Juristische Informationen
für die Unternehmensleitung

Cybersicherheit und IT-Compliance im Unternehmen

8. Auflage | **Mai 2024**

Dieser Leitfaden gibt einen Einblick in wichtige juristische Themengebiete, die für den Einsatz von IT und Internet in Unternehmen relevant sind. Dabei liegt der Schwerpunkt auf der Cybersicherheit. 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. eine Rechtsanwältin oder einen Rechtsanwalt ersetzen.

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

Vorwort

Den vielbeachteten Juristischen Leitfaden für IT Security bringt Trend Micro dieses Jahr bereits das 8. Mal heraus und stellt so sicher, dass Geschäftsführer, Vorstand oder Aufsichtsrat den einschlägigen rechtlichen Anforderungen gerecht werden können und ihren Pflichten nachkommen. Immerhin sind Cybersicherheit und IT-Compliance für die Geschäftsleitung von Unternehmen im Rahmen der Corporate Governance von großer Bedeutung.

Es freut mich besonders, dass wir auch für diese Neuauflage erneut Dr. Thomas Stögmüller als Autor gewinnen konnten. Basierend auf seiner langjährigen Expertise als Rechtsanwalt und Fachanwalt für Informationstechnologierecht hat er unseren Leitfaden auf den aktuellen Stand gebracht und insbesondere die NIS-2-Richtlinie und den Digital Operational Resilience Act (DORA) als neue Rechtsakte der EU zur Cybersicherheit ausführlich dargestellt. Gleichzeitig ist es ihm wieder gelungen, durch praxisnahe Beispiele auch komplexe Sachverhalte anschaulich zu vermitteln.

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, IoT bzw. IIoT (Internet of Things / Industrial Internet of Things) und KI (Künstliche Intelligenz) stellen die nächste Stufe technologischer Innovationen dar, die in Unternehmen zum Einsatz kommen.

Gerade die COVID-19-Pandemie hat gezeigt, wie wertvoll einerseits Cloud-Lösungen und Home Office sind, wie Unternehmen anderseits hierdurch auch anfällig werden. Denn die Informationstechnologie bietet nicht nur Vorteile: Sicherheitslücken und Datenlecks, Cyberangriffe, Datenschutzverstöße und der Missbrauch von IT-Systemen durch Mitarbeitende können die Geschäftstätigkeit erheblich beeinträchtigen und unter Umständen sowohl zu strafrechtlichen Konsequenzen als auch zu Schadensersatzforderungen gegen das Unternehmen und die Unternehmensleitung führen.

Wir hoffen, Verantwortlichen in Unternehmen auch mit der neuesten Auflage wieder eine Handreichung bieten zu können, die ihnen auch im Arbeitsalltag dabei hilft, Probleme in der Praxis zu lösen.

Garching bei München im Mai 2024

Hannes Steiner
Vice President DACH | Europe Sales & Marketing bei Trend Micro

Inhaltsverzeichnis

Die Themen im Überblick

Die Sicherstellung der Cybersicherheit 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 **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. Diese **Verpflichtung zur Cybersicherheit** wird durch die **NIS-2-Richtlinie** auf große Teile der Wirtschaft erweitert.

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.

Ein heikles Thema für die Beziehungen zwischen der Geschäftsleitung und den Mitarbeitenden 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.

Mit der COVID-19-Pandemie hat die **Home Office-Nutzung** in den Büroalltag Einzug gehalten zugenommen und das Arbeiten von zu Hause oder von unterwegs ist in vielen Unternehmen zur Regel geworden. Allerdings ist dies anfällig gegen

Datenschutzverstöße und es besteht die Gefahr, dass der Schutz von Geschäftsgeheimnissen verletzt wird. Unternehmen müssen dem durch geeignete Maßnahmen vorbeugen.

I. Cybersicherheit 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. Cybersicherheit und IT-Compliance bilden dabei wichtige Bausteine.

1. Bedeutung der Cybersicherheit

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

Das „Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik" (BSIG) stellt fest, dass Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse besonders schützenswert sind. Hiernach bedeutet **„Sicherheit in der Informationstechnik"** (...) „die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität 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 Schadsoftware („Malware", z.B. Ransomware), 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) Integrität

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**
- **Geschäftsgeheimnisse von Unternehmen.**

Der Zugriff auf derartige Daten und Informationen darf nur berechtigten Personen möglich sein. Im Rahmen der Cybersicherheit 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, selbst Telefonnummern können gefälscht übermittelt werden (Stichwort: Call ID Spoofing).

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 Cybersicherheit

Cybersicherheit 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 Cybersicherheit.
- 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 die IT-Leiterin bzw. der IT-Leiter können bei Verstößen gegen die Anforderungen der IT-Sicherheit gegebenenfalls wegen Verletzung ihrer arbeitsvertraglichen Pflichten in Anspruch genommen werden, wie im Praxisbeispiel zur Vorstandshaftung und Haftung des IT-Leiters in Kapitel I.10.g) näher dargestellt.

Anforderungen an die Cybersicherheit 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. Beispiele wären etwa, wenn ein Unternehmen keine geeigneten Sicherheitsmaßnahmen wie z.B. eine im konkreten Fall verbindlich vorgeschriebene 2-Faktor-Authentifizierung ergreift, als Betreiber kritischer Infrastrukturen (KRITIS) bzw. kritischer Anlagen der Verpflichtung des Einsatzes von Systemen zur Angriffserkennung (siehe hierzu Kapitel I.3.a und I.4.g) nicht nachkommt oder das IT-Sicherheitskennzeichen (siehe hierzu Kapitel I.3.e) unzutreffend verwendet.

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 Cybersicherheit 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 Cybersecurity 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" 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. Im Juni 2023 haben sich das Europäische Parlament und der Rat der EU auf eine finale Umsetzung des Basel III-Rahmenwerks in der EU geeinigt und die neuen Regeln müssen voraussichtlich ab dem 1. Januar 2025 angewendet werden. 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. Bedeutsam sind in diesem Zusammenhang die Unabhängigkeit und Integrität der Abschlussprüfer, die Prüfungsqualität und die besonders wichtige gesellschaftliche Funktion der Abschlussprüfer mit dem Ziel, eine strenge Prüfung börsennotierter Gesellschaften durchzuführen. Die Wirksamkeit des internen Kontroll- und Risikomanagementsystems kapitalmarktorientierter Kapitalgesellschaften ist durch den Aufsichtsrat oder einen von ihm bestellten Prüfungsausschuss zu kontrollieren. Die Verletzung der Pflichten bei Abschlussprüfungen durch Mitglieder eines Aufsichtsrats oder eines Prüfungsausschusses können strafbar sein.

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 Cybersicherheit kann sogar die gewerberechtliche Zuverlässigkeit des Unternehmens in Frage gestellt werden und eine **Gewerbeuntersagung** erfolgen.

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

Schutzziel des IT-Sicherheitsgesetzes ist die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen und IT-Systemen betreffen, durch **Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen** oder bei deren Anwendung. 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, sowie auf Unterrichtungen des BSI über Sicherheitsvorfälle zeitnah und angemessen reagieren. Unter **„kritischen Infrastrukturen (KRITIS)"** werden Einrichtungen und Anlagen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung verstanden, bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die kritischen Infrastrukturen werden durch die Verordnung zur Bestimmung Kritischer Infrastrukturen (**BSI-Kritisverordnung**) konkretisiert, die zuletzt mit Wirkung zum 1. Januar 2024 geändert wurde. Die BSI-Kritisverordnung wird alle zwei Jahre evaluiert, um eine flexible Möglichkeit der Anpassung der kritischen Dienstleistungen und Bereiche, auf die sie Anwendung findet, Anlagenkategorien und Schwellenwerte zu schaffen.

Unter dem Schlagwort **„IT-Sicherheitsgesetz 2.0"** wurde am 18. Mai 2021 das „Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" vom Bundestag beschlossen, um den qualitativ immer ausgefeilteren und gefährlicheren Angriffen, etwa durch Ransomware, Schwachstellen in Computerchips und einer weiteren **Verschärfung der Bedrohungslage** durch die zunehmende Verbreitung von IoT-Geräten zu begegnen (zu IoT siehe Kapitel IV).

Die wesentlichen Anforderungen an und Pflichten von KRITIS-Betreibern unter dem IT-Sicherheitsgesetz 2.0 sind nachfolgend dargestellt. Es wird darauf hingewiesen, dass sich diese Regelungen mit Umsetzung der nachfolgend in Kapitel I.4 dargestellten NIS-2-Richtlinie und Inkrafttreten des geplanten NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz ändern werden.

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 Verpflichtung, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst auch den **Einsatz von Systemen zur Angriffserkennung**. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. 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) Registrierung und Kontaktstelle

Die KRITIS-Betreiber müssen die von ihnen betriebenen Kritischen Infrastrukturen beim BSI registrieren und dem BSI eine Kontaktstelle benennen sowie sicherstellen, dass sie hierüber rund um die Uhr (24/7) erreichbar sind. Im Falle einer Unterrichtung der Kontaktstelle durch das BSI über Sicherheitsvorfälle muss der KRITIS-Betreiber darauf zeitnah und in angemessener Weise reagieren. Dies schließt sehr häufig die Suche nach bekannten Indikatoren einer Kompromittierung (IOC – Indicator of Compromise) oder eines Angriffes (IOA – Indicator of Attack) ein. Unternehmen wird empfohlen, hierzu sowohl technische Maßnahmen, die der Erkennung besagter Indikatoren dienen ***(Detection)***, als auch Prozesse zu entwickeln, um angemessen auf diese Erkenntnisse zu reagieren ***(Response)***.

Weil bei Vorfällen, die erst über externe Quellen – etwa durch die Unterrichtung durch das BSI – auffallen, von einem hohen Durchdringungsgrad ausgegangen werden muss, sollten Erkennungs- und Gegenmaßnahmen möglichst umfassend ***(extended)*** über die gesamte IT-Infrastruktur des Unternehmens erfolgen. Im Fachbereich werden koordinierte technische Maßnahmen zur Unterstützung dieser Anforderung als „e**X**tended **D**etection & **R**esponse" bezeichnet, abgekürzt **„XDR"**.

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 **fehlerhaftes Update oder fehlerhaften Patch**. **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 müssen zur Vermeidung weiterer Auswirkungen 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 (MIP)** unter https://mip.bsi.bund.de bereit. Üblicherweise wird der Eingang einer Störungsmeldung vom BSI innerhalb von 30 Minuten quittiert.

Das BSI ist zudem die **allgemeine Meldestelle für Cybersicherheit in Deutschland**, um umfassend Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen zentral sammeln und auswerten zu können. Es betreibt die Webseite www.allianz-fuer-cybersicherheit.de, 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 KRITIS-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-Systeme, Komponenten und Prozesse einsetzen, sondern auch die **Hersteller sind in der Pflicht, sichere IT-Produkte anzubieten und IT-Störungen zu vermeiden**.

Melde- und Registrierungspflichten sowie Verpflichtungen zur Einhaltung von Mindeststandards wurden durch das IT-Sicherheitsgesetz 2.0 **auf weitere Teile der Wirtschaft, nämlich sog. „Unternehmen im besonderen öffentlichen Interesse" ausgeweitet**, bei denen ein staatliches Sicherheitsinteresse besteht oder die eine gesamtgesellschaftliche Bedeutung haben. Dies betrifft zum einen **Rüstungshersteller** und **Hersteller von IT-Produkten** für die Verarbeitung staatlicher Verschlusssachen, zum anderen Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Zudem fallen hierunter **Zulieferer**, die wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung für solche Unternehmen sind, zum Beispiel, weil ein Ausfall der Zulieferung ihrer Produkte oder Dienstleistungen auch einen Ausfall der Wertschöpfung der größten Unternehmen bedeuten kann. Damit sind diese Zulieferer ebenfalls Unternehmen von besonderem öffentlichen Interesse. Die „Unternehmen im besonderen öffentlichen Interesse" werden durch eine Rechtsverordnung bestimmt und sollen sich am Hauptgutachten der Monopolkommission zur Ermittlung der 100 größten Unternehmen Deutschlands orientieren. Auch die maßgeblichen Alleinstellungsmerkmale für Zulieferer werden durch diese Rechtsverordnung bestimmt. Denkbar wäre bspw. ein Anbieter von Software zur Steuerung von Maschinen, die eines der 100 größten Unternehmen Deutschlands herstellt. Schließlich sind bestimmte Betriebe erfasst, die unter die Störfall-Verordnung fallen.

d) Aufgaben und Befugnisse des BSI
Während einer erheblichen Störung kann das BSI von den betroffenen Betreibern Kritischer Infrastrukturen die **Herausgabe der zur Bewältigung der Störung notwendigen Informationen** einschließlich personenbezogener Daten verlangen. Ihm steht zudem zum Zweck der Überprüfung das **Recht zum Betreten von Geschäfts- und Betriebsräumen** während der üblichen Betriebszeiten zu.

Zu Zwecken der IT-Sicherheit kann das BSI auch **informationstechnische Produkte und Systeme untersuchen** und hierbei von deren Herstellern alle notwendigen **Auskünfte, insbesondere auch zu technischen Details** verlangen. Sollte der Hersteller seiner Auskunftspflicht nicht nachkommen, kann das BSI unter Nennung des Namens des Herstellers und des betroffenen Produkts bzw. Systems die Öffentlichkeit informieren. Das BSI kann zudem unter bestimmten engen Voraussetzungen Informationen über Störungen öffentlich machen und vor **Sicherheitslücken in informationstechnischen Produkten und Diensten warnen**, 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.

Das BSI nimmt auch den **Verbraucherschutz** im Bereich der Cybersicherheit wahr. Hierbei soll es den Stand der Technik für IT-Produkte und Dienste im Verbraucherbereich definieren und laufend aktualisieren und **„Security by Design"** am Markt durchsetzen. Zudem ist explizit genannt, dass das BSI mit seiner Expertise im Bereich Cybersicherheit Abmahnungen und Klagen gegen verbraucherrechtswidrige Praktiken unterstützen soll.

e) IT-Sicherheitskennzeichen
Ein einheitliches, freiwilliges IT-Sicherheitskennzeichen soll die IT-Sicherheit von Verbraucherprodukten und Dienstleistungen im IT-Bereich sichtbar machen und der Information von Verbrauchern dienen. Hersteller können hierdurch die **IT-Sicherheit ihrer Produkte** darstellen und sich zu weniger sicheren Konkurrenzprodukten abgrenzen. **Das IT-Sicherheitskennzeichen besteht aus zwei Komponenten:**

- einer **Herstellererklärung**, mit der 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. Während der maßgeblichen Dauer der Herstellererklärung wird der Hersteller diese Vorgaben auch weiter erfüllen, etwa durch **Softwareupdates**.
- **BSI-Sicherheitsinformationen** zum Produkt.

Herstellererklärung 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. Allerdings ist das IT-Sicherheitskennzeichen nicht verpflichtend und stellt auch kein „Gütesiegel“ dar, da keine objektive Prüfung der IT-Sicherheitseigenschaften durch eine unabhängige Stelle erfolgt.

f) Einsatz kritischer Komponenten

Das IT-Sicherheitsgesetz 2.0 definiert den Begriff der **„kritischen Komponenten“** als IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können. Zusätzlich muss das IT-Produkt per Gesetz als kritische Komponente bestimmt werden oder eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren. Plant ein KRITIS-Betreiber den Einsatz einer solchen kritischen Komponente, hat er dies dem Bundesinnenministerium anzuzeigen und dann bis zu vier Monate mit deren Einsatz abzuwarten. Das Bundesinnenministerium kann während dieser Frist den **Einsatz untersagen**, falls dieser die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Dies ist etwa der Fall, wenn der **Hersteller von einer ausländischen Regierung oder ausländischen Streitkräften kontrolliert** wird oder der Einsatz der kritischen Komponente nicht im Einklang mit den **sicherheitspolitischen Zielen** der Bundesrepublik Deutschland, der Europäischen Union oder der NATO ist.

Die **Möglichkeit der Untersagung** ist notwendig, weil aufgrund der zunehmenden informationstechnischen Komplexität der eingesetzten kritischen Komponenten ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Schließen von Sicherheitslücken) beim Hersteller selbst oder auch der weiteren Lieferkette verbleibt. **Es muss vermieden werden, dass Hersteller missbräuchliche Zugriffmöglichkeiten auf Hard- und Software implementieren oder anderweitig Sabotage oder Spionage ermöglichen.**

Kritische Komponenten dürfen nur eingesetzt werden, wenn der **Hersteller eine Garantieerklärung** über seine Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat. Dabei muss der Hersteller seine Garantieerklärung in Bezug auf sein **Endprodukt** einschließlich aller ihm zugelieferten Teile abgeben, das heißt auch in Bezug auf die **Lieferkette**. Aus der Garantieerklärung muss hervorgehen, wie sichergestellt wird, dass die **kritische Komponente nicht für Sabotage, Spionage oder Terrorismus missbraucht** wird. Sollte sich herausstellen, dass bspw. die Angaben in der Garantieerklärung unwahr sind, der Hersteller nicht unverzüglich Schwachstellen oder Manipulationen beseitigt oder die kritische Komponente aufgrund von Mängeln ein erhöhtes Gefährdungspotential für die IT-Sicherheit aufweist, kann das Bundesinnenministerium deren weiteren Einsatz und in schwerwiegenden Fällen sogar den Einsatz aller kritischen Komponenten dieses Herstellers untersagen.

g) Detektion von Sicherheitsrisiken durch das BSI

Durch das IT-Sicherheitsgesetz 2.0 wurde die Befugnis zur **Durchführung von sogenannten Portscans** durch das BSI geschaffen, um das Bestehen von Sicherheitslücken und andere Sicherheitsrisiken in der IT des Bundes oder bei KRITIS-Betreibern, digitalen Diensten und Unternehmen im besonderen öffentlichen Interesse zu prüfen. Hierzu darf das BSI sog. **„aktive Honeypots"** einsetzen, also einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Die Analyse von Schadsoftware durch Honeypots ist gerade wegen der zunehmenden Verbreitung von Internet of Things (IoT)-Geräten von Bedeutung, da diese Geräte ihre eigentliche Funktion beibehalten und dennoch von Schadsoftware infiziert sein können. Eine darüberhinausgehende Ausforschung der fremden informationstechnischen Systeme ist unzulässig. Sollte das BSI ein Sicherheitsrisiko erkennen, muss es die Betriebsverantwortlichen des IT-Systems darüber unverzüglich informieren.

h) Anforderungen an technische und organisatorische Vorkehrungen von Anbietern von Telemedien

Durch das IT-Sicherheitsgesetz wurden zudem Anforderungen an technische und organisatorische Vorkehrungen von Anbietern von Telemedien wie etwa Betreiber werbefinanzierter Webseiten normiert. Diese sind verpflichtet, im Rahmen des technisch Möglichen und wirtschaftlich Zumutbaren sicherzustellen, dass kein unerlaubter Zugriff auf ihre technischen Einrichtungen möglich ist und diese gegen Störungen 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. Das Gesetz sieht ausdrücklich vor, dass eine Maßnahme hierunter insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens ist. Sollte es bei Angeboten von Telemedien wie einer Unternehmenswebseite aufgrund ungenügender technischer und organisatorischer Vorkehrungen zu unerlaubten Zugriffen oder Störungen, etwa aufgrund von Cyber-Angriffen kommen, kann das BSI gegenüber dem Diensteanbieter anordnen, dass dieser die Gefahr abstellen muss. Beispiele sind Sicherheitslücken in einer E-Commerce-Software oder Schadsoftware in Werbebannern.

i) Bußgeldvorschriften

Verstöße gegen das IT-Sicherheitsgesetz können mit **Geldbußen** bis zu 2 Millionen Euro geahndet werden. Im Falle einer **Geldbuße gegen juristische Personen** oder Personenvereinigungen beträgt das **Höchstmaß der Geldbuße 20 Millionen Euro**.

4. NIS-2-Richtlinie und NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Auch die EU hat das Thema Cybersicherheit auf der Agenda. Nach der **Richtlinie über Netz- und Informationssicherheit (NIS-Richtlinie)**, die am 8. August 2016 in Kraft getreten ist und in Deutschland im BSI-Gesetz umgesetzt wurde, hat die EU am 14. Dezember 2022 die neue **NIS-2-Richtlinie** erlassen, mit der der Anwendungsbereich und die Pflichten zur **Erreichung eines hohen gemeinsamen Cybersicherheitsniveaus in der EU** auf große Teile der Wirtschaft erweitert wurden. Es wird geschätzt, dass ca. 30.000 Unternehmen in Deutschland von der NIS-2-Richtlinie betroffen sind. Die NIS-2-Richtlinie beschränkt sich auf eine Mindestharmonisierung und muss bis zum 17. Oktober 2024 durch die Mitgliedstaaten in nationales Recht umgesetzt werden. In Deutschland soll dies durch das **„NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz"** (NIS2UmsuCG) erfolgen, das im Mai 2024, dem Bearbeitungsstand dieser 8. Auflage des Juristischen Leitfadens, als Referentenentwurf vorliegt und auch Regelungen vorsieht, die über die Vorgaben der NIS-2-Richtlinie hinausgehen. Da sich das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz noch im Gesetzgebungsverfahren befindet, bezieht sich die nachfolgende Darstellung vorrangig auf die NIS-2-Richtlinie und ergänzend auf den Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes mit Bearbeitungsstand 7. Mai 2024, sodass bis zur Verabschiedung des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes Änderungen gegenüber dieser Darstellung möglich sind. Mit der NIS-2-Richtlinie und dem Inkrafttreten des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz werden die bisherige NIS-Richtlinie ersetzt, das BSI-Gesetz grundlegend novelliert und die oben in Kapitel I.3 dargestellten Regelungen des IT-Sicherheitsgesetzes, insbesondere in Bezug auf KRITIS-Betreiber, erheblich geändert und erweitert.

a) Anwendungsbereich

Der Anwendungsbereich ist sehr umfassend. Zunächst ist zu ermitteln, ob eine „Einrichtung" – das können Unternehmen aber auch natürliche Personen oder Teile der öffentlichen Verwaltung sein – unter einen der elf Sektoren mit hoher Kritikalität oder der sieben sonstigen kritischen Sektoren der NIS-2-Richtlinie fällt.

Sektoren mit hoher Kritikalität sind:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser

- Digitale Infrastruktur, die Betreiber von Internet-Knoten, DNS-Diensteanbieter (ausgenommen Betreiber von Root-Namenservern), TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Vertrauensdiensteanbieter, Anbieter öffentlicher elektronischer Kommunikationsnetze und Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste umfasst
- Verwaltung von IKT-Diensten (Business-to-Business)
- Öffentliche Verwaltung
- Weltraum

Sonstige kritische Sektoren sind:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe / Herstellung von Waren in näher aufgelisteten Teilsektoren wie Herstellung von Datenverarbeitungsgeräten, Maschinenbau oder KFZ-Herstellung
- Anbieter digitaler Dienste wie Online-Marktplätze, Online-Suchmaschinen und soziale Netzwerke
- Forschung

Es wird darauf hingewiesen, dass der Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes die Sektoren mit hoher Kritikalität als „Sektoren besonders wichtiger und wichtiger Einrichtungen" und die „sonstigen kritischen Sektoren" als „Sektoren wichtiger Einrichtungen" bezeichnet und teilweise von der Darstellung der Sektoren in der NIS-2-Richtlinie abweicht.

Sodann ist festzustellen, ob eine „**kritische Anlage"** betrieben wird oder eine Einrichtung, die unter einen dieser Sektoren fällt, den jeweiligen **Schwellenwert** erreicht. In Abhängigkeit der Schwellenwerte werden die Einrichtungen unterteilt in „wesentliche Einrichtungen" bzw. (nach dem Wortlaut des deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurfs) **„besonders wichtige Einrichtungen"** und in **„wichtige Einrichtungen"**.

Kritische Anlagen

Die „kritische Anlage" löst den bisherigen Begriff der „Kritischen Infrastruktur" (KRITIS) ab. Erfasst werden nach dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf Anlagen in den Sektoren Energie, Transport und Verkehr, Finanz- und Versiche-

rungswesen, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum sowie Siedlungsabfallentsorgung, die in einer Rechtsverordnung festzulegende Schwellenwerte überschreiten und damit einen als bedeutend anzusehenden **Versorgungsgrad** haben. **Betreiber einer solchen kritischen Anlage werden unabhängig von ihrer Größe als „besonders wichtige Einrichtung" eingestuft.**

Besonders wichtige Einrichtungen

- Sektor mit hoher Kritikalität
- Mindestens 250 Mitarbeiter
- oder
- Jahresumsatz von über 50 Millionen Euro und Jahresbilanzsumme von über 43 Millionen Euro

Wichtige Einrichtungen

- Sektor mit hoher Kritikalität oder sonstiger kritischen Sektor
- Mindestens 50 Mitarbeiter
- oder Jahresumsatz und Jahresbilanzsumme von jeweils über 10 Millionen Euro

Hinsichtlich der Einstufung gibt es einige Spezialregelungen. So werden Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder öffentlichen Telekommunikationsnetzen, die mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen, sowie qualifizierte Vertrauensdiensteanbieter, Top Level Domain-Namenregister und DNS-Diensteanbieter unabhängig von deren Größe ebenfalls als besonders wichtige Einrichtung angesehen. Zudem finden auf einige Einrichtungen der Bundesverwaltung bestimmte Regelungen für besonders wichtige Einrichtungen Anwendung.

b) Registrierungspflicht

Besonders wichtige Einrichtungen und wichtige Einrichtungen, Betreiber kritischer Anlagen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, sich innerhalb von drei Monaten beim BSI unter Angabe von Name, Rechtsform, Handelsregisternummer, Anschrift und aktuellen Kontaktdaten (einschließlich E-Mail-Adressen, öffentliche IP-Adressbereiche und Telefonnummern), relevanten Sektoren und Auflistung der EU-Mitgliedstaaten, in denen die Dienste erbracht werden, zu registrieren.

c) Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Sowohl besonders wichtige als auch wichtige Einrichtungen sind verpflichtet, **geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen** zu ergreifen, um die **Risiken für die Sicherheit der Netz- und Informationssysteme zu beherrschen** und die **Auswirkungen von Sicherheitsvorfällen zu verhindern oder mög-**

lichst gering zu halten. Die **Sicherheit von Netz- und Informationssystemen** umfasst die Fähigkeit zur **Abwehr** von Ereignissen, die die **Verfügbarkeit, Integrität oder Vertraulichkeit von Daten oder Diensten beeinträchtigen** können. Bei den Maßnahmen sind der **Stand der Technik** und ggf. einschlägige europäische und internationale **Normen** zu berücksichtigen. Bei der **Bewertung der Verhältnismäßigkeit** dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen. Die Einhaltung dieser Verpflichtung ist durch die Einrichtungen zu dokumentieren.

Die **Risikomanagementmaßnahmen im Bereich der Cybersicherheit** müssen zumindest Folgendes umfassen:

- Konzepte in Bezug auf die **Risikoanalyse und Sicherheit für Informationssysteme**
- **Bewältigung von Sicherheitsvorfällen**
- Aufrechterhaltung des Betriebs, wie **Backup-Management** und **Wiederherstellung** nach einem Notfall, und Krisenmanagement
- **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Cybersicherheit
- Grundlegende Verfahren im Bereich der **Cyberhygiene** und **Schulungen im Bereich der Cybersicherheit**
- Konzepte und Verfahren für den **Einsatz von Kryptografie** und gegebenenfalls **Verschlüsselung**
- **Sicherheit des Personals**, Konzepte für die **Zugriffskontrolle** und Management von Anlagen
- Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Die **Bewältigung von Sicherheitsvorfällen** umfasst alle Maßnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon. Unter den Begriff der **„Cyberhygiene"** fallen z.B. Software- und Hardware-Updates, Passwortänderungen, Verwaltung neuer Installationen, Einschränkung von Zugriffskonten auf Administratorenebene und Datensicherung.

In sog. „Durchführungsrechtsakten" kann die EU-Kommission – ggf. sektorbezogen – **technische und methodische Anforderungen** an die Maßnahmen festlegen. Das Bundesinnenministerium kann diese Bestimmungen zudem durch eine Rechtsverordnung präzisieren und erweitern.

d) Sicherheit in der Lieferkette

Die Sicherheit in der Lieferkette ist ein besonderes Anliegen der NIS-2-Richtlinie. Hierzu müssen die wichtigen und besonders wichtigen Einrichtungen die spezifischen **Schwachstellen der einzelnen unmittelbaren Anbieter** sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter einschließlich der Sicherheit ihrer Entwicklungsprozesse berücksichtigen. Dies wird in der Praxis dazu führen, dass die betroffenen Unternehmen vor dem Abschluss von Vereinbarungen mit ihren Zulieferern und Dienstleistern eine **Due Diligence deren Cybersicherheit** durchführen und ihnen vertragliche Anforderungen an die Cybersicherheit wie Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen, Patchmanagement und Berücksichtigung von Empfehlungen des BSI in Bezug auf deren Produkte und Dienstleistungen auferlegen. Das Thema Cybersicherheit wird künftig also vermehrt **Gegenstand von Vertragsverhandlungen** zwischen wichtigen bzw. besonders wichtigen Einrichtungen und deren Lieferanten sein und in den Verträgen geregelt werden. Im Ergebnis werden **Verpflichtungen aus der NIS-2-Richtlinie daher mittelbar auch zahlreiche Unternehmen betreffen**, die zwar nicht unter den Anwendungsbereich der NIS-2-Richtlinie fallen, aber **Teil der Lieferkette** sind. In Bezug auf die **Sicherheit kritischer Lieferketten** sind zudem die Ergebnisse von durchgeführten koordinierten Risikobewertungen zu berücksichtigen.

e) Meldepflichten bei erheblichem Sicherheitsvorfall oder erheblicher Cyberbedrohung

Im Falle eines **erheblichen Sicherheitsvorfalls** sind besonders wichtige Einrichtungen und wichtige Einrichtungen zur Meldung gegenüber einer vom BSI und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichteten gemeinsamen Meldestelle verpflichtet. Dabei gilt ein **Sicherheitsvorfall als erheblich**, wenn er

- schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann, oder
- andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Folgende **Meldungen** sind abzugeben:

- **Frühwarnung** (im deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf als **„frühe Erstmeldung"** bezeichnet) unverzüglich, spätestens jedoch innerhalb von **24 Stunden** nach Kenntnisnahme, unter Angabe, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte

- **Meldung über den erheblichen Sicherheitsvorfall** unverzüglich, spätestens jedoch innerhalb von **72 Stunden** nach Kenntnisnahme unter Bestätigung bzw. Aktualisierung der Informationen der Frühwarnung und einer ersten Bewertung einschließlich Angaben zu Schweregrad, Auswirkungen und ggf. Kompromittierungsindikatoren (Indicators of Compromise)
- Auf Ersuchen des BSI **Zwischenmeldung** über relevante Statusaktualisierungen
- **Abschlussmeldung** (bzw. falls der Sicherheitsvorfall noch andauert **Fortschrittsmeldung**) spätestens ein Monat nach Übermittlung der Meldung mit folgenden Angaben:
    - **ausführliche Beschreibung des Sicherheitsvorfalls**, einschließlich seines Schweregrads und seiner Auswirkungen
    - Angaben zur **Art der Bedrohung** bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat
    - Angaben zu den getroffenen und laufenden **Abhilfemaßnahmen**
    - ggf. die **grenzüberschreitenden Auswirkungen** des Sicherheitsvorfalls
- Im Falle einer Fortschrittsmeldung ist die Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls vorzulegen

Im Fall einer Meldung einer Einrichtung übermittelt das BSI dieser unverzüglich, möglichst innerhalb von 24 Stunden, eine Eingangsbestätigung und auf Ersuchen Orientierungshilfen oder **operative Beratung zu Abhilfemaßnahmen**. Es kann auf Wunsch auch zusätzliche **technische Unterstützung** leisten.

Das BSI kann die Einrichtung anweisen, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten. Zudem kann das BSI selbst die **Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren**, falls eine diesbezüglich Sensibilisierung der Öffentlichkeit erforderlich ist oder die Offenlegung im öffentlichen Interesse liegt.

Besonders wichtige und wichtige Einrichtungen aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und Digitale Dienste müssen zudem die potenziell von einer **erheblichen Cyberbedrohung betroffenen Empfänger** ihrer Dienste hierüber und über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion hierauf ergreifen können, unterrichten.

Sowohl besonders wichtige und wichtige Einrichtungen als auch andere Unternehmen, die nicht unter die NIS-2-Richtlinie fallen, können auf **freiwilliger Basis Cyberbedrohungen und Beinahe-Vorfälle** an das BSI melden.

f) Billigungs-, Überwachungs- und Schulungspflicht für die Geschäftsleitung

Die Geschäftsleitung besonders wichtiger Einrichtungen und wichtiger Einrichtungen ist verpflichtet, die **Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen** und ihre **Umsetzung zu überwachen**. Sie muss zudem regelmäßig an **Schulungen**

teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben. Auch die übrigen Mitarbeitenden sollen regelmäßig an solchen Schulungen teilnehmen.

g) Besondere Anforderungen an Betreiber kritischer Anlagen

Betreiber kritischer Anlagen sollen nach dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf ähnlichen Anforderungen unterliegen, wie bislang KRITIS-Betreiber (vgl. oben Kapitel I.3.a). Sie sind bspw. zum **Einsatz von Systemen zur Angriffserkennung** verpflichtet.

h) Einsatz kritischer Komponenten

Auch die Regelungen zum Einsatz kritischer Komponenten aus dem IT-Sicherheitsgesetz 2.0 (vgl. oben Kapitel I.3.f) sollen nach dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf fortgeführt werden.

i) Verantwortlichkeit der Geschäftsleitung

Die Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen trägt die **zentrale Verantwortung für das Risikomanagement** und die **Umsetzung von Cybersicherheitsmaßnahmen**. Sie kann für Verstöße durch die betreffende Einrichtung verantwortlich gemacht werden. Zwar ist eine Delegation in Grenzen möglich, doch die **persönlich Letztverantwortung bleibt bei der Geschäftsleitung**. Geschäftsführer und Vorstände von Unternehmen, die unter die NIS-2-Richtline fallen, müssen also bei Verstößen gegen die gesetzlichen Anforderungen damit rechnen, **persönlich haftbar** gemacht zu werden. Dies betrifft insbesondere Schadensersatzansprüche des Unternehmens gegen sie, über die nach dem Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes unter gewissen Voraussetzungen noch nicht mal ein Vergleich wirksam ist. **Aufgrund der NIS-2-Richtlinie sind Mitglieder der Geschäftsleitung von besonders wichtigen und wichtigen Einrichtungen bei Verstößen gegen die IT-Governance erheblichen Ersatzansprüchen ausgesetzt.**

j) Aufsichts- und Durchsetzungsmaßnahmen

Die NIS-2-Richtlinie sieht einen umfassenden Katalog von **Aufsichts- und Durchsetzungsmaßnahmen** des BSI gegen besonders wichtige Einrichtungen vor, wie bspw. **Vor-Ort-Kontrollen**, externe Aufsichtsmaßnahmen, Stichprobenkontrollen, **Sicherheitsprüfungen**, **Sicherheitsscans** und Anforderung von Informationen zur Bewertung der ergriffenen Risikomanagementmaßnahmen. Gegenüber wichtigen Einrichtungen ist dieser Maßnahmenkatalog etwas abgeschwächt. Zudem kann das BSI gegenüber besonders wichtigen Einrichtungen **Maßnahmen zur Verhütung oder Behebung eines Cybersicherheitsvorfalls** oder eines festgestellten Mangels anordnen und eine Berichterstattung darüber verlangen.

k) Sanktionen
Der NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz-Entwurf sieht im Falle eines Verstoßes erhebliche Bußgelder vor. Die **Geldbußen** sollen bei **besonders wichtigen Einrichtungen** bis zu **10 Millionen Euro** oder **2 % des gesamten weltweiten Jahresumsatzes** des Unternehmens betragen, je nachdem, welcher Betrag höher ist. Bei **wichtigen Einrichtungen** sind die Höchstbeträge 7 Millionen Euro bzw. 1,4 % des gesamten weltweiten Jahresumsatzes des Unternehmens. Zudem können **Zwangsgelder bis zu 100.000 Euro** verhängt werden, um die Einstellung eines Verstoßes durchzusetzen.

5. Digital Operational Resilience Act (DORA)

Der Digital Operational Resilience Act (DORA) der Europäischen Union vom 14. Dezember 2022 beinhaltet einheitliche Anforderungen für die **digitale operationelle Resilienz im gesamten Finanzsektor, um diesen weniger anfällig für Cyberbedrohungen und IKT-Störungen zu machen**. Die Regelungen von DORA gehen bezüglich Finanzunternehmen der NIS-2-Richtlinie vor und gelten ab dem 17. Januar 2025 gegenüber diesen unmittelbar, sodass sich **Finanzunternehmen** wie bspw. Kredit- und Zahlungsinstitute, E-Geld-Institute und Versicherungsunternehmen bereits jetzt hierauf einstellen müssen. Aber auch **Dienstleister im Bereich der Informations- und Kommunikationstechnologie (IKT)** einschließlich Anbietern von Cloud-Computing-Diensten, Software und Rechenzentrumsleistungen werden von DORA erfasst, wobei IKT-Dienstleister, bei denen bspw. eine umfassende Betriebsstörung eine systemische Auswirkung auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen hat, als **„kritisch“** eingestuft werden können und dann einem strengen **Überwachungsrahmen** unterliegen. DORA wird durch Regelungen des sich noch im Entwurf befindlichen **Finanzmarktdigitalisierungsgesetzes** ergänzt.

Die **Anforderungen von DORA an Finanzunternehmen** umfassen insbesondere:

a) IKT-Risikomanagement
Die Leitungsorgane der Finanzunternehmen, d.h. Geschäftsführung bzw. Vorstand, nehmen beim IKT-Risikomanagement und der Gesamtstrategie für die digitale operationale Resilienz des Unternehmens eine zentrale und aktive Rolle ein. Ihnen obliegt die **Gesamtverantwortung für die Steuerung und Überwachung des IKT-Risikomanagements**. Hierunter fallen u.a.

- Einführung von Leitlinien, die darauf abzielen, hohe Standards in Bezug auf die **Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten** aufrechtzuerhalten
- Festlegung von klaren Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene **Governance-Regelungen**

- Festlegung der **Strategie für digitale operationelle Resilienz** und einer angemessenen **Toleranzschwelle** für das IT-Risiko des Unternehmens
- Zuweisung angemessener **Budgetmittel**
- Regelmäßiges Absolvieren spezieller **Schulungen**
- Dokumentation und Überprüfung des IKT-Risikomanagementrahmens

IKT-Systeme müssen zuverlässig, mit ausreichenden Kapazitäten ausgestattet und technologisch resilient sein.

Ferner wird unter dem IKT-Risikomanagement verlangt, dass Finanzunternehmen kontinuierlich alle **Quellen für IKT-Risiken ermitteln** und **Cyberbedrohungen und IKT-Schwachstellen bewerten**. Sie müssen die Sicherheit und das Funktionieren der IKT-Systeme überwachen und kontrollieren und durch den **Einsatz angemessener Sicherheitstools** und Verfahren die Auswirkungen von Risiken auf IKT-Systeme minimieren. Schließlich verlangt DORA, dass Finanzunternehmen über Mechanismen verfügen, um **anomale Aktivitäten** wie auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle umgehend zu **erkennen** und potenzielle Schwachstellen zu ermitteln. Auf Vorfälle muss rasch reagiert und es müssen Wiederherstellungsmaßnahmen vorgenommen werden. Auch sind Verfahren zum Backup und zur Wiederherstellung von Daten einzusetzen.

b) Meldung von schwerwiegenden IKT-bezogenen Vorfällen und erheblichen Cyberbedrohungen
Finanzunternehmen müssen sicherstellen, dass sie IKT-bezogene Vorfälle und erhebliche Cyberbedrohungen erkennen, behandeln und melden. Darunter fallen u.a. der Einsatz von Frühwarnindikatoren sowie Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend ihrer Priorität und Schwere. **Schwerwiegende IKT-bezogene Vorfälle** sind der zuständigen Behörde – in Deutschland ist dies die **Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)** – zu **melden**. **Erhebliche Cyberbedrohungen** können freiwillig gemeldet werden. Falls ein schwerwiegender IKT-bezogener Vorfall Auswirkungen auf die **finanziellen Interessen von Kunden** hat, sind auch diese unverzüglich zu unterrichten.

c) Tests der operationalen Resilienz
Finanzunternehmen müssen ein solides und umfassendes **Programm für das Testen der digitalen operationellen Resilienz** erstellen und umsetzen. Darunter fallen etwa **Schwachstellenbewertung** und -scans, Open-Source-Analysen, **Netzwerksicherheitsbewertungen**, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, **Leistungstests**, End-to-End-Tests und **Penetrationstests**. Die meisten Finanzunternehmen müssen zudem mindestens alle drei Jahre sog. **„Threat-Led Penetration Testing" (TLPT)** durchführen.

d) Management des IKT-Drittparteienrisikos
Finanzunternehmen sind verpflichtet, ihr IKT-Drittparteienrisiko zu managen. Das bedeutet, dass sie Art, Ausmaß, Komplexität und Relevanz ihrer **Abhängigkeiten von ihren IKT-Dienstleistern** und das **Risiko aus den vertraglichen Vereinbarungen** mit diesen berücksichtigen müssen. Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Erforderlich ist bereits vor Vertragsabschluss eine **Risikoanalyse** und eine **Due Diligence**. Die vertraglichen Vereinbarungen sind in einem **Informationsregister** zu erfassen, das der BaFin auf Verlangen vorzulegen ist.

Zudem legt DORA Anforderungen in Bezug auf bestimmte vertragliche Regelungen zwischen Finanzunternehmen und IKT-Dienstleistern fest, wie bspw. Auditrechte, Kündigungsregelungen, Exit-Strategien und Bestimmungen zur Datenmigration. Auch führt ein Katalog **wesentlicher Vertragsbestimmungen** auf, welche Regelungen in Vereinbarungen über die Nutzung von IKT-Dienstleistungen mindestens enthalten sein müssen, wie etwa zur Unterauftragsvergabe, zum Speicherort von Daten, zum Datenschutz, zur Unterstützung bei einem IKT-Vorfall und zu Service Levels, sodass ggf. entsprechende Anpassungen der Verträge erforderlich werden.

e) Sanktionen
Verstöße gegen DORA können zu verwaltungsrechtlichen Sanktionen einschließlich **Geldbußen** führen, die auch gegenüber Mitgliedern des Leitungsorgans (z.B. Geschäftsführer, Vorstand) oder anderen verantwortlichen Personen (z.B. IT-Leiter) auferlegt werden können. Das sich noch im Entwurf befindliche Finanzmarktdigitalisierungsgesetz sieht ein **Bußgeld bis zu 5 Millionen Euro** vor, wenn ein **schwerwiegender IKT-Sicherheitsvorfall** nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemeldet wird.

Nicht nur deshalb sondern auch wegen der Gesamtverantwortung der Geschäftsleitung für die Steuerung und Überwachung des IKT-Risikomanagements ist für Finanzunternehmen und betroffene IKT-Dienstleister die **fristgerechte Umsetzung und Einhaltung von DORA „Chefsache“**.

6. Cybersecurity Act

Mit dem „Rechtsakt zur Cybersicherheit“ – „Cybersecurity Act“ der EU vom 17. April 2019 soll die Abwehrfähigkeit der Europäischen Union gegen Cyberangriffe gestärkt werden. Der **Cybersecurity Act** regelt insbesondere:

- Einführung eines **EU-weiten Zertifizierungssystem für Cybersicherheit**, um sicherzustellen, dass zertifizierte Produkte, Dienste und Prozesse, 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, denn ein ausgestelltes **europäisches**

Cybersicherheitszertifikat wird in allen Mitgliedstaaten anerkannt. Nationale Behörde für die Cybersicherheitszertifizierung ist das BSI.

- **Stärkung der EU-Cybersicherheitsagentur ENISA**, die EU-Mitgliedstaaten bei der Vorbeugung gegen Cyberangriffe unterstützen soll.

7. Cyber Resilience Act

Der „Cyber Resilience Act" („Cyberresilienzgesetz") der EU, der vom Europäischen Parlament in erster Lesung am 12. März 2024 verabschiedet wurde, soll erstmalig horizontal geltende **Cybersicherheitsvoraussetzungen für nahezu alle vernetzten Produkte mit digitalen Elementen** schaffen, gleichwohl ob Hardware, Software oder eingebettete Systeme. Geregelt werden sollen das Inverkehrbringen solcher Produkte, grundlegende Anforderungen an deren Konzeption, Entwicklung und Herstellung sowie Pflichten der Wirtschaftsakteure in Bezug auf die Cybersicherheit dieser Produkte. Zudem soll der Cyber Resilience Act Anforderungen an die von den Herstellern festgelegten Verfahren zur **Behandlung von Schwachstellen** enthalten, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten.

8. 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 Sorgfaltspflicht die Erkennung und Bekämpfung von IT-Risiken umfasst. **Effektive Sicherungsmaßnahmen können demnach auch die Einrichtung eines IT-Sicherheitsbeauftragten umfassen.**

9. Maßnahmen zur Cybersicherheit und IT-Compliance

Nachfolgend werden einige **konkrete Maßnahmen zur Sicherstellung der Cybersicherheit 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 Cybersicherheit 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, Integrität 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 und VII.5), denn hier können die IT-Systeme des Unternehmens leichter angreifbar sein.

Der **Einsatz** entsprechender **Cybersecurity-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 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, zu manipulieren oder zu zerstören. Um APTs vorzubeugen, empfiehlt sich der Einsatz von **„eXtended Detection & Response" (XDR)**. Dabei handelt es sich um Lösungen für flexiblen Schutz vor individuellen Bedrohungen, mit der gezielte Angriffe auf Unternehmen erkannt und analysiert sowie Abwehrmechanismen angepasst werden können. XDR-Lösungen umfassen dabei einen konsolidierten und weitestgehend automatisierten Workflow, um schnellstmöglich auf oft einzigartige APTs und auch andere Angriffe zu reagieren. Hierbei geht es nicht nur darum, das aktuelle Problem zu bekämpfen, sondern auch dessen Ursache ***(root cause-Analyse)*** sowie Ausbreitungsweg im Netzwerk ***(lateral movement)*** zu ergründen, um mögliche Schwachstellen zu identifizieren. Die gewonnenen Erkenntnisse können zur individuellen Angriffsabwehr verwendet, oder – wie z.B. im Bereich KRITIS und unter der NIS-2-Verordnung gefordert (siehe Kapitel I.3.c und I.4.e) – an das BSI als Meldestelle für Cybersicherheit gemeldet werden. 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 Cybersicherheit 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 („eXtended Detection & Response")

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 **(„eXtended Detection & Response")**. 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 zehn Jahren am 14. Januar 2020 Support und Updates für Windows 7 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. Der IT-Grundschutz ist der bewährte Standard zum Aufbau eines **Information Security Management Systems (ISMS)** und hilft dabei, das Niveau der Informationssicherheit in einem Unternehmen anzuheben und aufrechtzuerhalten. Die Edition 2023 des IT-Grundschutz-Kompendiums enthält insgesamt 111 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 2001 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit und ist zum ISO-Standard 27001 kompatibel, der ähnlich strukturierte BSI-Standard 2002 etabliert drei Vorgehensweisen bei der Umsetzung des IT-Grundschutzes. Der BSI-Standard 2003 befasst sich mit der Risikoanalyse auf der Basis von IT-Grundschutz. Der modernisierte BSI-Standards 200-4 zeigt, wie sich ein **Business Continuity Management System (BCMS)** in der eigenen Institution aufbauen und etablieren lässt.

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 2001 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 https://www.isaca.org/resources/cobit).

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. **Cybersicherheit 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. Im Rundschreiben 05/2023 der BaFin vom 29. Juni 2023 werden diese Anforderungen konkretisiert und hierbei **Mindestanforderungen an das Risikomanagement (MaRisk)** aufgestellt. Die MaRisk umfassen insbesondere die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren. Banken und Finanzdienstleister müssen diese organisatorischen Pflichten beachten – insbesondere beim Outsourcing von IT-Leistungen. Zudem hat die BaFin die **„Bankaufsichtlichen Anforderungen an die IT" (BAIT)** veröffentlicht. Die BAIT geben einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Institute – insbesondere für das Management der IT-Ressourcen, das Informationsrisikomanagement und das Informationssicherheitsmanagement – vor, und präzisieren die Anforderungen des § 25b KWG. Für Zahlungs- und E-Geld-Institute gelten die an die BAIT angelehnten **„Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT)"** und für Versicherungen die ähnlichen **„Versicherungsaufsichtlichen Anforderungen an die IT" (VAIT)** der BaFin.

10. Haftung und Sanktionen bei Verstößen gegen Cybersicherheit und IT-Compliance

Bei Verstößen gegen Cybersicherheit 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.i), die NIS-2-Richtlinie (siehe Kapitel II.4.k) oder DORA (siehe Kapitel I.5.e) 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 Cybersicherheit. Die persönliche Verantwortlichkeit der Unternehmensleitung wird durch die NIS-2-Richtlinie noch verschärft (siehe Kapitel I.4.i).

e) Persönliche Haftung von Mitarbeitenden
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 Cybersicherheit, 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). Ein IT-Unternehmen darf einem Mitarbeiter, der als IT-Berater Zugang zu hochsensiblen Daten von Kunden hat, fristlos kündigen, wenn dieser eine bei einem Kunden erkannte Sicherheitslücke für eigene Zwecke ausnutzt, anstatt seinen Arbeitgeber und den Kunden darüber zu informieren (Urteil des Arbeitsgerichts Siegburg vom 15. Januar 2020 - Az. 3 Ca 1793/19). Auch die Installation und Nutzung von nicht zugelassener Software auf der Produktivumgebung ohne Genehmigung des Arbeitgebers kann wegen der damit verbundenen Gefährdung des Netzwerks einen wichtigen Grund für eine außerordentliche Kündigung darstellen (Urteil des Landesarbeitsgerichts Nürnberg vom 3. November 2020 - Az. 7 Sa 99/20).

Das **Ausspähen von Daten und der Angriff auf die IT-Infrastruktur von Unternehmen** können nach diversen Vorschriften strafbar sein (siehe Kapitel VIII). 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.

f) Weitere Konsequenzen

Zudem droht bei Verstößen gegen Cybersicherheit 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.

g) Praxisbeispiel zur Vorstandshaftung und Haftung des IT-Leiters

Ein Logistikunternehmen wickelt seine Kundenaufträge weitestgehend elektronisch über sein Online-Portal ab und führt die Warenauslieferung IT-gestützt durch. Der Chief Operating Officer (COO) hat als für die IT zuständiges Vorstandsmitglied den IT-Betrieb des Unternehmens auf den IT-Leiter delegiert.

Die Logistiksoftware zur Warenauslieferung wurde vor Jahren angeschafft und wird in der eingesetzten Version vom Hersteller nicht mehr unterstützt, da der Hersteller diese Version aufgrund „End of Life" (EOL) abgekündigt hat. Der IT-Leiter unterrichtet den COO, dass aufgrund des fehlenden Supports die Gefahr von Softwarefehlern besteht, und empfiehlt daher den Erwerb eines kostenpflichtigen Upgrades. Der COO lehnt dies ab, da für das Upgrade der Logistiksoftware kein Budget vorhanden sei und er zudem keine internen Ressourcen für dessen Installation bereitstellen möchte.

Bezüglich des Online-Portals ist ein Patch verfügbar, der eine erkannte Sicherheitslücke schließt. Allerdings würden durch den Patch einige Geschäftsprozesse beeinträchtigt. Der IT-Leiter trifft ohne Rücksprache mit dem COO und der Rechtsabteilung des Unternehmens die Entscheidung, den Patch nicht einzuspielen, denn zum einen will er auf die beeinträchtigten Geschäftsprozesse nicht verzichten, zum anderen rechnet er ohnehin damit, dass der COO ihm

die zusätzlichen internen Ressourcen zur Einspielung des Patches nicht gewähren wird.

Im Folgenden kommt es aufgrund eines Angriffs auf das Online-Portal zu einem mehrtägigen Ausfall und aufgrund der Fehler in der Logistiksoftware zu mehreren falschen Warenauslieferungen, die zur Stornierung von Kundenaufträgen führen. Der Angriff auf das Online-Portal hätte durch den Patch verhindert werden können, die Fehler in der Logistiksoftware wären im Upgrade nicht mehr enthalten gewesen.

A. Haftet der COO dem Unternehmen für die Schäden?

Bereits 1997 hat der Bundesgerichtshof (BGH, Az. II ZR 175/95) entschieden, dass dem Vorstand und damit in diesem Beispielsfall dem COO bei der Leitung der Geschäfte des Unternehmens ein weiter Handlungsspielraum zusteht. Es gilt die **„Business Judgment Rule"**: Der **COO haftet nicht**, wenn er bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der **Grundlage angemessener Information** zum **Wohle der Gesellschaft** zu handeln. Der BGH führt dies in o.g. Urteil wie folgt aus: „Eine Schadensersatzpflicht des Vorstands kann … erst in Betracht kommen, wenn die Grenzen, in denen sich ein von **Verantwortungsbewusstsein** getragenes, ausschließlich am **Unternehmenswohl** orientiertes, auf **sorgfältiger Ermittlung der Entscheidungsgrundlagen** beruhendes unternehmerisches Handeln bewegen muss, deutlich überschritten sind, die **Bereitschaft, unternehmerische Risiken einzugehen, in unverantwortlicher Weise überspannt** worden ist oder das Verhalten des Vorstands aus anderen Gründen als pflichtwidrig gelten muss."

Wichtig ist hierbei, ob der COO **ausreichende Informationen** eingeholt und eine **Risikoabwägung** vorgenommen hat. Damit die Business Judgment Rule Anwendung finden kann, muss eine **ausreichende Tatsachengrundlage** geschaffen worden sein. Eine entsprechende **Dokumentation** ist aus Nachweisgründen anzuraten. Hinsichtlich der fehlerhaften Logistiksoftware sind hierbei u.a. einerseits Budget- und Personalplanung, andererseits potenzielle Schäden aufgrund der Softwarefehler zu berücksichtigen. Eine Haftung des COO ist also durchaus denkbar, wenn er ohne nähere Risikoabwägung das Upgrade der Logistiksoftware von vornhinein aus Kostengründen abgelehnt hat, für seine Entscheidung keine ausreichende Tatsachengrundlage geschaffen hat, oder das mit der Entscheidung, kein Upgrade zu erwerben, verbundene Risiko in völlig unverantwortlicher Weise falsch beurteilt hat.

Doch auch in Bezug auf den nicht eingespielten Patch ist der COO möglicherweise wegen **Organisationsverschuldens** haftbar. Zwar kann er Aufgaben an eine nachgelagerte Ebene – hier an den IT-Leiter – delegieren, doch er unterliegt einer **Auswahl-, Einweisungs-, Überwachungs- und Aufsichtspflicht**. Aufgrund der Abhängigkeit des Unternehmens von einer funktionierenden IT ist **IT-Sicherheit Chefsache** und die hierfür zuständigen Fachleute wie der IT-Leiter müssen direkt an den Vorstand angebunden sein. So muss gewährleistet sein, dass der Vorstand umfassend informiert wird und ein Letztentscheidungsrecht hat.

Der IT-Leiter kann die an ihn delegierte Verantwortlichkeit an den COO zurückgeben, indem er diesen über Missstände informiert, über deren Beseitigung dann der COO zu entscheiden hat. Sollte der COO etwa die Tätigkeit des IT-Leiters nicht ausreichend überwacht, kein Reporting des IT-Leiters an den COO etabliert oder dem IT-Leiter gar mitgeteilt haben, dass generell keine internen Ressourcen zur Behebung von Sicherheitslücken bereitgestellt werden, kann er möglicherweise auch für den nicht eingespielten Patch haftbar gemacht werden.

B. Haftet der IT-Leiter dem Unternehmen für die Schäden?

Für einen Arbeitnehmer, der seinem Arbeitgeber einen Sach- oder Vermögensschaden zufügt, sieht das Gesetz keine besondere Entlastung vor. Das Bundesarbeitsgericht (BAG, Urteil vom 27. September 1994 – Az. GS 1/89 (A)) hat jedoch schon vor langer Zeit **Grundsätze für eine Haftungsbeschränkung** entwickelt:

- Voraussetzung für eine Haftungsbeschränkung ist, dass der Schaden durch eine **betriebliche Tätigkeit** verursacht wurde. Anders als nach der früheren Rechtsprechung ist unerheblich, ob die Tätigkeit „gefahrgeneigt" ist.

- Ob und in welchem **Umfang** ein Arbeitnehmer für Schäden aus einer **Pflichtverletzung** haftet, hängt insbesondere vom **Verschuldensgrad** ab:
  - Bei **Vorsatz** haftet der Arbeitnehmer in vollem Umfang
  - Bei **grober Fahrlässigkeit** besteht grundsätzlich eine volle Haftung des Arbeitnehmers, Haftungserleichterungen können nur in Ausnahmefällen gegeben sein
  - Bei **normaler Fahrlässigkeit** wird der Schaden zwischen Arbeitgeber und Arbeitnehmer geteilt
  - Bei **leichtester Fahrlässigkeit**, also bei einer nur geringen Sorgfaltspflichtverletzung oder einem verständlichen Versehen, besteht keine Haftung des Arbeitnehmers
- Nach § 254 BGB reduziert sich die Schadensersatzpflicht des Arbeitnehmers in dem Maße, in dem bei der Schadensentstehung ein **Verschulden des Arbeitgebers** mitgewirkt hat, was (hier) auch in einem sog. Organisationsverschulden (s.o.) bestehen kann.

- Bei der in Fahrlässigkeitsfällen stets gebotenen **Abwägung** sind insbesondere die Schadenshöhe, ein vom **Arbeitgeber einkalkuliertes Risiko**, eine Risikodeckung durch eine Versicherung, die **Stellung des Arbeitnehmers im Betrieb** und die Höhe der Vergütung des Arbeitnehmers zu berücksichtigen. Ferner können die persönlichen Verhältnisse des Arbeitnehmers und die Umstände des Arbeitsverhältnisses zu berücksichtigen sein, etwa die Dauer der Betriebszugehörigkeit, das Lebensalter, die Familienverhältnisse und das bisherige Verhalten.

Diese richterrechtlichen Grundsätze über die Haftungsbeschränkung der Arbeitnehmer sind einseitig zwingendes **Arbeitnehmerschutzrecht.** Von ihnen kann weder im Arbeitsvertrag noch durch Betriebsvereinbarung zu Lasten des Arbeitnehmers abgewichen werden.

Ob **leitende Angestellte** sich auf diese Grundsätze ebenfalls berufen können, ist in Rechtsprechung und Literatur noch nicht abschließend geklärt. In der Literatur wird eine beschränkte Haftung leitender Angestellter (entsprechend den vorgenannten Grundsätzen) überwiegend bejaht und mancher höchstrichterlichen Urteile kann man entnehmen, dass die Grundsätze der Haftungsprivilegierung – teils mit Einschränkungen – auch für leitende Angestellte gelten sollen, allerdings fehlt hierzu bislang gefestigte Rechtsprechung.

An diesen Maßstäben gemessen würde der **IT-Leiter** im Fall des nicht durchgeführten Upgrades der Logistiksoftware nicht haften, weil er den COO rechtzeitig, zutreffend und vollständig unterrichtet hat und ihm somit keine Pflichtverletzung vorwerfbar ist.

Bei dem nicht eingespielten Patch liegt die Sache jedoch anders. Hier hat der IT-Leiter seine **arbeitsvertragliche Pflicht**, die **Angelegenheit intern zu eskalieren** und den COO in Kenntnis zu setzen, schuldhaft verletzt. Da ihm insoweit wohl sogar grobe Fahrlässigkeit vorzuwerfen ist, haftet er für den eingetretenen Schaden grundsätzlich in vollem Umfang, falls nicht im Einzelfall besondere Umstände haftungsmindernd zu berücksichtigen sind; dies könnte im vorliegenden Fall etwa ein Organisationsverschulden seitens des Arbeitgebers sein.

Hinweis: Mit diesem hypothetischen Praxisbeispiel soll lediglich die Problematik der Vorstandshaftung und Haftung des IT-Leiters bei Softwarefehlern und IT-Sicherheitsvorfällen veranschaulicht werden. Es stellt weder eine Rechtsberatung noch eine Handlungsempfehlung dar. Jeder tatsächlich existente Fall ist anhand seines konkreten Sachverhalts individuell zu untersuchen und rechtlich zu würdigen.

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, Big Data-Anwendung und der Einsatz von KI sind aus datenschutzrechtlicher Sicht sorgfältig zu prüfen.

1. EU-Datenschutz-Grundverordnung

Das Datenschutzrecht wird durch die europaweit geltende EU-Datenschutz-Grundverordnung (DS-GVO) umfassend 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 beim Einsatz von Cookies von Drittanbietern 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.9.b) schützen und Betrug (wie z.B. durch Online-Skimming) verhindern. Weitere **Bedrohungsszenarien**, gegen die sich Unternehmen mittels Cybersicherheit-Lösungen 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 (z.B. Ransomware).

Bei der Abwehr solcher Angriffe werden forensische Verfahren wie **XDR („eXtended Detection and Response")** eingesetzt, bei denen aus den übermittelten Sensordaten der angeschlossenen Schutzprodukte wie bspw. E-Mail, Endpunkte, Server, Cloud-Workloads und Netzwerke des Unternehmens hinweg personenbezogene Daten etwa zu Art und Herkunft der Bedrohung, URL, IP-Adresse oder E-Mail-Adresse des Angreifers und des angegriffenen Endpunkts 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, wie also das **Spannungsverhältnis zwischen Datenschutz und IT-Sicherheit** zu lösen ist, wird nachfolgend in Unterabschnitt (xx) näher dargestellt.

(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, bleibt es dennoch für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Auftraggeber als Verantwortlicher muss nach Maßgabe des Art. 28 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.

Eine Auftragsverarbeitung ist dadurch gekennzeichnet, dass der Auftraggeber für die Verarbeitung der personenbezogenen Daten verantwortlich bleibt und der Auftragsverarbeiter seinen Weisungen unterliegt. Auch bei komplexen Anwendungen im Bereich der Cybersicherheit liegt in aller Regel eine **Auftragsverarbeitung** vor, so dass zwischen dem Kunden als datenschutzrechtlich Verantwortlichem und dem Anbieter der Cybersecurity-Lösung als Auftragsverarbeiter eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO – häufig als „Data Processing Addendum" bezeichnet – abzuschließen ist.

(XI) Technische und organisatorische Maßnahmen (TOM)
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 (TOM)** 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, Veränderung** oder **unbefugte Offenlegung** 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 wie auch aufgrund der Rechenschaftspflicht des Verantwortlichen 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 20 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, und zwar auch für einen entstanden **immateriellen Schaden**; hierzu hatte der Europäische Gerichtshof (EuGH) mit Urteil vom 4. Mai 2023 (Rs. C-300/21) entschieden, dass es nicht erforderlich ist, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat
- 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 Verbraucherschutzverbänden und Wettbewerbern
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 Verbraucherverbände (vzbv) und Meta (vormals Facebook) über das Vorliegen einer wirksamen datenschutzrechtlichen Einwilligung hat der Europäische Gerichtshof (EuGH) mit Urteil vom 28. April 2022 (Rs. C-319/20) die **Klagebefugnis von Verbraucherschutzverbänden** bejaht. Die Frage, ob auch Unternehmen Ansprüche gegen Mitbewerber wegen Verstößen gegen die DS-GVO unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken zustehen, liegt dem EuGH ebenfalls zur Entscheidung vor.

(XX) DSG-VO-Compliance beim Einsatz von Cybersicherheitslösungen
Für die Datenverarbeitung verantwortliche Unternehmen wie auch deren Auftragsverarbeiter sind **gesetzlich verpflichtet**, mittels **geeigneter technischer und organisatorischer Maßnahmen** sicherzustellen, dass die Verarbeitung personenbezogener Daten rechtmäßig und ein dem Risiko **angemessenes Schutzniveau** gewährleistet ist. Um ihrer Verpflichtung nachzukommen, die Vertraulichkeit und Integrität der Systeme, Dienste und personenbezogenen Daten zu wahren und Datenschutzverstöße wie etwa Datenlecks zu verhindern, werden Unternehmen in aller Regel **Cybersicherheitslösungen** wie bspw. **XDR („eXtended Detection and Response")** einsetzen. Allerdings werden im Rahmen der Bedrohungserkennung und Angriffsabwehr personenbezogene Daten, etwa zu Art und Herkunft der Bedrohung, URL, IP-Adresse oder E-Mail-Adresse des Angreifers, angegriffene Endpunkte sowie verdächtige Web-Aktivitäten von Nutzern oder verdächtige Dateien erhoben und für eine begrenzte Zeit gespeichert. Eine solche Datenverarbeitung muss ihrerseits dem **datenschutzrechtlichen Grundsatz der Rechtmäßigkeit der Datenverarbeitung** gerecht werden. Ob eine solche Erhebung und Verarbeitung personenbezogener Daten aus Gründen der Cybersicherheit 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 DSG-VO 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** besteht beispielsweise darin, 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 Speicherung personenbezogener Daten durch Cybersicherheitslösungen wie XDR 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.

Diesen Anforderungen werden Cybersicherheitslösungen wie XDR insbesondere dadurch gerecht, dass ein **mehrschichtiger Ansatz der Bedrohungserkennung** verfolgt wird, bei dem der Netzwerkdatenverkehr, E-Mails oder Dateien (z.B. ausführbare potenziell schädliche Dateitypen) des Unternehmens weitestgehend automatisiert und ohne menschliche Einfluss- und Kenntnisnahme auf Schadsoftware und Angriffe überprüft und analysiert werden und eine nähere individuelle Überprüfung lediglich von unbekannten Bedrohungen erfolgt, die durch autorisierte Sicherheitsverantwortliche des Kunden oder von Sicherheitsexperten im Auftrag des Kunden vorgenommen wird, und wenn soweit möglich lediglich Metadaten verarbeitet werden. Letztlich liegt es aber in der **Verantwortung des Kunden** als datenschutzrechtlich „Verantwortlicher", die Abwägung der Interessen des Unternehmens einerseits und der betroffenen Personen andererseits beim Einsatz von Cybersicherheitslösungen vorzunehmen.

Sofern im Rahmen der **IT-Compliance und Cybersicherheit** personenbezogene Daten im für die zur Bedrohungserkennung und Angriffsabwehr erforderlichen Umfang erhoben und verarbeitet werden, werden also die Interessen der betroffenen Personen meist nicht überwiegen, so dass eine solche Datenverarbeitung durch das Unternehmen **rechtmäßig** ist. Im Rahmen ihrer **Rechenschaftspflicht** müssen Unternehmen sowohl **geeignete technische und organisatorische Maßnahmen** zur Sicherstellung der Vertraulichkeit und Integrität der Systeme, Dienste und personenbezogenen Daten als auch die **Rechtmäßigkeit** der im Rahmen der Cybersecurity-Maßnahmen vorgenommenen Datenverarbeitung sicherstellen und dokumentieren.

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.

(XXI) 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/about/trust-center/privacy.html und https://success.trendmicro.com/dcx/s/data-collection-disclosure.

2. 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 über einen Rahmen** für **den freien Verkehr nicht-personenbezogener Daten in der EU**, 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.

3. Künstliche Intelligenz (KI)

Der Einsatz Künstlicher Intelligenz (KI), insbesondere von **generativen KI-Systemen** und **Large Language Models (LLM)** wie ChatGPT in Unternehmen hat zuletzt rapide zugenommen. Sofern beim Training oder der Nutzung von KI-Systemen personenbezogene Daten verwendet werden, sind die Anforderungen der DS-GVO zu beachten. Unternehmen, die KI-Systeme anwenden, müssen hierzu insbesondere prüfen:

- Auf welcher **Rechtsgrundlage** erfolgt die Datenverarbeitung, bspw. aufgrund Einwilligung oder Interessenabwägung
- Liegt eine **Auftragsverarbeitung** vor und – falls dem so ist – besteht eine Vereinbarung zur Auftragsverarbeitung mit dem Anbieter des KI-Systems
- Erfolgt eine **Übermittlung personenbezogener Daten in ein Drittland**, bspw. an einen in den USA ansässigen Anbieter des KI-Systems
- Sind geeignete **technische und organisatorische Maßnahmen** zum Schutz der personenbezogenen Daten getroffen
- Werden die betroffenen Personen über die Datenerhebung und -verarbeitung informiert
- Können die betroffenen Personen ihre Rechte wie bspw. auf Auskunft und Löschung geltend machen
- Sind die Anforderungen des Art. 22 DS-GVO an eine **automatisierte Entscheidung im Einzelfall** (einschließlich Profiling) einschlägig, weil eine solche automatisierte Entscheidung durch die KI beispielsweise in Zusammenhang mit Kunden- oder Supportanfragen vorgenommen wird
- Ist eine **Datenschutz-Folgenabschätzung** vorzunehmen

Derzeit prüfen die Datenschutzbehörden, ob die am Markt befindlichen Large Language Models grundsätzlich rechtmäßig sind. Das Bayerische Landesamt für Datenschutzaufsicht hat eine **Checkliste** mit Prüfkriterien nach der DS-GVO „Datenschutzkonforme Künstliche Intelligenz" (abrufbar unter www.lda.bayern.de/checkliste_ki) herausgegeben.

4. Datenübermittlung in ein Drittland, insbesondere in die USA

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, Japan und – in Folge des Brexit – das Vereinigte Königreich 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, die **Datenübermittlung in die USA** auf das sog. „EU-US-Datenschutzschild" (Privacy Shield) zu stützen. Der Europäische Gerichtshof (EuGH) erklärte jedoch mit seinem sog. **„Schrems II"-Urteil** vom 16. Juli 2020 (Rs. C-311/18) den **„Privacy Shield"-Beschluss für ungültig**. Er äußerte sich darüber hinaus auch zu den bisherigen **Standardvertragsklauseln**, welche für die Übermittlung von Daten an Auftragsverarbeiter außerhalb der EU genutzt werden können, und hielt diese zwar für grundsätzlich geeignet. Diese grundsätzliche Geeignetheit wird vom EuGH allerdings dadurch eingeschränkt, dass die Parteien auch bei vereinbarten Standardvertragsklauseln sicherstellen müssen, dass **wirksame Durchsetzungsmöglichkeiten für Betroffenenrechte** bestehen, und ggf. **zusätzliche technische, vertragliche und organisatorische Maßnahmen** vereinbart werden müssen.

Als Reaktion darauf hat die EU-Kommission am 4. Juni 2021 **neue Standardvertragsklauseln für den internationalen Datentransfer** beschlossen und dabei die Vorgaben aus dem „Schrems II"-Urteil berücksichtigt. Mit diesen Standardvertragsklauseln stellt die EU-Kommission ein übergreifendes Instrumentarium zur Verfügung, das eine breite Palette von Transferszenarien abdeckt. Sie bieten aufgrund eines modularen Ansatzes mehr Flexibilität bei komplexen Verarbeitungsketten sowie die Möglichkeit, dass die Klauseln auch mehr als zwei Parteien nutzen können. Sie sollen ein praktisches Werkzeug für die Einhaltung des „Schrems II"-Urteils darstellen, samt einer Übersicht der verschiedenen Maßnahmen, die Unternehmen ergreifen müssen, um diesem Urteil nachzukommen, sowie **Beispiele möglicher technischer und organisatorischer Maßnahmen wie Verschlüsselung und Pseudonymisierung**, die Unternehmen erforderlichenfalls ergreifen müssen. Die Parteien müssen zudem prüfen, ob Rechtsvorschriften des Bestimmungsdrittlandes den Datenimporteur an der Erfüllung seiner Pflichten aus den Standardvertragsklauseln hindern. Dies könnte etwa aufgrund von unverhältnismäßigen Offenlegungspflichten oder Zugangsmöglichkeiten öffentlicher Behörden zu den übermittelten personenbezogenen Daten der Fall sein. Aspekte, die hierbei zu berücksichtigen sind, sind u.a. die Art des Empfängers, der Zweck der Verarbeitung, Kategorien und Format der übermittelten personenbezogenen Daten und der Wirtschaftszweig, in dem die Übertragung erfolgt. Die Übermittlung von bspw. Metadaten in die USA ist hiernach weniger problematisch, als z.B. von Gesundheitsdaten. Zudem ist zu prüfen, ob Unternehmen **zusätzliche vertragliche, technische oder organisatorische Maßnahmen** während der Übermittlung und bei der Verarbeitung der personenbezogenen Daten im Bestimmungsland ergreifen müssen.

Zudem erleichtert der Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA vom 10. Juli 2023 (**„EU-US Data Privacy Framework"**) die Übermittlung personenbezogener Daten in die USA, allerdings nur hinsichtlich solcher US-Unternehmen, die auf der „Data Privacy Framework List" (DPF-Liste) des US-Department of Commerce gelistet sind. Zu diesem Zwecke können US-Unternehmen eine Selbstzertifizierung vornehmen, bei der sie sich zur Einhaltung detaillierter Datenschutzpflichten verpflichten müssen.

5. 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. Mit dem am 22. März 2018 durch den US-Kongress verabschiedeten **CLOUD Act (Clarifying Lawful Overseas Use of Data Act)** wurde jedoch 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 müssen daher US-Behörden Zugriff auch auf im Ausland wie etwa in der EU gespeicherte Benutzerdaten gewähren.**

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 bislang zwar z.B. das Vereinigte Königreich mit den USA ein Exekutivabkommen abgeschlossen hat, nicht aber Deutschland und die EU, ist davon auszugehen, dass solche Beschwerden bzgl. Deutschland erfolglos bleiben und **US-Anbieter von Internet-Diensten und Cloud-Lösungen aufgrund des CLOUD Acts auch solche Daten ihrer deutschen 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.

6. „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. 04 - 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 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.

III. Schutz von Geschäftsgeheimnissen

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) regelt den Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung. Besonders von Bedeutung sind die **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 bestehen zusätzliche Compliance-Anforderungen für Unternehmen, die ihr Know-How schützen wollen. Sie müssen insbesondere angemessene Geheimhaltungsmaßnahmen implementieren und dies im Streitfall auch nachweisen können, denn ohne solche Geheimhaltungsmaßnahmen fehlt es an einem Geschäftsgeheimnis und es besteht kein Unterlassungsanspruch im Falle dessen Nutzung durch Dritte. Nach einem Urteil des Oberlandesgerichts Hamm vom 15. September 2020 (Az. 4 U 177/19) bilden **branchenüblich Sicherheitsstandards** einen wichtigen Anhaltspunkt für die Angemessenheit von Geheimhaltungsmaßnahmen. Diese sind vergleichbar mit den in Kapitel I.9 beschriebenen **Maßnahmen zur Cybersicherheit** und den nach Art. 32 DS-GVO datenschutzrechtlich erforderlichen **technischen und organisatorischen Maßnahmen** und umfassen als Mindeststandards u.a. **Zugangs- und Zugriffsbeschränkungen auf „Need to know"-Basis** und **Schutz gegen Datenlecks („Data Leak Prevention") sowie das Schließen auftretender Datenlecks**. 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) und Industrial Internet of Things (IIoT)

Unter dem Schlagwort **„Internet of Things" (IoT)** („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. Mit dem stark vorangeschrittenen **Ausbau der Mobilfunknetze der 5. Generation (5G)** werden neue datenintensive IoT- und IIoT-Anwendungen möglich, wie die Optimierung von Fertigungsprozessen, Innovationen in der Telemedizin, Ausbau intelligenter Städte und sauberes Energiemanagement. IoT und IIoT ermöglicht zudem **Remote und Predictive Maintenance** von IT-Systemen und Maschinen.

Aus Sicht der **IT-Compliance und Cybersicherheit** sind in Bezug auf IoT und IIoT folgende Rechtsthemen hervorzuheben:

1. Rechte an Daten

IoT- bzw. IIoT-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 **Daten schutzfähig** sind, ist umstritten. Da ein Urheberrecht an maschinengenerierten Daten in der Regel nicht besteht, wird u.a. ein Datenbankherstellerrecht, ein eigentumsähnliches Recht an Daten, ein Know-How-Schutz nach dem Gesetz zum Schutz von Geschäftsgeheimnissen oder ein delikts- und strafrechtlicher Schutz von Daten diskutiert.

Mit der ab dem 12. September 2025 geltenden EU-Datenverordnung (**„Data Act"**) hat die EU Vorschriften zum **fairen Datenzugang** und zur **fairen Datennutzung** geschaffen. Hiernach müssen **vernetzte Produkte**, wie sie insbesondere bei IoT- bzw. IIoT-Anwendungen zum Einsatz kommen, so konzipiert und hergestellt werden, dass Nutzer – gleichwohl ob Unternehmen oder Verbraucher – auf die erzeugten Daten einfach und sicher zugreifen und diese verwenden und teilen können. Dateninhaber ist in der Regel das Unternehmen, das das vernetzte Produkt herstellt oder einen damit verbundenen Dienst anbietet. Nutzer des Produkts können auf die Daten zuzugreifen, die sie durch ihre Nutzung des vernetzten Produkts oder eines damit verbundenen Dienstes generieren.

Erwähnenswert ist in diesem Zusammenhang auch die EU-Richtlinie 2019/770 vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, die mit Wirkung zum 1. Januar 2022 in deutsches Recht umgesetzt wurde. 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 bzw. digitalen Dienstleistungen oder die Rechtsmängelhaftung, doch wird hierdurch der **hohe wirtschaftliche Wert von personenbezogenen Daten** anerkannt, die als Alternative zur monetären Gegenleistung für die Bereitstellung der digitalen Inhalte oder digitalen Dienstleistungen 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- bzw. IIoT-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.2 verwiesen. Zudem ist die **IT-Sicherheit** der IoT- bzw. IIoT-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- bzw. IIoT-Anwendung oder deren Datenquellen als auch zum **Schutz der durch die Smart Objects gesammelten und in der Cloud gespeicherten Daten**. Hersteller von IoT- bzw. IIoT-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. Weitere Maßnahmen zur IT-Sicherheit von IoT- bzw. IIoT-Anwendungen sind bspw. **Netzwerksegmentierung, Zugangskontrolle der Remote-Zugänge und Restricted Data Flow**.

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. Mit Cloud Computing werden zahlreiche Vorteile wie Flexibilität, Skalierbarkeit und bessere Verfügbarkeit gegenüber beim Kunden selbst betriebener Software verbunden. Durch den Einsatz von Cloud Computing-Lösungen können Unternehmen Kosten für eigene lokale Infrastruktur einsparen und die Auslastung von Ressourcen besser steuern. Auch die Europäische Kommission verfolgt in ihrer Cloud-Strategie („European Commission Cloud Strategy, Cloud as an enabler for the European Commission Digital Strategy" vom 16. Mai 2019) einen „Cloud-first"-Ansatz, der bedeutet, dass jede Neuentwicklung vorzugsweise cloud-nativ, also auf Grundlage cloud-basierter IT-Dienste sein sollte, und dass Systeme so konzipiert werden sollten, dass sie von den Vorteilen cloudbasierter Bereitstellungsmodelle profitieren können.

Cloud Computing führt allerdings zu gesteigerten Anforderungen sowohl in Bezug auf **Datenschutz**, da hierbei in der Regel personenbezogene Daten von Kunden an den Cloud-Anbieter übermittelt werden, als auch bezüglich der **Sicherheitsanforderungen** an die Nutzung externer Cloud-Dienste.

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 Cybersicherheit und IT-Compliance einhalten muss, sind Public Clouds hinsichtlich der vertraglichen Konditionen, des Datenschutzes 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 beispielsweise bestehende Datenbestände im Rechenzentrum, auf die jedoch Public Cloud-Dienste angewendet werden können.

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 Datensicherheit

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, mit dem der Kunde eine **Vereinbarung zur Auftragsverarbeitung** gem. Art. 28 DS-GVO schließt und der ausreichende **technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten** getroffen hat.

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 (siehe hierzu oben Kapitel II.4). 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.
- Es besteht die Gefahr der Überwachung durch Geheimdienste und Sicherheitsbehörden, die beim Cloud Provider auf Kundendaten zugreifen. Insbesondere bei US-amerikanischen Cloud Providern besteht solch ein Risiko, da – wie im Kapitel II.5 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.

3. Sicherheitsanforderungen an Cloud-Dienste

Aufgrund der Anforderungen an die Verfügbarkeit von Cloud-Diensten und in Abhängigkeit vom Schutzbedarf der zu verarbeitenden Daten nimmt die Cybersicherheit von Cloud-Diensten eine zunehmend zentrale Rolle ein.

Nach § 8 Abs. 1 BSIG legt das BSI **Mindeststandards** für die Sicherheit der Informationstechnik des Bundes fest, was bzgl. der Nutzung externer Cloud-Dienste durch

den Mindeststandard vom 15. Dezember 2022 (Version 2.1, abrufbar unter https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html) erfolgt ist. Hiernach müssen die unter § 8 Abs. 1 BSIG fallenden Stellen und Einrichtungen des Bundes mindestens die Umsetzung und Einhaltung der **Basiskriterien nach dem Kriterienkatalog C5** (Cloud Computing Compliance Criteria Catalogue) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.

4. Kriterienkatalog C5 und C5-Testat

Da Cloud Computing in den letzten Jahren stetig zugenommen hat und in vielen Bereichen zum Standard geworden ist, sieht es das BSI als seine Aufgabe an, sowohl Anbietern wie auch Anwendern Hilfen an die Hand zu geben, sodass Cloud Computing sicher angeboten und genutzt werden kann. Eine dieser Anwendungshilfen ist der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue). Er wurde 2016 erstmalig durch das BSI veröffentlicht, 2019 grundlegend überarbeitet und als neue Version „C5:2020" im Januar 2020 fertiggestellt (abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html). Der **Kriterienkatalog C5 spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, deren Prüfer und Kunden**. Er stellt für Cloud-Kunden eine **wichtige Orientierung** für die Auswahl eines Cloud-Anbieters dar und bildet die **Grundlage**, um ein **kundeneigenes Risikomanagement** durchführen zu können.

Der Kriterienkatalog C5 definiert „Cloud-Dienst" wie folgt: „Im Rahmen von Cloud Computing angebotenen Dienstleistung der Informationstechnik. Dies beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software." Er enthält Kriterien zur Informationssicherheit von Cloud-Diensten aus insgesamt 17 Bereichen wie Organisation der Informationssicherheit, physische Sicherheit, Identitäts- und Berechtigungsmanagement, Kryptographie und Schlüsselmanagement, Umgang mit Sicherheitsvorfällen, Business Continuity Management und Compliance, die ein umfassendes Spektrum an Cloud-Sicherheits- und Ausfallsicherheitsfunktionen abdecken. Die Kriterien gliedern sich ihrerseits in Basiskriterien und Zusatzkriterien, wobei die **Basiskriterien** aus Sicht des BSI das **Niveau an Informationssicherheit widerspiegeln, das ein Cloud-Dienst mindestens bieten muss**, wenn Cloud-Kunden mit diesem Informationen verarbeiten, die einen normalen Schutzbedarf haben. **Die Basiskriterien bilden den Mindestumfang einer Prüfung nach dem Kriterienkatalog C5 ab.** Die Zusatzkriterien stellen im Falle eines höheren Schutzbedarf einen Ausgangs- bzw. Ansatzpunkt für die Bewertung dar.

Der Nachweis der Konformität mit den C5-Kriterien, d.h. die Erteilung des **C5-Testats**, muss durch einen **unabhängigen und sachverständigen Wirtschaftsprüfer** unter Anwendung national und international etablierter Prüfungsstandards erfolgen. Der Wirtschaftsprüfer

erbringt seine Tätigkeit gegenüber dem Cloud-Anbieter, nicht gegenüber dem Kunden des Anbieters.

Trend Micro hat erstmals 2023 das Testat nach den Kriterien des C5:2020-Standards (Cloud Computing Compliance Criteria Catalogue) erhalten, das u.a. **Trend Micro Vision One** umfasst. Die unabhängige Prüfung nach dem Kriterienkatalog C5 wurde von der Wirtschaftsprüfungsgesellschaft Deloitte & Touche, Taiwan, durchgeführt und der Prüfungsbericht wird Kunden von Trend Micro auf Anfrage zur Verfügung gestellt.

5. Risikomanagement des Kunden

Das C5-Testat bietet Kunden eine wichtige Orientierung für die Auswahl eines Cloud-Anbieters. Allerdings muss der Kunde weiterhin ein **kundeneigenes Risikomanagement** durchführen, wenn er einen Cloud-Dienst anwenden möchte. Auf Grundlage des C5-Prüfungsberichts können sich Kunden ein angemessenes Bild von der Informationssicherheit des Cloud-Dienstes einschließlich der angewandten Grundsätze, Verfahren und Maßnahmen verschaffen. Dies soll dem Kunden ermöglichen, die **Eignung des Cloud-Dienstes für seinen Anwendungsfall zu beurteilen**, und es ihm erleichtern, mehrerer Cloud-Anbieter bzw. Cloud-Dienste, für die ein C5-Bericht ausgestellt wurde, zu vergleichen. Potenzielle Cloud-Kunden sollten ihre Entscheidung nicht nur auf eine vorhandene, aktuelle Berichterstattung nach diesem Kriterienkatalog gründen (unabhängig, ob diese sich auf die Basis- oder Zusatzkriterien bezieht), sondern sollten sich die Berichterstattung des Wirtschaftsprüfers vom Cloud-Anbieter regelmäßig vorlegen lassen und diese für ihren Anwendungsfall bewerten.

Die Kunden müssen zudem den **Mitwirkungspflichten** in ihrem Verantwortungsbereich nachkommen. Hierbei sind **korrespondierende Kriterien für Kunden** zu berücksichtigen, denn die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes obliegt nicht alleine dem Cloud-Anbieter. Die korrespondierenden Kriterien für Cloud-Kunden dienen dazu, aufzuzeigen, wo potenziell Mitwirkungspflichten bestehen und an welchen Stellen Cloud-Kunden eigene Maßnahmen entwickeln müssen, um die Sicherheit des Cloud-Dienstes zu gewährleisten. Es handelt sich dabei allerdings um keine abschließende und allgemein gültige Aufstellung.

VI. IT-Grundrecht und Schutz der Persönlichkeit

Der Schutz der Persönlichkeit und des Privatlebens ist durch mehrere verfassungsgerichtliche Entscheidungen geprägt , 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. 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**.

2. Urteile des Bundesverfassungsgerichts zum Grundrechtsschutz dynamischer IP-Adressen

Nach zwei Beschlüssen des Bundesverfassungsgerichts vom 24. Januar 2012 (Az. 1 BvR 1299/05) und 27. Mai 2020 (Az. 1 BvR 1873/13, 1 BvR 2618/13) fallen dynamische IP-Adressen unter das Telekommunikationsgeheimnis und genießen somit Grundrechtsschutz. **Damit ist äußerste Zurückhaltung angebracht, über dynamische IP-Adressen einzelne Nutzer zu identifizieren.**

3. Urteile des Europäischen Gerichtshofs zur Vorratsdatenspeicherung

Sowohl eine europäische Richtlinie als auch das Telekommunikationsgesetz 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 auf Vorrat zu speichern.

Der **Europäische Gerichtshof** hatte mit Urteil vom 8. April 2014 (Rs. C-293/12 und Rs. C-594/12) entschieden, dass 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.

Hinsichtlich der im deutschen **Telekommunikationsgesetz** (§§ 175 ff. TKG) geregelten **Pflicht zur Vorratsspeicherung von Verkehrsdaten** hat der Europäische Gerichtshof am 20. September 2022 (Rs. C-793/19 und Rs. C-794/19) entschieden, dass das EU-Recht nationalen Rechtsvorschriften entgegensteht, die präventiv zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen. Infolge dieses Urteils des EuGH hat das Bundesverwaltungsgericht (Urteile vom 14. August 2023, Az. 6 C 6.22 und 6 C 7.22) die **Regelungen des Telekommunikationsgesetz zur Vorratsdatenspeicherung von Verkehrsdaten für rechtswidrig** erklärt.

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 Verpflichtung** 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 Anbieter von geschäftsmäßig angebotenen Telemedien haben zudem **angemessene technische IT-Sicherheitsmaßnahmen** zu etablieren, zu denen auch als **sicher anerkannte Verschlüsselungsverfahren** zählen. Der **Einsatz von E-Mail-Verschlüsselung** ist somit für Unternehmen, Kaufleute, Behörden und Selbstständige in vielen Bereichen **rechtlich zwingend** geboten. Dies gilt zumindest für die **Transportverschlüsselung**, die die meisten E-Mail-Anbieter standardmäßig anbieten. Ob auch eine **Ende-zu-Ende-Verschlüsselung** notwendig ist, deren Implementierung aufwändiger ist, hängt nach einem Urteil des Verwaltungsgerichts Mainz vom 17. Dezember 2020 (Az. 1 K 778/19.MZ) davon ab, ob Daten übermittelt werden, die als besonders risikoreich einzustufen sind, was im Rahmen einer einzelfallbezogenen Betrachtung zu ermitteln ist. Ähnlich hat das Oberlandesgericht Karlsruhe mit Urteil vom 27. Juli 2023 (Az. 19 U 83/22) entschieden. Hiernach gibt es keine gesetzlichen Vorgaben für Sicherheitsvorkehrungen beim Versand von E-Mails im geschäftlichen Verkehr, sodass sich **Art und Umfang der erforderlichen Sicherheitsvorkehrungen nach den berechtigten Sicherheitserwartungen** des maßgeblichen Verkehrs unter Berücksichtigung der Zumutbarkeit bestimmen.

Eine Ende-zu-Ende-Verschlüsselung ist hiernach nur dann erforderlich, wenn an die versendeten Daten erhöhte Sicherheitsanforderungen zu stellen sind, wie das etwa bei **Geschäfts- und Betriebsgeheimnissen** der Fall ist. 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 Überweisung 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** – dem **eIDAS-Durchführungsgesetz** und dem **Vertrauensdienstegesetz (VDG)** 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 überwiegender Meinung der **Arbeitgeber** als **Diensteanbieter** im Sinne des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) anzusehen. Werden erlaubte private und betriebliche Nutzung nicht technisch getrennt, ist die gesamte Nutzung als privat zu qualifizieren. Der Arbeitgeber ist nach § 3 TTDSG zur **Wahrung des Fernmeldegeheimnisses** verpflichtet und unterliegt den **datenschutzrechtlichen Anforderungen** der §§ 9 ff. TTDSG. 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 Arbeit-

nehmervertretung – 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 Individualgrundrechtes (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 **Strafbarkeit** 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 Mitarbeitern**, 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. Fraglich war jedoch, in welchem Umfang **Betreiber öffentlicher WLAN-Hotspots** für **Rechtsverletzungen der Nutzer haften**.

Der Europäische Gerichtshof hat hierzu mit Urteil vom 15. September 2016 (Rs. C-484/14) 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 hierauf wurde im Telemediengesetz (TMG) klargestellt, dass die Haftungsprivilegierung für sog. 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 **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 Cybersicherheit 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 § 165 Abs. 1 Satz 1 Telekommunikationsgesetz (TKG) müssen Anbieter von Telekommunikationsdiensten **angemessene 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 Cyberecurity**. 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. Home Office

Mit der COVID-19-Pandemie hat die Bedeutung der Home Office-Nutzung stark zugenommen und das Arbeiten von zu Hause oder von unterwegs ist seitdem in vielen Unternehmen gängige Praxis. Allerdings ist dies anfällig gegen Datenschutzverstöße und es besteht die Gefahr, dass der Schutz von Geschäftsgeheimnissen verletzt wird. Unternehmen sollten daher folgende **Anforderungen an die Home Office-Nutzung** berücksichtigen:

a) Cybersicherheit
Im Rahmen der IT-Sicherheit muss das Unternehmen geeignete **technische und organisatorische Maßnahmen (TOM)** treffen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit seiner IT-Systeme einschließlich der im Home Office eingesetzten Geräte und deren Anbindung sicherzustellen (siehe Kapitel II.1(xi)). Für Home Office-Anwendungen bedeutet das u.a. eine wirksame und aktuelle Cybersecurity-Lösung und den Einsatz geeigneter Sicherheitsmaßnahmen wie Passwortschutz, 2-Faktor-Authentifizierung und ein Virtual Private Network.

b) Lösungen für Web-Konferenzen
Anbieter von Web-Konferenzen müssen unter Berücksichtigung deren DS-GVO-Konformität und deren TOM sorgfältig ausgewählt werden und das Unternehmen muss mit ihnen eine Vereinbarung zur Auftragsverarbeitung schließen, die den Anforderungen des Art. 28 DS-GVO entspricht. Es müssen hierbei **sichere Lösungen** für Web-Konferenzen verwendet oder diese entsprechend konfiguriert werden, um zu vermeiden, dass bspw. nicht zugelassene oder unbekannte Personen daran teilnehmen.

c) Schutz von Geschäftsgeheimnissen
Aufgrund des Gesetzes zum Schutz von Geschäftsgeheimnissen müssen Geschäftsgeheimnisse „Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen" sein (siehe Kapitel III). Problematisch ist dies bspw. bei **Web-Konferenzen**, bei denen **Geschäftsgeheimnisse** Gegenstand sind, so dass der Teilnehmerkreis streng begrenzt sowie Aufzeichnung und Dokumentenaustausch unterbunden werden sollte. Zudem sollten externe Teilnehmer mittels einer Vertraulichkeitsvereinbarung bzw. eines Non Disclosure Agreement (NDA) zur Geheimhaltung verpflichtet werden.

Informationen sind nur auf „Need-to-Know-Basis" zu übermitteln. Unternehmen sollten daher die **Zugriffsrechte auf sensible Informationen** prüfen und ggf. anpassen. Gerade bei der Home Office-Nutzung besteht nämlich das Risiko, dass einmal abgerufene Informationen dauerhaft die Unternehmenssphäre verlassen, wenn sie von einem Mitarbeiter auf dessen eigenem Rechner lokal gespeichert werden. So hat das Oberlandesgericht Stuttgart am 19. November 2020 (Az. 2 U 575/19) entschieden, dass das Zulassen des Speicherns von Dateien mit Geschäftsgeheimnissen auf privaten Datenträgern als äußerst kritisch anzusehen ist, insbesondere wenn diese nicht passwortgeschützt sind.

d) Schulung der Mitarbeitenden

Schließlich müssen Mitarbeitende hinsichtlich der aufgrund der Home Office-Nutzung gestiegenen Risiken bzgl. **Datenschutz und Schutz von Geschäftsgeheimnissen sensibilisiert und geschult** werden. Arbeiten zu Hause birgt größere Risiken, dass unbefugte Dritte – hierzu gehören auch Familienmitglieder und Besucher – Unternehmensinformationen zur Kenntnis nehmen. Klare **Verhaltensanweisungen** wie z.B. Sperren des Rechners bei Verlassen des Arbeitsplatzes, laufende Aktualisierung des Antiviren-Schutzes und Überprüfung des Kamerafeldes vor Beginn einer Videokonferenz sind dringend zu empfehlen.

5. BYOD (Bring your own Device) / Consumerization

Mitarbeiter verwenden private Smartphones, um dienstliche E-Mails zu bearbeiten. Die VPN-Verbindung zum Firmenrechner aus dem Home Office erfolgt über den privaten Internet-Anschluss. Auf Tablets werden Browserspiele gespielt und zugleich Firmendaten abgerufen. Im privaten 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 Cybersicherheit, Datenschutz und Archivierungspflichten.

a) Cybersicherheit

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 Cybersicherheit auch im Bereich der Consumerization gerecht zu werden, sollten Unternehmen eine **Sicherheitsstrategie** entwickeln und **Cybersecurity-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 der Mitarbeiter 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 dieses Risikos 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.

6. 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, insbesondere wenn hierbei IP-Adressen der Nutzer erhoben oder verarbeitet werden. Abhängig von Art und Umfang der Nutzung sowie Zweck der Speicherung ist zumeist die Einwilligung des Nutzers erforderlich, oder er ist zumindest über die Erhebung und Verarbeitung 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 verlet-

zen, 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. Nach einem Beschluss des Bundesgerichtshofs vom 13. Mai 2020 (Az. 5 StR 614/19) macht sich auch ein **Administrator des Ausspähens von Daten** strafbar, wenn er auf Daten zugreift, obwohl ihm dies verboten war, sich aber aufgrund seiner Administratorenrechte unter Manipulation der Zugriffsberechtigungen Zugang dazu verschaffen konnte.

2. Verletzung des Fernmeldegeheimnisses

Gemäß § 3 TTDSG unterliegen 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. 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. Hinsichtlich der **Fernwartung aus dem Ausland** erscheint das Erfordernis eines vergleichbaren Schutzniveaus im Ausland weniger dringlich als beispielsweise bei einer physischen Verlagerung von Daten ins Ausland, weil diese meist nur in einem begrenzten Zeitfenster und zudem unter Zuhilfenahme von Verschlüsselungstechniken stattfindet, sodass eine Beschlagnahme durch ausländische staatliche Stellen üblicherweise nicht zu befürchten ist.

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. Auch **Denial of Service-Attacken** und sog. **DDoS-Attacken** (Distributed Denial of Service-Attacken) erfüllen den Tatbestand des § 303b StGB. 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 ist bis zu zwei Jahre Freiheitsstrafe.

7. Datenhehlerei

Nach § 202d StGB ist 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.

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

Stand: Mai 2024 – 8. Auflage

Dr. Thomas Stögmüller, LL.M. (Berkeley)

ist Rechtsanwalt, Fachanwalt für Informationstechnologierecht und Gründungspartner von TCI Rechtsanwälte München. Er hat in München und Berkeley studiert, in München promoviert und verfügt über einen Master of Laws (LL.M.)-Abschluss der University of California in Berkeley. Zunächst war er Jurist im Bayerischen Wirtschaftsministerium, seit 1998 ist er als Rechtsanwalt tätig. Er berät deutsche und internationale Unternehmen zu IT-, Cloud , Outsourcing- und Projektverträgen sowie in den Bereichen Cybersicherheit und IT-Compliance, Datenschutz, Künstliche Intelligenz (KI), E-Commerce, Telekommunikationsrecht, Urheberrecht und Kartellrecht. Zudem war er mehrmals als Schiedsrichter in Schiedsverfahren mit Bezug zum IT-Recht tätig. Es ist außerdem Lehrbeauftragter, Dozent und Autor zahlreicher juristischer Fachveröffentlichungen.

Über Trend Micro

Trend Micro, einer der weltweit führenden Anbieter von Cybersicherheit, hilft dabei, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Basierend auf jahrzehntelanger Sicherheitsexpertise, globaler Bedrohungsforschung und beständigen Innovationen schützt unsere Cybersecurity-Plattform hunderttausende Unternehmen und Millionen von Menschen über Clouds, Netzwerke, Geräte und Endpunkte hinweg.

Mit 7.000 Mitarbeitern in 65 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyberbedrohungen ermöglicht Trend Micro Unternehmen, ihre vernetzte Welt zu vereinfachen und zu schützen.
https://www.trendmicro.com/de_de/business.html

TREND MICRO™ | Global Leader in Cybersecurity

Trend Micro Deutschland GmbH · Parkring 29 · 85748 Garching
www.trendmicro.com