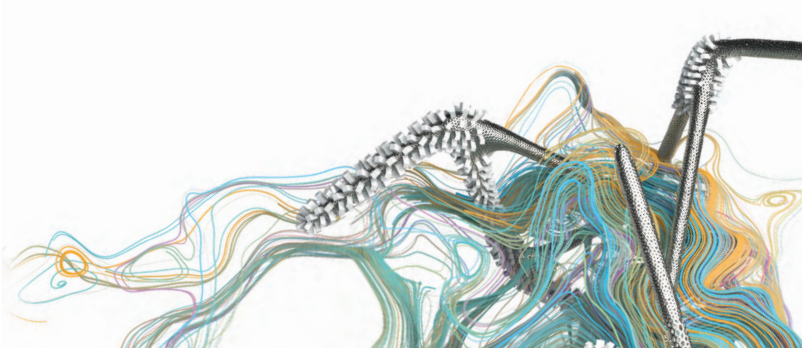
h) Handlungsanleitungen, Best Practice-Vorgaben und Minimum-Standards
Auch wenn es sich um keine für Unternehmen verbindliche Richtlinie handelt, stellt die **IT-Grundschutz-Vorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik** (BSI, www.bsi.de) zusammen mit dem IT-Grundschutz-Kompendium und dessen Empfehlungen von Standard-Sicherheitsmaßnahmen einen **De-Facto-Standard für IT-Sicherheit** dar. Anhand des IT-Grundschutz-Kompendiums und der Werkzeuge, die vom BSI zur Verfügung gestellt werden, können Unternehmen ein angemessenes IT-Sicherheitsniveau erreichen. Die Edition 2019 des IT-Grundschutz-Kompendiums enthält insgesamt 94 IT-Grundschutz-Bausteine. Sie sind in zehn Schichten aufgeteilt, bilden den aktuellen Stand der Technik ab und umfassen zahlreiche Themen der Informationssicherheit – von Anwendungen bis hin zum Sicherheitsmanagement. Bei der Erstellung der Bausteine wurde bereits eine Risikobewertung für Bereiche mit normalem Schutzbedarf durchgeführt.

Die BSI-Standards enthalten Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit. Sie sollen Anwendern aus Behörden und Unternehmen sowie Hersteller und Dienstleister darin unterstützen, Geschäftsprozesse und Daten sicherer zu gestalten. Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informations-

sicherheit und ist zum ISO-Standard 27001 kompatibel, der ähnlich strukturierte BSI-Standard 200-2 etabliert drei Vorgehensweisen bei der Umsetzung des IT-Grundschutzes. Der BSI-Standard 200-3 befasst sich mit der Risikoanalyse auf der Basis von IT-Grundschutz.

Des weiteren lassen sich die **ISO-Standards** der ISO-Normenfamilie 27000 sowie „ITIL", eine über Jahrzehnte gewachsene Sammlung von Best Practices zum IT Service Management, als **Best Practice-Vorgaben** heranziehen. Auch eine **Zertifizierung** des Informationssicherheits-Managementsystems nach ISO 27001 ist möglich. Der BSI-Standard 200 1 ist hierbei ISO 27001 kompatibel. ISO 31000 legt Leitlinien für ein Risikomanagement durch Organisationen fest. Hierbei wird ein allgemeiner Ansatz für das Behandeln jeglicher Art von Risiken während der gesamten Lebensdauer der Organisation verfolgt. Als weiterer Standard kann auf **„COBIT 2019"** (der auf „COBIT 5" basiert, aber flexibler gestaltet ist) zurückgegriffen werden. Hierbei handelt es sich um ein international anerkanntes Framework zu IT-Governance und Management von Unternehmens-IT, welches von der Non-Profit-Organisation „ISACA" veröffentlicht wird (abrufbar unter www.isaca.org).

i) Anforderungen an die Buchhaltung
§§ 239 und 257 HGB beinhalten Anforderungen an die Führung der Handelsbücher und die Aufbewahrung der Unterlagen. Hiernach sind die **Grundsätze ordnungsgemäßer Buchführung (GoB)** einzuhalten. Nach § 239 Abs. 4 Satz 2 HGB muss bei der Führung der Handelsbücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern insbesondere sichergestellt sein, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Zu beachten sind dabei die **„Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff" (GoBD)** der Finanzverwaltung. Hierin sind u.a. Anforderungen an die **Datensicherheit** und die Unveränderbarkeit von Aufzeichnungen enthalten. Der Steuerpflichtige hat sein EDV-System gegen Verlust (z.B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) zu sichern und gegen unberechtigte Eingaben und Veränderungen (z.B. durch Zugangs- und Zugriffskontrollen) zu schützen. Werden die Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen nicht ausreichend geschützt und können deswegen nicht mehr vorgelegt werden, so ist die Buchführung formell nicht mehr ordnungsmäßig, mit der Folge, dass die Finanzbehörde die Besteuerungsgrundlagen schätzen und ggf. einen Vorsteuerabzug ablehnen kann. **IT-Security ist somit für eine ordnungsgemäße Buchhaltung für Unternehmen existenziell**.



Je nach Art der Unterlagen beträgt die **Aufbewahrungsfrist** sechs bzw. zehn Jahre. Es ist sicherzustellen, dass auch bei einer Erneuerung der IT-Infrastruktur oder einer Datenmigration das Unternehmen den GoBD gerecht wird.

j) Einhaltung von Prüfungsstandards

Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) hat verschiedene Prüfungsstandards wie z.B. IDW PS 330 (Abschlussprüfung bei Einsatz von Informationstechnologie), IDW PS 331 (Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen) und IDW PS 880 (Die Prüfung von Softwareprodukten) herausgegeben, die bei Abschlussprüfungen zu beachten sind. Die IDW-Stellungnahme zur Rechnungslegung „Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Prozessen und Funktionen einschließlich Cloud Computing" (IDW RS FAIT 5) konkretisiert die Anforderungen beim IT-Outsourcing an die Führung der Handelsbücher mittels IT-gestützter Systeme und verdeutlicht die beim Einsatz von Cloud Computing möglichen Risiken für die Einhaltung der Grundsätze ordnungsmäßiger Buchführung.

k) Besondere Anforderungen an Banken und Finanzdienstleister

§ 25b Kreditwesengesetz (KWG) enthält besondere Organisationspflichten für Banken und Finanzdienstleister. Danach müssen **angemessene Sicherheitsvorkehrungen** für den Einsatz der elektronischen Datenverarbeitung getroffen werden. Sofern Bereiche auf ein anderes Unternehmen ausgelagert werden, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, dürfen weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen noch die Steuerungs- oder Kontrollmöglichkeiten der Geschäftsleitung, noch die Prüfungsrechte und Kontrollmöglichkeiten der **Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)** beeinträchtigt werden. In zwei Rundschreiben der BaFin aus dem Jahre 2017 werden diese Anforderungen konkretisiert und hierbei **Mindestanforderungen an das Risikomanagement (MaRisk) und Bankaufsichtliche Anforderungen an die IT (BAIT)** aufgestellt. Die MaRisk umfasst insbesondere die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren. Banken und Finanzdienstleister müssen diese organisatorischen Pflichten beachten – insbesondere beim Outsourcing von IT-Leistungen.

7. Haftung und Sanktionen bei Verstößen gegen IT-Security und IT-Compliance

Bei Verstößen gegen IT-Security und IT-Compliance können insbesondere folgende Sanktionen drohen:

a) Strafrechtliche Sanktionen

Vorsätzliche Verstöße – wie das Ausspähen von Daten, die Verletzung des Fernmeldegeheimnisses oder die Verletzung von Datenschutzvorschriften in Bereicherungsabsicht – sind mit Geld- oder Freiheitsstrafe bedroht.

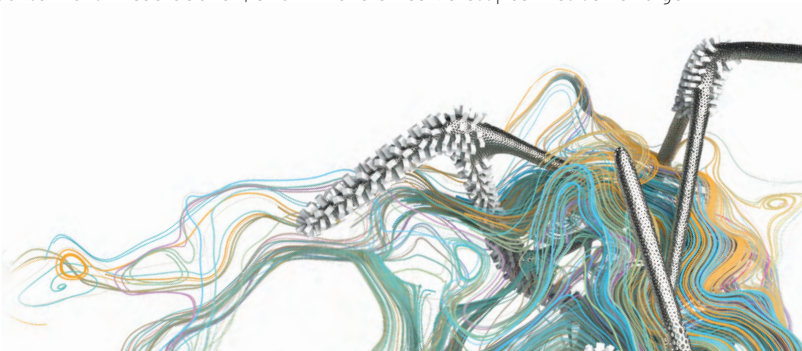
b) Ordnungswidrigkeiten
Verstöße gegen öffentlich-rechtliche Regelungen wie das Datenschutzrecht (siehe Kapitel II.1), das IT-Sicherheitsgesetz (siehe Kapitel I.3.f) oder das Kreditwesengesetz (KWG) können eine Ordnungswidrigkeit darstellen und Bußgelder nach sich ziehen.

c) Haftung des Unternehmens
Das Unternehmen selbst kann gegenüber Dritten haftbar sein. Dies gilt aufgrund **Organisationsverschuldens**, wenn keine ausreichenden Schutzvorrichtungen getroffen wurden, die beispielsweise den Missbrauch der IT-Infrastruktur durch Externe verhindern. Sofern dadurch Dritte geschädigt werden – z.B. weil über das IT-System des Unternehmens Spam oder Viren versendet oder Urheberrechte Dritter verletzt wurden – ist das Unternehmen **Unterlassungs- und Schadensersatzsprüchen** des Geschädigten ausgesetzt.

d) Persönliche Haftung der Unternehmensleitung
Vorstands- oder Aufsichtsratsmitglieder sowie Geschäftsführer oder geschäftsführende Gesellschafter sind der Gesellschaft persönlich zum Ersatz des Schadens verpflichtet, welcher der Gesellschaft aufgrund **schuldhafter Pflichtverletzung ihrer Organmitglieder** entsteht.

So hat das Landgericht München I (Urteil vom 10. Dezember 2013, Az. 5HK O 1387/10) in einem Präzedenzfall ein Vorstandsmitglied wegen Verstoßes gegen § 93 Abs. 2 Satz 1 Aktiengesetz zu einer Schadensersatzzahlung an sein ehemaliges Unternehmen von 15 Millionen Euro verurteilt. Das Gericht führte u.a. aus, dass die Einrichtung eines auf Schadensprävention und Risikokontrolle angelegten **Compliance-Systems** zur Sicherstellung der Einhaltung sämtlicher in- und ausländischen Rechtsvorschriften, die das Unternehmen betreffen, zur **Gesamtverantwortung des Vorstands** gehört. Hierunter fallen auch die gesetzlichen Anforderungen an IT-Compliance und IT-Security.

e) Persönliche Haftung von Mitarbeitern
Arbeitnehmer, besonders **IT-Sicherheitsverantwortliche**, können gegenüber ihrem Arbeitgeber schadensersatzpflichtig sein, wenn sie schuldhaft ihre Arbeitsleistung schlecht erbracht und dadurch den Arbeitgeber geschädigt haben. Verstoßen sie gegen Compliance-Anforderungen an die IT-Security, kann das je nach Grad des Verstoßes eine **Abmahnung** oder **fristlose Kündigung** nach sich ziehen. So hat zum Beispiel das Landesarbeitsgericht München bereits mit Urteil vom 8. Juli 2009 (Az. 11 Sa 54/09) entschieden, dass sich ein Unternehmen darauf verlassen können muss, dass seine Systemadministratoren die eingeräumten Zugriffsrechte nicht missbrauchen, und im Falle eines Verstoßes fristlos kündigen



darf. Ein wichtiger Grund für eine fristlose Kündigung liegt – so das Landesarbeitsgericht München in einer weiteren Entscheidung (Urteil vom 5. August 2009 - Az. 11 Sa 1066/08) – auch dann vor, wenn sich ein Mitarbeiter durch einen Trick ihm nicht zugewiesene Administratorenrechte verschafft. Allerdings muss zumindest ein dringender Tatverdacht gegen einen bestimmten Mitarbeiter bestehen; ist hingegen nicht nachweisbar, wer auf den betreffenden Computer zugegriffen hat, ist eine außerordentliche Kündigung nicht gerechtfertigt (Urteil des Landesarbeitsgerichts Hamm vom 6. Dezember 2013 - Az. 13 Sa 596/13).

f) Weitere Konsequenzen

Zudem droht bei Verstößen gegen IT-Security und IT-Compliance die Reduzierung oder der Verlust von Schadensersatzansprüchen gegenüber Dritten aufgrund überwiegenden Mitverschuldens, der Verlust von Versicherungsschutz, der Ausschluss von der öffentlichen Auftragsvergabe oder sogar die Gewerbeuntersagung.

8. Stärkung der EU gegen Cyberangriffe

Die EU erlässt einen „Rechtsakt zur Cybersicherheit" – Cybersecurity Act, mit dem die Abwehrfähigkeit der EU gegen Cyberangriffe gestärkt werden soll. Das Europäische Parlament hat den Cybersecurity Act am 12. März 2019 verabschiedet und er tritt möglicherweise noch im Laufe des Jahres 2019 in Kraft. Der Cybersecurity Act regelt insbesondere:

- **Einführung eines EU-weiten Zertifizierungssystem für Cybersicherheit, um sicherzustellen, dass zertifizierte Produkte, Verfahren und Dienstleistungen, die in der EU verkauft werden, den Cybersicherheitsstandards entsprechen; hierdurch sollen EU-einheitliche Kriterien für die Cybersicherheit und die Anerkennung von Produkten und Services geschaffen werden**
- **Stärkung der EU-Cybersicherheitsagentur ENISA, die EU-Mitgliedstaaten bei der Vorbeugung gegen Cyberangriffe unterstützen soll**

II. Datenschutz und IT-Sicherheit

Datenschutz hat für Unternehmen eine herausragende Bedeutung. Die Unternehmensleitung hat sicherzustellen, dass das einschlägige Datenschutzrecht – insbesondere die EU-Datenschutz-Grundverordnung (DS-GVO) – eingehalten wird, andernfalls drohen aufsichtsrechtliche Maßnahmen, Bußgelder, Schadensersatzansprüche und ggf. Unterlassungsklagen von Verbraucherschutzverbänden. IT-Sicherheit ist hierbei ein wichtiger Aspekt, damit ein Unternehmen datenschutzcompliant ist. Die Übermittlung personenbezogener Daten in Länder außerhalb der EU und Big Data-Anwendung sind aus datenschutzrechtlicher Sicht sorgfältig zu prüfen.

1. EU-Datenschutz-Grundverordnung

Das Datenschutzrecht wurde durch die neue, europaweit einheitliche EU-Datenschutz-Grundverordnung (DS-GVO) mit Wirkung zum 25. Mai 2018 umfassend neu geregelt. **Wesentliche Regelungen und Anforderungen an Unternehmen der EU-Datenschutz-Grundverordnung** sind:

(i) Anwendungsbereich
Der Anwendungsbereich der Datenschutz-Grundverordnung ist sehr weitreichend und umfasst **jede automatisierte Verarbeitung personenbezogener Daten durch Unternehmen** wie Kundendaten, Mitarbeiterdaten oder über das Internet erhobene Daten. Lediglich anonyme Informationen oder Daten juristischer Personen wie etwa eine Firmenanschrift stellen keine personenbezogenen Daten dar. Zwar wird vereinzelt den Bedürfnissen von Kleinstunternehmen sowie **kleinen und mittleren Unternehmen (KMU)** – dies sind Unternehmen, die weniger als 250 Personen beschäftigen und deren Jahresumsatz höchstens 50 Mio. Euro oder deren Jahresbilanzsumme höchstens 43 Mio. Euro beträgt – Rechnung getragen, doch auch diese fallen unter die Datenschutz-Grundverordnung. **Ausländische Unternehmen** haben sich ebenfalls der DS-GVO zu unterwerfen, wenn sie innerhalb der EU Waren oder Dienstleistungen – etwa über das Internet – anbieten oder das Verhalten von Personen in der EU beobachten, wie es beispielsweise bei Werbenetzwerken im Internet der Fall ist.

(ii) Grundsätze der Datenverarbeitung
Nach Art. 5 DS-GVO gelten folgende **Grundsätze für die Verarbeitung personenbezogener Daten**:

- Verarbeitung auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise
- **Zweckbindung**, d.h. keine Weiterverarbeitung für andere als die ursprünglich festgelegten Zwecke

- **Datenminimierung**
- **Richtigkeit** der personenbezogenen Daten
- **Begrenzung der Speicherung** personenbezogener Daten auf die erforderliche Zeit
- Gewährleistung der **Integrität** und **Vertraulichkeit** der personenbezogenen Daten durch geeignete **technische und organisatorische Maßnahmen**

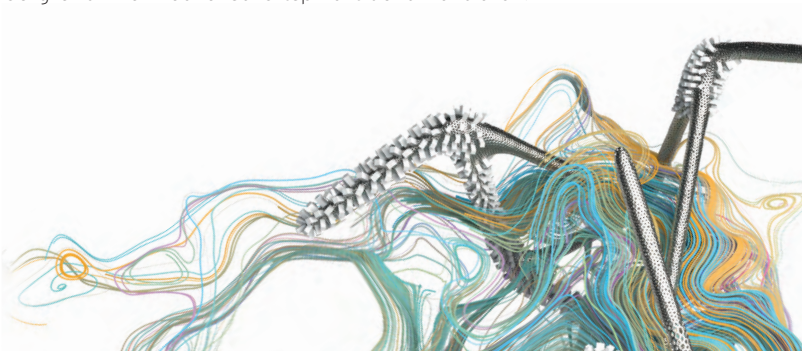
Das Unternehmen ist für die Einhaltung dieser Grundsätze verantwortlich und unterliegt diesbezüglich einer **Rechenschaftspflicht**.

(iii) Rechtmäßigkeit der Datenverarbeitung
Für die **Rechtmäßigkeit der Datenverarbeitung** muss eine der folgenden Bedingungen erfüllt sein:

- Die betroffene Person hat ihre **Einwilligung** erteilt. Die Anforderungen an eine solche Einwilligung sind hoch: Sie muss freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich erklärt sein und muss gesondert von anderen Regelungen erfolgen, so dass die Einwilligungserklärung z.B. nicht in den AGB versteckt sein darf
- Die Verarbeitung personenbezogener Daten dient der **Erfüllung eines Vertrages** oder der Durchführung vorvertraglicher Maßnahmen
- Die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der das Unternehmen unterliegt
- Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** zu schützen
- Die Verarbeitung erfolgt im **öffentlichen Interesse** oder in **Ausübung öffentlicher Gewalt**
- Die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Unternehmens** oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen

Sofern weder eine Einwilligung der betroffenen Person noch ein Vertrag mit dieser vorliegt, zu dessen Erfüllung die Verarbeitung personenbezogener Daten erforderlich ist, ist insbesondere auf die zuletzt genannte **Interessenabwägung** des Unternehmens abzustellen.

Liegt keine der vorgenannten Voraussetzungen vor, ist die Datenverarbeitung verboten und ein Verstoß führt zu den weiter unten dargestellten Sanktionen. Daher müssen Unternehmen die **Rechtmäßigkeit der Datenverarbeitung sorgfältig prüfen und ggf. abwägen** und dies aufgrund ihrer Rechenschaftspflicht **dokumentieren**.



(iv) Spannungsverhältnis zwischen Datenschutz und IT-Sicherheit

Um **Datenschutzverstöße zu verhindern** und die Integrität und Vertraulichkeit der personenbezogenen Daten zu wahren, werden Unternehmen häufig auf Softwarelösungen zum Schutz vor Angriffen und Schadsoftware und auf entsprechende Produkte und Dienste von Anbietern von Sicherheitstechnologien zurückgreifen, die sie vor Angriffen auf die IT-Infrastruktur (etwa durch Advanced Persistent Threats – APT – siehe Kapitel I.6.b) schützen und Betrug (wie z.B. durch Online-Skimming) verhindern. Weitere **Bedrohungsszenarien**, gegen die sich Unternehmen mittels IT-Sicherheitslösungen schützen können, sind die Gefährdung ihrer IT-Systeme durch Command-and-Control (C&C)-Kommunikation und Bot-Malware, die die Kontrolle über das System des Unternehmens übernimmt, die Gefährdung des Netzes durch Denial of Service (DoS)-Attacken und die Verbreitung von Spam oder Schadsoftware.

Bei der Abwehr solcher Angriffe werden forensische Verfahren wie **EDR (Endpoint Detection and Response)** eingesetzt, bei denen personenbezogene Daten, etwa zu Art und Herkunft der Bedrohung, und die URL, IP-Adresse oder E-Mail-Adresse des Angreifers und des angegriffenen Hosts erhoben und für eine begrenzte Zeit gespeichert werden. Mittels dieser Daten können Angriffe analysiert und abgewehrt sowie künftigen Bedrohungen vorgebeugt werden. Ob eine solche Erhebung und Verarbeitung personenbezogener Daten aus Gründen der IT-Sicherheit zur Verhinderung von Betrug oder zum **Schutz vor Angriffen auf die IT-Infrastruktur** von Unternehmen datenschutzrechtlich zulässig ist, ist im Rahmen einer **Interessenabwägung** zu ermitteln. In den Erwägungsgründen der Datenschutz-Grundverordnung ist diesbezüglich explizit ausgeführt, dass die Verarbeitung von personenbezogenen Daten durch **Anbieter von Sicherheitstechnologien und -diensten** ein berechtigtes Interesse des jeweiligen verantwortlichen Unternehmens darstellt, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, **Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren**, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den **Zugang Unbefugter** zu elektronischen Kommunikationsnetzen und die **Verbreitung schädlicher Programmcodes** zu verhindern sowie **„Denial of service"-Angriffe** und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren. Dies bedeutet, dass die **Erhebung, Verarbeitung und vorübergehende Speicherung personenbezogener Daten etwa mittels einer EDR-Lösung datenschutzrechtlich zulässig ist**, wenn sie zur Wahrung der berechtigten Interessen des Unternehmens, das sich gegen Angriffe auf seine IT-Infrastruktur schützt, erforderlich ist, und die Interessen der betroffenen Person nicht überwiegen. Faktoren, die im Rahmen dieser Interessenabwägung zugunsten des Unternehmens zu berücksichtigen sind, sind etwa Anonymisierung, Pseudonymisierung und Verschlüsselung personenbezogener Daten, Datenminimierung und die Begrenzung der Datenspeicherung auf die erforderliche Zeit.

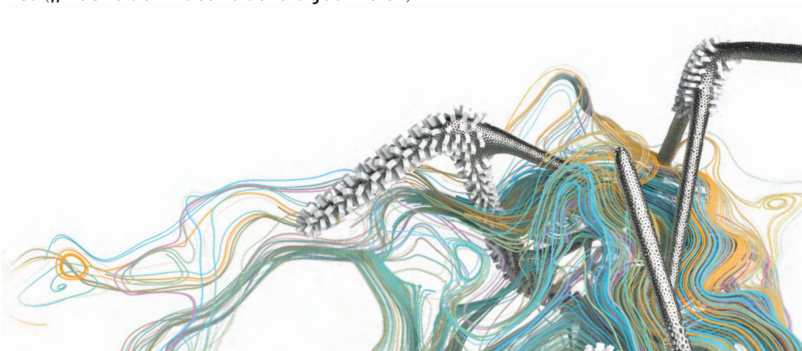
Dieses Ergebnis wird durch das Urteil des Europäischen Gerichtshofs (EuGH) in dem Fall Breyer ./. Bundesrepublik Deutschland vom 19. Oktober 2016 (Rs. C-582/14) gestützt. Der EuGH hatte hierin entschieden, dass Betreiber von Webseiten ein **berechtigtes Interesse** daran haben, die **generelle Funktionsfähigkeit ihrer Webseite über die konkrete Nutzung hinaus zu gewährleisten und hierzu personenbezogene Daten wie insbesondere die dynamischen IP-Adressen der Nutzer im erforderlichen Maße zu erheben und zu verwenden**, und zwar auch über das Ende eines Nutzungsvorgangs hinaus.

(v) Informationspflichten
Unternehmen unterliegen hinsichtlich der Erhebung der personenbezogenen Daten **umfassenden Informationspflichten**. So müssen sie die betroffenen Personen beispielsweise über ihre Kontaktdaten, den Zweck, die Rechtsgrundlage und ggf. die berechtigten Interessen für die Datenverarbeitung, den Empfänger der personenbezogenen Daten, eine etwaige Übermittlung an ein Drittland außerhalb der EU sowie ggf. über ihren Datenschutzbeauftragten unterrichten. Diese Informationen müssen in **präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache** erteilt werden.

(vi) Rechte der Betroffenen
Den Betroffenen stehen gegenüber Unternehmen, die ihre personenbezogenen Daten verarbeiten, u.a. ein **Auskunftsrecht**, ein Recht auf **Berichtigung** unrichtiger Daten, ein **Widerspruchsrecht** und ein **Beschwerderecht** zu. Über diese Rechte ist der Betroffene zum Zeitpunkt der Datenerhebung ebenfalls schriftlich oder elektronisch zu **unterrichten**.

(vii) Recht auf Vergessenwerden
Zudem kann eine Person die **Löschung** der über sie gespeicherten Daten von der für die Datenverarbeitung verantwortlichen Stelle (z.B. einem Internet-Unternehmen) verlangen, sofern nicht gesetzliche Aufbewahrungspflichten bestehen. Dieses Unternehmen muss das Löschungsersuchen auch an Dritte weiterleiten, bei denen die Daten repliziert sind, damit das **„Recht auf Vergessenwerden"** des Betroffenen auch umgesetzt werden kann.

(viii) Portabilität von Daten
Betroffene Personen sollen auf einfachere Weise auf ihre eigenen Daten, die sie z.B. einem Internet-Unternehmen bereitgestellt haben, zugreifen und verlangen können, dass diese Daten **direkt von einem Provider an einen anderen übermittelt** werden, soweit dies technisch machbar ist (**„Recht auf Datenübertragbarkeit"**).



(ix) Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Produkte und Services müssen bereits im Rahmen der Entwicklung datenschutzgerecht gestaltet **(data protection by design)** werden und datenschutzfreundliche Voreinstellungen **(data protection by default)** beinhalten, die den Datenschutzgrundsätzen wie Datenminimierung und Zweckbindung entsprechen.

(x) Auftragsverarbeitung

Sofern ein Unternehmen die Verarbeitung personenbezogener Daten an ein anderes Unternehmen im Wege der sog. Auftragsverarbeitung auslagert, bleiben es dennoch für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Auftraggeber als Verantwortlicher muss nach Maßgabe der Art. 28, 29 DS-GVO mit dem von ihm beauftragten Auftragsverarbeiter eine **Vereinbarung zur Auftragsverarbeitung** schließen. Hierin sind u.a. die Rechte des Verantwortlichen zur Überprüfung des Auftragsverarbeiters, die **technischen und organisatorischen Maßnahmen des Auftragsverarbeiters** und etwaige Unterauftragsverhältnisse festzulegen.

Allerdings ist jeweils im Einzelfall zu prüfen, ob tatsächlich eine Auftragsverarbeitung vorliegt. Diese ist dadurch gekennzeichnet, dass der Auftraggeber verantwortlich bleibt und der Auftragsverarbeiter seinen Weisungen unterliegt. Bei komplexen Anwendungen im Bereich der Internet Security verfügt der Kunde häufig nicht über das fachliche Know-How, zu einzelnen Arbeitsschritten Weisungen zu erteilen und die Einhaltung der Pflichten des Auftragsverarbeiters zu überprüfen, so dass je nach Ausgestaltung keine Auftragsverarbeitung nach Art. 28 DS-GVO vorliegt, sondern eine **gemeinsame Verantwortlichkeit von Internet Security-Anbieter und Kunde** gemäß Art. 26 DS-GVO.

(xi) Technische und organisatorische Maßnahmen

Für die Datenverarbeitung verantwortliche Unternehmen wie auch deren Auftragsverarbeiter müssen nach Art. 24 und 32 DS-GVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten **geeignete technische und organisatorische Maßnahmen** umsetzen, um sicherzustellen und den Nachweis dafür zu erbringen, dass die Verarbeitung personenbezogener Daten rechtmäßig ist und ein dem Risiko **angemessenes Schutzniveau** gewährleistet ist. Solche Maßnahmen schließen unter anderem ein:

- die **Verschlüsselung** personenbezogener Daten
- die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**

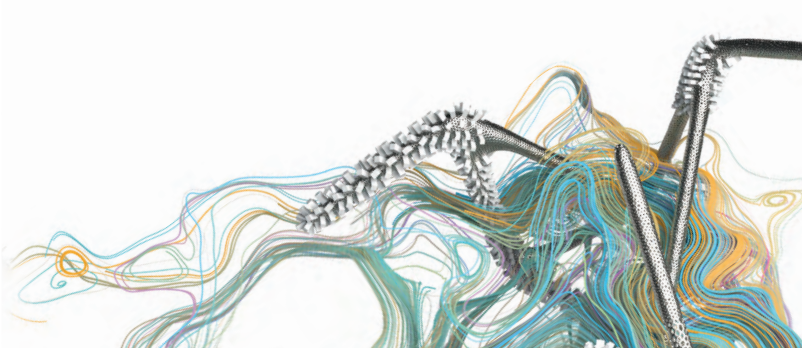
- ein Verfahren zur regelmäßigen **Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Bei der **Beurteilung des angemessenen Schutzniveaus** sind vor allem die **Risiken** zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – **Vernichtung, Verlust, Veränderun**g oder **unbefugte Offenlegun**g oder **unbefugten Zugang** zu personenbezogenen Daten.

(xii) Verzeichnis von Verarbeitungstätigkeiten
Viele Unternehmen wie auch Auftragsverarbeiter müssen ein Verzeichnis aller Verarbeitungstätigkeiten führen und dieses auf Anfrage der Aufsichtsbehörde zur Verfügung stellen. Hierin ist insbesondere auch eine **allgemeine Beschreibung der technischen und organisatorischen Maßnahmen** aufzunehmen. Aus diesem Grunde sind die technischen und organisatorischen Maßnahmen durch das Unternehmen nicht nur zu implementieren, sondern auch zu **dokumentieren**.

(xiii) Datenschutz-Folgenabschätzung
Im Falle eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen aufgrund der Art, des Umfangs, der Umstände und dem Zweck der Datenverarbeitung müssen Unternehmen vorab eine **Datenschutz-Folgenabschätzung** durchführen.

(xiv) One-Stop-Shop
Für Unternehmen, die in mehreren Ländern der EU tätig sind, ist **federführend die Datenschutzaufsichtsbehörde des Landes zuständig**, in dem das Unternehmen seine **Hauptniederlassung** hat. Allerdings können sich Bürger bei Datenschutzverstößen immer an die Datenschutzaufsicht und an die Gerichte des Landes ihres **Aufenthaltsorts** wenden, auch wenn das betreffende Unternehmen woanders ansässig ist. Nach der Datenschutz-Grundverordnung gibt es also einen **„One-Stop-Shop" für Unternehmen, die innerhalb der EU grenzüberschreitend tätig sind**, allerdings muss ein Unternehmen auch befürchten, sich gegenüber einer Aufsichtsbehörde oder eines Gerichts in dem Land verantworten zu müssen, in dem eine **von einem Datenschutzverstoß betroffene Person ansässig** ist. Zudem bestehen nach wie vor **nationale Besonderheiten** wie beispielsweise die Pflicht zur Bestellung eines Datenschutzbeauftragten oder spezielle Rechtsvorschriften zur Datenverarbeitung im Rahmen von **Beschäftigungsverhältnissen**.



(xv) Eingeschränkte Datenübermittlung an Behörden von Nicht-EU-Ländern
Ein Unternehmen (z.B. ein Cloud-Anbieter) in der EU darf **Daten an Behörden oder Gerichte von Nicht-EU-Ländern** nur nach Maßgabe der Datenschutz-Grundverordnung oder auf Grundlage internationaler Übereinkünfte übermitteln.

(xvi) Datenschutzbeauftragter
Zwar besteht nach der Datenschutz-Grundverordnung nur unter engen Voraussetzungen eine Verpflichtung zur Benennung eines Datenschutzbeauftragten, doch verlangt das deutsche Bundesdatenschutzgesetz (BDSG) die Benennung eines Datenschutzbeauftragten, wenn ein Unternehmen in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

(xvii) Unterrichtung über Datenschutzverstöße (Data Breach Notification)
Unternehmen müssen die Aufsichtsbehörde und ggf. auch betroffene Bürger unverzüglich, möglichst **binnen 72 Stunden über Datenschutzverstöße informieren**. Sofern eine solche Benachrichtigung der betroffenen Personen mit einem unverhältnismäßigen Aufwand verbunden wäre, hat stattdessen eine **öffentliche Bekanntmachung** über den Datenschutzverstoß zu erfolgen. Um dieser Pflicht nachzukommen, müssen Unternehmen sicherstellen, etwaige Datenschutzverstöße und deren Folgen zu erkennen. Zur Vermeidung von Maßnahmen der Aufsichtsbehörde und eines erheblichen **Reputationsverlusts** ist es daher umso wichtiger, eine Verletzung des Schutzes personenbezogener Daten von vornherein durch umfassende Sicherheitsmaßnahmen zu unterbinden.

(xviii) Maßnahmen und Sanktionen
Die Maßnahmen und Sanktionen bei einer Verletzung der Regelungen der Datenschutz-Grundverordnung sind streng:

- Betroffene Personen können **Schadensersatzansprüche** geltend machen
- Der Aufsichtsbehörde stehen umfangreiche Untersuchungsbefugnisse zu, wie **Datenschutzüberprüfungen (Audits)** und Zugang zu den Geschäftsräumen des Unternehmens einschließlich aller Datenverarbeitungsanlagen und -geräte
- Die Aufsichtsbehörde kann aufsichtsrechtliche Maßnahmen erlassen, von einer Verwarnung bis hin zum **Verbot der rechtswidrigen Datenverarbeitung**
- **Geldbußen** gegenüber dem Unternehmen können bis zu **4 % des gesamten weltweiten Jahresumsatzes** oder bis zu **20 Millionen Euro** betragen

(xix) Unterlassungsansprüche von Wettbewerbern und Verbraucherschutzverbänden
Umstritten ist, ob eine Verletzung von Datenschutzvorschriften zugleich einen Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb (UWG) darstellt, mit der Folge, dass Wettbewerber und Verbraucherschutzverbände hiergegen Unterlassungsansprüche geltend machen und mit einer **Abmahnung** und **einstweiligen Verfügung** vorgehen können. In einem Rechtsstreit zwischen dem Bundesverband der Verbraucherzentralen und Ver-

braucherverbände (vzbv) und Facebook über das Vorliegen einer wirksamen datenschutzrechtlichen Einwilligung hat der Bundesgerichtshof (BGH) mit Beschluss vom 11. April 2019 (Az. I ZR 186/17) das Verfahren ausgesetzt, um eine Entscheidung des Europäischen Gerichtshof (EuGH) zu diesen Fragen in einem Parallelverfahren abzuwarten.

(xx) Weitergehende Informationen
Trend Micro informiert umfassend zur DS-GVO-Compliance und zur Umsetzung der Anforderungen der DS-GVO auf den Webseiten von Trend Micro unter https://www.trendmicro.com/de_de/business/capabilities/solutions-for/gdpr-compliance.html und https://success.trendmicro.com/data-collection-disclosure.

2. E-Privacy-Verordnung

Neben der Datenschutz-Grundverordnung plant die EU den Erlass der „Verordnung über Privatsphäre und elektronische Kommunikation", sog. **E-Privacy-Verordnun**g. Geregelt werden sollen hierin u.a. die **Anforderungen an Cookies**. Endnutzern sollen hiernach verschiedene Einstellungsmöglichkeiten zur Privatsphäre mit unterschiedlichem Schutzniveau – insbesondere bezüglich Cookies von Drittanbietern – angeboten werden. Allerdings befindet sich der Verordnungsvorschlag der EU-Kommission vom 10. Januar 2017 nach wie vor in der Diskussion und ein Inkrafttreten der E-Privacy-Verordnung wird vermutlich nicht vor 2020 erfolgen, ihre Anwendbarkeit nicht vor 2022.

3. Big Data

„Big Data" bezeichnet die Auswertung einer großen Menge unterschiedlicher und unstrukturierter Daten aus unterschiedlichen Quellen in hoher Geschwindigkeit zur Erkennung von Mustern, Zusammenhängen oder Ursächlichkeiten, so dass sich hierauf unternehmerische Entscheidungen stützen lassen. Viele Big Data-Anwendungen sind datenschutzrechtlich neutral, da keine personenbezogenen Daten betroffen sind, wie es etwa bei Wetterdaten oder Produktionsdaten aus Fertigungsprozessen der Fall ist. Hierfür sieht die **„EU-Verordnung Nr. 2018/1807 für freien Verkehr nicht-personenbezogener Daten"**, die seit 28. Mai 2019 gilt, den freien Datenverkehr innerhalb der EU vor, denn diesem wird nach Einschätzung der EU eine entscheidende Bedeutung dabei zukommen, datengetriebenes Wachstum und Innovationen zu generieren. Die EU weist in den Erwägungsgründen dieser Verordnung darauf hin, dass das wachsende **Internet der Dinge (IoT, siehe Kapitel IV), künstliche Intelligenz und maschinelles Lernen** bedeutende Quellen für nicht-personenbezogene Daten darstellen. Als Anwendungsbeispiele nennt die EU den Einsatz in

automatisierten industriellen Produktionsprozessen, aggregierte und anonymisierte Datensätze für Big Data-Analysen oder Daten zum Wartungsbedarf von Industriemaschinen.

Ist es hingegen – eventuell auch erst durch technologische Neuentwicklungen – möglich, solche anonymisierten Daten wieder in personenbezogene Daten umzuwandeln, müssen diese als personenbezogene Daten behandelt werden. Dies hat zur Folge, dass für solche Big Data-Anwendungen Datenschutzrecht und insbesondere die DS-GVO gilt. Sofern hiernach personenbezogene Daten verarbeitet werden, ist auch bei Big Data-Anwendungen der **datenschutzrechtliche Grundsatz der Datenminimierung** zu beachten. Um Big Data-Anwendungen **datenschutzkonform** auszugestalten, bieten sich folgende Ansätze:

- **Anonymisierung der Datensätze**
- **Einholung einer informierten Einwilligung der Betroffenen**
- **Datenschutzrechtliche Untersuchung der Zulässigkeit im Rahmen einer Interessenabwägung unter Berücksichtigung des datenschutzrechtlichen Grundsatzes der Zweckbindung einerseits und von abmildernden Schutzmaßnahmen wie Aggregation, Pseudonymisierung und Verschlüsselung andererseits**

Der Verantwortliche muss zudem durch **technische und organisatorische Maßnahmen** sicherstellen, dass die Daten vertraulich behandelt werden und das genutzte System integer ist. Bereits unmittelbar nach der Erhebung der Daten sind **geeignete Schutzmaßnahmen** zu treffen, wie Anonymisierung und Aggregation, Privacy-Preserving Data Mining oder logische Separierung, um einem Missbrauch durch Verkettung von Daten zu begegnen.

4. Datenübermittlung und EU-US-Datenschutzschild (Privacy Shield)

Es liegt in der Natur des Internets, dass die Datenübermittlung an nationalen Grenzen keinen Halt macht. Das Datenschutzniveau der EU unter der Datenschutz-Grundverordnung gilt nicht weltweit. Für mache Länder wie z.B. die Schweiz, Israel, Argentinien, Kanada und seit 23. Januar 2019 auch Japan hat die EU anerkannt, dass deren Datenschutzniveau angemessen ist. Sofern personenbezogene Daten von der EU in andere Länder übermittelt werden sollen, lässt sich durch die Verwendung sog. **Standardvertragsklauseln der EU** oder mittels **verbindlicher Unternehmensregelungen („Binding Corporate Rules")** ein solcher internationaler Datentransfer datenschutzrechtlich absichern. Möglich ist auch die **datenschutzrechtliche Zertifizierung von Unternehmen** und die **Einhaltung verbindlicher Verhaltensregeln**, sofern diese von der EU-Kommission für allgemein gültig erklärt worden sind.

Im Verhältnis zu den USA bestand zudem die Möglichkeit einer Selbst-Zertifizierung des Datenimporteurs nach den zwischen der EU und den USA abgeschlossenen **Safe Harbour-Regelungen**, die allerdings vom Europäischen Gerichtshof (EuGH) mit Urteil vom 6. Oktober 2015 (Rs. C-362/14) **für ungültig erklärt** wurden. In diesem Verfahren gegen

Facebook hatte der EuGH ausgeführt, dass in den USA die Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der USA Vorrang vor den Safe-Harbour-Regelungen hätten, so dass US-amerikanische Unternehmen ohne jede Einschränkung verpflichtet seien, die Safe-Harbour-Regelungen nicht anzuwenden, wenn sie in Widerstreit zu solchen Erfordernissen stehen. Der EuGH wies deutlich darauf hin, dass amerikanische Behörden auf die aus der EU in die USA übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten können, die über das hinausgeht, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig ist. Eine Regelung, die es Behörden gestattet, generell und ohne irgendeine Differenzierung auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze das Grundrecht auf Achtung des Privatlebens.

Da nach dem Urteil des EuGH eine Datenübermittlung in die USA nicht mehr durch die Anwendung der Safe-Harbour-Regelungen gerechtfertigt werden konnte, haben die EU und die USA im Juli 2016 mit dem **„EU-US-Datenschutzschild" (Privacy Shield) einen neuen Rahmen für den transatlantischen Austausch von personenbezogenen Daten** geschaffen. Sofern US-Unternehmen die hierin geregelten Datenschutzgrundsätze einhalten, dürfen an sie personenbezogene Daten aus der EU übermittelt werden. Die **wesentlichen Anforderungen** des Privacy Shield sind:

- Amerikanische Unternehmen müssen sich für die Aufnahme in die **Datenschutzschild-Liste** registrieren lassen und jährlich mittels einer Selbstzertifizierung bestätigen, dass sie die festgelegten Anforderungen erfüllen. Das US-Handelsministerium überwacht kontinuierlich, ob die Unternehmen sich an die Grundsätze des Privacy Shield halten. Ist dem nicht so, werden betroffene Unternehmen von der Liste gestrichen.
- Die USA haben zugesichert, dass der Datenzugriff von Behörden aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit klaren Beschränkungen, Garantien und Aufsichtsmechanismen unterliegt, und den **anlasslosen Massenzugriff auf Daten von EU-Bürgern ausgeschlossen**. Für Beschwerden, die den möglichen Datenzugriff nationaler Nachrichtendienste betreffen, wird eine unabhängige Ombudsstelle eingerichtet.
- EU-Bürgern stehen mehrere **Beschwerdemöglichkeiten** zu. So können sie sich im Falle einer mutmaßlichen Datenschutzverletzung nicht nur an das entsprechende US-Unternehmen wenden, sondern auch an die eigene **nationale Datenschutzbehörde**, die die Beschwerde an das US-Handelsministerium weiterleitet. Zudem können sie eine **unabhängige Streitbeilegungsstelle** anrufen und als letztes Mittel ein **Schiedsverfahren** einleiten, dessen Entscheidung für das US-Unternehmen verbindlich ist. Schließlich gewährt der **„Judicial Redress Act"** EU-Bürgern hinsichtlich bestimmter Datenschutzrechte Zugang zu US-Gerichten.

Das Privacy Shield wird von der EU-Kommission unter Hinzuziehung von Vertretern der Datenschutzbehörden der EU jährlich daraufhin überprüft, ob es weiterhin ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet. Die zweite Überprüfung fand im Dezember 2018 statt. Aus dem entsprechenden Bericht geht hervor, dass die USA nach wie vor ein angemessenes Schutzniveau für die personenbezogenen Daten gewährleisten, die aus der EU im Rahmen des Privacy Shields an teilnehmende Unternehmen in den USA übermittelt werden. **Zwar wird auch das Privacy Shield teilweise für datenschutzrechtlich bedenklich angesehen, doch solange es nicht vom EuGH für ungültig erklärt worden ist, kann ein Datentransfer an US-Unternehmen, die auf der Datenschutzschild-Liste gelistet sind, hierauf gestützt werden.**

5. Überwachung von Unternehmen durch Geheimdienste und Sicherheitsbehörden – USA Freedom Act

Ungeachtet der datenschutzrechtlichen Zulässigkeit eines internationalen Datentransfers können Daten, die in das Nicht-EU-Ausland übermittelt werden, durch Geheimdienste und Sicherheitsbehörden überwacht werden. Insbesondere die USA steht hier im Fokus: Unter dem sog. **USA Freedom Act**, der im Juni 2015 den sog. Patriot Act abgelöst hat, können US-Sicherheitsbehörden von Unternehmen Zugang zu den bei ihnen gespeicherten Daten verlangen. Mit Hilfe eines „National Security Letters" (NSL) sind beispielsweise bei Telefongesellschaften, Internet Service Providern und Anbietern von Web-basierten Diensten Eingriffe zum Zwecke der nationalen Sicherheit zulässig. Auch mittels einer „FISA Order", einer Anordnung des nicht-öffentlich verhandelnden Foreign Intelligence Surveillance Court (FISA Court) können Sicherheitsbehörden an Beweisstücke zur Terrorismusbekämpfung gelangen. NSL und FISA Order ist gemeinsam, dass sie einer sog. „Gag Order" unterliegen, wonach der Empfänger über die Anordnung und ihren Inhalt umfänglich schweigen muss, so dass die betroffenen Kunden, deren Daten von US-Sicherheitsbehörden angefragt worden sind, hierüber keine Kenntnis erhalten und sich hiergegen auch nicht gerichtlich zur Wehr setzen können. Diese Eingriffsmöglichkeiten stehen US-Behörden gegenüber Personen zu, die tatsächlich oder rechtlich in der Lage sind, Zugang zu den angeforderten Unterlagen zu erhalten. Dies betrifft insbesondere in den USA ansässige Konzernunternehmen, die ihrerseits gegenüber ausländischen Tochterunternehmen mittels Weisungsbefugnis die Herausgabe solcher Unterlagen verlangen können. Faktisch bedeutet dies, dass auch in Europa gespeicherte Kundendaten von Internet-Unternehmen, die zu einem US-Konzern gehören, dem **Zugriff der US-Sicherheitsbehörde**n unterliegen. Die Vergabekammer Bund hat dies in einem Beschluss vom 24. Juni 2014 (Az. VK 2-39/14) wie folgt formuliert:

„Die in Rede stehende Datenweitergabe geht zurück auf den USA Patriot Act. Dieser ist Teil der US-amerikanischen Rechtsordnung. Danach sind US-Unternehmen verpflichtet, den US-Sicherheitsbehörden (FBI, NSA, CIA) Zugriff auf ihre Server zu gestatten, und zwar auch ohne richterliche Anordnung. **Diese Verpflichtung gilt in gleicher Weise für ausländische Tochtergesellschaften von US-amerikanischen Unternehmen** ..., und zwar

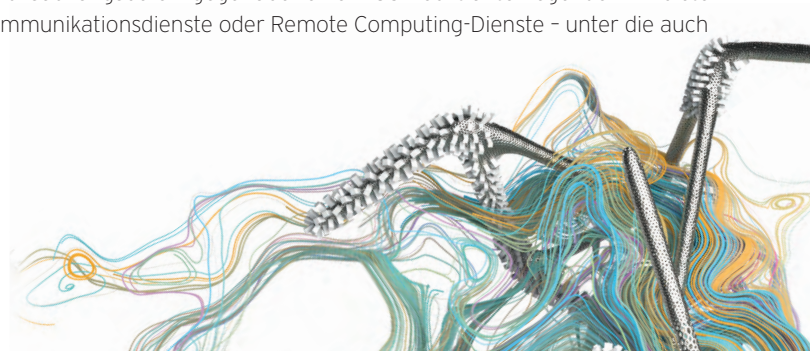
auch dann, wenn die Datenweitergabe gegen die für die ausländische Tochtergesellschaft geltenden örtlichen Gesetze verstößt."

Auch in anderen Ländern gibt es Pflichten zur Datenvorhaltung, die es nationalen Sicherheitsbehörden ermöglichen, hierauf zuzugreifen. So sind ab 1. September 2015 russische und ausländische Unternehmen verpflichtet, **personenbezogene Daten russischer Staatsangehöriger** in Datenbanken zu speichern, die sich auf russischem Staatsgebiet befinden. Mag der Vollzug dieses Gesetzes gegenüber ausländischen Unternehmen problematisch sein, ist es jedenfalls russischen Anbietern von Cloud-Lösungen zumindest hinsichtlich Daten russischer Staatsbürger untersagt, diese ausschließlich innerhalb der Europäischen Union zu speichern, so dass zumindest hierfür keine „EU-Cloud" (wie in Kapitel V „Cloud Computing" näher beschrieben) in Betracht kommt.

6. Offenlegung von Cloud-Daten an US-Ermittlungsbehörden – CLOUD Act der USA

Um die Daten ihrer Nutzer vor dem Zugriff durch US-Ermittlungsbehörden zu schützen, gingen US-Anbieter von Internet-Diensten und Cloud-Lösungen vermehrt dazu über, diese Daten nur auf Servern außerhalb der USA zu speichern. Dies hatte zu einem seit 2013 andauernden Rechtsstreit zwischen Microsoft und den USA geführt: Am 4. Dezember 2013 hatte ein New Yorker Richter **Microsoft** mit einem **Durchsuchungsbefeh**l („warrant to search") verpflichtet, Daten hinsichtlich eines E-Mail-Kontos – u.a. IP-Adressen, Adressbuch und Inhalte aller gespeicherten E-Mails –, die sich auf einem Server in Dublin befinden, an die ersuchende US-Behörde herauszugeben. Der Richter begründete dies damit, Microsoft hätte über diese Daten Kontrolle und es finde US-Recht Anwendung. Das Urteil wurde zunächst am 25. April 2014 bestätigt (United States District Court Southern District Of New York, Az. 13 Mag. 2814). Das Berufungsgericht, der U.S. Court of Appeals for the Second Circuit (Case 14-2985) hat allerdings am 14. Juli 2016 entschieden, dass US-Gerichte nicht die Herausgabe von Daten anordnen können, die ausschließlich auf Servern außerhalb der USA gespeichert sind. Hiergegen legte das U.S. Department of Justice im Juni 2017 Revision beim U.S. Supreme Court ein, um klären zu lassen, ob Anbieter von Cloud-Lösungen im Falle eines Durchsuchungsbefehls in der EU gespeicherte Daten gegenüber US-Behörden offenlegen müssen.

Dieser Entscheidung kam der US-Kongress mit der Verabschiedung des **CLOUD Act (Clarifying Lawful Overseas Use of Data Act)** am 22. März 2018 zuvor. Hierin wird klargestellt, dass ein Durchsuchungsbefehl gegenüber einem US-Recht unterliegendem Anbieter elektronischer Kommunikationsdienste oder Remote Computing-Dienste – unter die auch



Cloud-Dienste fallen – sich auch auf solche Kommunikation, Aufzeichnungen und andere Informationen den Kunden betreffend bezieht, die sich außerhalb der USA befinden. **US-Unternehmen** wie im konkreten Fall Microsoft **müssen daher US-Behörden Zugriff auch auf im Ausland wie etwa in der EU gespeicherte Benutzerdaten gewähren**. Da die US-Behörden kurz nach Inkrafttreten des CLOUD Act einen neuen Durchsuchungsbefehl erlassen haben, hat der U.S. Supreme Court das Revisionsverfahren eingestellt.

Rechtsmittel gegen solche Beschlüsse unter dem CLOUD Act sind nur eingeschränkt möglich. Der Cloud-Anbieter kann binnen 14 Tagen nach Zustellung des Durchsuchungsbefehls hiergegen Beschwerde bei dem zuständigen US-Gericht einlegen und vortragen, dass der betroffene Kunde kein US-Bürger sei und dass die **Offenlegung der Daten ein erhebliches Risiko begründe, dass der Anbieter die Gesetze einer ausländischen Regierung verletzt**. Voraussetzung hierfür ist allerdings, dass zwischen den USA und dieser ausländischen Regierung wie etwa der deutschen ein entsprechendes **Exekutivabkommen** geschlossen wurde. Da dies bislang nicht der Fall ist, wird davon auszugehen sein, dass solche Beschwerden erfolglos bleiben und **US-Anbieter von Internet-Diensten und Cloud-Lösungen aufgrund des CLOUD Acts auch solche Daten ihrer Kunden gegenüber US-Ermittlungsbehörden offenlegen, die nur auf Servern außerhalb der USA – also etwa nur in der EU – gespeichert sind.**

Deutsche Sicherheitsbehörden dürfen ihrerseits Durchsuchungen bei einem Cloud-Anbieter sowie Online-Durchsuchungen nur mit einem Gerichtsbeschluss und nur innerhalb Deutschlands vornehmen.

7. „No-Spy-Erlass" bei IT-Auftragsvergaben der öffentlichen Hand

Diese Risiken des Zugriffs auf Daten und Informationen durch ausländische Sicherheitsbehörden haben erheblichen Einfluss auf die **Vergabe von öffentlichen Aufträgen mit möglicher Sicherheitsrelevanz**. Der sog. **„No-Spy-Erlass"** vom 30. April 2014 (Az. O4 - 11032/23#14) an das Beschaffungsamt des Bundesministeriums des Innern (BMI) betrifft Fälle, bei denen beauftragte ausländische Unternehmen nicht freiwillig, sondern auf Grund ausländischer Rechtsvorschriften Erkenntnisse aus Aufträgen an ausländische Behörden weitergeben oder sonst Informationsabflüsse ermöglichen müssen und zudem eine solche Informationsweitergabe nicht offenlegen dürfen. Danach kann in einem **Vergabeverfahren** ein **Bieter abgelehnt** werden, wenn nachgewiesen wird, dass er einer **rechtlichen Verpflichtung zur Datenweitergabe an ausländische Sicherheitsbehörden** unterliegt.

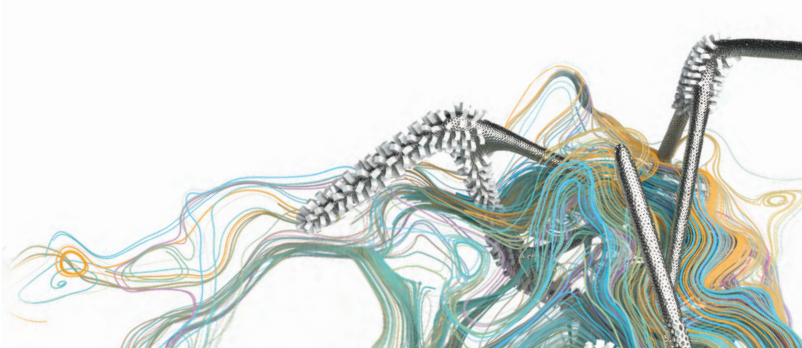
In einer Handreichung zum No-Spy-Erlass vom 19. August 2014 stellt das BMI einheitliche Definitionen und Vorgehensweisen bei Vergabeverfahren mit möglicher Sicherheitsrelevanz auf. Erfasst sind hiernach auch Umstände, die einen Erkenntnisabfluss insbesondere in technischer Hinsicht vorbereiten können, indem sie eine Schwachstellenanalyse ermög-

lichen. Hierzu gehört Wissen über die genaue Ausgestaltung von Hard- und Software zur Regierungskommunikation.

In der Handreichung adressiert das BMI die Thematik, dass wegen der Rechtslage in einzelnen Staaten Unternehmen nicht in der Lage sind, entsprechende in dem „No Spy-Erlass" geforderte Zusagen zu geben. Wie gezeigt sind US-amerikanische Unternehmen ggf. verpflichtet, US-Behörden und US-Nachrichtendiensten auch ohne richterliche Anordnung Zugriff auf ihre Server zu gewähren und über entsprechende Auskunftsersuchen und Informationsweitergaben Stillschweigen zu wahren. Vor diesem Hintergrund wird ein **US-amerikanisches Unternehmen** möglicherweise weder im Angebot oder im Vergabeverfahren noch während der Vertragsdurchführung auf entsprechende Fragen wahrheitsgemäß antworten oder den Auftraggeber hierüber unterrichten dürfen. Betroffene Bieter haben zwar die Möglichkeit, organisatorisch oder z.B. durch ein Handeln nach dem Grundsatz der Datenminimierung schützenswerte Informationen der Reichweite fremdstaatlicher Offenlegungspflichten zu entziehen. Ein solches Vermeidungskonzept ist allerdings im Bereich der **Internet- und IT-Security** meist nicht möglich, denn der Anbieter wird in der Regel eine Schwachstellenanalyse des Auftraggebers durchführen und die genaue Ausgestaltung der zu schützenden Hard- und Software kennen.

In einem Nachprüfungsverfahren über die Vergabe eines öffentlichen Auftrags für Virenschutzsoftware hat das Oberlandesgericht Düsseldorf (Az. VII-Verg 28/14) am 21. Oktober 2015 anerkannt, dass Forderungen der Vergabestelle nach Datensicherheit als besondere Anforderungen an die Auftragsausführung statthaft sind, sofern der öffentliche Auftraggeber für die Forderung der Datensicherheit einen anerkennenswerten und durch den Auftragsgegenstand gerechtfertigten sachlichen Grund hat, wie einen **Schutz sensibler, für den Schutz des Staates relevanter Daten**. Im konkreten Fall musste der Auftragnehmer gewährleisten, dass er **keine Informationen an fremde Nachrichtendienste übermittelt** oder dies wissentlich duldet.

Datenabflüsse an US-amerikanische Behörden und Nachrichtendienste lassen sich hingegen kaum verhindern, wenn Internet- und IT-Security-Lösungen eines Anbieters eingesetzt werden, der den Regelungen des USA Freedom Acts und anderen US-amerikanischen Gesetzen zur Datenweitergabe unterliegt, so dass solche Anbieter unter dem „No-Spy-Erlass" und der Handreichung hierzu bei **IT-Auftragsvergaben der öffentlichen Hand** ggf. von vornhinein **abzulehnen** sind.



8. Online-Durchsuchung und Quellen-TKÜ („Staatstrojaner")

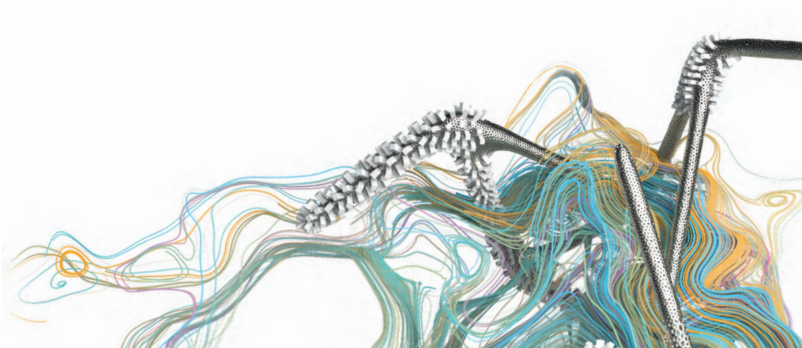
Das Bundeskriminalamt ist unter bestimmten Voraussetzungen gesetzlich zu **Online-Durchsuchungen** berechtigt. Auch einzelne Landespolizeigesetze gestatten Ermittlungsbehörden, mit technischen Mitteln in informationstechnische Systeme einzugreifen und aus ihnen Daten zu erheben. Allerdings bestehen über diese Online-Durchsuchung durch den Einsatz eines **„Staatstrojaners"** unzutreffende Vorstellungen. So behauptet ein Anbieter von Internet-Sicherheitslösungen, durch den Einsatz seiner Software würde ein solcher Staatstrojaner „vermutlich erkannt". Hierbei wird übersehen, dass gesetzlich nicht näher geregelt ist, wie eine Online-Durchsuchung erfolgt, sei es durch den Einsatz eines Trojaners oder durch andere Arten eines Angriffs auf den zu durchsuchenden Computer.

Eine andere Form des „Staatstrojaners" dient der sog. **Quellen-Telekommunikationsüberwachung (TKÜ)**. Dies ist die Überwachung von verschlüsselter Voice-over-IP-Kommunikation, wie sie etwa mit dem Programm Skype erfolgt, und verschlüsselten E-Mail-Verkehrs durch Aufzeichnung der Daten und Übermittlung an die Ermittlungsbehörden vor der Kryptierung durch Installation eines entsprechenden Programms auf dem Rechner des Beschuldigten. Das Bundesverfassungsgericht hat auf eine Verfassungsbeschwerde gegen Neuregelungen im BKA-Gesetz mit Urteil vom 20. April 2016 (Az. 1 BvR 966/09, 1 BvR 1140/09) entschieden, dass die Vorschriften zur Quellen-TKÜ nicht verfassungswidrig sind, so dass die Ermittlungsbehörden diese Maßnahmen auch weiter einsetzen können. Lediglich die Online-Durchsuchung des Computers ist im Rahmen der Quellen-TKÜ unzulässig. Allerdings sind weitere Verfassungsbeschwerden gegen Staatstrojaner anhängig.

Die Ermittlungsbehörden werden also von Fall zu Fall entscheiden, wie sie die Online-Durchsuchung oder die Quellen-TKÜ durchführen, und hierzu **individuelle Einzelanfertigungen als „Ermittlungssoftware**" programmieren oder **kommerziell vertriebene Überwachungssoftware** beschaffen. So hat Presseberichten zufolge das Bundeskriminalamt einen Trojaner selbst entwickelt sowie eine Überwachungssoftware von einem kommerziellen Anbieter erworben, und setzt beide Programme ein.

Die 2017 errichtete **„Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITiS)** unterstützt die Forschung und Entwicklung neuer Methoden und Strategien, um die Fähigkeiten des Bundeskriminalamts, der Bundespolizei und des Bundesamtes für Verfassungsschutz zur Telekommunikationsüberwachung zu sichern. ZITiS selbst führt zwar keine Telekommunikationsüberwachung durch, stellt jedoch Werkzeuge hierzu wie etwa Staatstrojaner bereit und berät die Behörden hinsichtlich deren Einsatzes. Strafverfolgungsbehörden und Geheimdienste sollen in die Lage versetzt werden, verschlüsselte Botschaften im Netz mitzulesen. Daher lassen sich keine seriösen Aussagen darüber treffen, ob und in welchem Umfang **Internet-Sicherheitslösungen Schutz gegen solche Trojanersoftware oder gegen das Mitlesen verschlüsselter Nachrichten** bieten. Allerdings

sind nach deutschem Recht Anbieter von Internet-Sicherheitslösungen nicht zum aktiven Mitwirken beim Zugriff auf gespeicherte Daten oder verschlüsselte Kommunikation verpflichtet, so dass sie nicht etwa eine „Backdoor" für den „Staatstrojaner" bereitstellen müssen. Vielmehr geht das Bundesverfassungsgericht in seinem Urteil zum IT-Grundrecht (vgl. unten Kapitel VI.1) trotzt der staatlichen Befugnis einer Online-Durchsuchung davon aus, dass **technische Selbstschutzmöglichkeiten wie Antiviren-Programme** eingesetzt werden, um einen Zugriff von außen zu verhindern.

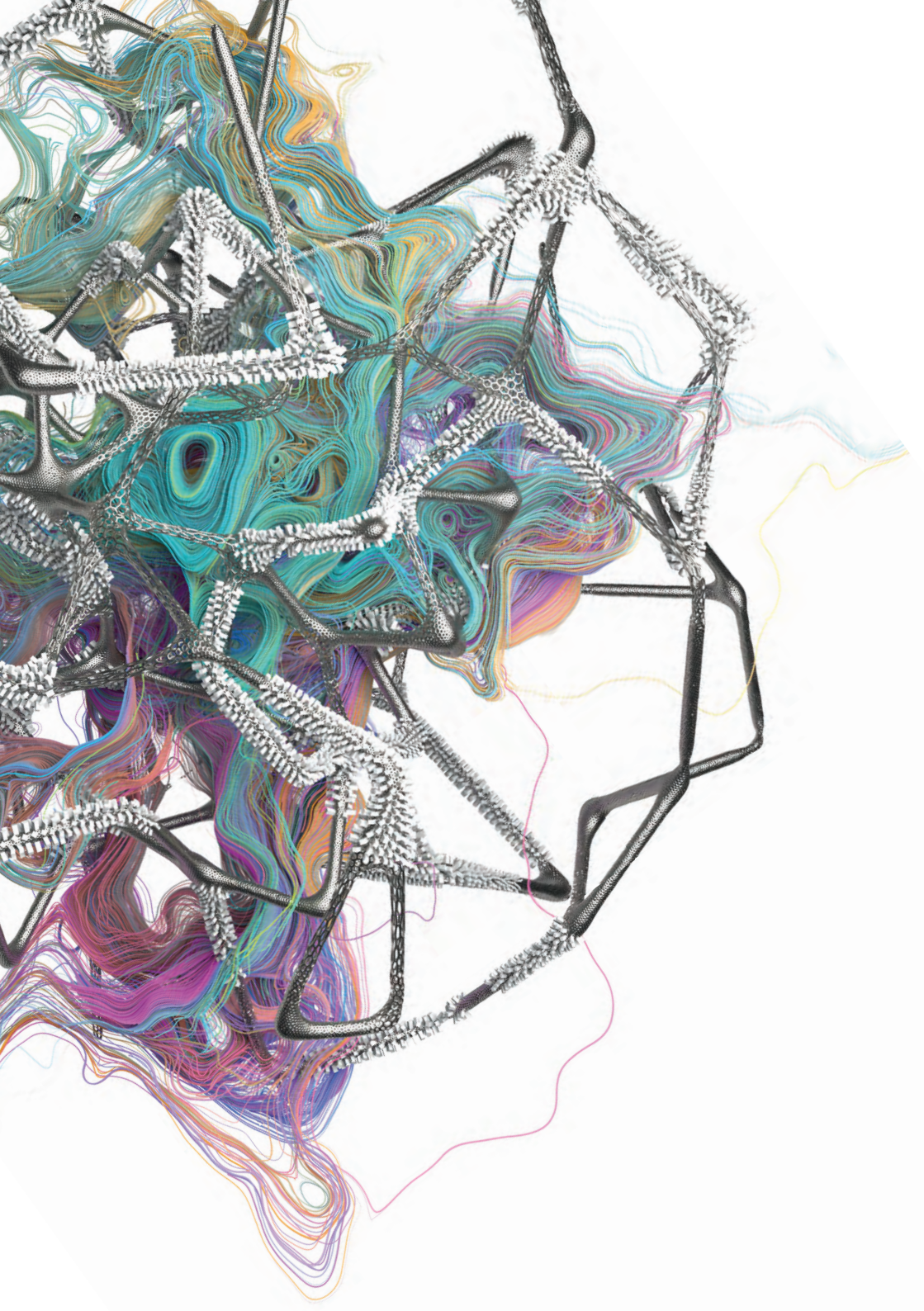


III. Schutz von Geschäftsgeheimnissen

Am 26. April 2019 ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Kraft getreten, das den Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung neu regelt und die bisherige Regelung hierzu in §§ 17 bis 19 des Gesetz gegen den unlauteren Wettbewerb (UWG) ablöst. Besonders von Bedeutung sind die **gestiegenen Anforderungen an das Vorliegen eines Geschäftsgeheimnisses**. Ein Geschäftsgeheimnis liegt nur dann vor, wenn die entsprechenden Informationen

- **nicht allgemein bekannt oder ohne Weiteres zugänglich und daher von wirtschaftlichem Wert sind,**
- **Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen sind und**
- **ein berechtigtes Interesse an der Geheimhaltung daran besteht.**

Hierdurch kommen zusätzliche Compliance-Anforderungen auf Unternehmen zu, die ihr Know-How schützen wollen. Sie müssen insbesondere angemessene Geheimhaltungsmaßnahmen implementieren und dies im Streitfall auch nachweisen können. Diese sind vergleichbar mit den in Kapitel I.6 beschriebenen **Maßnahmen zur IT-Security** und den nach Art. 32 DS-GVO datenschutzrechtlich erforderlichen **technischen und organisatorischen Maßnahmen** und umfassen beispielsweise **Zugangs- und Zugriffsbeschränkungen auf „Need to know"-Basis und Schutz gegen Datenlecks („Data Leak Prevention")**. Zudem sind Mitarbeiter wie auch Geschäftspartner mittels **Non Disclosure Agreements (NDA)** oder einer Geheimhaltungsklausel auf die Vertraulichkeit der Geschäftsgeheimnisse zu verpflichten. Zudem empfiehlt sich, vertraglich Reverse Engineering zu untersagen.



IV. Internet of Things (IoT)

Unter dem Schlagwort **„Internet of Things" (Io**T) („Internet der Dinge") wird die Vernetzung „intelligenter Gegenstände" („Smart Objects") untereinander wie auch mit dem Internet verstanden. Von Alltagsgegenständen bis hin zu Produktionsmaschinen (dann spricht man auch vom **„Industrial Internet of Things" – IIoT**) werden Geräte mit Prozessoren, Sensoren und Netzwerktechnik ausgestattet und mit einer IP-Adresse versehen und so in das Internet eingebunden. Es entsteht die Möglichkeit des Austauschs der Smart Objects mit dem Nutzer über Cloud Services als auch untereinander per **M2M (Machine-to-Machine)**. Anwendungsfelder reichen von der per App steuerbaren Kaffeemaschine über Anwendung im Gesundheitsbereich wie „Wearables" bis hin zur Robotik.

Die mit dem IoT verbundenen Rechtsfragen sind vielfältig und befinden sich in weiten Bereichen noch in der Entwicklung und Diskussion. Aus Sicht der **IT-Compliance und IT-Security** sind folgende Rechtsthemen hervorzuheben:

1. Rechte an Daten

IoT-Anwendungen produzieren große Datenmengen. Als Beispiel sei eine autonome Drohne genannt, die zur Belieferung von abgelegenen Gebieten eingesetzt wird und hierbei z.B. Wetterdaten aufzeichnet. Wem stehen diese Daten zu, dem Hersteller der Drohne, dem Eigentümer, dem Betreiber oder dem Kunden, der für den Einsatz der Drohne zahlt? Ob solche **Date**n nach dem geltenden Recht **schutzfähi**g sind, ist umstritten. Da ein Urheberrecht an maschinengenerierten Daten in der Regel nicht besteht, wird nach derzeitiger Rechtslage u.a. ein Datenbankherstellerrecht, ein eigentumsähnliches Recht an Daten, ein Know-How-Schutz nach dem neuen Gesetz zum Schutz von Geschäftsgeheimnissen oder ein delikts- und strafrechtlicher Schutz von Daten diskutiert. Denkbar ist auch, dass der Gesetzgeber künftig ein **neues „Datenrecht"** einführt, das einerseits regelt, wem das Recht an den Daten zusteht, andererseits interessierten Dritten Zugangsrechte zu diesen Daten gewährt.

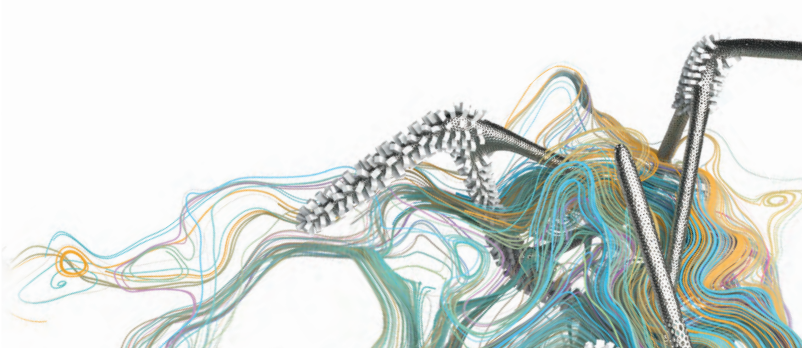
Erwähnenswert ist in diesem Zusammenhang auch ein Vorschlag der EU-Kommission vom 9. Dezember 2015 für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, der sich derzeit im Gesetzgebungsverfahren befindet. Zwar betrifft diese Richtlinie lediglich die Bereitstellung digitaler Inhalte an einen Verbraucher im Rahmen eines B2C-Vertrages und regelt hierbei nur Einzelfragen wie die Vertragsmäßigkeit der digitalen Inhalte oder die Rechtsmängelhaftung, doch wird hierdurch der **wirtschaftliche Wert von Daten** anerkannt, die als Alternative zur monetären Gegenleistung für die Bereitstellung der digitalen Inhalte verwendet werden können.

2. Haftung

Aus dem vorstehenden Beispiel der autonomen Drohne zur Belieferung von abgelegenen Gebieten ist ersichtlich, dass bei IoT-Anwendungen Haftungsfragen von erheblicher Bedeutung sind, etwa wenn die Drohne aufgrund einer autonomen Entscheidung – z.B. wegen schlechter Wetterverhältnisse – einen Einsatz abbricht oder den Kurs ändert und hierbei **Personen zu Schaden kommen**, etwa weil ein dringend benötigtes Medikament nicht ausgeliefert wird oder die Drohne abstürzt. Falls hier kein menschliches Verschulden und kein Produktfehler vorliegen, stellt sich die Frage, wer für den Schaden aufzukommen hat. Diskutiert werden Ansätze einer **verschuldensunabhängigen Gefährdungshaftung** und einer **Versicherungspflicht**, wie sie z.B. für Kraftfahrzeuge bestehen.

3. Datenschutz und IT-Sicherheit

Sofern im Rahmen von IoT-Anwendung personenbezogene Daten erhoben werden, sind die datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung einzuhalten (siehe hierzu Kapitel II.1). Bezüglich **Big Data-Analysen** der erhobenen Daten wird auf Kapitel II.3 verwiesen. Zudem ist die **IT-Sicherheit** der IoT-Anwendungen von erheblicher Bedeutung, denn ein **Hackerangriff auf autonome Systeme** kann erhebliche Konsequenzen nach sich ziehen (in dem vorstehenden Beispiel der autonomen Drohne zur Belieferung von abgelegenen Gebieten könnte der Hacker etwa die Drohne unter seine Kontrolle bringen). Aus diesem Grunde sind auch und gerade für IoT- und IIoT-Anwendungen technische und organisatorische Schutzmaßnahmen nach dem Stand der Technik von wesentlicher Bedeutung. Erforderlich ist der Einsatz von Sicherheitslösung sowohl zum **Schutz gegen Angriffe von außen** z.B. auf die IoT-Anwendung oder deren Datenquellen als auch zum **Schutz der durch die Smart Objects gesammelten und in der Cloud gespeicherten Daten**. Hersteller von IoT-Anwendungen sollten bereits in den Smart Objects – in vorstehendem Beispiel in der Drohne – Schutzvorkehrungen implementieren, die z.B. Anomalien bei der Datenerzeugung erkennen können, die auf einen Angriff hindeuten könnten. Entsprechend dem datenschutzrechtlichen Grundsatz „data protection by design" lässt sich hier von **„IT-security by design"** sprechen.



V. Cloud Computing

Unter **„Cloud Computing"** wird ein Netzwerk verstanden, das IT-Infrastrukturen dynamisch an den Bedarf des Nutzers anpasst und diese über das Internet zur Verfügung stellt. Die IT-Infrastruktur eines Unternehmens wird in die „Wolke" Internet verlagert. Hard- und Software werden hierbei voneinander entkoppelt. Durch den Einsatz von Cloud Computing-Lösungen können Unternehmen Kosten für eigene lokale Infrastruktur einsparen und die Auslastung von Ressourcen besser steuern.
Für die **rechtliche Beurteilung** wird grundsätzlich zwischen der **Private Cloud**, die unter der Kontrolle des Unternehmens steht und bei der die Daten die unternehmensspezifische Wolke nicht verlassen, und der **Public Cloud**, bei der Daten und Dienste auf die IT-Infrastruktur externer Dienstleister ausgelagert werden, unterschieden. Während bei einer Private Cloud das Unternehmen weiterhin die Kontrolle behält und diesbezüglich die Anforderungen an die IT-Security und IT-Compliance einhalten muss, sind Public Clouds hinsichtlich der vertraglichen Konditionen, dem Datenschutz und der Sicherheit kritisch zu prüfen, bevor ein Unternehmen diese Technologie einsetzt. In der Praxis gibt es zudem unterschiedliche Mischformen, wie etwa eine Hybrid Cloud. Dies ist eine Kombination einer Cloud mit anderen IT-Infrastrukturkomponenten wie virtualisierten Systemen oder klassischen Rechenzentren. Dabei verbleiben bestehende Datenbestände und Anwendungen im Rechenzentrum, neue Daten oder Dienste werden hingegen in die Cloud migriert.

1. Vertragliche Konditionen

Dem Unternehmen muss klar sein, von welchem Cloud Provider zu welchen vertraglichen Konditionen die Cloud-Services erbracht werden. Neben der Person und dem Sitz des Cloud Providers sind etwa das anwendbare Recht, Regelungen zur **Gewährleistung** und **Haftung, Service Levels** und die Einschaltung von Unterauftragnehmern kritisch zu prüfen. Wichtig ist auch, dass bei Vertragsbeendigung eine **Rückmigration des Datenbestandes** möglich ist.

2. Datenschutz und IT-Sicherheit

Wenn sowohl das Unternehmen als auch der Cloud Provider innerhalb der Europäischen Union niedergelassen sind und personenbezogene Daten die EU nicht verlassen (sog. **„EU-Cloud"**), besteht ein **einheitliches angemessenes europäisches Datenschutzniveau**. Die Übermittlung personenbezogener Daten an einen Cloud Provider wird dann datenschutzrechtlich als zulässig einzustufen sein, wenn es sich um einen zuverlässigen Cloud Provider handelt, der sich an die Datenschutz-Grundverordnung (DS-GVO) hält und ausreichende **technische und organisatorische Maßnahmen zum Schutz der Daten** getroffen hat. Die Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises haben am 9. Oktober 2014 eine **„Orientierungshilfe Cloud Computing"**

über die datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing herausgegeben (abrufbar unter http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.pdf?__blob=publicationFile&v=7). Diese Orientierungshilfe wurde zwar noch nicht an die DS-GVO angepasst, Unternehmen sollten sich dennoch daran halten.

Sofern der Cloud Provider **außerhalb der EU** ansässig ist, sind Datenschutz und Datensicherheit hingegen wesentlich **problematischer** zu sehen:

- Die **Datenübermittlung** in Länder **außerhalb der EU** muss datenschutzrechtlich zulässig sein. Dies kann etwa durch den Einsatz sog. EU-Standardvertragsklauseln sichergestellt werden. Von besonderer Bedeutung ist hierbei, dass der Cloud Provider die Unternehmensdaten nicht beliebig in das Internet auslagern darf, sondern nur an explizit genannte Unterauftragsverarbeiter, die ihrerseits ebenfalls die Pflichten nach den EU-Standardvertragsklauseln akzeptieren müssen.
- Im Falle eines Cloud Providers mit Sitz in den **USA** ist zu prüfen, ob dieser nach dem **„EU-US-Datenschutzschild" (Privacy Shield)** zertifiziert und auf der Datenschutzschild-Liste registriert ist; ist dies der Fall, dürfen an ihn personenbezogene Daten aus der EU übermittelt werden (siehe hierzu oben Kapitel II.4).
- Es besteht die Gefahr der **Überwachung durch Geheimdienste und Sicherheitsbehörde**n, die beim Cloud Provider auf Kundendaten zugreifen. Insbesondere bei US-amerikanischen Cloud Providern besteht solch ein Risiko, da – wie im Kapitel II.5 und II.6 dargestellt – US-Unternehmen ggf. verpflichtet sind, **US-Sicherheitsbehörden** (FBI, NSA, CIA) Zugriff auf ihre Server zu gestatten, und zwar auch ohne richterliche Anordnung. Dies gilt gleichermaßen für die Speicherung von Kundendaten durch ein ausländisches Tochterunternehmen außerhalb der USA, da die Kontrolle über die Daten bei der US-amerikanischen Muttergesellschaft liegt. Auch bei **russischen Cloud Providern** muss damit gerechnet werden, dass die russischen Sicherheitsbehörden auf Kundendaten zugreifen können, da der Cloud Provider zumindest in Bezug auf personenbezogene Daten russischer Staatsangehöriger verpflichtet ist, diese in Datenbanken zu speichern, die sich auf russischem Staatsgebiet befinden.

Das BSI hat in seinem **Anforderungskatalog Cloud Computing (Cloud Computing Compliance Controls Catalogue – kurz: C5)** Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten aufgestellt. Der Anforderungskatalog legt eine Basislinie für Cloud Security aus Sicht des BSI fest und erlaubt die Prüfung und den Nachweis durch einen unabhängigen, vertrauenswürdigen Dritten wie etwa einem Wirtschaftsprüfer von aufbau- und ablauforganisatorischen Sicherungs- und Überwachungsmaßnahmen des Cloud-Anbieters. Cloud-Kunden sollten prüfen, ob ihr Cloud-Anbieter über ein entsprechendes **C5-Testat** verfügt.

VI. IT-Grundrecht und Schutz der Persönlichkeit

Der Schutz der Persönlichkeit und des Privatlebens ist geprägt durch mehrere verfassungsgerichtliche Entscheidungen der letzten Jahre, die Schranken gegenüber einem umfassenden Einblick in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers setzen. Diese Entscheidungen haben zumindest mittelbare Auswirkung auf Unternehmen und den Schutz der Daten ihrer Mitarbeiter.

1. Urteil des Bundesverfassungsgerichts zum „IT-Grundrecht"

Mit seinem Urteil vom 27. Februar 2008 (Az. 1 BvR 370/07) hat das Bundesverfassungsgericht ein neues **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität** informationstechnischer Systeme geschaffen, das in der Öffentlichkeit als **„IT-Grundrecht"** bezeichnet wird. Es ist dann anzuwenden, wenn ein Zugriff auf IT-Systeme es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Zwar werden von diesem Grundrecht nicht Server, Großrechenanlagen und die Steuerung technischer Geräte erfasst, denn hierüber verfügt der Arbeitnehmer nicht selbstbestimmt, aber beispielsweise ein dem Arbeitnehmer überlassenes Notebook, elektronischer Terminkalender und Mobiltelefon.

Um den Grundrechtsschutz seiner Mitarbeiter und anderer Nutzer der IT-Infrastruktur auf Integrität der IT-Systeme zu gewährleisten, wird von einem Unternehmen verlangt werden müssen, **ausreichende Überwachungsmaßnahmen** einzurichten. Die Anforderungen an Unternehmen zur **Gewährleistung der IT-Sicherheit und IT-Compliance** sind durch das Urteil des Bundesverfassungsgerichts gestiegen. Hiernach sind nicht nur Vorkehrungen gegen wirtschaftliche Schäden und Risiken wie Datenverluste zu treffen, sondern auch zur **Gewährleistung der Vertraulichkeit und Integrität der IT-Systeme**.

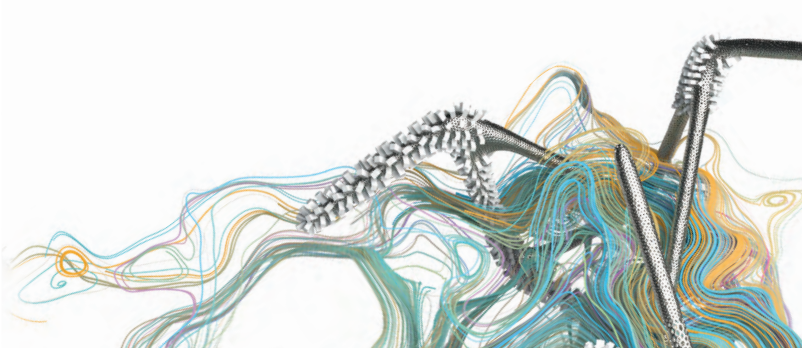
Das IT-Sicherheitsgesetz 2.0 (siehe hierzu Kapitel I.3) sieht die Einführung einer neuen Strafvorschrift mit der Bezeichnung „Unbefugte Nutzung informationstechnischer Systeme" vor, nach der u.a. bestraft werden soll, wer sich oder einem Dritten unbefugt Zugang zu einem IT-System verschafft, mit dem personenbezogene Daten verarbeitet werden oder das Teil einer kritischen Infrastruktur ist. Ziel der Gesetzesänderung ist es, den **strafrechtlichen Schutz des IT-Grundrechts** effektiver auszugestalten und bei dessen Verletzung auch eine Rechtsgrundlage für Schadensersatzansprüche des Verletzten zu schaffen. Hierunter nicht bestraft werden allerdings Fälle, bei denen Sicherheitslücken im IT-System eines Unternehmens durch Hacker oder Anbieter von IT-Sicherheitslösungen aufgespürt werden, sofern diese durch das Unternehmen hierzu beauftragt worden sind.

2. Urteil des Bundesverfassungsgerichts zum Grundrechtsschutz dynamischer IP-Adressen

Nach einem Beschluss des Bundesverfassungsgerichts fallen dynamische IP-Adressen unter das Telekommunikationsgeheimnis und genießen somit Grundrechtsschutz. **Damit ist äußerste Zurückhaltung angebracht, über dynamische IP-Adressen einzelne Nutzer zu identifizieren**.

Am 24. Januar 2012 hat das Bundesverfassungsgericht (Az. 1 BvR 1299/05) gewisse Regelungen des Telekommunikationsgesetzes (TKG) zur Speicherung und Verwendung von Telekommunikationsdaten für teilweise verfassungswidrig erklärt. Hiernach berechtigt das damals in § 113 Abs. 1 Satz 1 TKG geregelte manuelle Auskunftsverfahren, wonach Telekommunikationsunternehmen aber auch bspw. Krankenhäuser zur Auskunft über Kundendaten verpflichtet sind, nicht zur Erteilung von Auskünften über den Inhaber einer dynamischen IP-Adresse. Das Bundesverfassungsgericht hat mit diesem Urteil klargestellt, dass die Identifizierung des Nutzers einer dynamischen IP-Adresse einen Eingriff in das nach Art. 10 Abs. 1 GG grundgesetzlich geschützte **Fernmeldegeheimnis** darstellt. Denn für die Identifizierung einer dynamischen IP-Adresse müssen die Telekommunikationsunternehmen die entsprechenden Verbindungsdaten ihrer Kunden sichten und somit auf konkrete Telekommunikationsvorgänge zugreifen, die vom Schutzbereich des Art. 10 GG umfasst sind. Aufgrund dieses Bundesverfassungsgerichtsurteils wurde die Bestandsdatenauskunft mit Wirkung zum 1. Juli 2013 neu geregelt, die unter gewissen Voraussetzungen die Auskunft über den Nutzer einer dynamischen IP-Adresse – also die Mitteilung des Namens – gestattet.

Die Identifizierung von **statischen IP-Adressen** hat das Bundesverfassungsgericht hingegen gebilligt, da diese zum gegenwärtigen Zeitpunkt in aller Regel nur Institutionen und Großnutzern, nicht aber privaten Nutzern als Einzelkunden zugewiesen werden, und die Abfragemöglichkeit somit nur geringeres Gewicht hat. Diese Rechtsansicht kann sich allerdings mit Einführung des IPv6-Protokolls, mit dem eine feste Adresse pro Gerät bereitgestellt werden kann, ändern, so dass künftig jede IP-Adresse unter das Telekommunikationsgeheimnis fällt.



3. Urteile des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zur Vorratsdatenspeicherung

Sowohl das Telekommunikationsgesetz als auch eine europäische Richtlinie sahen die sog. Vorratsdatenspeicherung vor. Hiernach waren Telekommunikationsunternehmen verpflichtet, bestimmte Verkehrsdaten ihrer Kunden wie z.B. die Rufnummer des Anrufers und des Angerufenen, E-Mail-Adressen und die IP-Adresse beim Zugang zum Internet für mindestens sechs Monate zu speichern.

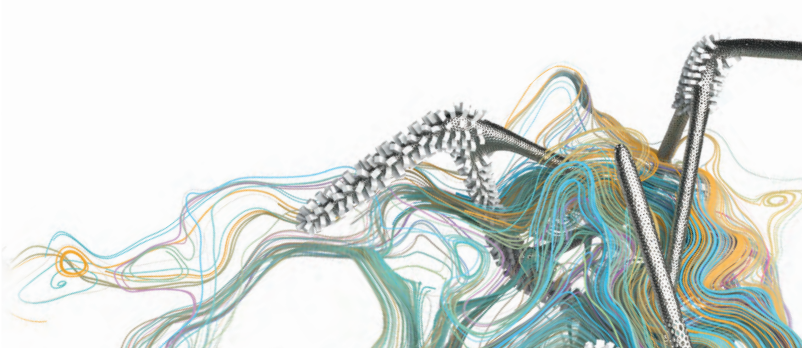
Mit Urteil vom 2. März 2010 (Az. 1 BvR 256/08) hat das **Bundesverfassungsgericht** die die Vorratsdatenspeicherung regelnden §§ 110a und 110b TKG als einen **Verstoß gegen das Grundrecht auf Schutz des Fernmeldegeheimnisses** angesehen und für nichtig erklärt. Die Vorratsdatenspeicherung stellt hiernach einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt", dar: „Erfasst werden über den gesamten Zeitraum von sechs Monaten praktisch sämtliche Telekommunikationsverkehrsdaten aller Bürger ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation. Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist." Aus diesen Daten lassen sich „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen". Eine Vorratsdatenspeicherung kann „die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen".

Der **Europäische Gerichtshof** hat sodann mit Urteil vom 8. April 2014 (Rs. C-293/12 und Rs. C-594/12) entschieden, dass auch die EU-Richtlinie zur Vorratsdatenspeicherung ungültig ist. Aus der Gesamtheit der auf Vorrat gespeicherten Daten können Schlüsse auf das Privatleben der betreffenden Personen wie ihre Gewohnheiten des täglichen Lebens, Aufenthaltsorte und Sozialbeziehungen gezogen werden. Dieser Eingriff in die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten ist „von großem Ausmaß und von besonderer Schwere" und somit unverhältnismäßig.

Allerdings wurde mit dem **„Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten"** vom 10. Dezember 2015 eine neue Vorratsdatenspeicherung eingeführt. Nach §§ 113a bis 113g Telekommunikationsgesetz müssen Telekommunikationsunternehmen u.a. die Rufnummer des Anrufers und des Angerufenen sowie Datum und Dauer des Telefonats speichern. Beim Internetzugang sind die IP-Adresse sowie Beginn und Ende der Internetnutzung zu speichern. Inhalte der Kommunikation und von E-Mails sowie Daten über aufgerufene Internetseiten dürfen unter dem neuen Gesetz allerdings nicht gespeichert werden. Die Speicherfrist beträgt zehn Wochen, für Standortdaten vier Wochen. Zwar wären diese neuen Regelungen zur Verkehrsdatenspeicherung

bis zum 1. Juli 2017 umzusetzen gewesen, allerdings hat kurz zuvor das Oberverwaltungsgericht Nordrhein-Westfalen festgestellt, dass ein hiergegen klagender Internetzugangsdiensteanbieter bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens nicht zur Speicherung der Telekommunikationsverkehrsdaten verpflichtet ist (Beschluss vom 22. Juni 2017, Az. 13 B 238/17). **Aufgrund dieser Entscheidung sieht die Bundesnetzagentur derzeit von Anordnungen und Maßnahmen zur Durchsetzung der Verkehrsdatenspeicherung gegenüber allen Anbietern von Telekommunikationsdiensten ab.**

Faktisch bedeutet dies, dass es derzeit **keine gesetzliche Speicherverpflichtung oder Speichererlaubnis von Verkehrsdaten für Zwecke der Strafverfolgung** in Deutschland gibt. Für eine Auskunftserteilung hinsichtlich Verbindungsdaten auf Ersuchen von Sicherheitsbehörden mit Aufgaben im Bereich der Strafverfolgung, Gefahrenabwehr oder der Nachrichtendienste dürfen Unternehmen daher ausschließlich Daten verwenden, die aus betrieblichen Gründen rechtmäßig gespeichert sind. Nach Urteilen des Bundesgerichtshofs vom 13. Januar 2011 (Az. III ZR 146/10) und 3. Juli 2014 (Az. III ZR 391/13) ist zu Zwecken der Erkennung, Eingrenzung und Beseitigung von Störungen ohne konkreten Anlass eine **Speicherung von IP-Adressen höchstens sieben Tage** zulässig. Das Oberlandesgericht Köln (Urteil vom 14. Dezember 2015, Az. 12 U 16/13) hat zudem klargestellt, dass es für die Speicherung der IP-Adressen keiner bereits aufgetretenen Störung bedarf, sondern dass es genügt, dass die Speicherung erforderlich ist, um einer später auftretenden Störung begegnen zu können. Diese Höchstspeicherfrist gilt gleichermaßen für alle Verkehrsdaten wie insbesondere Telefonnummern. Für Unternehmen bedeutet dies, dass sie die IP-Adressen und Verbindungsdaten ihrer Mitarbeiter **spätestens nach sieben Tagen löschen** müssen, es sei denn, die Speicherung ist im Einzelfall – z.B. zur Entgeltabrechnung – länger zulässig.



VII. E-Mail und Internet im Unternehmen

E-Mail-Kommunikation und die Nutzung des Internets durch Mitarbeiter im Unternehmen sind spätestens seit dem Siegeszug von Smartphones und Tablet-Computern nicht mehr wegzudenken. Unternehmen haben hierbei einige **rechtliche Anforderungen** zu berücksichtigen.

1. E-Mails im Unternehmensverkehr

a) Unternehmensangaben auf geschäftlichen E-Mails

Alle Unternehmen, die nach Handelsrecht oder gesellschaftsrechtlichen Vorschriften Pflichtangaben in ihre Geschäftsbriefe aufnehmen müssen, insbesondere Einzelkaufleute, OHG, KG, Partnerschaftsgesellschaft, AG und GmbH sind auch verpflichtet, diese Angaben in ihre **E-Mail-Signatur** zu übernehmen. Solche Pflichtangaben umfassen insbesondere Firma, Rechtsform und Sitz der Gesellschaft, Handelsregisterangaben und die Namen aller Geschäftsführer. Auch geschäftliche E-Mails, die etwa von Smartphones versendet werden, müssen mit einer solchen Signatur versehen sein.

b) Verpflichtung zur Verschlüsselung von E-Mails

Es bestehen zahlreiche Fallgestaltungen, bei denen entweder eine **gesetzliche Verpflichtun**g besteht, **E-Mail-Verschlüsselungstechnologien** einzusetzen, wie etwa bei der öffentlichen Auftragsvergabe oder bei der elektronischen Übermittlung von Sozialdaten, oder bei denen eine E-Mail-Verschlüsselung zur Wahrung der Vertraulichkeit rechtlich geboten ist oder empfohlen wird. Dies gilt insbesondere für den Schutz von Geschäftsgeheimnissen, personenbezogenen Daten, Sozialdaten sowie des Bankgeheimnisses und des Fernmeldegeheimnisses. Auch im E-Mail-Verkehr mit Behörden müssen bestimmte E-Mails verschlüsselt werden, wie etwa im Falle der Übermittlung von Gehaltsdaten per E-Mail an das Finanzamt und die Sozialbehörden. Unternehmen generell, insbesondere jedoch Kreditinstitute und Finanzdienstleistungsinstitute, aber auch Diensteanbieter von geschäftsmäßig angebotenen Telemedien haben zudem **angemessene technische IT-Sicherheitsmaßnahmen** zu etablieren, zu denen auch **sichere Verschlüsselungsverfahren** zählen. Der **Einsatz von E-Mail-Verschlüsselun**g ist somit für Unternehmen, Kaufleute, Behörden und Selbstständige in vielen Bereichen rechtlich zwingend geboten. Verschlüsselungstechnologien sind schließlich auch ein Kernelement des **De-Mail-Gesetzes**, durch das ein sicherer, vertraulicher und nachweisbarer Geschäftsverkehr für jedermann im Internet gewährleistet werden soll.

c) Elektronische Signatur

Beim Austausch von E-Mails im Internet besteht die Gefahr, dass diese entweder nicht von der Person stammen, die sich als Absender ausgibt, oder diese E-Mails von unbefugten Dritten verändert worden sind. Besonders gefährlich ist hierbei der als **„Chef-Masche“**

oder **„CEO Fraud“** bezeichnete E-Mail-Betrug, bei dem kriminelle Täter versuchen, durch gefälschte E-Mails, deren Absender angeblich ein Vorstand oder Geschäftsführer ist, dazu berechtigte Mitarbeiter in Unternehmen zur Überweisungen von hohen Geldbeträgen zu veranlassen. Um die **Authentizität** und **Integrität** im elektronischen Rechtsverkehr sicherzustellen, also um den Absender der E-Mail eindeutig identifizieren zu können und einer Verfälschung des Inhalts vorzubeugen, wurde das **elektronische Signaturverfahren** eingeführt. Eine elektronische Signatur ist ein mit einem geheimen Schlüssel erzeugtes elektronisches Dokument. Dieses hat eine kryptographische Prüfsumme, die mit dem öffentlichen Schlüssel des Urhebers überprüft werden kann. Die elektronische Signatur ist in der EU-Verordnung Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen – sog. **eIDAS-Verordnung** – das **eIDAS-Durchführungsgesetz** und das **Vertrauensdienstegesetz (VDG)** vom 18. Juli 2017 näher geregelt. Es gibt sie in drei unterschiedlichen Stufen, der „elektronischen Signatur“, der „fortgeschrittenen elektronischen Signatur“ und der „qualifizierten elektronischen Signatur“.

Nur die Verwendung der **qualifizierten elektronischen Signatur** gemeinsam mit dem Namen des Ausstellers erfüllt die sog. **„elektronische Form“**, die gemäß § 126a BGB der Schriftform gleichsteht. Allerdings ist zu berücksichtigen, dass einige Vorschriften weiterhin ausdrücklich die Schriftform erfordern und die elektronische Form explizit ausschließen. Ein Beispiel ist die Bürgschaftserklärung, die in Schriftform erfolgen muss. Hingegen ist die Bürgschaftserklärung des Kaufmanns gemäß § 350 HGB formfrei, solange sie ein Handelsgeschäft betrifft.

Werden in einem **Gerichtsverfahren** private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, vorgelegt, haben sie die gleiche Beweiskraft wie private Urkunden. Dies gilt gleichermaßen für eine von einem **„De-Mail-Konto“** versandte elektronische Nachricht. Der Anschein der Echtheit der Erklärung kann nur bei ernstlichen Zweifeln an der Urheberschaft der Nachricht erschüttert werden.

d) Archivierungspflichten

Nach dem Handelsgesetzbuch besteht für Unternehmen eine Aufbewahrungspflicht für empfangene und abgesandte Handelsbriefe. Unter einem Handelsbrief ist jedes Schreiben zu verstehen, welches der Vorbereitung, dem Abschluss, der Durchführung oder auch der Rückgängigmachung eines Geschäfts dient. Hierunter fallen auch entsprechende **E-Mails**. Die **Aufbewahrungsfristen** sind in der Regel **sechs Jahre**, bei bestimmten Unterlagen auch **zehn Jahre**. Es muss sichergestellt werden, dass auch über **private Endgeräte**

versendete „Handelsbriefe", also etwa E-Mails mit einem entsprechenden Inhalt, aufbewahrt werden. Während Firmen-E-Mails noch unproblematisch synchronisiert werden können, erscheint eine Aufbewahrung von SMS oder einer Korrespondenz über Messanger-Dienste oder in sozialen Netzwerken, die durchaus ebenfalls etwa der Vorbereitung eines Geschäfts dienen können, schon problematischer. Hier empfiehlt sich der Einsatz angemessener **Sicherheits- und Verwaltungstools** sowie die Aufnahme von Vorgaben in die **IT-Anwenderrichtlinie**.

2. E-Mail- und Internet-Nutzung durch Unternehmensmitarbeiter und Externe

Hinsichtlich der Nutzung von E-Mail und Internetzugang durch Mitarbeiter eines Unternehmens besteht in vielen Unternehmen erhebliche **Rechtsunsicherheit** oder gar **Rechtsunkenntnis**. Insbesondere die Nutzung dieser betrieblichen Arbeitsmittel für **private Zwecke der Mitarbeiter** ist nämlich rechtlich problematisch.

a) Betriebliche Nutzung

Im Falle der betrieblichen Nutzung des ihnen jeweils zugeteilten E-Mail-Accounts und des Internetzugangs durch die Mitarbeiter eines Unternehmens ist der Arbeitgeber grundsätzlich zur Einsichtnahme in die E-Mails und zur Kontrolle der E-Mail und Internetnutzung befugt. Das gilt auch, wenn ein Arbeitnehmer Internet oder E-Mail-Account **unerlaubt privat nutzt**, allerdings darf auch hier **klar erkennbare private Korrespondenz** nicht eingesehen werden. Zudem ist auch bei einer betrieblichen Nutzung keine **Vollkontrolle** des Arbeitnehmers gestattet, sondern nur **Stichproben**, etwa zur Aufdeckung einer Straftat oder zur Überprüfung der Einhaltung von **Compliance-Verpflichtungen**.

b) Private Nutzung

Wird die private Nutzung erlaubt, ist nach wohl herrschender Meinung der **Arbeitgeber** als **Diensteanbieter** im Sinne des Telekommunikationsgesetzes (TKG) bzw. des Telemediengesetzes (TMG) anzusehen. Werden erlaubte private und betriebliche Nutzung nicht technisch getrennt, ist die gesamte Nutzung als privat zu qualifizieren. Der Arbeitgeber ist nach § 88 TKG zur **Wahrung des Fernmeldegeheimnisses** verpflichtet und unterliegt den **datenschutzrechtlichen Anforderungen** der §§ 91 ff. TKG. Danach ist ohne Einwilligung des Arbeitnehmers eine Verarbeitung von Verkehrsdaten letztlich nur zu Abrechnungszwecken und zur Störungserkennung und -beseitigung zulässig. Ein Zugriff auf Inhaltsdaten zur Kontrolle des vereinbarten Nutzungsrahmens ist ohne Einwilligung unzulässig.

Dennoch sollte zum Schutz des Arbeitgebers eine Kontrolle von E-Mail-Nutzung und Internetzugang auch bei privater Nutzung erfolgen. Eine dahingehende Regelung kann der Arbeitgeber aber weder einseitig auf Grund seines Direktionsrechts noch mit der Arbeitnehmervertretung – etwa in Form einer Betriebsvereinbarung – treffen. (Letzteres kommt allenfalls für Aspekte einer damit zugleich möglichen Leistungskontrolle in Betracht.) Denn das Brief-, Post- und Fernmeldegeheimnis hat den Rang eines Individual-

grundrechtes (Art. 10 des Grundgesetzes) und entzieht sich somit Einschränkungen durch eine Kollektivvereinbarung oder betriebliche Anweisungen.

Es bleibt also nur die Möglichkeit einer (unter dem Gesichtspunkt der Gleichbehandlung) einheitlich gestalteten **Vereinbarung mit jedem einzelnen Mitarbeiter**. Diese Vereinbarung sollte mindestens das Folgende regeln:

- **Zielsetzung**
- **Umfang der E-Mail- und Internetnutzung**
- **Einwilligung in Protokollierung und Kontrolle**
- **Vertretungsregelung bei Ausscheiden oder längerer Krankheit des Mitarbeiters**
- **Leistungs- und Verhaltenskontrolle**
- **Datenschutz für E-Mail- und Internetnutzung**
- **Sanktionen**
- **Verhaltensgrundsätze (v.a. Beachtung der gesetzlichen Vorschriften)**

Wo allerdings die (gelegentliche) private Nutzung ohne eine solche vorherige Vereinbarung nur stillschweigend oder ausdrücklich (etwa durch einen Hinweis in Organisationsrichtlinien des Arbeitgebers) geduldet wird, kann daraus eine sog. **„betriebliche Übung"** erwachsen. Sie kann nur schwer – nämlich durch Änderungskündigungen – auf die Grundlage von Individualvereinbarungen umgestellt werden, in denen die bei erlaubter privater Nutzung unbedingt benötigten Regelungen getroffen werden.

Auch ein nachträgliches völliges Verbot der privaten Nutzung von betrieblichen E-Mail-Accounts ließe sich daher bei einer einmal entstandenen betrieblichen Übung kaum durchsetzen. Wenn jedoch ein solches Verbot wirksam geworden ist – aber auch wenn das Verbot schon bei erstmaliger Einführung von E-Mail im Unternehmen ausgesprochen worden ist –, muss seine Einhaltung durch **Kontrollmaßnahmen** bis hin zur Abmahnung und zu weiteren Konsequenzen durchgesetzt werden, um dem Entstehen einer (neuen) betrieblichen Übung vorzubeugen.

Als Alternative für seine Mitarbeiter kann der Arbeitgeber ihnen den **Internetzugang für die Nutzung ihrer privaten E-Mail-Accounts** gestatten, sofern er es nicht auf sich nehmen will, ihnen ein zweites E-Mail-Account für die private Nutzung auf dem betrieblichen Server zu eröffnen. Das kann jedoch Probleme im Rahmen von Archivierungspflichten mit sich bringen. Möglich wäre auch die Bereitstellung eines **öffentlichen WLAN-Anschlusses**, über den die Mitarbeiter mit ihren eigenen Geräten wie Smartphones während der

Arbeitspausen E-Mails empfangen und versenden können (in diesem Zusammenhang wird auf die rechtlichen Voraussetzungen für öffentliche WLAN-Hotspots verwiesen, die im nachfolgenden Abschnitt dargestellt werden).

Die **erlaubte private Nutzung von betrieblichen E-Mail-Accounts** hingegen kann den Arbeitgeber bzw. die für sein Handeln Verantwortlichen in die Nähe einer **Strafbarkei**t nach § 206 StGB bringen, wenn sie das danach geschützte **Fernmeldegeheimnis** ihrer Mitarbeiter verletzen sollten. Ob der Schutzbereich des Fernmeldegeheimnisses überhaupt betroffen ist, hängt davon ab, ob der **Übermittlungsvorgang** bereits beendet ist. Wenn sich eine E-Mail im alleinigen Herrschaftsbereich des Empfängers befindet, also z.B. auf dessen lokaler Festplatte, ist sie nicht mehr vom Fernmeldegeheimnis geschützt.

Im Ergebnis ist der **Zugriff des Arbeitsgebers auf E-Mail-Accounts von Mitarbeiter**n, denen die **private E-Mail-Nutzung gestattet** wurde oder diese zumindest gebilligt wird, ohne eine entsprechende Einwilligung des Mitarbeiters **unzulässig**. Bis zum Abschluss des Übermittlungsvorgangs kann sich der Arbeitgeber hierdurch der Verletzung des Fernmeldegeheimnisses strafbar machen.

c) Öffentliche WLAN-Hotspots

Aufgrund internetfähiger Endgeräte wie Smartphones und Tablets möchten Nutzer ständig online sein. Unternehmen reagieren hierauf mit Hotspots, die einen kostenlosen Internetzugang ermöglichen. In Cafés, Hotels und Universitäten werden offene WLAN immer öfter angeboten, und auch Unternehmen stellen Mitarbeitern, Kunden und Gästen solche Internetzugänge zur Verfügung. Umstritten ist jedoch, in welchem Umfang **Betreiber öffentlicher WLAN-Hotspots** für **Rechtsverletzungen der Nutzer haften**.

In zahlreichen Urteilen der letzten Jahre haben Gerichte entschieden, dass der Inhaber eines Internetanschlusses für eine damit begangene Rechtsverletzung als Störer einstehen muss, auch wenn er die Handlungen gar nicht selbst vorgenommen hat. Die **Haftung des Inhabers eines WLAN-Anschlusses** ist höchstrichterlich bejaht worden: Der Bundesgerichtshof hat in seinem Urteil vom 12. Mai 2010 – Az. I ZR 121/08 („Sommer unseres Lebens") – entschieden, dass der Inhaber eines WLAN-Anschlusses, der es unterlässt, die im Kaufzeitpunkt des WLAN-Routers marktüblichen Sicherungen ihrem Zweck entsprechend anzuwenden, als **Störer auf Unterlassung** haftet, wenn Dritte seinen Anschluss missbräuchlich nutzen. Allerdings hat diese sog. Störerhaftung dazu geführt, dass in Deutschland öffentliches WLAN weniger verbreitet ist, als in vielen anderen Ländern.

Die Frage, ob diese **Störerhaftung** auch für Unternehmen gilt, die ein zu ihrem Gewerbe gehöriges WLAN betreiben, war auf ein entsprechendes Vorabentscheidungsersuchen des Landgerichts München I (Az. 7 O 14719/12) hin Gegenstand eines Urteils des Europäischen Gerichtshofs vom 15. September 2016 (Rs. C-484/14). Der EuGH hat hierbei entschieden,

dass ein Geschäftsinhaber, der der Öffentlichkeit kostenloses WLAN zur Verfügung stellt, zwar für Urheberrechtsverletzungen des Nutzers nicht verantwortlich ist, allerdings gegen ihn ggf. eine gerichtliche Anordnung ergehen kann, zur Vorbeugung von Urheberrechtsverletzungen seinen WLAN-Anschluss durch ein geeignetes Passwort zu sichern. Zudem sei es – so der EuGH – erforderlich, dass die Nutzer des WLAN ihre Identität offenbaren müssen, bevor sie das erforderliche Passwort erhalten.

Als Reaktion auf diese Urteile wurde zum 13. Oktober 2017 das Telemediengesetz (TMG) geändert und klargestellt, dass die Haftungsprivilegierung für Access Provider hinsichtlich fremder Informationen auch für öffentliche WLAN-Hotspots gilt, so dass WLAN-Betreiber nicht auf Unterlassung und Schadensersatz in Anspruch genommen werden können. **Hierdurch wurde die Störerhaftung hinsichtlich der WLAN-Betreiber zurückgedrängt**. Bei Verletzung von Rechten am geistigen Eigentum können diesen gegenüber allerdings nach § 7 Abs. 4 TMG Ansprüche auf Internetzugangssperre geltend gemacht werden, so dass auch trotz der jüngsten Gesetzesänderungen **Betreiber öffentlicher WLAN-Hotspots** befürchten müssen, gerichtlich zumindest auf **Sperrung des Zugangs zu bestimmten Internetportalen** in Anspruch genommen zu werden.

3. Einsatz von Antiviren-Programmen und Spam-Filtern im Unternehmen

Wie gezeigt ist der **Einsatz von Virenschutzprogrammen in Unternehmen** aus Gründen der IT-Security dringend und zwingend geboten. Aus **rechtlichen Gründen** sind besondere Voraussetzungen zu beachten:

§ 206 StGB stellt eine Verletzung des Post- oder Fernmeldegeheimnisses unter Strafe. Eine solche Verletzung liegt u.a. dann vor, wenn ein Unternehmen eine zur Übermittlung anvertraute Sendung unterdrückt. Unter den Begriff „Unternehmen" in dieser Strafvorschrift fällt jede Betätigung im Geschäftsverkehr, die nicht ausschließlich hoheitlich erfolgt oder auf eine private Tätigkeit beschränkt ist. Unternehmen, die ihren Mitarbeitern auch die **private E-Mail-Nutzung** gestatten, können sich der Verletzung des Post- oder Fernmeldegeheimnisses strafbar machen, wenn sie an einen Mitarbeiter adressierte E-Mails **ausfiltern**.

Gemäß § 109 Abs. 1 Satz 1 Telekommunikationsgesetz (TKG) müssen Diensteanbieter **erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses** und gegen die Verletzung des Schutzes personenbezogener Daten treffen. Dabei ist der **Stand der Technik zu berücksichtigen**. Wie dargestellt,

bestehen umfassende **gesetzliche Anforderungen an die IT-Compliance und IT-Security**. Daraus lässt sich ableiten, dass zumindest dann ein **Ausfiltern von E-Mails zulässig** ist, wenn diese mit Viren behaftet sind oder es sich um eine andere Art von Malware handelt, denn diese könnte Störungen oder Schäden an den Telekommunikations- oder Datenverarbeitungssystemen des Unternehmens auslösen (so auch bereits das OLG Karlsruhe in dem nachfolgend erwähnten Beschluss vom 10. Januar 2005).

Problematisch bleibt hingegen der Fall, dass ein Unternehmen **Spam-E-Mails**, also unverlangt zugesendete Werbe-E-Mails, löscht. So hatte das Oberlandesgericht Karlsruhe in einem Beschluss vom 10. Januar 2005 (Az. 1 Ws 152/04) – der bis heute von Bedeutung ist – entschieden, dass der Straftatbestand der Unterdrückung einer anvertrauten Sendung dann vorliegen kann, wenn der Arbeitgeber durch technische Eingriffe – Ausfiltern einer E-Mail – verhindert, dass die Nachricht den Empfänger vollständig und unverstümmelt erreicht.

Um drohender Strafbarkeit beim Einsatz von Spam-Filtern vorzubeugen, bieten sich folgende **Lösungsmöglichkeiten** an:

- **Dem Arbeitnehmer wird die private Nutzung seines dienstlichen E-Mail-Accounts untersagt.**
- **Der Arbeitnehmer stimmt dem Einsatz von Spam-Filtern zu.**
- **Die Spam-E-Mails werden in einen Quarantäne-Ordner verschoben, der betroffene Arbeitnehmer wird darüber informiert. Er hat so die Möglichkeit, die Spam-E-Mails entweder einzusehen oder sie ungesehen zu löschen.**

4. BYOD (Bring your own Device) / Consumerization

Mitarbeiter verwenden private Smartphones, um dienstliche E-Mails zu bearbeiten. Die VPN-Verbindung zum Firmenrechner im Urlaub erfolgt über den privaten Internet-Anschluss im Ferienhaus. Auf Tablets werden Browserspiele gespielt und zugleich Firmendaten abgerufen. Im privaten XING-oder LinkedIn-Account werden Firmenkontakte offengelegt und gepflegt. Dies alles sind Beispiele für **„BYOD (Bring your own Device)“** bzw. **„Consumerization“**, bei dem Mitarbeiter **eigene private Endgeräte** dazu verwenden, **berufliche Tätigkeiten** auszuüben. Die Grenze zwischen privater und beruflicher IT-Infrastruktur verschwimmt. Die wesentlichen rechtlichen Risiken liegen hierbei in den Bereichen IT-Security, Datenschutz und Archivierungspflichten.

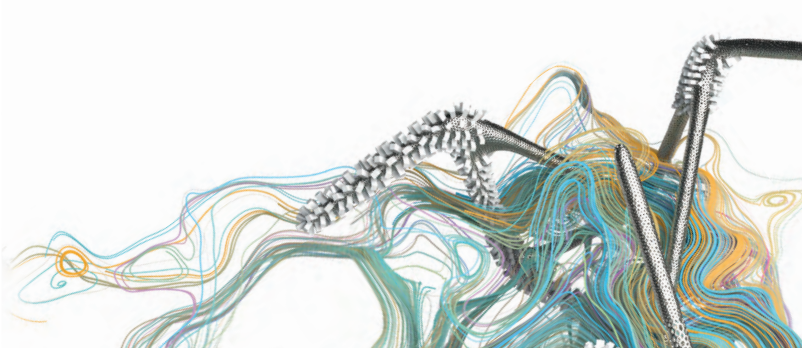
a) IT-Security

BYOD-Endgeräte können Einfallstore in die IT-Sicherheit und den Datenschutz von Unternehmen sein, denn sie befinden sich im Besitz der Mitarbeiter und ermöglichen den Einsatz von kritischen Applikationen. Über Messenger-Dienste können Firmenkontakte

ausgespäht werden, Sprachassistenten können ungewollt Gespräche aufzeichnen. Um den Anforderungen an die IT-Security auch im Bereich der Consumerization gerecht zu werden, sollten Unternehmen eine **Sicherheitsstrategie** entwickeln und **IT-Security-Richtlinien** aufstellen. Hierin können etwa geregelt werden,

- **wie Home Office-Arbeitsplätze technisch einzurichten und zu schützen sind,**
- **welche Endgeräte im Rahmen von BYOD genutzt werden dürfen,**
- **welche Sicherheitssoftware einzusetzen ist,**
- **wie Endgeräte gegen unberechtigten Zugriff geschützt werden, etwa im Falle eines Verlusts oder Diebstahls,**
- **wie Zugriffe auf das Firmennetzwerk, Home Office-Systeme und Datenverbindungen geschützt werden,**
- **wie sichergestellt wird, dass private Applikationen kein Sicherheitsrisiko darstellen, etwa durch Sperren des Zugriffs von Apps auf Firmenkontakte, Mikrofon und Kamera des Smartphones,**
- **wie das Unternehmen auf das Endgerät und dessen Inhalte zugreifen kann und darf,**
- **wann und unter welchen Voraussetzungen BYOD durch das Unternehmen beendet werden kann, und**
- **wie bei einer Beendigung des Arbeitsverhältnisses die geschäftlichen Daten von dem privaten Endgerät gelöscht werden.**

Durch entsprechende technische und organisatorische Maßnahmen muss das Unternehmen zudem sicherstellen, dass die Sicherheitsstrategie auch umgesetzt wird. Wichtig ist hierbei, dass das Unternehmen die Kontrolle über das Endgerät behält, dieses administrieren und ggf. auch Daten löschen kann. Zudem muss das Unternehmen in der Lage sein, auch im Falle von BYOD geeignete Sicherheitssoftware auf den Endgeräten zu installieren und zu überprüfen, damit zum Beispiel verhindert wird, dass ein Smartphone eines Mitarbeiters gehackt und dessen Firmenkontakte ausgespäht oder vertrauliche Nachrichten über Messenger-Dienste abgefangen werden.



b) Datenschutz

Wie oben näher dargestellt, empfiehlt es sich auch im Bereich der Consumerization, den Umfang der Privatnutzung, die Einhaltung von Sicherheitsanforderungen durch Mitarbeiter und die Kontrollrechte des Arbeitgebers mit den Mitarbeitern zu regeln. Ein wichtiger Aspekt ist hierbei die **Trennung von privaten und beruflichen Daten auf dem Endgerät**, damit der Arbeitgeber auf letztere Zugriff nehmen kann, ohne die Privatsphäre des Mitarbeiters in Bezug auf erstere zu verletzen. Eine solche Regelung kann durch einen Zusatz zum Arbeitsvertrag, durch eine Betriebsvereinbarung mit dem Betriebsrat oder auch durch eine IT-Anwenderrichtlinie der Unternehmensleitung erfolgen, wobei jeweils von Fall zu Fall geprüft werden muss, welche dieser Maßnahmen die sinnvollste und erfolgversprechendste ist und wie sie rechtswirksam umgesetzt werden kann.

Besondere datenschutzrechtliche Relevanz haben **Mobile Apps**, die der Arbeitnehmer auf sein Smartphone lädt, denn viele davon greifen auf persönliche Informationen des Nutzers wie etwa dessen Standort oder personenbezogene Daten wie das elektronische Telefonbuch zu. Das Problem liegt oft im Detail: So kann **Spracherkennungssoftware** die Nutzung des Smartphones erleichtern, etwa indem Nachrichten diktiert oder vorgelesen werden. Der Inhalt dieser Nachrichten wird aber nicht auf dem Smartphone gespeichert, sondern im Cloud-Speicher des Softwareanbieters. Durch den Einsatz mobiler Apps können also sensible Unternehmensinformationen die Unternehmenssphäre verlassen und dem Zugriff Dritter unterliegen, ohne dass das Unternehmen und der Mitarbeiter sich diesem Risiko überhaupt bewusst sind. Sofern die Verwendung solcher Mobile Apps nicht ohnehin die Einwilligung des Arbeitgebers erfordert, empfiehlt sich der **Einsatz mobiler Sicherheitssoftware**, die nicht nur Angriffe auf das Smartphone blockt, sondern auch **Datenschutzrisiken in Mobile Apps** erkennt und ggf. den Einsatz verhindert.

c) Archivierungspflichten

Hierfür gelten die Ausführungen in Kapitel VII.1.d) gleichermaßen.

5. Social Media in Unternehmen

Unternehmen, die Social Media wie Facebook und Twitter zur Unternehmenskommunikation einsetzen sowie ihren Mitarbeitern eine Nutzung während der Arbeitszeit gestatten, müssen zahlreiche rechtliche Anforderungen beachten. Die wichtigsten sind:

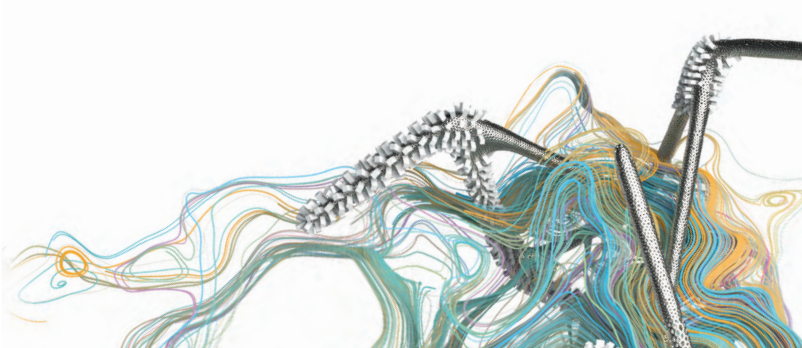
a) Impressumspflicht

Auch für Unternehmensseiten in Social Media besteht eine **Impressumspflicht** nach § 5 Telemediengesetz (TMG), d.h. auch bei Facebook, XING, Twitter u.ä. sind insbesondere Angaben zur Firma, Rechtsform, Adresse, E-Mail-Adresse und zum Handelsregister zu machen. Ein mit „Info" beschrifteter Button, der auf den Internetauftritt des Unternehmens mit dem dort enthaltenen Impressum verweist, genügt nach einem Urteil des Oberlandesgerichts Düsseldorf vom 13. August 2013 (Az. I-20 U 75/13) hierfür nicht.

b) Gewerblicher Rechtsschutz und Wettbewerbsrecht
Die Nutzung fremder **Marken** oder **Urheberrechte** auf Social Media-Seiten ohne eine Lizenz hierfür verletzt die gewerblichen Schutzrechte Dritter. So stellt es ein rechtswidriges „Account Grabbing" dar, wenn ein Unternehmen unter dem Firmennamen eines Wettbewerbers ein Twitter-Account einrichtet. Vorsicht ist auch bei Meinungsforen geboten, damit hier keine **Haftung für fremde Inhalte**, die beispielsweise beleidigend sind, übernommen werden muss. Aus wettbewerbsrechtlicher Sicht ist es unzulässig, wenn ein Unternehmen sich auf einem Bewertungsportal selbst lobt, dies jedoch durch ein Pseudonym verschleiert. Ein Unternehmen, das zum Beispiel auf Facebook ein **Preisausschreiben** veranstaltet, muss hierfür nicht nur die Anforderungen des Gesetzes gegen den unlauteren Wettbewerb (UWG) beachten, sondern auch die entsprechenden **Richtlinien des Betreibers der Social Media-Plattform**.

c) Datenschutz
Der Einsatz von **Cookies, „Like-Buttons"** und Optimierungsdiensten wie Geo Targeting ist datenschutzrechtlich kritisch zu sehen, wenn hierbei IP-Adressen der Nutzer erhoben oder verarbeitet werden. Abhängig von Art und Umfang der Nutzung ist entweder die – ggf. elektronische – Einwilligung des Nutzers erforderlich oder er ist zumindest über die Nutzung im Rahmen der **Datenschutzhinweise** zu unterrichten.

d) Social Media Guidelines
Es ist Unternehmen zu empfehlen, in sog. **„Social Media Guidelines"** Handlungsanweisungen für Mitarbeiter für den rechtskonformen und sicheren Umgang mit Social Media-Portalen zu geben. Hierzu zählt zum Beispiel, wer im Namen des Unternehmens Accounts anlegen und Inhalte einstellen darf, in welchem Umfang die private Nutzung von sozialen Netzwerken während der Arbeitszeit gestattet ist, wie mit Angaben über das Unternehmen in privaten Accounts umzugehen ist, welche Inhalte zulässig sind und keine Betriebsgeheimnisse verletzen, sowie Aufklärung über die „Netiquette" in sozialen Netzwerken. Der Betriebsrat kann zu einzelnen Regelungen ein Mitbestimmungsrecht haben.



VIII. Strafrechtliche Konsequenzen beim Missbrauch von IT-Infrastruktur und Datendiebstahl

Erfolgt ein Missbrauch von IT-Infrastruktur oder ein Datendiebstahl vorsätzlich, können **strafrechtliche Konsequenzen** eintreten.

1. Ausspähen von Daten

§ 202a StGB stellt das **Ausspähen von Daten** unter Strafe. Geschützt werden nur solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Erfasst werden auch nur solche Daten, die nicht für den Täter selbst bestimmt sind. Diese müssen gegen unberechtigten Zugang besonders gesichert sein. Das können z.B. **softwaretechnische Schutzmaßnahmen** wie Passwörter, Verschlüsselungen oder Zugangssicherungen der Hardware wie der mechanische Kopierschutz oder biometrische Verfahren sein, sofern diese Maßnahmen geeignet erscheinen, einen wirksamen Schutz zu erreichen. Bei schwachen Passwörtern wie „1234" darf dies bezweifelt werden. Abgesehen davon sind schwache Passwörter auf jeden Fall zu vermeiden, da das Hacken eines Accounts und damit ein Identitätsdiebstahl häufig aus der Verwendung schwacher Passwörter resultiert. Eine alleinige Warnung, die Daten dürften nicht eingesehen werden, ist nicht ausreichend. Auch das **Hacking**, bei dem der Hacker für ihn nicht bestimmte Daten lediglich zur Kenntnis nimmt, ohne diese zu verändern, fällt unter § 202a StGB, denn es ist bereits strafbar, sich oder einem anderen Zugang zu Daten zu verschaffen, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind. Damit wird das „Hacking" unter Strafe gestellt, selbst wenn der Täter sich dadurch keine Daten verschafft. Zu diesen Attacken zählen unter anderem der Einsatz von Key-Logging-Trojanern, Sniffern oder Backdoorprogrammen.

2. Verletzung des Fernmeldegeheimnisses

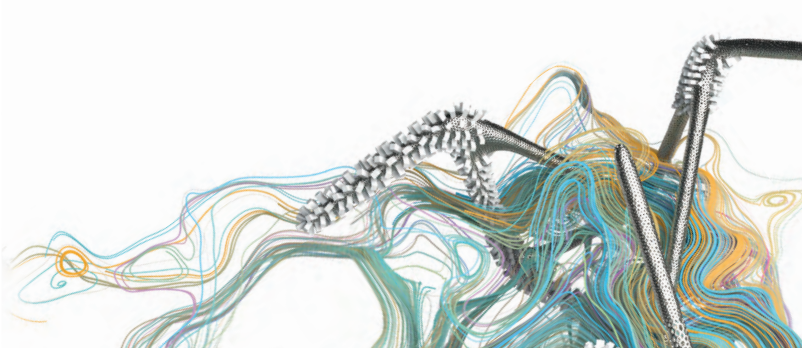
Gemäß § 88 TKG unterliegt der Inhalt der Telekommunikation und ihre näheren Umstände dem Fernmeldegeheimnis, wozu insbesondere auch die Tatsache zählt, ob jemand an einem bestimmten Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich zudem auf die näheren Umstände erfolgloser Verbindungsversuche. Nach § 206 StGB ist es u.a. strafbar, wenn eine unbefugte Mitteilung über den Inhalt privater E-Mail-Korrespondenz an andere gesendet oder die Weiterleitung privater E-Mails unterdrückt wird. Sofern die **private E-Mail-Nutzung untersagt** ist, kann der Arbeitgeber grundsätzlich davon ausgehen, dass sämtliche E-Mail-Korrespondenz dienstlich veranlasst ist, und somit deren Vorlage verlangen.

3. Verletzung von Privatgeheimnissen

§ 203 StGB regelt, dass Angehörige und Mitarbeiter bestimmter Berufsgruppen wie Ärzte, Rechtsanwälte oder einer Krankenversicherung ihnen anvertraute Privatgeheimnisse nicht unbefugt offenbaren dürfen. Allerdings können solche **Berufsgeheimnisträger** bestimmte Tätigkeiten wie etwa Betrieb und Wartung ihrer IT auf externe Anbieter **outsourcen**, sofern der Geheimnisträger dafür Sorge trägt, dass diese externen Dienstleister ebenfalls zur Geheimhaltung verpflichtet sind. Rechtsanwaltskanzleien dürfen auch **Dienstleister oder Subunternehmer im Ausland** einsetzen, wenn der dort bestehende Geheimnisschutz mit dem Schutz in Deutschland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet. In der Gesetzesbegründung (BT-Drucksache 18/12940 vom 27. Juni 2017, S. 13 f.) hierzu heißt es: „Sind beispielsweise die übermittelten Daten aus sich selbst heraus kaum verständlich, weil sie nur Teile eines umfassenden Prüfungsprozesses sind, kann das Schutzbedürfnis aufgrund der Art der übermittelten Daten geringer sein als bei Übermittlung eines gesamten in sich geschlossenen Vorgangs. Ein weiteres Beispiel … kann die **Fernwartung aus dem Ausland** sein. Das Erfordernis eines vergleichbaren Schutzniveaus im Ausland erscheint in den Fällen der Fernwartung schon deshalb als weniger dringlich als beispielsweise bei einer physischen Verlagerung von Daten ins Ausland, weil in den Fällen der Fernwartung praktisch in den allermeisten Fällen vor dem Hintergrund, dass die Fernwartung in einem begrenzten Zeitfenster stattfindet und zudem zumeist unter Zuhilfenahme von Verschlüsselungstechniken zwischen Dienstleister und Berufsgeheimnisträger stattfindet, eine Beschlagnahme durch ausländische staatliche Stellen üblicherweise nicht zu befürchten ist, außer, es liegen konkrete Anhaltspunkte dafür vor."

4. Datenveränderung

§ 303a StGB stellt die rechtswidrige Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von Daten unter Strafe. Darunter fallen nur fremde Daten, an denen eine andere Person ein unmittelbares Recht auf Verarbeitung, Löschung oder Nutzung hat. Erfasst wird auch das „logische" Verstecken von Daten, das zu einer Einschränkung der Verwendbarkeit führt. Dies kann beispielsweise durch die unbefugte Umbenennung von Dateien oder die Einfügung von Zugriffsbeschränkungen erfolgen.



5. Computersabotage

§ 303b StGB regelt die Computersabotage. Darunter fallen unter anderem Störungen der Datenverarbeitung und erhebliche Beeinträchtigungen der reibungslosen Datenverarbeitung. **Viren-Attacken** können als Computersabotage strafbar sein. Unter § 303b StGB sind auch **Denial of Service-Attacken** verboten. So hat zum Beispiel das Landgericht Düsseldorf in einem Urteil vom 22. März 2011 (Az. 3 KLs 1/11) entschieden, dass sog. DDoS-Attacken (Distributed Denial of Service-Attacken) den Tatbestand des § 303b StGB erfüllen. Bei einer DDoS-Attacke erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus und nicht – wie bei der DoS-Attacke – von einem einzelnen System. In besonders schweren Fällen wird in § 303b StGB eine Freiheitsstrafe von bis zu zehn Jahren angedroht.

6. Vorbereitung des Ausspähens und Abfangens von Daten

Nach § 202c StGB ist die Vorbereitung von Taten nach §§ 202a oder 202b StGB strafrechtlich relevant, wenn der Täter Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Straftat ist, herstellt oder sich verschafft. Sanktioniert wird hierdurch das Herstellen, Überlassen, Verbreiten oder Verschaffen von **„Hacker-Tools"**, die nach Art und Weise ihres Aufbaus illegalen Zwecken dienen können. Allgemeine Programmier-Tools, -Sprachen oder sonstige Anwendungsprogramme fallen nicht unter diese Strafvorschrift, selbst wenn sie zum Hacken eingesetzt werden. In einem Beschluss vom 18. Mai 2009 (Az. 2 BvR 2233/07) hat das Bundesverfassungsgericht dies klargestellt und entschieden, dass **Dual Use-Tools** nicht unter § 202c StGB fallen. Werden Computerprogramme im Sinne dieser Vorschrift beschafft oder weitergegeben, um im Rahmen von Penetrations- und Sicherheits-Tests im Auftrag und somit im Einverständnis mit den über die überprüften Computersysteme Verfügungsberechtigten verwendet zu werden, fehlt es am Tatbestandsmerkmal des „unbefugten Handelns", so dass insoweit auch Schadprogramme, deren objektiver Zweck in der Begehung von Computerstraftaten liegt, beschafft oder weitergegeben werden dürfen – und zwar auch dann, wenn aufgrund der Herkunft der Programme der Verdacht nahe liegt, dass andere Nutzer keine lauteren Absichten verfolgen. Der unter § 202c StGB angedrohte Strafrahmen wurde Ende 2015 von bisher bis zu einem Jahr Freiheitsstrafe auf bis zu zwei Jahre Freiheitsstrafe angehoben, was die **zunehmende Bedeutung der Vorschrift** verdeutlicht.

7. Datenhehlerei

Seit 2015 ist nach § 202d StGB die Hehlerei mit illegal gewonnenen Daten mit bis zu drei Jahren Freiheitsstrafe strafbar.

8. Fälschung beweiserheblicher Daten

§ 269 StGB stellt die Fälschung beweiserheblicher Daten unter Strafe. Demnach ist es verboten, im Rechtsverkehr beweiserhebliche Daten derart zu speichern oder zu verändern, dass sie bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde hervorbringen würden. Dieser Straftatbestand lässt sich als **„elektronische Urkundenfälschung“** verstehen.

9. Störung von Telekommunikationsanlagen

Nach § 317 StGB ist strafbar, wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, dass eine hierfür dienende Sache zerstört, verändert oder unbrauchbar gemacht oder der Strom abgestellt wird. Dieser Straftatbestand ist z.B. dann erfüllt, wenn der E-Mail-Verkehr einer Behörde durch einen **Viren-Angriff** nicht nur kurzzeitig zum Erliegen kommt.

10. Verletzung von Geschäftsgeheimnissen

Das Gesetz zum Schutz von Geschäftsgeheimnissen stellt eine Verletzung von Geschäftsgeheimnissen unter Strafe, wie z.B. unbefugtes Aneignen oder unbefugtes Kopieren von Gegenständen oder elektronischen Dateien, die das Geschäftsgeheimnis enthalten. So kann der **Quellcode eines Computerprogramms** ein Geschäftsgeheimnis darstellen und ein Mitarbeiter, der diesen unbefugt kopiert und an einen Wettbewerber weitergibt, macht sich strafbar.

11. Datenschutzdelikte

Bei **Verstößen gegen Datenschutzrecht** können nach der EU-Datenschutz-Grundverordnung **Geldbußen** bis zu 4 % des weltweiten Jahresumsatzes oder bis zu 20 Millionen Euro verhängt werden. Das Bundesdatenschutzgesetz sieht bei vorsätzlichen Datenschutzverstößen, die gewerbsmäßig, gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht erfolgen, **Geld- oder Freiheitsstrafe** vor.

Das Ausspähen von Daten und der Angriff auf die IT-Infrastruktur von Unternehmen können nach diversen Vorschriften strafbar sein. Sofern ein Unternehmen von eigenen Mitarbeitern geschädigt wird, kann es mit **arbeitsrechtlichen Maßnahmen** (Abmahnung,

fristlose Kündigung), **Schadensersatzansprüchen** und gegebenenfalls einer **Strafanzeige** reagieren. Für eine wirksame fristlose Kündigung eines Mitarbeiters muss es hierbei nach einem Urteil des Landesarbeitsgerichts Hamm vom 6. Dezember 2013 (Az. 13 Sa 596/13) objektiv feststehen bzw. ein dringender Tatverdacht bestehen, dass genau dieser Mitarbeiter rechtswidrige Handlungen wie illegale Downloads vorgenommen hat, wobei sich der Nachweis im Einzelfall für den Arbeitgeber als schwierig darstellen kann. Sollte ein Mitarbeiter das IT-System seines Arbeitgebers nachweisbar zur Durchführung solcher strafbarer Handlungen benutzen und so Dritte schädigen, kann das Unternehmen hierfür gegebenenfalls zivilrechtlich haftbar gemacht werden, falls es nicht **ausreichende Sicherheitsvorkehrungen** gegen einen solchen Missbrauch getroffen hat. Eine **strafbare Verantwortlichkeit der Geschäftsführung** für strafbare Handlungen eines Mitarbeiters, die dieser „privat" begangen hat, scheidet hingegen in aller Regel mangels Vorsatz aus.

12. Verschärfung des Cyberstrafrechts sowie neue Ermittlungsinstrumente für die Polizei und Staatsanwaltschaft

Das IT-Sicherheitsgesetz 2.0 (siehe Kapitel I.3) sieht die Einführung von zwei neuen Strafvorschriften im Bereich des Cyberstrafrechts sowie neue Ermittlungsinstrumente für die Polizei und Staatsanwaltschaft vor:

Eine neue Strafvorschrift in § 126a StGB mit der Bezeichnung **„Zugänglichmachung von Leistungen zur Begehung von Straftaten"** soll das Betreiben von Internet-Plattformen insbesondere im **Darknet** unter Strafe stellen, die auf die Förderung, Ermöglichung oder Erleichterung von illegalen Zwecke ausgerichtet sind.

Eine weitere neue Strafvorschrift in § 202e StGB **„Unbefugte Nutzung informationstechnischer Systeme"** sieht vor, dass u.a. bestraft werden soll, wer sich oder einem Dritten unbefugt Zugang zu einem IT-System verschafft, mit dem personenbezogene Daten verarbeitet werden oder das Teil einer kritischen Infrastruktur ist. „Informationstechnische Systeme" sind hiernach allerdings nur solche IT-Systeme, die entweder der Verarbeitung personenbezogener Daten oder bestimmten Zwecken wie bspw. Wirtschaft oder Sport dienen oder die kritischen Bereichen wie Energie oder Telekommunikation angehören. Erfasst werden sollen z.B. **Apps, die die Nutzer bewusst über die eingeräumten Zugriffsrechte täuschen**. Hierunter nicht strafbar sind allerdings Fälle, bei denen Sicherheitslücken im IT-System eines Unternehmens durch Hacker oder Anbieter von IT-Sicherheitslösungen aufgespürt werden, sofern diese durch das Unternehmen hierzu beauftragt worden sind.

Um den Ermittlungsbehörden die Kommunikation im Darknet zu ermöglichen und dort Straftaten insbesondere im Bereich des illegalen Handels und der Kinderpornografie aufklären zu können, sollen Ermittler die **digitale Identität**, d.h. die **aktiven Accounts von Beschuldigten auch gegen deren Willen übernehmen und weiterführen** können.

Um an die Zugangsdaten zu gelangen, um das Account übernehmen zu können, können staatliche Stellen u.a. verdeckte Ermittlungsmaßnahmen oder Durchsuchungen bei Dritten durchführen (siehe Kapitel II.8). Sie können schließlich den Verdächtigen selbst mittels Ordnungs- und Zwangsmitteln bis hin zur Beugehaft zwingen, seine Zugangsdaten, also sein **Passwort herauszugeben**.

Rechtsanwalt und Fachanwalt für Informationstechnologierecht Dr. Thomas Stögmüller, LL.M. (Berkeley), TCI Rechtsanwälte München

Stand: Juni 2019 – 6. Auflage

Dr. Thomas Stögmüller, LL.M. (Berkeley) | Rechtsanwalt und Fachanwalt für Informationstechnologierecht | TCI Rechtsanwälte München
Dr. Thomas Stögmüller berät deutsche und internationale Unternehmen insbesondere in den Bereichen IT-, E-Commerce-, Telekommunikationsrecht und Datenschutz sowie Urheberrecht, gewerblicher Rechtsschutz und Kartellrecht. Er ist Gründungspartner von TCI Rechtsanwälte, die ihren Branchenfokus in den Bereichen Technology, Communications, Information hat, auf denen die Kurzbezeichnung „TCI" beruht. Dr. Thomas Stögmüller studierte und promovierte an der Ludwig-Maximilians-Universität München und an der University of California in Berkeley. Er war wissenschaftlicher Mitarbeiter am Max-Planck-Institut für ausländisches und internationales Patent-, Urheber- und Wettbewerbsrecht (US-Referat) und Jurist im Telekommunikationsreferat des Bayerischen Staatsministeriums für Wirtschaft, Verkehr und Technologie. 1995 wurde er als Rechtsanwalt zugelassen und war vor der Gründung von TCI Rechtsanwälte 2011 in namhaften Kanzleien in Frankfurt und München als Partner tätig.

Über Trend Micro

Als einer der weltweit führenden Anbieter von IT-Sicherheit verfolgt Trend Micro mit Leidenschaft das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen – heute und in Zukunft. Unsere innovativen Lösungen für Privatanwender, Unternehmen und Behörden bieten dank der XGen™ Sicherheitsstrategie vernetzten Schutz für Rechenzentren, Cloud-Workloads, Netzwerke und Endpunkte. Unsere Connected Threat Defense ermöglicht das nahtlose Teilen von Bedrohungsinformationen und bietet zentrale Transparenz und Kontrolle, um Organisationen bestmöglich zu schützen.

Mit über 6.500 Mitarbeitern in 50 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyberbedrohungen bietet Trend Micro Schutz für eine vernetzte Welt.

Weitere Informationen: **www.trendmicro.com**.

TREND MICRO™

Securing Your Connected World

Trend Micro Deutschland GmbH
Zeppelinstrasse 1 • 85399 Hallbergmoos
Tel.: +49 (0) 811 / 88 99 0 - 700
Fax: +49 (0) 811 / 88 99 0 - 799
www.trendmicro.com

Stand: Juni 2019 – 6. Auflage – **Version 6**