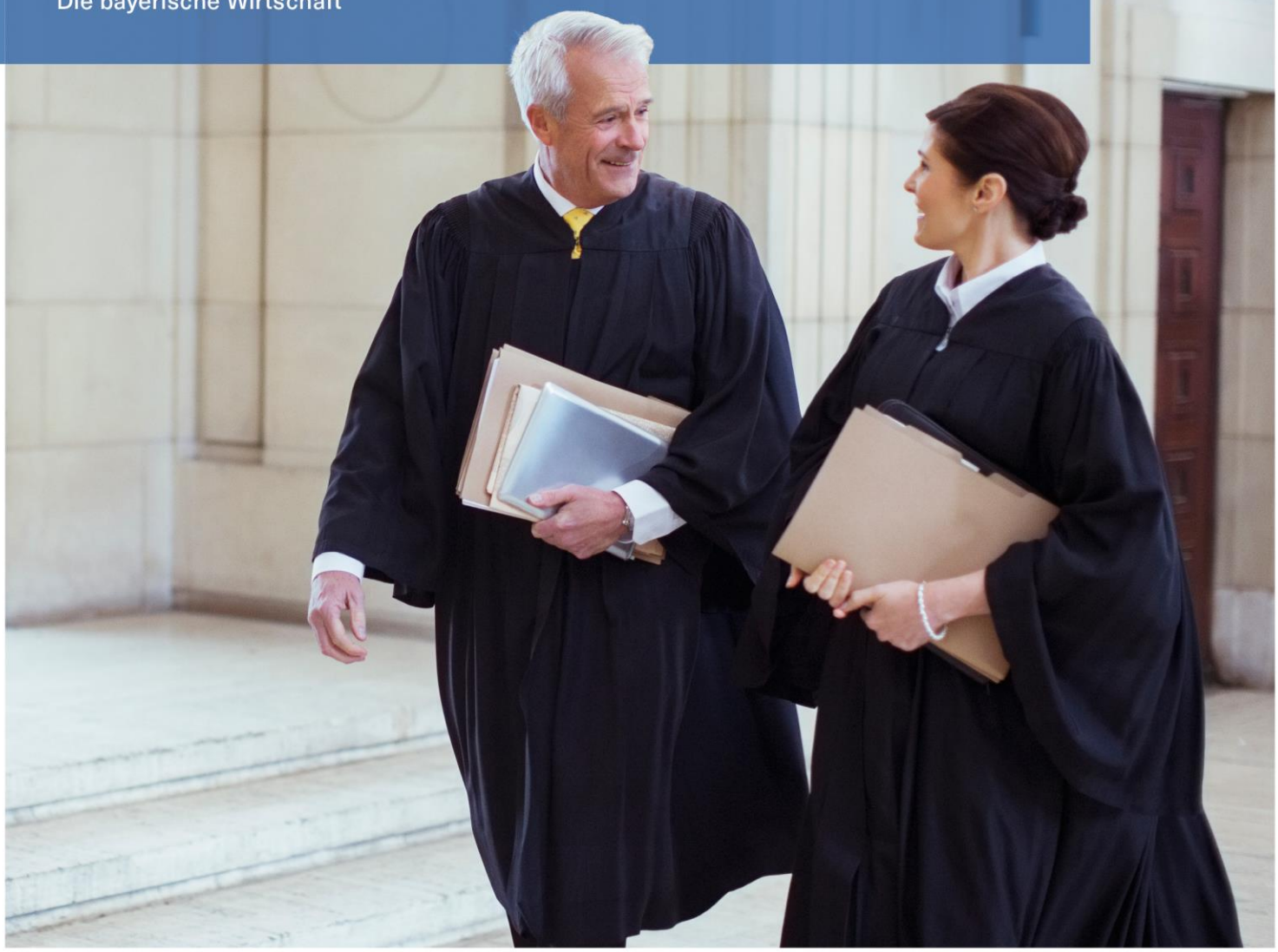
Recht

IT-Sicherheit als Rechtspflicht

vbw

Leitfaden
Stand: September 2023

Die bayerische Wirtschaft



Hinweis

Vorwort

Digitale Infrastrukturen sicher gestalten

In allen Lebensbereichen nimmt die Digitalisierung zu. Die Unternehmen steuern ihre Geschäftsprozesse mittlerweile weitgehend elektronisch und automatisieren ihre Abläufe zunehmend. Es ist daher unerlässlich, die digitalen Infrastrukturen gegen Angriffe von innen oder außen zu schützen, um die Risiken möglichst gering zu halten und wirtschaftliche Schäden zu vermeiden.

Der deutschen Wirtschaft ist im Jahr 2022 ein Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage entstanden. Nach dem aktuellen Bericht des Bundesamtes für Sicherheit in der Informationstechnik ist die Bedrohung im Cyber-Raum so hoch wie nie.

Unser Leitfaden erläutert die Grundlagen der IT-Sicherheit und zeigt Haftungsrisiken auf. Er berücksichtigt die aktuelle Rechtslage und geht insbesondere auf die Entwicklungen um die NIS-2-Richtlinie und ihre deutsche Umsetzung, den Entwurf des Cyberresilience-Acts, die Produkthaftungsrichtlinie sowie aktuelle EuGH-Rechtsprechung ein. Konkrete Handlungsempfehlungen geben praktische Hilfestellungen.

Bertram Brossardt
28. September 2023

Inhalt

1 Was ist IT-Sicherheit?

Einhaltung von Sicherheitsstandards

1.1 Begriffsbestimmung

IT-Sicherheit ist die Lebensader der digitalen Gesellschaft. Die zunehmende Digitalisierung aller Lebensbereiche (von E-Commerce und E-Business über E-Government und E-Health bis hin zu Smart Home, Smart Metering und Autonomen Fahren) setzt zwingend voraus, dass elektronisch gesteuerte Geschäftsprozesse, digitale Infrastrukturen und automatisierte Abläufe reibungslos funktionieren und gegenüber schädlichen Einflüssen von innen und außen hinreichend geschützt sind. So plausibel die überragende Bedeutung von IT-Sicherheit ist, so erstaunlich ist ihre Vernachlässigung in Politik und Rechtspraxis – auch wenn sich in den letzten Jahren einiges getan hat, sowohl auf europäischer, Bundes- und Landesebene. Gleichwohl gibt es bis heute keine einheitliche, umfassende Bestimmung des Begriffs der IT-Sicherheit, weder in der Rechtsprechung noch in der Literatur. Selbst das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) enthält keine grundlegende Begriffsbestimmung und Systematisierung.

Eng verwandt, wenngleich nicht identisch mit dem Begriff IT-Sicherheit, ist die Cyber-Sicherheit.[1] Insbesondere in letzter Zeit wird diese auf Seiten des europäischen Gesetz-gebers herangezogen, beispielsweise in Gestalt des Vorschlags für eine Verordnung „über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020“[2] oder der Richtlinie (EU) 2022/2555 vom 14. Dezember 2022 über „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)“.[3]

Auch der deutsche Gesetzgeber greift immer öfter auf diesen zurück, zuletzt beispielsweise mit der Cybersicherheitsstrategie für Deutschland 2021 oder der Cybersicherheitsagenda des BMI (2022).[4] Cybersicherheit stellt mehr auf den digitalen Raum („Cyberraum“) ab,[5] während IT-Sicherheit eher technisch und spezifisch im Hinblick auf das einzelne IT-System als solches verstanden wird.[6] Im allgemeinen Sprachgebrauch und auch dem der Techniker werden beide Begriffe allerdings häufig synonym verwendet.

Eine unionsrechtliche Definition für Cybersicherheit lässt sich den aktuellen VOen (EU) 2021/694, hier Art. 2 Nr. 9, und (EU) 2021/887, dort Art. 2 Nr. 1, entnehmen: Nach beiden

---

[1] Hornung/Schallbruch/Schallbruch, IT-Sicherheitsrecht, 2021, § 5 Rn. 6.
[2] COM/2022/454 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454).
[3] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555.
[4] https://www.bundesregierung.de/breg-de/suche/cybersicherheitsagenda-2060864, kritisch Kipker: „Kaffeesatzleserei im Namen der öffentlichen Sicherheit“ (https://community.beck.de/2022/07/12/neue-cybersicherheitsagenda-des-bmi-kaffeesatzleserei-im-namen-der-oeffentlichen-sicherheit).
[5] Kipker, in: Kipker, Cybersecurity, 2. Aufl. 2023 Kapitel 1 Rn. 4 versteht Cybersecurity als den generellen Oberbegriff.
[6] Hornung/Schallbruch/Schallbruch, IT-Sicherheitsrecht, 2021, § 5 Rn. 6.

meint Cybersicherheit „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen“.

Der Begriff der IT-Sicherheit wird hingegen zumeist anhand seiner Schutzkomponenten definiert. Einen ersten Anhaltspunkt zur Bestimmung der Schutzkomponenten der IT-Sicherheit bietet § 2 Abs. 2 BSIG,[7] der den Begriff der „Sicherheit in der Informations-technik“ legaldefiniert.

§ 2 Abs. 2 BSIG

„(2) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder

2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“

Neben den Schutzkomponenten der Verfügbarkeit, Unversehrtheit sowie Vertraulichkeit bedarf die Definition einer Erweiterung um die Komponente der Authentizität. Diese Erweiterung ist geboten, da durch IT-Sicherheit nicht nur die Unverfälschtheit des Datengehalts, sondern auch die Zurechenbarkeit der Informationen zu einem Kommunikationspartner gewährleistet werden soll (Authentizität).

Damit lässt sich der Begriff der IT-Sicherheit unter Zugrundelegung dieser Schutzkomponenten folgendermaßen definieren:

Definition der IT-Sicherheit

IT-Sicherheit ist gewährleistet, wenn die in einem informationstechnischen System hinterlegten Informationen verfügbar sind, und zwar einschränkend immer dann, wenn dies erforderlich (und vereinbart) ist [Zugänglichkeit/Verfügbarkeit], für jeden Nutzer, der hierzu berechtigt ist (und dies nachweist), und zwar nur für diesen [Vertraulichkeit] und mit genau dem Inhalt, den der Urheber geschaffen hat [Unversehrtheit/Integrität]. Zusätzlich müssen die Informationen jedem Urheber in dem Maße zurechenbar sein, in dem der

[7] Zukünftig in § 2 Abs. 1 Nr. 36 BSIG-E neu geregelt, vgl. https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/.

Zweck der Informationsverarbeitung diese Zurechnung fordert [Zurechenbarkeit/Authentizität].[8]

Die Schutzkomponenten der IT-Sicherheit, die zur Begriffsdefinition herangezogen werden, finden sich auch in § 8a Abs. 1 S. 1 BSIG wieder. Diese im Rahmen des IT-Sicherheitsgesetzes erfolgte Ergänzung des BSIG verpflichtet die Betreiber Kritischer Infrastrukturen zu angemessenen organisatorischen und technischen Vorkehrungen in Bezug auf die vier Schutzkomponenten der IT-Sicherheit. Auch in Erwägungsgrund 49 der DS-GVO finden sich diese vier Komponenten.

Aktuell ist der Begriff Kritische Infrastruktur noch die deutsche Übersetzung der Anforderungen aus der NIS-1-RL. Zukünftig (aus dem „alten" 8a BSIG wird § 39 BSIG-E) wird es begrifflich komplizierter: Was früher KRITIS war, wird durch das NIS-2-UmsetzungsG zu einer „kritischen Anlage" und liegt oberhalb der Anforderungen der mindestharmonisierenden NIS-2-RL.[9]

1.2 Schutzkomponenten der IT-Sicherheit

Die Schutzkomponenten der IT-Sicherheit – Verfügbarkeit, Unversehrtheit, Vertraulichkeit und Authentizität – sind nicht schon von sich heraus verständlich und bedürfen daher einer näheren Begriffsbestimmung.

1.2.1 Verfügbarkeit

Die Verfügbarkeit meint den Schutz vor Informationsverlust, Informationsentzug, Informationsblockade sowie Informationszerstörung. Allgemein meint die Verfügbarkeit damit, dass die Daten, Soft- und Hardware des IT-Systems grundsätzlich zugänglich sind, sobald und soweit dies im Rahmen bestimmter Zwecksetzungen erforderlich ist.

Die Komponente der Verfügbarkeit ist insofern grundlegende Voraussetzung der Gewährleistung der IT-Sicherheit, da alle anderen Schutzkomponenten – Integrität, Vertraulichkeit sowie Authentizität – zunächst einen autorisierten Datenzugriff voraussetzen. Man könnte auch sagen: Es geht um die Verfügbarkeit der richtigen Daten (Integrität) des wahren Urhebers (Authentizität) für den berechtigten Empfänger, und nur für diesen (Vertraulichkeit).

---

[8] Heckmann, in: Heckmann/Paschke, jurisPK Internetrecht, 7. Aufl. 2021, Kapitel 5 Rn. 307; Heckmann, K&R 2009, 1, 6; Heckmann, MMR 2006, 280 ff.
[9] Näheres hierzu bei Kipker/Dittrich, MMR 2023, 481 ff.

Praxistipp: Wie kann dieses Schutzziel erreicht werden?

Die Implementierung von Datensicherungen durch Backups oder auch die Nutzung von Ausweichrechenzentren können zur Sicherstellung der Verfügbarkeit beitragen („Redundanz“).

1.2.2 Unversehrtheit/Integrität

Die Unversehrtheit beziehungsweise Integrität als Element der IT-Sicherheit umfasst den Schutz vor jeglichen unbewussten, ungewollten oder nicht autorisierten Informations-veränderungen. Der Begriff der Integrität ist hierbei nicht lediglich auf Daten beschränkt, sondern erfasst auch das IT-System als solches. Nach den Ausführungen des BSI-Grundschutz-Katalogs meint die Integrität die inhaltliche Korrektheit (Unversehrtheit) von Daten und die korrekte Funktionsweise von Systemen. Integrität ist spätestens dann nicht mehr gegeben, wenn Informationen unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.[10]

Praxistipp: Wie kann dieses Schutzziel erreicht werden?

Die Integrität von Daten kann z. B. mittels elektronischer Signaturen sichergestellt werden. Selbst wenn eine Datenveränderung faktisch nicht verhindert werden kann, ist es wichtig, dass sie zumindest nicht unerkannt bleibt. Insoweit kann die Bildung von Hashwerten zur Zielerreichung beitragen, weil die Signaturprüfung bei Abweichung eines Hashwertes auf eine Manipulation beziehungsweise Datenveränderung hinweist.

1.2.3 Vertraulichkeit

Die Vertraulichkeit der Informationsverarbeitung ist gewahrt, wenn ein Informationszugriff durch Unberechtigte wirksam ausgeschlossen wird. Die Gewährleistung der Vertraulichkeit dient insbesondere dem Schutz vor Informationsausspähung. Lediglich befugten Personen soll der Zugriff auf die Daten erlaubt sein.

[10] BSI (Hrsg.), IT-Grundschutz-Kataloge, Band I, Abschnitt 4, S. 5.

Praxistipp: Wie kann dieses Schutzziel erreicht werden?

Dieses Schutzziel kann durch kryptographische Verfahren erreicht werden. Diese sorgen dafür, dass nur der Berechtigte die Informationen in den ursprünglichen Inhalt zurückverwandeln und verwenden kann.

Auch durch das Verstecken von Informationen (Steganographie) und die Verhinderung des Zugriffs auf Daten (Zugriffskontrolle) kann das Ziel der Vertraulichkeit gestärkt werden.

Vielfach kann ein vertraulicher Informationszugriff durch ein technisch und organisatorisch sicher konzipiertes Rollen-/Rechtemanagement erreicht werden.

1.2.4 Authentizität

Der Schutz vor Informationsentwertung wird durch die Schutzrichtung der Authentizität verfolgt. Die fehlende Zurechenbarkeit von Informationen an die Quellen oder bestimmte Personen führt zu einer Entwertung der Informationen. Insbesondere rechtsverbindliche Willenserklärungen sind unwirksam, wenn sie keinem Urheber zugeordnet werden können.

Praxistipp: Wie kann dieses Schutzziel erreicht werden?

Dieses Schutzziel kann durch die Verwendung fortgeschrittener (und erst recht qualifizierter) elektronischer Signaturen im elektronischen Rechtsverkehr erreicht werden. Durch Einsatz kryptographischer Verfahren kann dieses Schutzziel ebenfalls gefördert werden.

1.3 Zielkonflikte

1.3.1 Zielkonflikte innerhalb der Schutzkomponenten der IT-Sicherheit

Die vier anerkannten Schutzkomponenten der IT-Sicherheit stehen nicht isoliert nebeneinander, sondern beeinflussen sich gegenseitig. So sind sowohl Verstärkungen der Ziele als auch der teilweise Widerspruch zwischen den einzeln verfolgten Zielen möglich.

Beispielsweise konkurrieren die Ziele der Vertraulichkeit und der Authentizität hinsichtlich ihrer Zielerreichung miteinander. So wird durch eine Anonymisierung der Informationen zwar die Vertraulichkeit als Element des Rechts auf informationelle Selbstbestimmung gefördert, gleichwohl zugleich die Authentizität beeinträchtigt.

Auch Vertraulichkeit und Verfügbarkeit können gegebenenfalls in einen gewissen Widerspruch zueinander geraten, wenn die Maßnahmen zur Sicherstellung der Vertraulichkeit derart intensiv angesetzt werden, dass dadurch die dauernde und einfache Verfügbarkeit der Informationen in Mitleidenschaft gezogen wird.

Ähnliches sollte für Integrität und Verfügbarkeit gelten, wenn Maßnahmen zum Schutz vor Informationsveränderungen in einem die Verfügbarkeit beeinträchtigenden Umfang eingesetzt werden.

Im Gegensatz zu den Zielkonflikten sind aber auch Verstärkungen denkbar. So können beispielsweise Maßnahmen zur Erhöhung der Vertraulichkeit der Informationen zugleich die Integrität fördern und umgekehrt. Diese beiden Ziele sind damit grundsätzlich in der Lage sich gegenseitig zu verstärken.

Die Gewährleistung von IT-Sicherheit erfordert also auch eine angemessene Balance bei der Umsetzung ihrer Schutzziele.

1.3.2 Zielkonflikte mit anderen Zielen

Nicht außer Acht gelassen werden darf außerdem, dass nicht nur die vier anerkannten Ziele in Konfliktsituationen geraten können, sondern auch sog. nichttechnische Ziele, wie wirtschaftliche Erwägungen, Nutzerfreundlichkeit (Usability) und Akzeptanz den Zielen der IT-Sicherheit widersprechen können.

Auch der (im Aspekt der Vertraulichkeit bereits angelegte) Datenschutz als Ausprägung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG beziehungsweise Art. 7 f. GrCH kann in einen Konflikt mit IT-sicherheitsrechtlichen Maßnahmen kommen. Denn nicht jede Maßnahme, die die IT-Sicherheit fördert, stärkt zugleich den Datenschutz.

Beispielsweise kann die Speicherung aller Vorgänge an den Rechnern in einem Unternehmen zwar die IT-Sicherheit fördern, indem Schwachstellen schneller erkannt und Verhaltensweisen besser analysiert werden können. Allerdings stünde eine solche Totalüberwachung diametral den Grundsätzen des Datenschutzrechts entgegen.

Im Bereich der elektronischen Kommunikation sind Konflikte mit dem einfachgesetzlichen Fernmeldegeheimnis nach § 3 TTDSG[11] möglich, soweit der Verantwortliche in den Anwendungsbereich des TTDSG fällt. Die Kontrolle von Informationszugriffen kann, je nachdem wie intensiv die Überwachungsmaßnahme erfolgt, geschützte Interessen des Überwachten beeinträchtigen. Letztlich muss ein Unternehmen immer für einen angemessenen Interessenausgleich sorgen. Allerdings müssen IT-Sicherheit und Datenschutz wiederum

[11] Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (TTDSG).

zusammenwirken, um die Ziele der DS-GVO erreichen zu können. Denn ohne IT-Sicherheit drohen Verletzungen der Vertraulichkeit der Daten.

Auf europäischer Ebene soll dieser Konflikt dadurch gelöst werden, dass die Europäische Agentur für Netz- und Informationssicherheit (ENISA) die DS-GVO mit einbezieht. Dies soll dadurch geschehen, dass die ENISA die europäische Datenschutzbehörde bei deren Leitlinienerstellung berät, vor allem im Hinblick auf technische Details. ENISA soll darüber hinaus Meldungen zu Datenschutzverletzungen und Cybersicherheits-Attacken bündeln und Empfehlungen in beiden Bereichen abgeben.

2 IT-Sicherheitsrecht

Rechtsquellen

Ein einheitliches, umfassend reguliertes IT-Sicherheitsrecht besteht – wie eingangs erwähnt – nicht. Vielmehr finden sich die Regelungen zur IT-Sicherheit – auch für Unternehmen – in einer Vielzahl von Normen. Dabei lassen lediglich die neueren Regelungen auf den ersten Blick ihre IT-sicherheitsrechtliche Zielsetzung klar erkennen. Während man in den letzten Jahren stärker auf informelle und kooperative Strategien und damit ein Element der Freiwilligkeit gesetzt hatte, um IT-Sicherheit zu gewährleisten, ist nunmehr ein „Prozess der Institutionalisierung und Verrechtlichung im IT-Sicherheitsrecht im Gange“.[12]

2.1 Quellen des IT-Sicherheitsrechts

2.1.1 Europarechtliche und internationale Vorgaben

2.1.1.1 Allgemeine Vorgaben

Die allgemeinen Vorgaben zur IT-Sicherheit folgen im internationalen Bereich aus dem Sarbanes Oxley Act (SOX) und im europäischen Bereich aus dem EuroSOX, den Basel II und III-Abkommen sowie aus Solvency II.

2.1.1.1.1 Sarbanes Oxley Act (SOX)

Der Sarbanes Oxley Act (SOX) wurde in den USA im Jahre 2002 aufgrund spektakulärer Unternehmenszusammenbrüche erlassen. Der persönliche Anwendungsbereich des SOX umfasst US-amerikanische Unternehmen, die an der US-Börse notiert sind, sowie sog. „Foreign Issuers“, deren Papiere an der US-Börse gehandelt werden. Hauptsächlich bezweckt SOX die Verbesserung interner Kontrollen sowie die Förderung der Transparenz von Unternehmen. Unternehmenszusammenbrüche infolge fehlender Corporate Governance sollen verhindert werden. Dies hat auch Auswirkungen auf die IT-Sicherheit. In diesem Bereich erfordert SOX den Nachweis der Sicherheit der Datenverarbeitung und die Gewährleistung der Sicherheit der Kontrollprozesse der IT-Infrastruktur.[13]

[12] Wischmeyer, Informationssicherheit, 2023, S. 6.
[13] Conrad/Huppertz, in: Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 33 Rn. 323 ff.

2.1.1.1.2 EuroSOX

EuroSOX (RL 2006/43/EG) enthält im Wesentlichen ähnliche Vorgaben wie SOX. Hauptforderung des EuroSOX ist Transparenz für interne Kontroll- und Risiko-Management-Systeme.[14] Auch im Rahmen des EuroSOX – parallel zum SOX – liegt das Augenmerk auf der IT-Sicherheit und der Protokollierung der IT-Infrastruktur.[15] Diese Richtlinie wurde in das deutsche Recht durch das Gesetz zur Modernisierung des Bilanzrechts (BilMoG) umgesetzt.

2.1.1.1.3 Basel II und III-Abkommen

Das Basel II-Abkommen erlegt den Banken die Pflicht auf, dass sie vor der Vergabe von Krediten eine Risikoeinschätzung des kreditbegehrenden Unternehmens vornehmen. Dabei sind auch operationelle Risiken des Kreditnehmers zu berücksichtigen. Dies hat zur Folge, dass auch der IT-Sicherheitsstandard des Unternehmens eine Rolle für die Kreditvergabe seitens der Banken spielt.[16] Je schlechter die IT-Sicherheit des kreditbegehrenden Unternehmens zu bewerten ist, desto höhere Zinsen müssen von diesem Unternehmen verlangt werden, um die durch das Basel II-Abkommen verlangte erhöhte Eigenkapitalquote des Kreditgebers abzufedern.

Das Basel III-Abkommen, das 2007 als Reaktion auf die Wirtschaftskrise auf den Weg gebracht wurde, erhöht die Anforderungen an das Eigenkapital der Kreditinstitute. Diese Anforderungen weisen zwar keinen direkten IT-sicherheitsrechtlichen Bezug auf, begründen aber IT-sicherheitsrechtliche Folgewirkungen. Die Daten, die zur Bestimmung der Erreichung der Vorgaben des Basel III-Abkommens benötigt werden, müssen belastbar sein. Dies sind die Daten allerdings nur, wenn sie den Anforderungen der IT-Sicherheit genügen. Daher kann auch das Basel III-Abkommen als IT-sicherheitsrechtliche Regulierungsmaterie angesehen werden.

Die unter „Basel III: Finalising post-crisis reforms“ seit Dezember 2017 firmierenden Regeln des Baseler Ausschusses für Bankenaufsicht (im Bankenjargon teilweise als „Basel IV“ bezeichnet) sollen ab 2023 in nationales Recht umgesetzt werden Sie sind bislang noch nicht (vollständig) in die Kapitaladäquanzverordnung (CRR) und Eigenkapitalrichtlinie (CRD) eingeflossen. Im Oktober 2021 stellte die EU-Kommission einen Entwurf zur Umsetzung der neuen Regelungen in der EU vor. Hierzu soll insbesondere die CRR erneut angepasst werden, was aber erst für 2025 vorgesehen ist.

---

[14] Schlaghecke, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Auflage, 2016, § 43 Rn. 1 ff.
[15] Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Auflage, 2016, § 28 Rn. 48.
[16] Heckmann, MMR 2006, 280 (284); Conrad/Huppertz, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 33 Rn. 340 ff.; Schmidl/Tannen, in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 8 Corporate Governance und Compliance Rn. 16.

2.1.1.1.4 Solvency II

Das zum 01. Januar 2016 in vollem Umfang in Kraft getretene richtlinienbasierte Solvency II-Projekt stellt ähnliche Kriterien wie Basel II und III auf, allerdings für die Versicherungswirtschaft. Ebenso wie im Rahmen von Basel II und III hat dieses Regelwerk indirekten Einfluss auf die IT-Sicherheit. Die bestehende IT-Sicherheit und die IT-Sicherheitsrisiken fließen in die Bewertung der Unternehmen ein und haben Einfluss auf die konkreten Versicherungskonzepte.

Aktuell ist eine Überarbeitung der Solvency-II-Richtlinie in Vorbereitung, deren Abschluss noch nicht absehbar ist.[17]

2.1.1.2 Im Besonderen: Die IT-Sicherheitspolitik in der EU

2.1.1.2.1 Aktuelle Zuständigkeitsbereiche innerhalb der EU im Bereich der IT-Sicherheit

Primär fällt die IT-Sicherheit in die Zuständigkeit der Mitgliedstaaten. Die Rolle der EU beschränkt sich traditionell auf die Schaffung eines gemeinsamen Rahmens. Die aktuellen Zuständigkeitsbereiche innerhalb der EU betreffend die IT-Sicherheit ergeben sich aus dem folgenden Schaubild:

Abbildung 1
Cybersicherheit in der EU: Zuständigkeitsbereiche

Tabelle
Cybersicherheit in der EU: Zuständigkeitsbereiche

	Frieden, Sicherheit, Justiz	*Binnenmarkt*	*GSVP: Cyberverteidigung*	*GASP: Cyberdiplomatie*
EU	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT-Netzwerk CERT-EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU-Hybrid Fusion Cell ERCC
National	Exekutiv- und Datenschutzbehörden	Für die NIS zuständige Behörden Nationale CSIRTs	Verteidigungs-, Militär- und Sicherheitsbehörden	Außenministerien

Quelle: Bendiek, Die EU als Friedensmacht in der internationalen Cyberdiplomatie, SWP-Aktuell 22, S. 11 ff.

[17] https://www.gdv.de/gdv/themen/politik/solvency-ii-review-der-zeitplan-62866.

2.1.1.2.2 Cybersicherheitspolitik der EU-Kommission (bis 2020)

Um Cyberbedrohungen gerecht zu werden, verfolgt die EU-Kommission mit ihrer Cybersicherheitsstrategie einen Ansatz, der an drei Säulen anknüpft. Diese lassen sich mit drei Schlagworten – Stärkung der Cyberabwehrfähigkeit der EU, Schaffung eines EU-Rahmens zur wirksamen Abschreckung und Stärkung der internationalen Zusammenarbeit – beschreiben. Die neue Strategie „soll die EU in die Lage versetzen, diesen Bedrohungen wirksamer zu begegnen. Er soll einen Beitrag zur Erhöhung der Abwehrfähigkeit und der strategischen Autonomie sowie der technologischen Kapazitäten und Kompetenzen leisten und zudem den Aufbau eines soliden Binnenmarktes fördern.“

2.1.1.2.2.1 Stärkung der Cyberabwehrfähigkeit der EU

Die Stärkung der Cyberabwehrfähigkeit der Europäischen Union soll durch einen umfassenden gemeinsamen Ansatz erreicht werden. Die Kommission stellt insofern eingangs fest, dass es sich bei der Cybersicherheit um eine gesamtgesellschaftliche Herausforderung handelt. Die Einbindung mehrerer Ebenen der Regierung, der Wirtschaft und der Zivilgesellschaft ist hierfür von Nöten.

Die Cyberabwehrfähigkeit der Union soll nach den Vorstellungen der Kommission allem voran durch die Stärkung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), durch die Schaffung eines Binnenmarktes für Cybersicherheit, durch die vollständige Umsetzung der NIS-Richtlinie, durch die Einführung schneller Reaktionsmechanismen im Cyberangriffsfall, durch die Etablierung eines Netzes von Cybersicherheitskompetenzzentren samt eines Europäischen Kompetenzzentrums für Cybersicherheitsforschung sowie durch die individuelle Kompetenzstärkung der letztlich betroffenen Personen gefördert werden.

Als Hauptmaßnahmen listet die EU-Kommission zur Stärkung der Cyberabwehrfähigkeit folgenden Katalog:

Abbildung 2
Hauptmaßnahmen

Hauptmaßnahmen

- Vollständige Umsetzung der Richtlinie über die Sicherheit von Netz- und Informationssystemen;
- rasche Annahme der Verordnung über das neue Mandat der ENISA und einen europäischen Zertifizierungsrahmen durch das Europäische Parlament und den Rat[58];
- eine gemeinsame Initiative von Kommission und Wirtschaft zur Festlegung des Grundsatzes der „Sorgfaltspflicht" im Hinblick auf die Reduzierung von Produkt- oder Softwareschwachstellen und die Förderung der „konstruktiven Sicherheit";
- zügige Umsetzung des Konzeptentwurfs für eine grenzübergreifende Reaktion auf schwerwiegende Sicherheitsvorfälle;
- Einleitung einer Folgenabschätzung zur Untersuchung der Möglichkeit für einen von der Kommission 2018 vorzulegenden Vorschlag für den Aufbau eines Netzes von Cybersicherheitskompetenzzentren und eines Europäischen Kompetenzzentrums für Cybersicherheitsforschung;
- Unterstützung der Mitgliedstaaten bei der Ermittlung der Bereiche, in denen gemeinsame Cybersicherheitsprojekte für eine Förderung durch den Europäischen Verteidigungsfonds in Frage kommen;
- Einrichtung einer unionsweiten zentralen Anlaufstelle für Opfer von Cyberangriffen, die Informationen über die neuesten Bedrohungen zur Verfügung stellt sowie praktische Beratung und Werkzeuge für die Cybersicherheit anbietet;
- Maßnahmen der Mitgliedstaaten, die Cybersicherheit durchgängig in Bildungsprogramme, in elektronische Behördendienste und in Sensibilisierungskampagnen aufzunehmen;
- Maßnahmen der Wirtschaft, ihr Personal in Fragen der Cybersicherheit fortzubilden und das Konzept der „konstruktiven Sicherheit" auf ihre Produkte, Dienste und Prozesse anzuwenden.

Quelle: Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, 2017, S. 4.

2.1.1.2.2.2 Schaffung eines EU-Rahmens zur wirksamen Abschreckung

Flankiert wird die Stärkung der Cyberabwehrfähigkeit von der Schaffung eines EU-Rahmens zur wirksamen Abschreckung. Nach der Ansicht der Kommission ist „eine wirksamere Strafverfolgung mit Schwerpunkt auf Enttarnung, Rückverfolgbarkeit und Verfolgung von Cyberkriminellen (…) für eine wirksame Abschreckung von grundlegender Bedeutung."

Im Mittelpunkt der Maßnahmen soll dabei die Enttarnung, Rückverfolgbarkeit und Verfolgung etwaiger Cyberkrimineller stehen. Auch in diesem Bereich hat die Kommission einen Maßnahmenkatalog aufgestellt, den es im Folgenden darzustellen gilt. Im Bereich der Identifizierung krimineller Akteure im Internet setzt die Kommission darauf, dass der Standard IPv6 alsbald umfassend eingesetzt wird, da die Zuordnung einer IP-Adresse an einen Nutzer die Strafverfolgung deutlich erleichtert. Weiterhin soll die grenzüberschreitende Zusammenarbeit bei der Strafverfolgung insbesondere mit Blick auf den (grenzüberschreitenden) Zugang zu elektronischen Beweismitteln gestärkt werden. Darüber hinaus soll bei

der Strafverfolgung im Internet verstärkt der Schulterschluss mit dem privaten Sektor gesucht werden. Auf politischer Ebene sollen die Maßnahmen im Bereich der gemeinsamen Außen- und Sicherheitspolitik intensiviert werden, wobei zugleich die Cyberabwehrkompetenzen der einzelnen Mitgliedstaaten gestärkt werden sollen. Zusammenfassend sollen die folgenden Hauptmaßnahmen im Bereich der Abschreckung ergriffen werden:

Abbildung 3
Hauptmaßnahmen

Hauptmaßnahmen

- Initiative der Kommission für den grenzübergreifenden Zugang zu elektronischen Beweismitteln (Anfang 2018);
- rasche Annahme der vorgeschlagenen Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln durch das Europäische Parlament und den Rat;
- Einführung von Anforderungen in Bezug auf IPv6 bei der EU-Beschaffung, -Forschung und -Projektfinanzierung; freiwillige Vereinbarungen zwischen den Mitgliedstaaten und Internetdienstanbietern zur Förderung der Einführung von IPv6;
- neuer/erweiterter Schwerpunkt bei Europol auf Cyberforensik und Überwachung des Darknets;
- Umsetzung des Rahmens für eine gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten;
- Erhöhung der finanziellen Unterstützung für nationale und transnationale Projekte, die zur Verbesserung der Strafverfolgung im Cyberraum beitragen;
- Einrichtung einer Bildungsplattform für den Bereich der Cybersicherheit im Jahr 2018, um dem derzeitigen Kompetenzdefizit bei Cybersicherheit und Cyberabwehr zu begegnen.

Quelle: Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, 2017, S. 22.

2.1.1.2.2.3 Stärkung der internationalen Zusammenarbeit

Als dritte Säule der gesamtheitlichen Strategie sieht die Kommission die Stärkung der internationalen Zusammenarbeit in der Cybersicherheit vor.

Es sollen Kooperationen mit Drittländern aufgebaut, ausgebaut und gefestigt werden, um globalen Bedrohungen für die Cybersicherheit wirksam begegnen zu können. Neben dem Kompetenzausbau bei Drittländern soll die Zusammenarbeit mit der NATO im Bereich der Cyberabwehr vorangetrieben werden. Das fordert zwischenzeitlich auch das EU-Parlament.

In ihrem Maßnahmen-Katalog nennt die Kommission folgende Hauptmaßnahmen:

Abbildung 4
Hauptmaßnahmen

Hauptmaßnahmen

- Weiterentwicklung des strategischen Rahmens für Konfliktprävention und Stabilität im Cyberraum
- Aufbau eines neuen Netzwerks für den Kapazitätsaufbau, um Drittländer in ihrer Fähigkeit, Cyberbedrohungen entgegenzutreten, zu unterstützen, und Ausarbeitung von EU-Leitlinien für den Kapazitätsaufbau im Bereich Cybersicherheit, um die EU-Maßnahmen besser priorisieren zu können
- Ausweitung der Zusammenarbeit zwischen der EU und der NATO, u. a. Beteiligung an parallelen und koordinierten Übungen und bessere Interoperabilität bei den Cybersicherheitsstandards

Quelle: Kommission, Gemeinsame Mitteilung an das Europäische Parlament und den Rat – Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, 2017, S. 25.

2.1.1.2.3 Cybersicherheitspolitik der EU-Kommission (ab 2020)

Am 16. Dezember 2020 hat die Kommission die „Cybersicherheitsstrategie der EU für die digitale Dekade“ dem europäischen Parlament und dem europäischen Rat mitgeteilt.[18] Einleitend bezeichnet die Kommission Cybersicherheit als integralen Bestandteil der Sicherheit der Europäer. Des Weiteren wird ausgeführt, dass die Cybersicherheit von entscheidender Bedeutung sei, um ein resilientes, grünes und digitales Europa zu schaffen. Auch die Auswirkungen der Corona-Pandemie werden genannt. Als Problemfelder werden insbesondere geopolitische Spannungen, Kontrolle über die Technologien entlang der Lieferketten und böswillige Angriffe auf kritische Infrastrukturen sowie ein Mangel an Cybersicherheitskompetenz identifiziert.

Die Strategie ist auf zwei Säulen aufgeteilt: Schaffung eines offenen und globalen Internets einerseits und einheitliche Gewährleistung von Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU durch einheitliche, verbindliche Vorschriften andererseits.

Die erste Säule möchte ein offenes und globales Internet verwirklichen. Hierfür sieht sie drei Hauptinstrumente vor:

1. Resilienz, technologische Souveränität und Führungsrolle

Der Fokus liegt hier auf den kritischen Infrastrukturen und wesentlichen Diensten entlang der Lieferkette. Dies ist Gegenstand der sog. NIS-2-RL (vgl. hierzu die Ausführungen unter 2.1.1.3.4.), die wiederum als Grundlage für spezifische weitere Regelungen dient,

[18] JOIN (2020) 18 final.

beispielsweise einen „Netzkodex“. Allgemein werden die einzelnen kritischen Sektoren weiter reguliert.

Darüber hinaus ist der Aufbau eines europäischen Cyberschutzschilds vorgesehen, das sich als Netz von Sicherheitseinsatzzentren in der gesamten EU präsentieren soll. Auch eine extrem sichere Kommunikationsinfrastruktur in Gestalt einer Quantenkommunikationsinfrastruktur (QCI) soll geschaffen werden. Die 5G-Technik soll zeitnah ermöglicht werden. Das Internet der Dinge soll ein Internet der sicheren Dinge werden, insbesondere mittels transparenter Sicherheitslösungen, Zertifizierungen, neuer Sorgfaltspflichten für Hersteller vernetzter Geräte etc.

Weiterhin soll eine höhere globale Internetsicherheit erreicht werden, indem Notfallpläne im Falle einer Beeinträchtigung der Integrität und Verfügbarkeit des globalen DNS-Root-Systems erarbeitet werden; auch sollen ein öffentlicher europäischer DNS-Auflösungsdienst aufgebaut („DNS4EU“) sowie wichtige Internetstandards (IPv6) verbreitet werden. Die Anfälligkeit der technologischen Lieferkette soll gemindert werden, indem hier eine verstärkte Präsenz gezeigt wird; das CCCN (Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren) soll hier unterstützend miteinbezogen werden. Zuletzt bedarf es der verstärkten Ausbildung qualifizierter Cyberfachkräfte.

Abbildung 5
Strategische Initiativen

Strategische Initiativen

Die EU sollte für Folgendes sorgen:

- Verabschiedung der überarbeiteten NIS-Richtlinie;
- Regulierungsmaßnahmen für ein Internet der sicheren Dinge;
- öffentliche und private Investitionen von bis zu 4,5 Mrd. EUR im Zeitraum 2021–2027 mithilfe der CCCN-Investitionen in die Cybersicherheit (insbesondere im Rahmen der Programme Digitales Europa und Horizont Europa und der Aufbau- und Resilienzfazilität);
- Aufbau eines EU-Netzes KI-gestützter Sicherheitseinsatzzentren und einer extrem sicheren Kommunikationsinfrastruktur, die Quantentechnik nutzt;
- breite Einführung von Cybersicherheitstechnik durch eine gezielte Unterstützung von KMU im Rahmen der digitalen Innovationszentren;
- Entwicklung eines DNS-Auflösungsdienstes als sichere und offene Alternative für den Internetzugang der Bürger, Unternehmen und öffentlichen Verwaltungen in der EU;
- Abschluss der Umsetzung des 5G-Instrumentariums bis zum zweiten Quartal 2021 (siehe Anhang).

Quelle: Cybersicherheitsstrategie der EU für die digitale Dekade vom 16.12.20, JOIN(2020) 18 final

2. Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion

Weil aus Cybervorfällen enorme Schäden entstehen können, sind diese unter allen Umständen zu verhindern.

Hierfür soll eine gemeinsame Cyberstelle als virtuelle und physische Plattform für die Zusammenarbeit dienen, schwerpunktmäßig wäre die operative und technische Koordinierung bei schwerwiegenden grenzüberschreitenden Vorfällen betroffen. Dies soll insbesondere zwei Lücken ausmerzen, nämlich das bisherige Fehlen eines gemeinsamen Raums für eine strukturierte Zusammenarbeit und zweitens die bisher nicht mögliche Ausschöpfung des vollen Potenzials der Zusammenarbeit. Als zusätzliche eigenständige Einrichtung ist die Cyberstelle aber nicht gedacht. Die Umsetzung ist in Gestalt von vier Etappen geplant: Definieren, Vorbereiten, Einführen, Expandieren.

Ein Hauptaugenmerk liegt zurecht auf der Bekämpfung der Cyberkriminalität: Denn deren wirksame Bekämpfung ist Schlüsselfaktor für die Gewährleistung der Cybersicherheit. Daher soll die Strafverfolgung in diesem Bereich verbessert werden, insbesondere im Hinblick auf die Zusammenarbeit. Die Kapazitäten der Strafverfolgungsbehörden sollen hier erweitert und erhöht werden (Aktionsplan). Ferner sollen gemeinsame forensische Standards geschaffen werden. Als essentiell für die Erreichung dieses Ziels betrachtet die Kommission hier die richtige und vollständige Umsetzung der Richtlinien durch die Mitgliedstaaten. Ein „Paket zu elektronischen Beweismitteln“ soll die grenzüberschreitende Strafverfolgung erleichtern.

Das Instrumentarium für die Cyberdiplomatie soll durch die Einrichtung einer Arbeitsgruppe der Mitgliedstaaten für EU-Cybernachrichtendienste gestärkt werden. Der Hohe Vertreter der Union soll außerdem einen Vorschlag zur Cyberabschreckung vorlegen, hier insb. zum Schutz kritischer Infrastruktur sowie der Lieferketten. Allgemein soll die Abschreckung um weitere Maßnahmen ergänzt werden.

Auch die Cyberabwehr muss gestärkt werden. Daher hat eine Überprüfung des Rahmens für die Cyberabwehr zu erfolgen. Eine besonders wichtige Rolle spielt auch weiterhin das militärische CERT-Netz. Ganz allgemein soll in diesem Bereich die Forschung und Entwicklung vorangetrieben werden.

Abbildung 6
Strategische Initiativen

Die EU sollte

- den europäischen Rahmen für das Krisenmanagement im Bereich der Cybersicherheit vervollständigen und die Verfahren, die Etappenziele und den Zeitplan für die Einrichtung der gemeinsamen Cyberstelle festlegen;
- die Umsetzung der Agenda zur Bekämpfung der Cyberkriminalität im Rahmen der Strategie für die Sicherheitsunion fortsetzen;
- die Mitgliedstaaten zur Einsetzung einer Arbeitsgruppe „Cyberintelligenz" im Rahmen des EU-INTCEN anhalten und dazu beitragen;
- die EU-Cyberabschreckung voranbringen, um für Vorbeugung, Abschreckung und Reaktion im Hinblick auf böswillige Cyberaktivitäten zu sorgen;
- den Rahmen für die Cyberabwehr überprüfen;
- die Entwicklung einer „militärischen Vision und Strategie der EU für den Cyberraum als Einsatzbereich" für militärische GSVP-Missionen und -Operationen fördern;
- Synergien zwischen der zivilen, der Verteidigungs- und der Weltraumindustrie unterstützen und
- die Cybersicherheit kritischer Weltrauminfrastrukturen im Rahmen des Weltraumprogramms stärken.

Quelle: Cybersicherheitsstrategie der EU für die digitale Dekade vom 16.12.20, JOIN(2020) 18 final

3. Förderung eines globalen offenen Cyberraums

Auch Im Cyberraum sind die Werte unserer Gesellschaft hochzuhalten. Das betrifft die Rechtsstaatlichkeit, die Menschenrechte, die Grundfreiheiten und allgemein die demokratischen Werte, zur weltweiten Förderung des sozialen, wirtschaftlichen und politischen Fortschritts. Ziel ist die Entwicklung einer ganzheitlichen internationalen Cyberpolitik.

Die EU soll eine Führungsrolle bei Standards, Normen und Rahmenbedingungen für den Cyberraum einnehmen. Hierbei ist mehr Einsatz für internationale Normung erforderlich, um die Unionswerte im Cyberraum festzuschreiben. Auch will sich die EU für verantwortungsvolles staatliches Handeln im Cyberraum einsetzen. Denn die EU sei am besten in der Lage, die Standpunkte der Mitgliedstaaten international geltend zu machen. Dies schließt beispielsweise ein Aktionsprogramm der Vereinten Nationen zur Förderung von verantwortungsvollem staatlichem Handeln im Cyberraum mit ein. Angesichts Überwachung und Zensur müssen Menschenrechte und Grundfreiheiten gerade im Internet gestärkt werden. Drittländer können über das Budapester Übereinkommen über Computerkriminalität miteingebunden werden.

Ganz generell bedarf es eines intensivierten Dialogs mit Drittländern und insbesondere eines strukturierten Austauschs mit regionalen Organisationen, beispielsweise der Afrikanischen Union, dem ASEAN-Regionalforum, der Organisation Amerikanischer Staaten etc. Hierbei sollte die EU ein EU-Netz für Cyberdiplomatie errichten. Ganz besonders wichtig ist auch die weitere Zusammenarbeit zwischen EU und NATO. Was die Internet-Governance angeht, steht die EU weiterhin für das Multi-Stakeholder-Modell.

Zuletzt sollen die globalen Kapazitäten zur Erhöhung der globalen Widerstandsfähigkeit gestärkt werden. Aus Gesichtspunkten der Gesamtkohärenz soll die EU eine Agenda für den Aufbau externer Cyberkapazitäten entwickeln, die sich auf den westlichen Balkan, die Nachbarschaft der EU und die Partnerländer konzentrieren soll, in denen die digitale Entwicklung schnell voranschreitet. Hierfür soll auch ein Gremium für den Cyberkapazitätsaufbau eingerichtet werden.

Abbildung 7

Strategische Initiativen

Strategische Initiativen

Die EU sollte

- eine Reihe von Zielen für internationale Normungsverfahren festlegen und diese Ziele auf internationaler Ebene fördern;
- die internationale Sicherheit und Stabilität im Cyberraum stärken, insbesondere durch einen Vorschlag der EU und ihrer Mitgliedstaaten für ein Aktionsprogramm der Vereinten Nationen zur Förderung von verantwortungsvollem staatlichen Handeln im Cyberraum;
- praktische Orientierungshilfe zur Einhaltung der Menschenrechte und Beachtung der Grundfreiheiten im Cyberraum bieten;
- Kinder besser vor sexuellem Missbrauch und sexueller Ausbeutung schützen und eine Strategie für die Rechte des Kindes verabschieden;
- das Budapester Übereinkommen über Computerkriminalität stärken und fördern, u. a. durch die Arbeiten am zweiten Zusatzprotokoll zu dem Übereinkommen;
- den Cyber-Dialog der EU mit Drittländern, regionalen und internationalen Organisationen ausweiten, u. a. durch ein informelles EU-Netz für Cyberdiplomatie;
- den Austausch mit der Multi-Stakeholder-Gemeinschaft verstärken, insbesondere durch einen regelmäßigen und strukturierten Austausch mit dem Privatsektor, der Wissenschaft und der Zivilgesellschaft;
- eine EU-Agenda für den Aufbau externer Cyberkapazitäten und die Einrichtung eines EU-Gremiums für den Cyberkapazitätsaufbau vorschlagen.

Quelle: Cybersicherheitsstrategie der EU für die digitale Dekade vom 16.12.20, JOIN(2020) 18 final

Die zweite Säule zielt auf die einheitliche Gewährleistung von Cybersicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU durch einheitliche, verbindliche Vorschriften ab. Denn diese seien regelmäßiges Ziel von feindseliger und komplexer werdenden Cyberangriffen. Verschlusssachen müssen kohärenter und einheitlicher behandelt werden, um die reibungslose Informationsübermittlung zu vereinfachen. Außerdem wird die Kommission gemeinsame verbindliche Vorschriften zur Informationssicherheit sowie zur Cybersicherheit für alle Organe, Einrichtungen und sonstigen Stellen der EU vorschlagen. Auch Cyberreife beziehungsweise Cyberhygiene soll verbessert werden, um eine gemeinsame Kultur der Cybersicherheit zu fördern. Damit einher geht eine Stärkung des CERT-EU.

Zusammengefasst ergeben sich die folgenden strategischen Initiativen.

Abbildung 8
Strategische Initiativen

Strategische Initiativen

1. Verordnung über die Informationssicherheit in den Organen, Einrichtungen und sonstigen Stellen der EU,
2. Verordnung über gemeinsame Cybersicherheitsvorschriften für die Organe, Einrichtungen und sonstigen Stellen der EU,
3. neue Rechtsgrundlage für das CERT-EU zur Stärkung seines Mandats und seiner Finanzausstattung.

Quelle: Cybersicherheitsstrategie der EU für die digitale Dekade vom 16.12.20, JOIN(2020) 18 final

Hiervon verspricht sich die Kommission eine digitale Dekade der Cybersicherheit in der EU und eine Stärkung der Position der EU in der Welt allgemein. Sowohl Kommission als auch der Hohe Vertreter werden über die Umsetzung der Strategie wachen.

2.1.1.3 Spezifische Vorgaben zur IT-Sicherheit in der EU

Die spezifischen Vorgaben zur IT-Sicherheit auf internationaler und europäischer Ebene ergeben sich insbesondere aus den folgenden Regelungsmaterien:

2.1.1.3.1 Datenschutz-Grundverordnung (Verordnung EU 2016/679)[19]

Die Datenschutz-Grundverordnung (Verordnung EU 2016/679, DS-GVO), die ab 25. Mai 2018 Geltung erlangte und die Datenschutzrichtlinie RL 95/46/EG abgelöst hat, enthält

[19] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.

diverse Bestimmungen zur IT-Sicherheit. Zentrale Bedeutung nehmen die Art. 5 Abs. 1 lit. f, Art. 24, 25 und Art. 32 bis 34 der Verordnung ein.

Eine dem Grunde nach § 9 BDSG a. F. entsprechende Vorschrift findet sich zu Beginn der Verordnung in Art. 5 Abs. 1 lit. f. Diese schreibt für die verantwortliche Stelle die Einhaltung der „Integrität und Vertraulichkeit“ vor: Personenbezogene Daten müssen danach „in einer Weise bearbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“.

Nach Art. 24 DS-GVO hat der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Das kann insbesondere auch Maßnahmen erfassen, die als Maßnahmen der IT-Sicherheit anzusehen sind.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung („Privacy by design“, „Privacy by default“) werden in Art. 25 der Verordnung verpflichtend vorgeschrieben. Diese beiden essenziellen Elemente des Datenschutzes enthalten auch Bezüge zur IT-Sicherheit, etwa in Form von Sicherungen gegen den Verlust von Daten oder gegen den unberechtigten Zugriff auf Daten. Können diese Ziele im Einzelfall mit den eingesetzten IT-Komponenten nicht eingehalten werden, verbietet sich deren Einsatz.

Die Art. 32 bis 34 der Verordnung stehen im Abschnitt 2, der mit „Sicherheit personen-bezogener Daten“ betitelt ist, und stellen damit schon aufgrund ihrer systematischen Stellung in der DS-GVO die wesentlichen Bestimmungen zur IT-Sicherheit dar. Hierbei schreibt Art. 32 die Sicherheit der Verarbeitung personenbezogener Daten vor und Art. 33, 34 die sog. Data Breach Notification in Form von Meldepflicht und Benachrichtigungsverpflichtung.

Erwartet wird 2023 noch eine Entscheidung des EuGH zu der Frage, ob immaterieller Schadenersatz („Schmerzensgeld“) bei IT-Sicherheitsvorfällen zu leisten ist.[20] In dem Vorlageverfahren[21] geht es um einen Hackerangriff auf eine öffentliche Behörde Bulgariens, wonach der Kläger immateriellen Schadensersatz allein deshalb verlangt, weil er einen möglichen zukünftigen Missbrauch seiner Daten befürchtet. Konkret geht es um Steuer- und Sozialversicherungsdaten. Der datenschutzrechtliche Verstoß der bulgarischen Behörde liegt vermutlich in unzureichenden Maßnahmen zur Datensicherheit nach Art. 32 DSGVO. Letztinstanzlich geklärt ist das allerdings noch nicht.

[20] Nachstehende Ausführungen übernommen aus Bronner/Ziegler, DSGVO-Schadensersatz nach Hacker-Angriff, BayWiDI-Briefing 2023/3, S. 6 f.
[21] Hierzu EuGH C-340/21 mit Anmerkung Tinnefeld/Schulze, GRUR-Prax 2023, 503.

In den Schlussanträgen des Generalanwalts gibt dieser erstmals Hinweise auf Auslegungsfragen, die der EuGH bisher noch nicht beantwortet hat. Zum einen hinsichtlich der Frage, welche technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO angemessen sind. Hier hat der datenschutzrechtlich Verantwortliche ein gewisses Ermessen. Der Generalanwalt stellt hier klar, dass es zu Data Breaches aber auch kommen kann, wenn man geeignete Maßnahmen nach dem Stand der Technik getroffen hat: Cyberkriminelle können diese – abhängig vom Einsatz ihrer Ressourcen – umgehen. Wer Daten als datenschutzrechtlich Verantwortlicher verarbeitet, muss zukünftig nach der Ansicht des Generalanwalts nachweisen, dass die von ihm getroffenen technischen und organisatorischen Maßnahmen tatsächlich geeignet sind im Sinne des Art. 32 DSGVO. Aus dem Grundsatz der Rechenschaftspflicht leitet er eine Beweislastumkehr zulasten der Verantwortlichen her. Dem Betroffenen wäre ein solcher Nachweis wohl in der Praxis gar nicht möglich, doch auch die Verantwortlichen wird dies wohl zukünftig belasten.

Zum anderen beantwortet der Generalanwalt auch die Kernfrage der Vorlage: Allein Befürchtungen und Ängste vor einem möglichen künftigen Missbrauch personenbezogener Daten – obwohl ein solcher noch nicht festgestellt werden kann und ansonsten auch noch kein Schaden entstanden ist – sollen für einen immateriellen Schadensersatz ausreichen. Begründet wird dies dadurch, dass der Schadensbegriff der DSGVO weit auszulegen ist. Wo aber die Grenze zwischen Schaden und bloßen „sonstigen Nachteilen, die sich aus der Nichteinhaltung von Rechtsvorschriften ergeben“ liegt, soll den Mitgliedsstaaten und deren Gerichten überlassen bleiben.

2.1.1.3.2 eIDAS-Verordnung

Die am 18. September 2014 in Kraft getretene Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, kurz: eIDAS-Verordnung, die zu einer Stärkung des Vertrauens in den elektronischen Rechtsverkehr beitragen soll, enthält einige IT-sicherheitsrechtliche Bestimmungen.

In Art. 19 eIDAS-Verordnung finden sich Sicherheitsanforderungen an Vertrauensdiensteanbieter. Gemäß Abs. 1 werden die qualifizierten und nichtqualifizierten Vertrauensdiensteanbieter zum Ergreifen geeigneter technischer wie organisatorischer Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihnen erbrachten Vertrauensdiensten verpflichtet. Die Maßnahmen müssen den neuesten Stand der Technik berücksichtigen. Abs. 2 enthält außerdem Melde- und Benachrichtigungsverpflichtungen im Falle von Sicherheitsvorfällen.

Weiter enthält beispielsweise Art. 29 Abs. 1 der Verordnung i. V. m. Anhang II Bestimmungen zur IT-Sicherheit für qualifizierte elektronische Signaturerstellungseinheiten.

2.1.1.3.3 NIS-Richtlinie

Die im August 2016 in Kraft getretene NIS-Richtlinie (Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union) nimmt die Betreiber wesentlicher Dienste und Anbieter digitaler Dienste in die Pflicht und weist damit einen weiteren Anwendungsbereich als das deutsche IT-Sicherheitsgesetz auf.

So müssen die Mitgliedstaaten eine nationale NIS-Strategie entwickeln, die strategische Ziele und konkrete Regulierungsmaßnahmen enthält, mit denen eine hohe Netz- und Informationssicherheit erreicht wird. Außerdem ist eine für die NIS zuständige, ausreichend ausgestattete nationale Behörde zu benennen, die die Anwendung dieser Richtlinie auf nationaler Ebene überwacht und zu ihrer einheitlichen Anwendung in der Union beiträgt. Weiterhin hat jeder Mitgliedstaat ein IT-Notfallteam (Computer Emergency Response Team – CERT) einzurichten, das für die Bewältigung von Sicherheitsvorfällen und Risiken nach einem konkret festgelegten Ablauf zuständig sein soll. Hinzu kommt die Pflicht zur Errichtung eines Frühwarnsystems und anderer IT-Sicherheitsmaßnahmen.

2.1.1.3.4 NIS-2-Richtlinie

Die NIS-2-Richtlinie, die die NIS-RL ablöst, ist am 16. Januar 2023 in Kraft getreten.[22] Hiermit will der europäische Gesetzgeber die in den letzten Jahren gezeigten Mängel der Vorgängerrichtlinie schließen und das IT-Sicherheitsniveau in der EU insgesamt steigern. Die Mitgliedsstaaten müssen bis Oktober 2024 die in der NIS-2-Richtlinie getroffenen Regelungen national umsetzen. Der vorliegende Referentenentwurf zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz beinhaltet in der aktuellen Fassung bereits über die Richtlinie hinausgehende Regelungen zur Stärkung der IT-Sicherheit.[23]

Aufgrund der zunehmenden Digitalisierung und damit verbundenen gestiegenen Bedrohungslage ist ein Ziel der NIS-2-Richtlinie die Stärkung der Cybersicherheits- und Reaktionskapazitäten, d. h. den Ausbau der Kapazitäten in den zuständigen IT-Sicherheitsbehörden sowie die Erweiterung ihrer Befugnisse und die Verbesserung der Zusammenarbeit zwischen allen Mitgliedstaaten. Hierfür wird in jedem Mitgliedsstaat ein Koordinator zur Unterstützung des grenzüberschreitenden Informationsaustauschs zwischen den Mitgliedsstaaten benannt.

Zudem wird die Anwendung der Cybersicherheitsvorschriften auf weitere Sektoren und Einrichtungen ausgeweitet. Diese neuen Sektoren sind in Anhang I der NIS-2-Richtlinie zu finden (neu hierbei: Abwasser, Weltraum und öffentliche Verwaltung). In den genannten Sektoren werden mittlere und große Unternehmen, nicht aber kleine und Kleinstunternehmen, Art. 2 Abs. 1. Art. 2 Abs. 2 von den Regelungen dieser Richtlinie erfasst.

---

[22] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32022L2555.
[23] Der aktuelle Referentenentwurf ist abrufbar unter https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/. Zu dem nationalen Referentenentwurf vgl. Kipker/Dittrich, MMR 2023, 481.

Unternehmen, die in keine dieser Sektoren fallen, könnten dennoch von der nationalen Umsetzung der Richtlinie erfasst sein, da die Mitgliedsstaaten über diese Regelungen hinausgehende Vorgaben treffen können. Es soll nämlich eine Kultur der Sicherheit in allen Sektoren, die für die Wirtschaft und Gesellschaft von Bedeutung sind und die auf Informations- und Kommunikationstechnik angewiesen sind, gefördert werden. Für die Eindämmung von Bedrohungen gegenüber den Netz- und Informationssystemen, um das reibungslose Funktionieren der Wirtschaft und Gesellschaft zu unterstützen, sind durch die Mitgliedstaaten nationale Cybersicherheitsstrategie zu erstellen (Art. 7), die weitere Maßnahmen beinhalten.[24] Zudem ist ein Reaktionsteam für IT-Sicherheitsvorfälle (Art. 10 ff.) zu errichten. Ferner werden Meldepflichten ausgeweitet und Unternehmen aus den genannten Sektoren müssen die in Art. 21 Abs. 2 benannten Mindestanforderungen des Risikomanagements erfüllen.

Risikomanagementmaßnahmen aus Art. 21 Abs. 2 der NIS-2-Richtlinie umfassenden insbesondere:

- 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 gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Mit Art. 34 der Richtlinie wird auch ein erhöhter Bußgeldrahmen im Falle eines Verstoßes gegen die Vorgaben dieser Richtlinie den Mitgliedsstaaten für die Umsetzung vorgegeben. So sollen für wesentliche Einrichtungen bei Verstößen gegen diese Vorgaben Bußgelder bis zu mindestens 10 Mio. EUR oder mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes festgesetzt werden. Bei wichtigen

[24] Die aktuelle Cybersicherheitstrategie von 2021 wird somit 2024 aktualisiert werden müssen, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/09/cybersicherheitsstrategie-2021.html.

Einrichtungen soll der Höchstbetrag bei mindestens 7 Mio. EUR oder mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes angesetzt werden.

Ergänzt wird die NIS-2-Richtlinie durch die Resilienz-RL, die künftig die Sicherheit bei Kritische Infrastrukturen verbessern soll. Hierzu gehört insbesondere die Stärkung deren physischen Schutzes.

2.1.1.3.5 Verordnungen zur Errichtung und über die Agentur für Netz- und Informationssicherheit/Cybersicherheit (ENISA)

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) – gewissermaßen das europäische Pendant zum BSI – wurde 2004 errichtet.[25] Zweck der Agentur ist insbesondere die Gewährleistung der Sicherheit informationstechnischer Systeme. Dabei soll die ENISA „[…] die Aufgaben wahrnehmen, die ihr nach Rechtsakten der Union im Bereich der elektronischen Kommunikation übertragen werden, und generell zu mehr Sicherheit im Bereich der elektronischen Kommunikation und zu einem besseren Schutz der Privatsphäre und personenbezogener Daten beitragen […]“.

Die VO (EG) 460/2004 wurde zunächst abgelöst durch die Verordnung (EU) Nr. 526/2013 vom 21. Mai 2013. Durch VO (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), EU Cybersecurity Act, wurde das Regelungsregime wiederum neugestaltet.

2.1.1.3.6 Cybersecurity-Act / Rechtsakt zur Cybersecurity

Am 13. September 2017 hat die Europäische Kommission einen Entwurf für eine Verordnung über die EU-Cybersicherheitsagentur (ENISA) und zur Aufhebung der Verordnung (EU) 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit / Cybersecurity Act) auf Grundlage ihrer überarbeiteten Cybersicherheitsstrategie vorgelegt.

Die allgemeine Zielsetzung des Entwurfs – Stärkung der Cybersicherheit - soll durch einen Ausbau der Kapazitäten und der Abwehrbereitschaft der Mitgliedstaaten sowie Unternehmen und die Verbesserung der Zusammenarbeit und Koordinierung der einzelnen Akteure erreicht werden. Auch auf EU-Ebene sollen die Kapazitäten entsprechend erweitert werden. Ferner sollen Bürger und Unternehmen ausreichend sensibilisiert werden, um dem ganzheitlichen Ansatz hinreichend Rechnung zu tragen.

---

[25] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit und Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004.

Der Cybersecurity-Act bezweckt außerdem die Stärkung der Stellung der ENISA und die Schaffung eines einheitlichen Rechtsrahmens für Cybersicherheits-Zertifizierungen. Das Mandat der ENISA ist dann auf unbegrenzte Zeit festgelegt. Die ENISA soll als „Informationsdrehkreuz“ innerhalb der Europäischen Union etabliert werden. Auch sollen ihre präventiven und operativen Fähigkeiten gestärkt werden. Hierfür sollen die erforderlichen Kompetenzen bereitgestellt werden. Der Entwurf sieht für ENISA zudem tragende Rollen in der operativen Zusammenarbeit und im Krisenmanagement vor. Im Bereich der Forschung und Entwicklung wird ihr ein Einbringen von Fachkompetenz ermöglicht. Insgesamt sieht der Entwurf eine starke Stellung der ENISA vor.

Am 07. Juni 2019 wurde das Gesetzgebungsverfahren in Gestalt der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) erfolgreich mit der Veröffentlichung im Amtsblatt der EU beendet. Das Ziel der Stärkung der IT-Sicherheit soll mit einem umfassenden Bündel von Maßnahmen erreicht werden. Nach Art. 1 Abs. 1 geschieht dies insbesondere in Form der ENISA, der Agentur der EU für Cybersicherheit, sowie durch einen Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung, mit dem Ziel, für IKT-Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und mit dem Ziel, eine Fragmentierung des Binnenmarkts bei Zertifizierungsschemata in der Union zu verhindern. Hierzu im Einzelnen:

Titel II der VO behandelt die ENISA in den Art. 3-45.

Kapitel I behandelt Mandat und Ziele der ENISA. Mit ihrem Mandat verbunden ist die Erreichung eines hohen gemeinsamen Maßes an Cybersicherheit in der gesamten Union und Defragmentierung des Binnenmarktes (Art. 3 Abs. 1). Wesentliche Ziele sind dabei die Rolle als Kompetenzzentrum für die Cybersicherheit sowie die vielfältige Unterstützung der Mitgliedstaaten und Organe der Union (Art. 4 Abs. 2, 3). Die Unterstützungstätigkeit soll sich unter anderem auf die Ausarbeitung von Strategien und die Optimierung des Schutzes der Netze beziehen. Weiter soll die Agentur zur Sensibilisierung der Bürger und Unternehmen beitragen (Art. 4 Abs. 7). Auch wird die Agentur die Zusammenarbeit und Koordinierung zwischen Mitgliedstaaten, Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen Interessenträgern, auch des Privatsektors, fördern (Art. 4 Abs. 4). Die Agentur baut die Cybersicherheitskapazitäten auf Unionsebene aus, um insbesondere bei grenzüberschreitenden Vorfällen die Maßnahmen der Mitgliedstaaten ergänzen zu können (Art. 4 Abs. 5). In Bezug auf den zweiten Regelungskomplex (→ Zertifizierungsrahmen) wird die Agentur die Nutzung der Zertifizierung fördern, indem sie zum Aufbau und zur Pflege des Cybersicherheitszertifizierungsrahmens auf Unionsebene beiträgt (Art. 4 Abs. 6). Die ENISA kann als Äquivalent des Unionsrechts für das BSI bezeichnet werden.[26]

[26] Paal/Pauly/Martini, DS-GVO, 3. Aufl. 2021, Art. 32 Rn. 17.

In den Art. 5-12 des Cybersecurity-Acts werden umfassend die erweiterten und ergänzten Aufgaben der ENISA konkretisiert. Zur bisherigen Rolle als überwiegend beratende und unterstützende Stelle in Angelegenheiten der Netz- und Informationssicherheit werden der Agentur zusätzlich erweiterte beziehungsweise neue Aufgaben zugewiesen: Hervorzuheben sind dabei insbesondere die Entwicklung sektorspezifischer Strategien und Rechtsetzungsinitiativen (Art. 5; vgl. auch Art. 4 Abs. 2) und die Unterstützung der CERT-EU (Art. 6 Abs. 1 lit. c). Ferner hat die Agentur die Aufgabe, die Mitgliedstaaten beim Aufbau von CSIRTs nach der RL (EU) 2016/1148 (NIS-RL) zu unterstützen (Art. 6 Abs. 1 lit. d, g). Die Agentur muss außerdem jährliche, groß angelegte Cybersicherheits-Übungen auf Unionsebene organisieren (Art. 6 Abs. 1 lit h, Art. 7 Abs. 6). Sie erleichtert die Einrichtung sektorspezifischer Informationsaustausch- und -analysezentren (ISACs) und unterstützt diese dauerhaft (Art. 6 Abs. 2). Der Agentur obliegt außerdem die Erstellung technischer Lageberichte auf Grundlage von frei zugänglichen Informationen, eigenen Analysen und Berichten (Art. 7 Abs. 7) und Durchführung diverser Analysen (Art. 9 lit. a, b).

Der ENISA obliegt die Aufgabe einer „Marktbeobachtungsstelle“, die Trends auf dem Cybersicherheitsmarkt analysieren soll (Art. 8 Abs. 1, 7). Neu hinzugekommen ist die Aufgabe, bei der Öffentlichkeit das Bewusstsein für Cybersecurity-Bedrohungen zu erhöhen oder diese zu unterstützen (Art. 10 lit. a). Hierzu hat sie mit den Mitgliedstaaten und Einrichtungen der EU regulär Kampagnen zu führen (Art. 10 lit. b). Sie soll zudem eine enge Koordination und einen Austausch im Hinblick auf best practices für die Cybersecurity-Erziehung und -Bildung zwischen den Mitgliedstaaten unterstützen (Art. 10 lit. d).

Das Kapitel III enthält Bestimmungen zur Organisation der Agentur. In den Art. 13-28 werden Vorgaben zu Organisation, Aufbau und Struktur der Sicherheitsagentur getroffen, wobei die grundlegenden Strukturen mit den bisherigen Bestimmungen zur ENISA übereinstimmen.[27]

Im Kapitel IV (Art. 29-33) werden die Aufstellung und Gliederung des Haushaltsplans adressiert. Das Kapitel V (Art. 34-37) enthält Bestimmungen zum Personal der Agentur. Allgemeine Bestimmungen, etwa zur Rechtsform, Haftung, Sprachenregelung und Schutz personenbezogener Daten finden sich in Kapitel VI (Art. 38-44). Hervorzuheben ist hier die Regelung zur internationalen Zusammenarbeit in Art. 42 Cybersecurity-Act. Diese erweitert die Möglichkeiten der Zusammenarbeit.[28] Die Agentur kann mit zuständigen Behörden von Drittländern oder internationalen Organisationen Arbeitsvereinbarungen nach vorheriger Genehmigung durch die Kommission treffen (Art. 42 Abs. 1). Sie steht auch der Beteiligung von Drittländern offen (Art. 42 Abs. 2). Dem Verwaltungsrat obliegt die Aufgabe insoweit eine Strategie für die Beziehungen zu Drittländern oder internationalen Organisationen zu entwickeln (Art. 42 Abs. 3).

Von besonderer Bedeutung ist die Schaffung eines europäischen Systems für die Cyber-Sicherheitszertifizierung. Dies wird in Titel III (Art. 46-65) verwirklicht. Die Schaffung eines einheitlichen Rahmens für Zertifizierungssysteme für die Cybersicherheit soll der

[27] Zum Entwurf Kipker, MMR-Aktuell 2017, 395945.
[28] Zum Entwurf Kipker, MMR-Aktuell 2017, 395945.

uneinheitlichen Rechtslage entgegenwirken. Die damit zusammenhängenden hohen Kosten und erhöhter Verwaltungsaufwand sollen reduziert werden. Die Kommission betont im Entwurf insbesondere die folgenden Vorteile eines einheitlich europäischen Zertifizierungsmechanismus: Durch die VO wird eine zentrale Cybersicherheitszertifizierungsstelle für Unternehmen innerhalb der Union etabliert und die Zertifizierungsmaßnamen werden vereinheitlicht. Vor allem werden nationale Parallelsysteme verdrängt. Die Akzeptanz und Anerkennung etwaiger Zertifizierungsmaßnahmen im unternehmerischen Bereich soll gefördert werden. Die Herstellung eines einheitlichen Rechtsrahmens dient auch der Umsetzung der NIS-Richtlinie. Ferner soll eine europäische Cybersicherheitspolitik durch die Harmonisierung der Anforderungen einer Zertifizierung unterstützt und gefördert werden.

Nach Art. 48 Abs. 1 Cybersecurity-Act obliegt der ENISA im Auftrag der Kommission die Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung. Unterstützt wird die ENISA bei dieser Aufgabe von der Europäischen Gruppe für die Cybersicherheitszertifizierung (SOG-IS), Art. 49 Abs. 5, die sich aus den nationalen Aufsichtsbehörden für die Zertifizierung zusammensetzt (Art. 62 Abs. 1, 2).

Dieses System muss den Anforderungen der Art. 51 bis 54 genügen. Die Sicherheitsziele, die bei der Ausarbeitung des Systems berücksichtigt werden müssen, werden in Art. 51 Cybersecurity-Act umfassend beschrieben. Mit Blick auf die unterschiedlichen Sicherheitsanforderungen der jeweiligen IKT-Produkte und Dienste ermöglicht Art. 52 Cybersecurity-Act ein abgestuftes Zertifizierungssystem. Gem. Art. 52 Abs. 1 Cybersecurity-Act können die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ sowie „hoch“ eingeführt werden. Deren Voraussetzungen sind im Detail in Art. 52 Abs. 5-8 geregelt.

Art. 54 Cybersecurity-Act nennt verpflichtende Elemente des Zertifizierungssystems. Beispielsweise muss das System detaillierte Spezifikationen der Cybersicherheitsanforderungen, auf deren Einhaltung die jeweiligen IKT-Produkte und Dienste geprüft werden.

Art. 56 Cybersecurity-Act regelt die Wirkungen der Zertifizierung auf Grundlage eines anerkannten europäischen Systems: Für zertifizierte Produkte und Dienste greift die Vermutung der Konformität mit den Vorgaben des Cybersicherheitssystems, vgl. Art. 56 Abs. 1 Cybersecurity-Act. Die Vermutung gilt gem. Art. 56 Abs. 9 Cybersecurity-Act allerdings höchstens für eine bestimmte Zeit. Nach Ablauf dieser Zeit bedarf es einer erneuten Zertifizierung. Art. 56 Abs. 2 Cybersecurity-Act statuiert die Freiwilligkeit der Zertifizierung, vorbehaltlich anderslautenden Unionsrechts. Die Wirksamkeit der Zertifizierung soll durch die Kommission regelmäßig überprüft werden und es soll überprüft werden, ob nicht gewisse Zertifikate als verpflichtend eingestuft werden sollen (Art. 56 Abs. 3).

Das Verhältnis zu nationalen Cybersicherheitszertifizierungssystemen bestimmt Art. 57 Cybersecurity-Act: Demnach werden nach Abs. 1 S. 1 nationale Systeme ab dem Zeitpunkt unwirksam, der in dem nach Art. 49 Abs. 7 zu erlassenden Durchführungsrechtsakt festgelegt wird. Dagegen bleiben bereits vorhandene Systeme, die nicht unter ein europäisches System für die Cybersicherheitszertifizierung fallen, bestehen (Art. 57 Abs. 1 S. 2). Ferner bestimmt Art. 57 Abs. 2, dass die Mitgliedstaaten keine neuen nationalen Systeme, die unter ein europäisches System für die Cybersicherheitszertifizierung fallen, einführen dürfen.

Für vorhandene Zertifikate auf Grundlage nationaler Systeme enthält Art. 57 Abs. 3 eine Privilegierung dahingehend, dass diese bis zum Ende ihrer Gültigkeitsdauer bestehen blieben. Es wird zudem eine Notifizierungspflicht bei der Einführung neuer Zertifizierungen durch die Mitgliedstaaten eingeführt (Art. 57 Abs. 4), um eine Fragmentierung des Binnenmarkts zu verhindern.

Gemäß Art. 58 Cybersecurity-Act haben die Mitgliedstaaten jeweils Aufsichtsbehörden für die Zertifizierung zu benennen, die mit spezifischen Aufgaben und Befugnissen versehen sind (Art. 58 Abs. 7 und 8).

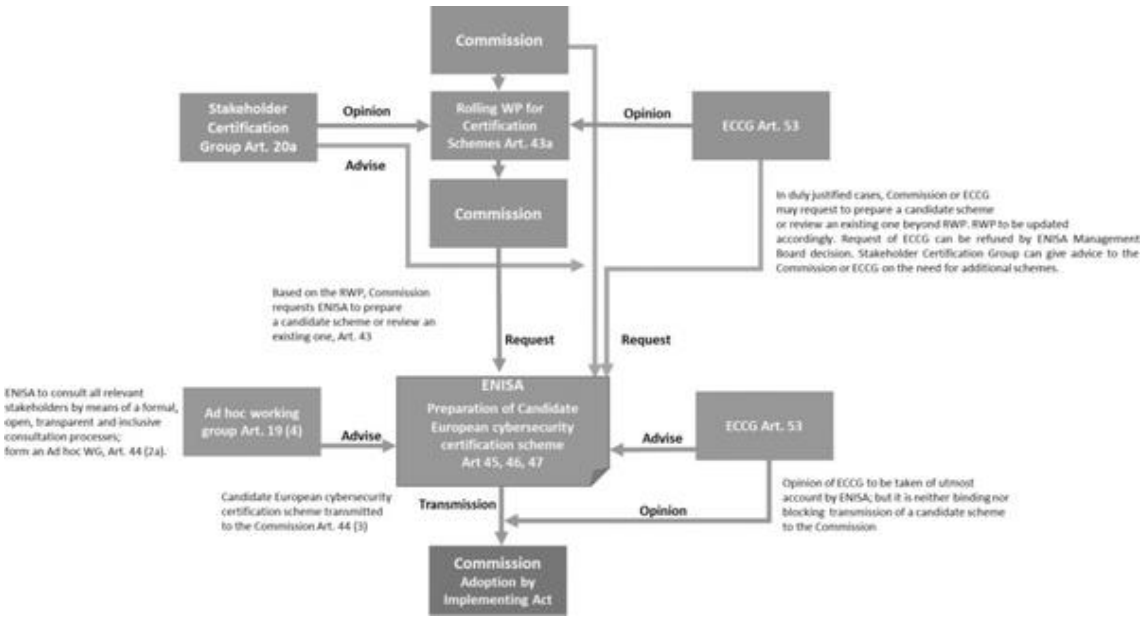
Nationale Cybersecurity-Zertifizierungen sollen einem peer review unterworfen werden (Art. 59 Abs. 1). Die Maßstäbe, Voraussetzungen und Folgen sind in Art. 59 Abs. 2 bis 6 niedergelegt.

Die Zertifizierung an sich wird von sog. Konformitätsbewertungsstellen (Art. 60), die zuvor von den nationalen Aufsichtsbehörden notifiziert werden müssen (Art. 61), vorgenommen (Art. 56 Abs. 4). In Ausnahmefällen erfolgt die Zertifizierung durch staatliche Stellen (Art. 56 Abs. 5).

Gemäß Art. 65 Cybersecurity-Act haben die Mitgliedstaaten entsprechende Sanktionsmechanismen zu erlassen.

Abbildung 9

Europäische Arbeits- und Abstimmungsprozesse im Rahmen des EU Cybersecurity-Act



Quelle: Kipker Cybersecurity, Kap. 21 Internationaler Rahmen Rn. 22

2.1.1.3.7 Entwurf eines Cyberresilience-Acts (CRA-E)

Die Europäische Kommission hat am 15. September 2022 den Entwurf eines Cyberresilience-Acts vorgelegt, der die Cybersicherheit von Produkten mit digitalen Elementen verbessern soll.[29] Diese Richtlinie soll künftig das IT-Sicherheitsniveau sowohl für Verbraucher als auch Unternehmen, die entsprechende Produkte einsetzen, erhöhen. Die neu geschaffenen Regelungen von Produkten mit digitalen Elementen sollen daher branchenübergreifend gelten. Sie sollen grundsätzlich für alle Produkte anwendbar sein, die mittels Software direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind und auf dem europäischen Markt in Verkehr gebracht werden. Dies gilt auch wenn die Software- und die Hardwarekomponente getrennt vermarktet werden. Es soll lediglich Ausnahmen im Zusammenhang mit Open Source-Software geben sowie bei Dienstleistungen, die bereits anderweitig reguliert sind. Dies ist beispielsweise der Fall bei Medizinprodukten, Kraftfahrzeugen mit automatisierten und autonomen Fahrfunktionen und in der Luftfahrt sowie Produkte für die nationale Sicherheit und militärische Zwecke. Der CRA-E wird voraussichtlich einen sehr weitreichenden Anwendungsbereich haben. Da er jedoch voranging Produkte und deren Hersteller, Importeure und Händler adressiert und damit Anbieter kritischer Infrastrukturen ausblendet, besteht dieses Regelwerk neben den Vorgaben der NIS-2-Richtlinie. Die Abgrenzung dieses Rechtsakts mit der künftigen KI-Verordnung[30], der Verordnung über die allgemeine Produktsicherheit 2023/988 vom 10. Mai 2023, der künftigen KI-Haftungs- und Produkthaftungsrichtlinien sowie der EU-Maschinenverordnung 2023/1230 vom 14. Juni 2023 wird sich im Einzelnen noch zeigen müssen.

Mit dem CRA-E sollen künftig Sicherheitslücken in Produkten mit digitalen Elementen sowie mit dem Internet verbundener Software geschlossen werden, da ihre IT-Sicherheit bisher vielfach unzureichend sind und keine ausreichenden Sicherheitsupdates zur Verfügung gestellt werden. Die Art. 5 ff CRA-E in Verbindung mit den Anlagen I-III sehen daher harmonisierende Anforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte in Bezug auf die IT-Sicherheit vor (Art. 10 ff. CRA-E).

Zudem sollen Anforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Produktlebenszyklus zu gewährleisten, errichtet werden. In diesem Zusammenhang soll eine Meldepflicht für Hersteller solcher Produkte mit digitalen Elementen bzw. entsprechender Software eingeführt werden (Art. 11 CRA-E).

Bisher können Verbraucher und Unternehmer häufig nicht feststellen, wie sicher entsprechende Produkte bzw. Software sind und mit welchen Maßnahmen sie IT-Sicherheit in diesem Zusammenhang umsetzen könnten. Dem soll künftig mit einer CE-Kennzeichnung begegnet werden, vgl. Art. 21 f. CRA-E.

---

[29] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[30] Aktuelle Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206.

Abschließend beinhaltet der Rechtsakt Vorschriften für die Marktüberwachung und Durchsetzung der zuvor genannten Vorschriften und Anforderungen.

Nach Inkrafttreten der Richtlinie werden die Mitgliedsstaaten 24 Monate Zeit haben die getroffenen Regelungen national umzusetzen. Bereits heute gibt es mit § 327f BGB eine Aktualisierungspflicht für Produkte mit digitalen Inhalten. Diese gilt bisher jedoch nur für Verbraucherverträge. Insoweit könnte die Regelung künftig in Bezug auf IT-Sicherheitsupdates weiter verschärft werden.

2.1.1.3.8 Entwurf einer Produkthaftungsrichtlinie

Die Kommission hat am 28. September 2022 einen Vorschlag für eine Richtlinie über die Haftung für fehlerhafte Produkte (ProdHaftRL-E) vorgelegt. Ziel der Produkthaftungsrichtlinie ist die unionsweite Vereinheitlichung für Entschädigungen für Körper- und Sachschäden, bei durch fehlerhafte Produkte erlitten wurden. Erstmalig wird mit dieser Neuregelung Software in den Anwendungsbereich der Produkthaftungsrichtlinie einbezogen. Der Produktbegriff wird um Elektrizität, digitale Bauunterlagen und Software erweitert, Art. 4 Abs. 1 ProdHaftRL-E. Künftig können daher auch Softwarefehler und damit auch verwirklichte IT-Sicherheitsrisiken als Produktfehler gewertet werden, die Schadensersatzansprüche auslösen. In dem Richtlinienentwurf wurde das Fehlen der Sicherheitsanforderungen des Produkts einschließlich sicherheitsrelevanter Cybersicherheitsanforderungen explizit aufgenommen (Art. 6 Nr. 1 lit. f ProdHaftRL-E).

Ferner wird der Zeitraum, in dem der Produktfehler einem Hersteller zugerechnet werden kann, ausgeweitet. Nach Art. 10 Abs. 2 lit. c ProdHaftRL-E ist ein Produkt auch dann fehlerhaft, wenn ein Update nach dem Inverkehrbringen unterlassen wurde, obwohl es zur Aufrechterhaltung der Sicherheit des Produkts erforderlich ist. Den Zeitraum, in dem entsprechende Updates bereitzuhalten sind, wurde nicht näher bestimmt. Mit dieser Regelung wird neben der bereits bestehenden Regelung des § 327f BGB, der eine Aktualisierungspflicht bei Verbraucherverträgen im maßgeblichen Zeitraum für Produkte mit digitalen Elementen vorsieht, eine Haftungsanknüpfung an fehlende Sicherheitsupdates geschaffen.

Der deutsche Gesetzgeber wird in der Folge dahingehend das Produkthaftungsgesetz (ProdHaftG) anpassen müssen.

2.1.1.3.9 Schaffung eines CERT-EU

Im Dezember 2017 haben die EU-Institutionen eine interinstitutionelle Vereinbarung getroffen, wonach ein ständiges CERT-EU (Computer Emergency Response Team) (https://cert.europa.eu/) für die europäischen Organe, Einrichtungen und Agenturen eingerichtet werden soll. Es dient dem Schutz vor Cyber-Bedrohungen für die EU-Institutionen.

2.1.1.3.10 Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und des Netzes nationaler Koordinierungszentren

Ziel dieser Verordnung ist die europaweite Koordinierung der Forschung und der Ausbau der Cybersicherheit. Sie hat mittlerweile das Gesetzgebungsverfahren (2018/0328(COD)) erfolgreich durchlaufen und wurde als Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren verabschiedet. Sie ist am 28. Juni 2021 in Kraft getreten (ABl. L 202 vom 08. Juni 2021, S. 1 ff.). Ziel der VO ist es, Kapazitäten für Cybersicherheit zu erhöhen, Gesellschaft und Wirtschaft gegen Cyberangriffe zu verteidigen sowie Industrie und Forschung auf diesem Gebiet zu fördern.

Das einzurichtende Kompetenzzentrum mit Sitz in Bukarest soll die Forschungsförderung im Rahmen der Programme „Digitales Europa“ und „Horizont Europa“ verantworten (vgl. hierzu Ausführungen auf S. 31). Es soll die Aufgaben durch Unterorganisationen erfüllen. Es dient der Förderung von Nutzern aus der Industrie (auch KMU), dem öffentlichen Sektor sowie Forschung und Wissenschaft.

Daneben sollen nationale Koordinierungszentren eingerichtet werden („Netzwerk nationaler Koordinierungszentren, Art. 1 Abs. 1). Das Kompetenzzentrum ist insoweit für Koordination, Vernetzung und Aufgabenteilung unter den Koordinierungszentren zuständig. Koordinierungszentren sind für die Akkreditierung von Mitgliedern zuständig und dienen als Ansprechpartner innerhalb der Länder.

Es soll daneben eine Kompetenzgemeinschaft gebildet werden. In ihr können industrielle, akademische und gemeinnützige Forschungseinrichtungen und Verbände sowie sonstige öffentliche und andere Einrichtungen Mitglieder werden, die sich mit betrieblichen und technischen Fragen der Cybersicherheit befassen. Die Kompetenzgemeinschaft soll das Kompetenzzentrum und die nationalen Koordinierungszentren unterstützen.

2.1.1.3.11 E-Evidence-VO

Nach langem Anlauf ist nunmehr auch die „Verordnung über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren“ (sog. E-Evidence-VO) beschlossen worden (2018/0108 (COD)).[31] Sie wird zusätzliche Befugnisse von Strafverfolgungsbehörden zur Beschaffung digitaler Beweismittel begründen, ohne hierbei die nationalstaatlichen Befugnisse zu beschränken. Vorgesehen sind „Europäische Herausgabeanordnungen“ beziehungsweise „Europäische Sicherungsanordnungen“. Hierzu soll es nicht erforderlich sein, die Behörden des Mitgliedstaats, in dem der Dienstanbieter niedergelassen oder vertreten ist, mitwirken zu lassen. Sie soll nach ihrer

[31] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32023R1543.

Zielsetzung nicht nur der Aufklärung, sondern auch der Abschreckung von „Cyberkriminellen“ dienen; sie hat also eine duale Zielsetzung, nämlich die Strafverfolgung und die Stärkung der IT-Sicherheit.

Der Europäische Rat hat die E-Evidence-VO am 27. Juni 2023 nebst begleitender Richtlinie (Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren) angenommen. Beide sind im Amtsblatt veröffentlicht worden (VO: ABl. EU 2023 L 191 vom 28. Juli 2023, S. 118 ff.; RiLi, ebenda, S. 181 ff.). Die Verordnung wird allerdings erst 36 Monate nach ihrem Inkrafttreten, also erst im Jahr 2026 anwendbar, Art. 28.

2.1.1.3.12 Warenkaufrichtlinie und Update-Pflichten

Fehlende Sicherheitsupdates internetfähiger Geräte können zu massiven Einbußen an IT-Sicherheit führen. Hieran knüpft die sog. Warenkaufrichtlinie an.[32] Diese sieht in ErwG 28 vor, dass Käufer und Verkäufer eine Updatepflicht vereinbaren könnten, weil sich die digitalen Inhalte beziehungsweise Dienste ständig weiterentwickeln. Daher ist die Ware insbesondere dann als (subjektiv) vertragsmäßig zu betrachten, wenn sie wie im Kaufvertrag bestimmt, Aktualisierungen erhält, Art. 6 lit. d.

Darüber hinaus finden sich in der RL aber auch objektive Anforderungen an die Vertragsmäßigkeit: Bei Waren mit digitalen Elementen hat der Verkäufer dafür Sorge zu tragen, dass der Verbraucher über Aktualisierungen, einschließlich Sicherheitsaktualisierungen, die für den Erhalt der Vertragsmäßigkeit dieser Waren erforderlich sind, informiert wird und solche auch innerhalb eines bestimmten Zeitraums tatsächlich erhält (Art. 7 Abs. 3). Es handelt sich zumindest um notwendige Updates, grundsätzlich nicht um Verbesserungen oder Funktionserweiterungen (ErwG 30); Ziel ist es, dass die Ware angesichts technischer Weiterentwicklungen so funktioniert wie im Zeitpunkt der Lieferung (ErwG 31). Jedenfalls teilweise auch im Geiste der IT-Sicherheit ergibt sich nach Art. 7 Abs. 4 für den Verbraucher die Obliegenheit, die Updates auch zu installieren, ansonsten ist der Verkäufer von der Haftung freigestellt. Insoweit ist etwa Schutzsoftware fortlaufend zu aktualisieren, um die Funktionsfähigkeit zu gewährleisten; mittelbar wird damit die IT-Sicherheit gefördert.

Die vorliegenden Änderungen für Verbraucherverträge, die Produkte mit digitalen Inhalten betreffen, hat der deutsche Gesetzgeber in §§ 327 a ff. BGB umgesetzt. Die Aktualisierungspflicht befindet sich in § 327f BGB. Danach hat ein Unternehmer, der entsprechende Produkte anbietet, sicherzustellen, dass dem Verbraucher während des maßgeblichen Zeitraums Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit des digitalen Produkts erforderlich sind, bereitgestellt werden und der Verbraucher über diese Aktualisierungen informiert wird. Der maßgebliche Zeitraum bestimmt sich bei einem Vertrag über die dauerhafte Bereitstellung eines digitalen Produkts nach dem Bereitstellungszeitraum. In allen anderen Fällen fällt hierunter der Zeitraum, den der Verbraucher aufgrund der Art

[32] Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG an. ABl. L 136 vom 22. Mai 2019, S. 28 ff.

und des Zwecks des digitalen Produkts und unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann. Zu den erforderlichen Aktualisierungen gehören insbesondere auch Sicherheitsaktualisierungen (§ 327f Abs. 1 Satz 2 BGB).

Wird dem Verbraucher die entsprechende Aktualisierung (Update) bereitgestellt und unterlässt es der Verbraucher, diese Aktualisierung innerhalb einer angemessenen Frist zu installieren, so haftet der Unternehmer nicht für einen Produktmangel, der allein auf das Fehlen dieser Aktualisierung zurückzuführen ist, sofern er den Verbraucher über die Verfügbarkeit der Aktualisierung und die Folgen einer unterlassenen Installation informiert hat und die Tatsache, dass der Verbraucher die Aktualisierung nicht oder unsachgemäß installiert hat, nicht auf eine dem Verbraucher bereitgestellte mangelhafte Installationsanleitung zurückzuführen ist.

2.1.1.3.13 Know-How-RL

Die RL (EU) 2016/943 stellt erhöhte Anforderungen an Unternehmen, ihr geheimes Wissen auf einen begrenzten Personenkreis zu beschränken, aktiv zu schützen und die Schutzvorkehrungen zu dokumentieren. Zum 26. April 2019 ist die deutsche Umsetzung in Form des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG, BGBl. I 2019 S. 466 ff.) in Kraft getreten. Der Entwurf ist auf ein geteiltes Echo gestoßen. Teils wurde die Umsetzung in dieser Form überwiegend begrüßt (z. B. Bitkom), teils wurden weitgehende Änderungen gefordert (z. B. Ausnahme für den Bereich der Meinungs-, Informations- und Medienfreiheiten). Nach alter Rechtslage war die Einstufung als Geheimnis im Wesentlichen subjektiv bestimmt. Nunmehr ist insbesondere kein Geheimhaltungswille mehr erforderlich.[33] Zu den Geheimhaltungsmaßnahmen, die ein Unternehmen zu treffen hat, gehören nämlich auch solche der IT-Sicherheit.[34]

2.1.1.3.14 Ausbau von Strafverfolgungsbehörden: Europol

Ein Teilaspekt der Cybersicherheitsstrategie der EU-Kommission ist die Abschreckung und Verfolgbarkeit von Straftätern. Um das zu ermöglichen, soll das „European Cybercrime Centre (EC3)“ bei Europol gestärkt werden. Das soll vor allem in den Bereichen der Cyberabwehrfähigkeit und Cyberforensik geschehen. Auch sollen Maßnahmen wie „predictive policing“, machine learning und KI erforscht werden, um Straftaten mit IT-Bezug zu bekämpfen.

[33] Köhler/Bornkamm/Feddersen/Alexander, GeschGehG, 39. Aufl. 2021, § 2 Rn. 20.
[34] Scholtyssek/Judis/Krause, CCZ 2020, 23 (27); BayWiDI Briefing 2022/4 S. 2 f.

2.1.1.3.15 Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln

Die Richtlinie[35] verpflichtet die Mitgliedstaaten, bestimmte Handlungen mit IT-Bezug als Straftat einzustufen und dementsprechend zu verfolgen. Auch hierdurch kann die IT-Sicherheit gesteigert werden, jedenfalls soll eine Verfolgbarkeit bei Verstößen ermöglicht werden. Inhaltlich wird insbesondere ein Tatbestand für Betrug im Zusammenhang mit Informationssystemen (Art. 6) geschaffen. Die Richtlinie ist mit dem 61. Gesetz zur Änderung des Strafgesetzbuches vom 10. März 2021 (BGBl. I 2021 S. 333 ff.) im deutschen Recht umgesetzt worden. Nunmehr regelt § 263a Abs. 3 Nr. 1 StGB einen Straftatbestand für die Herstellung, Verschaffung, Feilhaltung, Verwahrung oder Überlassung von Computerprogrammen, deren Zweck die Begehung eines Computerbetrugs ist.

2.1.1.3.16 Vorschlag zur „Cyber-Hygiene“

Am 26. Mai 2021 hat die Kommission Leitlinien zur Stärkung des Verhaltenskodex für den Bereich der Desinformation vorgelegt (COM(2021) 262 final). Einerseits sollen die Unterzeichner noch stärker in die Pflicht genommen werden, andererseits soll auch eine größere Beteiligung am Kodex erreicht werden. Finanzielle Anreize für Desinformation sollen verringert werden und die Nutzerstellung gestärkt werden. Außerdem soll eine Faktenprüfung besser ermöglicht und ein Datenzugang für Forschungszwecke geschaffen werden. Für die IT-Sicherheit relevant ist insbesondere die Stärkung der Integrität,[36] der Kodex setzt außerdem die Existenz von Cybersecurityteams voraus.[37]

Nunmehr hat die EU-Kommission am 16. Juni 2022 den unionsweiten Verhaltenskodex gegen Desinformation im Internet veröffentlicht.[38] Dieser dient mittelbar der IT-Sicherheit, da Online-Systeme „zur Verbesserung der Rückverfolgbarkeit und Identifizierung von Anbietern von Informationen sowie zur Stärkung des Vertrauens in die Interaktionen, Informationen und ihre Quellen im Internet und deren Zuverlässigkeit“ gefördert werden sollen. Daneben sollen „Mitgliedstaaten bei der Absicherung von Wahlen gegen zunehmend komplexe Cyberbedrohungen, wie Desinformation im Internet und Cyberangriffe“ unterstützt werden. Auch die Stärkung der Medienkompetenz ist ein Ziel. Auch während der Covid-19-Pandemie gaben die Unterzeichner entsprechende Berichte zur Desinformation im Hinblick auf das Coronavirus ab. Zu den ursprünglichen Unterzeichnern gehörten insbesondere Facebook, Google, Twitter, Mozilla. Später kamen Microsoft und TikTok hinzu.

Eine besondere Rolle im Hinblick auf Cyber-Hygiene kommt ENISA zu.[39]

---

[35] Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates (ABl. L 123 vom 10. Mai 2019, S. 18).
[36] Vgl. COM (2021) 262 final S. 11.
[37] COM (2021) 262 final S. 12.
[38] https://digital-strategy.ec.europa.eu/de/policies/code-practice-disinformation.
[39] Beispielsweise Im Hinblick auf die Gewährleistung von Cyber-Hygiene während der Covid-19 Pandemie, https://www.enisa.europa.eu/news/enisa-news/top-ten-cyber-hygiene-tips-for-smes-during-covid-19-pandemic.

2.1.1.3.17 EECC-Richtlinie

Mit der Richtlinie (EU) 2018/1972 vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (EECC-Richtlinie) wird ein harmonisierter Rahmen für die Regulierung elektronischer Kommunikationsnetze, elektronischer Kommunikationsdienste, zugehöriger Einrichtungen und zugehöriger Dienste sowie bestimmter Aspekte der Endeinrichtungen errichtet (Art. 1 Abs. 1). In Art. 40 werden die Mitgliedstaaten verpflichtet, sicherzustellen, dass die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste angemessene und verhältnismäßige technische und organisatorische Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten ergreifen (Abs. 1) und einen Sicherheitsvorfall mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Bereitstellung der Dienste unverzüglich mitteilen (Abs. 2).

2.1.1.3.18 Verordnung (EU) 2021/697 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Einrichtung des Europäischen Verteidigungsfonds und zur Aufhebung der Verordnung (EU) 2018/1092

Das Ziel des Europäischen Verteidigungsfonds ist die Stärkung von Wettbewerbsfähigkeit, Effizienz und Innovationsfähigkeit der europäischen Verteidigungsindustrie. Es sollen nach Erwägungsgrund 34 Synergien zwischen der bisherigen Cybersicherheitsstrategie und den hierdurch finanzierten Vorhaben sowie zwischen ziviler und verteidigungsbezogener Cybersicherheit angestrebt werden. Ende 2020 wurde eine vorläufige Einigung über die Verordnung erzielt, am 29. April 2021 hat das Parlament dem Vorschlag zugestimmt.[40] Seit Mai 2021 ist die Verordnung in Kraft.

Wie schon ihre Vorgängerverordnung (dort: Art. 14 Abs. 2 lit. b) nimmt die derzeit geltende VO auf Cyberabwehr und Cybersicherheit Bezug: Gem. Art. 24 Abs. 3 lit. b ist ein auf ein Jahr (im Unterschied zur Vorgängerverordnung; damals noch zwei Jahre) angelegtes Arbeitsprogramm zu erstellen, aus dem ersichtlich wird, wieweit die Finanzierung für Cyberabwehr und Cybersicherheit geht.

2.1.1.3.19 DORA-VO

Mit dem EU Digital Operational Resilience Act (DORA – kurz DORA-VO)[41] haben Finanzunternehmen über interne Governance- und Kontrollrahmen zu verfügen, die eine wirksame und umsichtige Steuerung aller IKT-Risiken gewährleisten (Art. 5 Abs 1). Art. 6 Abs. 1 schreibt einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen vor, der es den Finanzunternehmen ermöglicht, IKT-Risiken rasch, effizient und umfassend anzugehen und ein hohes Maß an digitaler Betriebsstabilität zu gewährleisten, das den geschäftlichen Bedürfnissen, der Größe und der Komplexität des Unternehmens

[40] ABl. L 170 vom 12.05.2021, S. 149 ff.
[41] Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 (COM/2020/595 final beziehungsweise 2020/0266(COD).

entspricht. Nach Art. 7 müssen IKT Systeme auf dem neuesten Stand und insb. zuverlässig und technisch stabil sein. Die IKT-Systeme sind fortlaufend zu überwachen (Art. 9). Strategien für Datensicherung und Wiederherstellungsverfahren sind zu entwickeln (Art. 12). Nach Art. 14 sind IKT-bezogene Vorfälle zu kommunizieren.

Die DORA-VO enthält weiter Vorschriften zur Behandlung von IKT-Vorfällen (Art. 17 ff.), zur Prüfung der digitalen Betriebsstabilität (Art. 24 ff.), Regelungen zur Involvierung von IKT-Drittanbietern (Art. 28 ff.) und zu Vereinbarungen über den Austausch von Informationen (Art. 45).

Sie ist lex specialis gegenüber der NIS-2-RL[42] und gilt ab dem 17. Januar 2025.[43]

2.1.1.3.20 Etablierung von Forschungsprogrammen

Das Programm „Digitales Europa“ soll Investitionen in Bereichen wie etwa Hochleistungsrechnern, künstlicher Intelligenz, Cybersicherheit, fortgeschrittener digitaler Kompetenzen und die Verbreitung digitaler Technologien in Wirtschaft und Gesellschaft fördern. Am 06. Juni 2018 hat die Kommission einen Vorschlag für eine VO zur Aufstellung des Programms „Digitales Europa“ für den Zeitraum 2021-2027 (COM(2018) 434 final) veröffentlicht, woraufhin die VO schließlich als Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Aufstellung des Programms „Digitales Europa“ und zur Aufhebung des Beschlusses (EU) 2015/2240 am 11. Mai 2021 im Amtsblatt verkündet (ABl. L 166 vom 11. Mai 2021, S. 1 ff) wurde und bereits in Kraft getreten ist.

Die Cybersicherheit spielt hier eine große Rolle, vgl. ErwG 12, 14, 15, 17, 36 ff., 44, 48, 63. Auch findet sich hier eine Definition der Cybersicherheit, nämlich dahingehend, dass der Begriff „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen“ erfasse (Art. 2 Nr. 9).

Konkret normiert Art. 3 Abs. 2 lit. c i. V. m. Art. 6 sowie Anhang I als „Spezifisches Ziel 3“ die Cybersicherheit, was insb. Unterstützung der Mitgliedstaaten bei Ausstattung, Kompetenz, Kapazitäten, Sicherheitslösungen etc. auf dem Gebiet der Cybersicherheit meint. Die inhaltliche Beschreibung ist hier im Vergleich zur Entwurfsfassung noch einmal deutlich detaillierter ausgefallen. Auch die Ziele 4 und 5 weisen Synergieeffekte auf (vgl. die explizite Benennung von Cybersicherheit in den Art. 7, 8). Für die Verwirklichung dieses Ziels werden für den Finanzierungszeitraum 2021-2027 von den ursprünglich im Entwurf vorgesehenen fast zwei Milliarden Euro immerhin noch 1,65 Milliarden Euro bereitgestellt. Erwähnenswert ist auch die Schaffung europäischer digitaler Innovationszentren (Art. 16), das insb. KMU und Midcap-Unternehmen den Zugang insb. zu Cybersicherheit bereitstellen oder sicherstellen soll.

---

[42] COM (2020) 823 final S. 2.
[43] Näheres bei Dittrich/Heinelt, RDi 2023, 309 ff.

Das Programm „Horizon 2020“ dient der Schaffung eines EU-weiten Netzes von Cyber-Sicherheitszentren einschließlich eines Europäischen Forschungs- und Kompetenzzentrums für Cybersicherheit. In Gestalt der VO (EU) 2021/695 vom 28. April 2021 zur Einrichtung von „Horizont Europa“, dem Rahmenprogramm für Forschung und Innovation, sowie über dessen Regeln für die Beteiligung und die Verbreitung der Ergebnisse und zur Aufhebung der Verordnungen (EU) Nr. 1290/2013 und (EU) Nr. 1291/2013[44] ist dieses realisiert worden. Die Ziele des Programms sind in Art. 3 festgeschrieben, der durch den Anhang konkretisiert wird. Gem. Anhang I, der die Grundzüge der Tätigkeiten betrifft, umfasst die Säule II („Globale Herausforderungen und industrielle Wettbewerbsfähigkeit Europas“) das Cluster „Zivile Sicherheit für die Gesellschaft“; als Interventionsbereich ist hier auch die Cybersicherheit genannt. Auch im Hinblick auf Synergien mit anderen Unionsprogrammen (Anhang IV) wird die Cybersicherheit aufgegriffen, nämlich bzgl. des (bereits erwähnten) Programms „Digitales Europa“.

Das Programm „Connecting Europe“ dient der Unterstützung transeuropäischer Netze in den Bereichen Verkehr, Telekommunikation und Energie. Ziel ist auch der Ausbau der Sicherheit in diesen Verkehrsnetzen und dient damit folglich zumindest in Teilen auch der IT-Sicherheit. Derzeit befindet sich das Programm als Vorschlag für eine VO zur Schaffung der Fazilität „Connecting Europe“ und zur Aufhebung der Verordnungen (EU) Nr. 1316/2013 und (EU) 283/2014 (COM(2018) 438 final) im Gesetzgebungsverfahren (2018/0228/COD). Nach dem Verordnungsvorschlag sieht Art. 8 Abs. 3 lit. f vor, dass Finanzierungspriorität diejenigen Projekte haben, die dem neuesten Stand der Technik entsprechen, was Interoperabilität, Datenschutz, Weiterverwendung und insb. auch Cybersicherheit einschließt. Auch hier sind Synergieeffekte mit dem Programm Digitales Europa zu erwarten, mit Horizont Europa besteht kein Überschneidungsrisiko.[45]

2.1.1.3.21 Gemeinsame diplomatische Reaktion der EU auf böswillige Cyberaktivitäten („Cyber Diplomacy Toolbox“, 2018/2004(INI))

Auch mit einem gemeinsamen Auftreten der EU bei Fragen der Cybersicherheit soll die IT-Sicherheit gestärkt werden. Das kann dadurch geschehen, dass für eine Kohärenz zwischen den Cyberinitiativen der EU gesorgt wird und dass sich die EU im Bereich der Cyberdiplomatie kontinuierlich einsetzt. Das betrifft auch – aber nicht nur – staatliche Akteure, die eine IT-Unsicherheit schaffen. Es sollen aber friedliche Lösungen angepeilt werden: Durch eine verstärkte internationale Zusammenarbeit soll die Sicherheit und Stabilität im Cyberraum erhöht und gegebenenfalls das Risiko einer Fehleinschätzung, Eskalation oder eines Konflikts infolge von IKT-Vorfällen verringert werden. Dieses Verhalten der EU soll potentielle Angreifer beeinflussen und die Sicherheit der EU erhöhen. In diesem Kontext ist auch die Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen (ABl. L 129I vom 17. Mai 2019, S. 1 ff.) zu nennen.

---

[44] ABl. L 151 vom 07. Juni 2019, S. 15 ff.
[45] Vgl. Finanzbogen 1.4.4.

2.1.1.3.22 Ausbau internationaler Übereinkommen

Noch auf Ebene von Gesprächen wollen die EU und die NATO über eine intensivierte Zusammenarbeit in dem Bereich der Cybersicherheit und -verteidigung beraten. Die Basis hierfür ist ein Übereinkommen über die Zusammenarbeit auf dem Gebiet der Cybersicherheit aus dem Jahr 2016. Ziel soll die Schaffung von Interoperabilität sein. Das soll durch kohärente Cybersicherheitsanforderungen und -standards geschehen. Daneben soll die Kooperation ein gemeinsames Training und Übungen vorsehen. Die Cybersicherheitsforschung und technologische Innovationen sollen ebenfalls vorangetrieben werden. Auch soll ein Krisenmanagementsystem etabliert werden. Auch in letzter Zeit gibt es weiter Aufrufe, die Zusammenarbeit zu intensivieren.[46]

Auch die EU-Mitgliedstaaten untereinander sollen unter anderem im Bereich der IT-Sicherheit enger zusammenarbeiten (Permanent Structures Cooperation – „PESCO“). Im November 2019 wurde das Cyber and Information Domain Coordination Centre (CIDCC) daher als PESCO Projekt eingerichtet.[47] Hauptaufgabe ist die Erstellung und Bewertung von einer einheitlichen Struktur folgenden Lagebildern des Cyberraums. Die erste Sitzung fand vom 21. - 22. April 2021 statt.

Einige EU-Staaten haben unter Federführung von Litauen ein Cyber Rapid Response Team (CRRT) aufgebaut. Auch dieses Projekt resultierte in der Schaffung einer PESCO.[48]

2.1.2 Nationale Vorgaben

Wegen des bereits aufgezeigten Fehlens einer einheitlichen gesetzlichen Niederlegung der rechtlichen Bedingungen der IT-Sicherheit befinden sich die normativen Vorgaben für diese in unterschiedlichen Gesetzen.

2.1.2.1 Organisationspflichten für Unternehmen: Risikomanagementsystem

Die Organisationspflichten hinsichtlich der IT-Sicherheit richten sich in erster Linie an die Unternehmensleitung.

Das KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) aus dem Jahr 1998 verpflichtet Unternehmen zur Schaffung eines unternehmensinternen Risikofrüherkennungssystems.

Diese Pflicht wurde in § 91 Abs. 2 AktG dahingehend konkretisiert, dass der Vorstand geeignete Maßnahmen zur Früherkennung gefährdender Entwicklungen zu treffen hat.

---

[46] Vgl. Committee on Foreign Affairs, Draft Report on the state of EU cyber defence capabilities, 2020/2256(INI) Nr. 21.
[47] https://pesco.europa.eu/project/cyber-and-information-domain-coordination-center-cidcc/.
[48] https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

Im Gleichlauf hierzu wurde das Handelsgesetzbuch insofern geändert, dass nach § 317 Abs. 4 HGB das Bestehen eines Früherkennungssystems Teil der Abschlussprüfung von Aktiengesellschaften ist.

Nach § 43 GmbHG ist der Geschäftsführer einer GmbH zur Einhaltung der Sorgfalt eines ordentlichen Geschäftsmannes verpflichtet. Diese Sorgfalt umfasst – in Anlehnung an das KonTraG – auch die Sicherstellung eines Risikomanagements,[49] welches auch die Gewährleistung der Sicherheit und Funktionsfähigkeit der IT enthalten muss.

Das Risikomanagement umfasst nicht nur die Risikofrüherkennung, sondern auch als wesentliche Aufgabe der Unternehmensleitung die Prävention. Durch das KonTra-Gesetz wurde festgestellt, dass zur „üblichen Sorgfalt“ der Unternehmensführung auch das Erkennen und Bekämpfen von Risiken, die den Bestand des Unternehmens gefährden, zählen. Darunter ist insbesondere aus IT-sicherheitsrechtlicher Sicht die Abwehr von IT-Risiken zu fassen.

Durch die GoB (Grundsätze ordnungsgemäßer Buchführung) sowie GoBS (Grundsätze ordnungsgemäßer DV-gestützter Buchführung), die Teil der GoB sind, werden die Unternehmensleitungen zu einer ordnungsgemäßen Buchführung verpflichtet. Textziffer 5 der GoBS enthält Vorgaben zur Datensicherheit. Die Unternehmensleitung ist mithin gehalten, die Daten gegen unberechtigte Kenntnisnahme und Datenverlust zu schützen.

Bereichsspezifische Normen zur IT-Sicherheit finden sich in § 25a KWG, dessen Vorgaben in dem von der BaFin als Rundschreiben erlassenen MaRisk Konkretisierung erfahren haben, § 15b, § 33 WpHG sowie § 64a VAG.

2.1.2.2 Datenschutzrechtliche Vorgaben zur IT-Sicherheit

Die zentrale IT-sicherheitsrechtliche Vorschrift des bis 2018 geltenden BDSG fand sich in § 9 BDSG a.F. Öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erhoben, verarbeiteten oder nutzten, hatten nach § 9 BDSG a.F. die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich waren, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Diese Vorgaben sind durch die DS-GVO hinfällig geworden und wurden aufgehoben.

Im BDSG finden sich vereinzelt Vorgaben in Bezug auf die IT-Sicherheit.

Nach § 22 Abs. 2 S. 2 BDSG muss der Verantwortliche, wenn er besondere Kategorien personenbezogener Daten § 22 Abs. 1 BDSG verarbeitet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und

[49] Vgl. Wolf, BC 2011, 353, 353; Scherer, CCZ 2012, 201, 205.

Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bestimmte Maßnahmen der IT-Sicherheit ergreifen.

Im Rahmen des Anwendungsbereichs des dritten Teils des BDSG müssen der Verantwortliche und deren Auftragsverarbeiter gem. § 64 BDSG Maßnahmen zur Gewährleistung der IT-Sicherheit ergreifen. Hierbei sind die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

§ 65 BDSG sieht bei der Verletzung des Schutzes personenbezogener Daten Meldepflichten an den BfDI beziehungsweise bei Auftragsverarbeitern an den Verantwortlichen vor.

In den Fällen des § 66 BDSG sind die Betroffenen zu benachrichtigen.

§ 71 BDSG sieht Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen vor (vgl. hierzu die Ausführungen zu Art. 25 DS-GVO).

2.1.2.3 IT-Sicherheit für Telemedien nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Von besonderer IT-sicherheitsrechtlicher Bedeutung beim Einsatz von Telekommunikation und Telemedien ist das TTDSG. Für die Telemedien gilt die Regelung des § 19 TTDSG. Der Anwendungsbereich dieser Norm setzt das geschäftsmäßige Angebot eines Telemediums durch einen Diensteanbieter voraus. § 19 TTDSG dient der Umsetzung der ePrivacy-Richtlinie und damit der Datensicherheit in der Telekommunikation, wie dies auch für die Datenübermittlung über das Internet und mithin Telemedien gilt. Im Übrigen lässt sich das geforderte IT-Sicherheitsniveau auch aus Art. 32 DS-GVO herleiten.

Nach § 19 Abs. 4 TTDSG haben Unternehmen, die eine Homepage betreiben, durch technische und organisatorische Vorkehrungen die Sicherheit der IT und Daten nach dem Stand der Technik herzustellen. Diesen Unternehmen legt § 19 Abs. 4 TTDSG die Verpflichtung auf, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist. Daneben sind die Diensteanbieter gehalten, die Telemedien gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, zu sichern. Dabei haben die Verpflichteten den Stand der Technik zu berücksichtigen (§ 19 Abs. 4 S. 2 TTDSG). Als Maßnahme i. S. v. § 19 Abs. 4 S. 1 TTDSG kann die Anwendung eines als sicher anerkannten Verschlüsselungssystems dienen, vgl. § 19 Abs. 4 S. 3 TTDSG. Sofern Anordnungen des BSI nach § 7d S. 1 BSIG getroffen wurden, bleiben diese von der Regelung des § 19 Abs. 4 TTDSG unberührt.

Beispiele für technische und organisatorische Vorkehrungen[50]

Technische Maßnahmen

- Verschlüsselungsverfahren
- Scannen der gehosteten Daten
- Installation einer Firewall

Organisatorische Maßnahmen

- Administratorenrechte
- Zugriffsrechte auf bestimmte personenbezogene Daten
- Schulung und Überwachung der Berechtigten
- vertragliche Abreden mit Geschäftspartnern
- vertragliche Auslagerung von Sicherheitsmaßnahmen an spezialisierte Dienstleister

Die anzuwendenden Maßnahmen stehen allerdings insgesamt unter dem Vorbehalt des technisch Möglichen und wirtschaftlich Zumutbaren. Beide Vorbehalte tragen zwar dem Verhältnismäßigkeitsprinzip Rechnung, führen aber zugleich zu Unsicherheiten in der konkreten Bestimmung der erforderlichen Maßnahmen.

Kriterien[51]

- Maßnahmenkosten
- Effektivität der Maßnahme
- Auswirkungen auf die Webseite, insbesondere auf Layout und Funktionsumfang
- Folgen für die Umsatz- und Gewinnspanne sowie die sonstigen verkehrswerten Vorteile, die aus dem Betrieb der Webseite resultieren
- Gefahren einer Unterlassung der Maßnahme
- Wahrscheinlichkeit der Störung/des äußeren Angriffs
- alternative Maßnahmen zur Verhinderung der Gefahren

2.1.2.4 IT-Sicherheit nach dem Telekommunikationsgesetz (TKG)[52]

Mit dem IT-Sicherheitsgesetz 2.0 sind auch die IT-Sicherheitsvorgaben des TKG reformiert worden. Diese befinden sich nunmehr in § 165 bis § 169 TKG.

[50] Djeffal, MMR 2015, 716, 719 ff.
[51] Djeffal, MMR 2015, 716, 718.
[52] Ab dem 01. Dezember 2021 gilt die durch das Telekommunikationsmodernisierungsgesetz beschlossene neue Fassung des TKG. Die technischen und organisatorischen Schutzmaßnahmen sind dann in § 165 TKG n. F. geregelt. Näher hierzu Marx, in: Heckmann/Paschke, jurisPraxiskommentar, 7. Aufl. 2021, Kap. 1.2 Rn. 29 ff.

§ 165 TKG trägt der besonderen Bedeutung der IT-Sicherheit im Rahmen der Telekommunikation Rechnung. Demnach muss jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, nach § 165 Abs. 1 TKG die angemessenen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten treffen. Dabei ist nach § 165 Abs. 1 S. 2 TKG der Stand der Technik zu berücksichtigen.

Während in der Vergangenheit noch die Frage im Raum stand, wer überhaupt als Diensteanbieter i. S. d. TKG galt, wurde der Wortlaut insoweit geweitet, dass jeder der Telekommunikationsdienste erbringt oder daran mitwirkt die technischen und organisatorischen Schutzmaßnahmen des TKG erfüllen muss. In der Vergangenheit hatte der EuGH bestimmt, dass die kostenpflichtige Variante von Skype als entsprechender Dienst einzuordnen sei,[53] der unentgeltliche OTT-Dienst Gmail jedoch kein elektronischer Kommunikationsdienst i. S. d. TKG.[54]

Die Betreiber öffentlicher Telekommunikationsnetze oder Erbringer öffentlicher Telekommunikationsdienste werden nach § 165 Abs. 2 TKG in die Pflicht genommen. Durch das IT-Sicherheitsgesetz wurde der „Stand der Technik“ als Maßstab in § 165 Abs. 2 TKG aufgenommen, sodass die dort bezeichneten IT-Sicherheitsmaßnahmen und Vorkehrungen ein höheres Maß an Aktualität erreichen dürften. Kritische Komponenten sind bei Betreibern öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur zulässig, wenn sie von einer anerkannten Zertifizierungsstelle erfolgreich geprüft und zertifiziert worden sind, § 165 Abs. 2 S. 4 TKG.

§ 166 Abs. 1 TKG verpflichtet den Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglicher Telekommunikationsdienste zur Benennung eines Sicherheitsbeauftragten, eines in der EU ansässigen Ansprechpartners sowie zur Erstellung eines Sicherheitskonzepts. Letztes ist der Bundesnetzagentur vorzulegen, § 166 Abs. 2 TKG. Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die in dem Sicherheitskonzept aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden, § 166 Abs. 3 TKG. Gemäß § 166 Abs. 5 TKG soll mindesten alle zwei Jahre eine Überprüfung des Sicherheitskonzepts durch die Bundesnetzagentur erfolgen.

Die Bundesnetzagentur legt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gem. § 167 TKG durch Allgemeinverfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest:

[53] EuGH, Urteil vom 05. Juni 2019, C-142/18 Rn. 49.
[54] EuGH, Urteil vom 13. Juni 2019, C-193/18 Rn. 41.

1. Einzelheiten der nach § 165 Abs. 1 bis 7 TKG zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste,
2. welche Funktionen kritische Funktionen i.S.v. § 2 Abs. 13 S. 1 Nr. 3 lit. b BSIG sind, die von kritischen Komponenten i.S.v. § 2 Abs. 3 BSIG realisiert werden und
3. wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist.

Die Verpflichteten haben nach § 167 Abs. 2 TKG die Vorgaben des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden.

§ 168 TKG beinhaltet Mittelungspflichten für Sicherheitsvorfälle bei öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten. Diese haben sowohl die BNetzA wie auch das BSI bei einem Sicherheitsvorfall mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich zu informieren.

Eine weitere Benachrichtigungspflicht besteht für öffentlich zugängliche Telekommunikationsdienste bei einer Verletzung des Schutzes personenbezogener Daten nach § 169 TKG. Diese haben nach § 169 Abs. 1 S. 1 TKG die Bundesnetzagentur und den BfDI zu informieren. Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Endnutzer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich nach § 169 Abs. 1 S. 2 TKG die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen.

2.1.2.5 IT-Sicherheit nach dem BSIG

Das IT-Sicherheitsrecht für Kritische Infrastrukturen wurde mit dem IT-Sicherheitsgesetz vom 17. Juli 2015 als Artikelgesetz in das BSIG eingepflegt. Das IT-Sicherheitsgesetz 2.0 trat nach „Kompetenzgerangel zwischen Bund und Ländern“[55] mit Wirkung zum 28. Mai 2021 in Kraft und reguliert nunmehr auch Unternehmen im besonderen öffentlichen Interesse. Es richtet sich in erster Linie an die Betreiber sog. Kritischer Infrastrukturen. An die Qualifizierung als Kritische Infrastruktur knüpfen die neu geschaffenen Pflichten im BSIG an. Neben der Sicherstellung der IT-Sicherheit durch bestimmte technische und organisatorische Maßnahmen wurden auch Melde- und Nachweispflichten etabliert. Zusätzlich werden jetzt auch Unternehmen im besonderen öffentlichen Interesse miteinbezogen (§ 2 Abs. 14 BSIG); hierbei handelt es sich um Rüstungshersteller, Unternehmen von erheblicher volkswirtschaftlicher Bedeutung und Betriebe, die mit Gefahrstoffen umgehen. Auch das BSI

[55] Hierzu Kipker, IT-SiG 2.0: Kompetenzgerangel zwischen Bund und Ländern, abrufbar unter https://community.beck.de/2021/02/09/it-sig-20-kompetenzgerangel-zwischen-bund-und-laendern.

erhält eine Vielzahl neuer Aufgaben und Befugnisse; aus Sicht der Unternehmen relevant sind insb. die §§ 7c, 7d BSIG: Hiernach kann das BSI zur Abwehr konkreter erheblicher Gefahren gegenüber Anbietern von TK-Diensten oder Telemediendiensten bestimmte Anordnungen treffen.

So schreibt § 8a Abs. 1 S. 1 BSIG vor, dass Betreiber Kritischer Infrastrukturen spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Abs. 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, getroffen haben. Hierbei ist der Stand der Technik einzuhalten (§ 8a Abs. 1 S. 2 BSIG). Die Angemessenheit der Maßnahmen bestimmt sich danach, ob der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht (§ 8a Abs. 1 S. 3 BSIG). Die Erfüllung dieser Verpflichtung haben die Betreiber Kritischer Infrastrukturen mindestens alle zwei Jahre auf geeignete Weise nachzuweisen (§ 8a Abs. 3 S. 1 BSIG). Der Gesetzgeber hat den Betreibern Kritischer Infrastrukturen und ihren Branchenverbänden freigestellt, die branchenspezifischen Sicherheitsstandards zur Gewährleistung der angemessenen organisatorischen und technischen Vorkehrungen zu bestimmen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Einvernehmen mit im Gesetz genannten Behörden die Eignung der Standards fest. Seit der Novelle zum BSIG durch das IT-Sicherheitsgesetz 2.0 erfasst die Verpflichtung, organisatorische und technische Vorkehrungen zu treffen, ab dem 01. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung, § 8a Abs. 1a BSIG; hierfür müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich erfasst und ausgewertet werden. Außerdem müssen fortwährend Bedrohungen identifiziert und vermieden sowie eingetretene Störungen behoben werden. Eine nähere Beschreibung dieser Systeme wurde in § 2 Abs. 9b BSIG ergänzt.

Zusätzlich zur Benennung der Kontaktstelle besteht nunmehr die explizite Pflicht zur Registrierung einer Kritischen Infrastruktur, § 8b Abs. 3 BSIG. Nach § 8b Abs. 3a BSIG kann das BSI die Vorlage der aus seiner Sicht erforderlichen Unterlagen verlangen, um zu prüfen, ob ein Betreiber ggfs. zur Registrierung verpflichtet, dieser Pflicht aber nicht nachgekommen ist. Zu den Unterlagen gehören die erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen, die ggfs. geeignet sind, soweit der Geheimnisschutz oder überwiegende Sicherheitsinteressen nicht entgegenstehen. Im Falle einer erheblichen Störung kann das BSI vom betroffenen Betreiber die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen, § 8b Abs. 4a BSIG; damit einhergehend wird eine Befugnisnorm für die Datenübermittlung im notwendigen Umfang normiert.

Das neu geschaffene Unternehmen im öffentlichen Interesse wird in dem neuen § 8f BSIG reguliert. Nach § 8f Abs. 1 BSIG müssen diese innerhalb derselben Frist wie Betreiber Kritischer Infrastrukturen (und danach mindestens alle zwei Jahre) eine Selbsterklärung zur IT-Sicherheit beim BSI vorlegen (ggfs. nach Maßgabe eines vom BSI herausgegebenen

Formulars, § 8f Abs. 2 BSIG), die Zertifizierungen (Nr. 1), sonstige durchgeführte Sicherheitsaudits oder Prüfungen (Nr. 2) oder anderweitig aufzeigt, inwieweit die für das Unternehmen besonders schützenswerten IT-Systeme, Komponenten und Prozesse angemessen geschützt werden und ob der Stand der Technik erreicht wird (Nr. 3). Auch Unternehmen im besonderen öffentlichen Interesse müssen sich ggfs. registrieren und einen Ansprechpartner benennen (§ 8f Abs. 5, 6 BSIG).

In Umsetzung der NIS-Richtlinie wurden auch Vorgaben für digitale Dienste (§ 2 Abs. 11, 12 BSIG) eingeführt. Diese finden sich in § 8c BSIG. Die Anbieter digitaler Dienste haben nach § 8c Abs. 1 BSIG geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

§ 8c BSIG sieht bei bestimmten Sicherheitsvorfällen eine Meldepflicht an das BSI vor. Bei Unternehmen im besonderen öffentlichen Interesse regelt dies § 8f Abs. 7, 8 BSIG.

§ 8d BSIG sieht zahlreiche Ausnahmen vom Anwendungsbereich vor, z. B., wenn Kleinstunternehmen betroffen wären oder bereits anderweitig eine Regulierung besteht.

§ 9a BSIG bezieht sich auf eine Cybersicherheitszertifizierung, weist diese unionsrechtlich vorausgesetzte Aufgabe aber tatsächlich nur dem BSI zu (Abs. 1). Die Vorschrift dient der „Umsetzung“ der ENISA-VO, indem die Öffnungsklauseln ausgefüllt werden.

Eine weitere Sonderregelung trifft der ebenfalls neu eingefügte § 9b BSIG: Die Vorschrift greift den neuen Begriff der kritischen Komponente (§ 2 Abs. 13 BSIG) auf und knüpft an diesen weitere Rechtsfolgen. So ist die Verwendung (neuer, vgl. § 9b Abs. 1 S. 2 BSIG) kritischer Komponenten zunächst einmal beim Innenministerium anzeigepflichtig (§ 9b Abs. 1 S. 1 BSIG). Beizulegen ist eine Garantieerklärung des Herstellers über die Vertrauenswürdigkeit der kritischen Komponente (§ 9b Abs. 3 BSIG). Sofern die öffentliche Ordnung oder Sicherheit Deutschlands voraussichtlich beeinträchtigt ist, kann die Verwendung untersagt werden. Auch die Verwendung einer bereits genehmigten kritischen Komponente kann untersagt werden (§ 9b Abs. 4 BSIG), auch für die Komponente bei anderen Betreibern Kritischer Infrastrukturen (§ 9b Abs. 6 BSIG). Als Untersagungsgrund genügt hier, auch, dass der Hersteller nicht vertrauenswürdig ist; Regelbeispiele sind in § 9b Abs. 5 BSIG normiert.

Schließlich führt § 9c BSIG ein freiwilliges IT-Sicherheitskennzeichen ein. Es dient dem Verbraucherschutz, § 9c Abs. 1 BSIG, setzt sich aus einer Herstellererklärung und einer Sicherheitsinformation zusammen (§ 9c Abs. 2 BSIG) und soll eine Information über die IT-Sicherheit (nicht hingegen den Datenschutz!) von Produkten geben. Es dürfen nur freigegebene IT-Sicherheitskennzeichen verwendet werden (§ 9c Abs. 4-8 BSIG).

Mittelbare Relevanz auf die IT-Sicherheit hat auch die Komplettüberarbeitung des Bußgeldkatalogs mit stark erhöhten Bußgeldern, vgl. § 14 BSIG n. F.

Ein Entwurf für die Zweite Verordnung zur Änderung der BSI-Kritisverordnung befindet sich derzeit im Diskussionsstadium.[56] Neu ist insbesondere, dass nunmehr auch Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind, eine Anlage i. S. d. Verordnung darstellen (§ 1 Nr. 1 lit. c). Auch die Anlage zum Sektor Informationstechnik und Telekommunikation wurde überarbeitet, die Top-Level-Domain-Name-Registry wurde explizit aufgenommen. Außerdem wurde der Begriff der gemeinsamen Anlage eingeführt und eine Regelung zur Verantwortlichkeit bei zwei oder mehr Betreibern eingefügt. Für die Praxis besonders zu beachten ist, dass die Schwellenwerte deutlich abgesenkt werden und einige neue Anlagen hinzukommen.[57]

Die Umsetzung der NIS-2-Richtlinie erfolgt durch ein „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG).[58]

Die wesentlichen Inhalte des Entwurfs stellen eine umfassende Reform des BSIG dar. Neben der Erweiterung der Befugnisse des BSI und einer Ergänzung der Vorgaben für das IT-Sicherheitsmanagements des Bundes, beinhaltet die Reform auch neue Regelungen, die sich an Wirtschaftsakteure richten.

Hierzu gehört insbesondere die Übernahme der Anforderungen an Risikomanagementmaßnahmen aus Art. 21 Abs. 2 NIS-2-RL (siehe Tabelle unter 2.1.1.3.4).

2.1.2.6 Sektorspezifische Kritische Infrastrukturen

Sektorspezifische Vorgaben zur IT-Sicherheit Kritischer Infrastrukturen ergeben sich beispielsweise aus dem Atomgesetz (AtG), dem Energiewirtschaftsgesetz (EnWG; durch das IT-Sicherheitsgesetz 2.0 ist insbesondere der hier relevante § 11 Abs. 1d und 1e BSIG hinzugekommen) oder dem Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (MsbG). Im Zuge des IT-Sicherheitsgesetzes vom 17. Juli 2015 wurden bereits einzelne Bestimmungen in den genannten Gesetzen überarbeitet oder neue Vorgaben ergänzt.

Aus dem Gesundheitswesen ist auf § 75b SGB V (IT-Sicherheit im vertragsärztlichen Bereich) und § 75c SGB V (IT-Sicherheit in Krankenhäusern) hinzuweisen. Im BSIG sind nur wirklich große Krankenhäuser als KRITIS erfasst, nämlich solche, die mehr als 30.000 stationäre Behandlungsfälle pro Jahr aufweisen (§§ 2 Abs. 10 Nr. 1, 10 Abs. 1 BSIG i. V. m. § 6 BSI-KritisV i. V. m. Anlage 5 Teil 3 BSI-Kritis-V).

---

[56] Die folgenden Ausführungen basieren auf dem Bearbeitungsstand des Referentenentwurfs des Bundesministeriums des Innern, für Bau und Heimat vom 22. April 2021. Weitere im Internet kursierende Versionen sind nicht bestätigt.
[57] Siehe hierzu die Synopse unter https://www.openkritis.de/it-sicherheitsgesetz/kritis-anlagen_kritisv_itsig20.html.
[58] Der aktuelle Referentenentwurf ist abrufbar unter https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/. Zu dem nationalen Referentenentwurf vgl. *Kipker/Dittrich*, MMR 2023, 481.

2.1.3 Standards der IT-Sicherheit

Keinen verpflichtenden, aber richtungsweisenden Charakter haben die internationalen und nationalen Standards zur IT-Sicherheit. Diese können als Leitfaden für objektive Mindeststandards dienen. Vielfach enthalten diese auch Best-Practice-Angaben. Unter IT-Sicherheitsstandards können „Bedingungen für die hinreichende, dem Stand der Technik entsprechende und die Integrität der informationstechnischen Systeme wahrende Festlegungen zur IT-Sicherheit“ verstanden werden.[59]

Beispiele für Standards[60]

- ISO/IEC 27001
- ISO/IEC 20000
- ISO/IEC 27018 für Cloud Computing
- IT-Grundschutz-Kompendium des BSI
- CobiT
- ITIL

Eine detaillierte Übersicht finden Sie in den Anhängen 1 und 2.

Die Standards entfalten in mehrerlei Hinsicht rechtliche Relevanz[61], siehe hierzu 2.3.

2.1.4 Internationale Entwicklungen

Auch mit Blick auf das Nicht-EU-Ausland gibt es in jüngster Zeit diverse Entwicklungen der IT-Sicherheitsregulierung zu verzeichnen.

2.1.4.1 Japanisches „Cyber/Physical Security Framework“

Exemplarisch genannt sei zunächst der vom japanischen Ministerium für Wirtschaft, Handel und Industrie (METI) erlassene Entwurf eines japanischen „Cyber/Physical Security Framework“ im Januar 2019. Mit dem Framework werden die bisher in Japan schon bestehenden Regelungen – insbesondere was die Sicherheit staatlicher und kritischer Infrastrukturen betrifft – ergänzt.

Inhalte des Frameworks – das vorrangig an die „Connected Industry“ und die smarte Sozialinfrastruktur („Society 5.0“) adressiert ist – sind Maßnahmen zur IT-Sicherheit wie

[59] Denkhaus/Richter/Bostelmann, OZG, 2019, § 5 Rn. 4 m.w.N.
[60] Eine Übersicht bietet: http://kompass-sicherheitsstandards.de/Welche-Standards-gibt-es.
[61] Angelehnt an Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=3, Rn. 142 ff.

Security by Design, ganzheitlicher Schutz von Versorgungsstrukturen und -ketten sowie die Sicherheit von im Netzwerk zirkulierenden Daten. Darüber hinaus umfasst das Framework auch Use Cases, Vorgaben zur Risikoanalyse und Regelungen zum Umgang mit IT-Sicherheitsrisiken.

2.1.4.2 Chinese Cybersecurity Law

Ähnlich aktuell zeigt sich der chinesische Gesetzgeber mit seiner Konkretisierung des „Chinese Cybersecurity Law“ vom 15. September 2018.[62]

Im Zuge dieser Konkretisierung wurden „Regulations for Internet Security Supervision and Inspection by Public Security Organs“ eingeführt, innerhalb derer IT-Sicherheit aus Perspektive der allgemeinen öffentlichen Sicherheit betrachtet wird. Der Anwendungs-bereich der Regelungen beschränkt sich dabei auf Internet Service Provider und Netzwerkbenutzer. Beispiele hierfür sind Internetdatencenter oder auch das Anbieten von Internetinformationsdiensten.

Inhalt der Konkretisierung ist unter anderem das Vorhalten technisch-organisatorischer Maßnahmen zur Datenspeicherung, die Etablierung eines Sicherheitsmanagements und die Einführung von Meldepflichten und Überwachungsmaßnahmen (auch „Vorratsdatenspeicherung“). Geregelt werden zudem die Überprüfungsrechte staatlicher Behörden sowie die Einführung von Verwaltungs- und Strafaktionen. Die Betrachtung der IT-Sicherheit erfolgt aus Perspektive der öffentlichen Sicherheit.

Am 10. Juni 2021 hat der ständige Ausschuss des Nationalen Volkskongresses in China ein neues Datensicherheitsgesetz (Data Security Law – DSL) verabschiedet, der ab dem 01. September 2021 in Kraft ist. Das DSL führt neue Konzepte wie “key data" und “important data” und beinhaltet strikte Sicherheitsmaßnahmen.

2.1.4.3 Gesetz zur Regelung von Anforderungen an connected devices in Kalifornien

Ebenfalls im September 2018 in Kraft getreten ist im US-Bundesstaat Kalifornien ein Gesetz zur Regelung von Anforderungen an connected devices (IoT). Durch dieses Gesetz sind sowohl Hersteller solcher Geräte als auch Unternehmen, die sich Dritter zur Herstellung der Geräte bedienen, verpflichtet, jene Geräte im Hinblick auf Art, Funktion und gespeicherte Daten mit angemessenen Sicherheitsmerkmalen auszurüsten. Davon ist nicht nur der Schutz personenbezogener Daten umfasst. Zielrichtung des Gesetzes ist es, unbefugten Zugriff, die Modifizierung oder Offenlegung von Informationen zu verhindern. Erreicht werden soll dies beispielsweise durch individuelle Passwörter pro Gerät oder das notwendige Erstellen eines eigenen Passworts nach erstmaliger Anmeldung.

[62] Hierzu Köstner/Nonn, MMR 2020, 591; Wagner, ZD 2020, 140 (142); Kipker/Müller, DSRITB 2018, 713 (719 f.).

2.1.4.4 Australisches Sicherheitsgesetz

In Australien wurde Ende des Jahres 2018 ein Gesetz verabschiedet, durch das Unternehmen gezwungen sind, Sicherheitslücken in Hard- und Software einzubauen, sodass Verschlüsselungsvorkehrungen zu Zwecken der Strafverfolgung umgangen werden können. Sofern ein Ersuchen auf Zugriff vorlag, sind Unternehmen aber nicht befugt, dies offen zu legen.

2.1.4.5 Israelisches Cybersicherheitsgesetz

Ebenfalls 2018 wurde in Israel ein Entwurf für ein neues Cybersicherheitsgesetz „Memorandum on Cyber Protection and the National Cyber Directorate“ veröffentlicht.[63] Zwei der mit dem Entwurf einhergehenden Ziele sind die Entwicklung von Definitionen im Bereich Cybersicherheit sowie die Bestimmung eines nationalen Regulierungsrahmens. Darüber hinaus sollen die Zwecke und Funktionen des „National Cyber Directorate (NCD)“ bestimmt sowie die Befugnisse des NCD festgelegt werden.

2.1.4.6 Weltwirtschaftsforum

Auch das Weltwirtschaftsforum befasste sich im vergangenen Jahr im Zuge der Errichtung eines “Global Centre for Cybersecurity” mit der Thematik IT-Sicherheit. Das Global Centre for Cybersecurity zielt zum einen auf die Konsolidierung bestehender, das Thema IT-Sicherheit betreffender Initiativen des Weltwirtschaftsforums ab. Daneben soll der Informationsaustausch der Forumsmitglieder auch mit Blick auf die Errichtung eines Frühwarnsystems für Cyberattacken und eines unabhängigen Wissensspeichers für IT-Sicherheitsmaßnahmen verbessert werden. Insgesamt soll im Rahmen des Global Centre for Cybersecurity eine agile, zweckdienliche Rahmenstruktur für IT-Sicherheit entstehen.

2.1.4.7 Russisches Cyber-Sicherheitsgesetz

Russland hat seine Cyber-Security-Doctrine 2018 reformiert.[64] Die neuen Regelungen sind inhaltlich zumindest teilweise vergleichbar mit dem BSIG oder der NIS-RL.

2.2 Zentrale Weichenstellung: Kritische Infrastrukturen / Anbieter digitaler Dienste

Die Betrachtung des auf Unternehmen anwendbaren IT-Sicherheitsrechts zeigt, dass zwei Regelungsregime für die IT-Sicherheit in der Wirtschaft vorhanden sind.

[63] Vgl. hierzu Kipker/Müller, DSRITB 2018, 713 (722 f.).
[64] Vgl. Kipker/Müller, DSRITB 2018, 713 (717 f.).

Einerseits das Regelungsregime für Kritische Infrastrukturen und Anbieter digitaler Dienste sowie Unternehmen im besonderen öffentlichen Interesse, das durch das IT-Sicherheitsgesetz beziehungsweise durch die Umsetzung der NIS-RL eine Normierung erfahren hat und die NIS-2-RL weiter geschärft wird, und andererseits das IT-Sicherheitsrecht für alle sonstigen Unternehmen, das sich verstreut in allgemeinen und besonderen Einzelregelungen findet.

Zentrale Weichenstellung hinsichtlich des auf Unternehmen anwendbaren IT-Sicherheitsrechts ist damit entweder die Qualifizierung eines Unternehmens als Kritische Infrastruktur i. S. v. § 2 Abs. 10 BSIG, als Anbieter digitaler Dienste gem. § 2 Abs. 12 BSIG oder als Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 BSIG.

In § 2 Abs. 10 BSIG findet sich die Legaldefinition der Kritischen Infrastrukturen i. S. d. BSIG.

§ 2 Abs. 10 BSIG

---

(10) [1]Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

[2]Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

Die Bestimmung, ob eine Einrichtung, Anlage oder Teile davon eine Kritische Infrastruktur darstellen, bestimmt sich anhand von zwei Kriterien. Zum einen nach der Zuordnung zu einem der genannten Sektoren in Nr. 1 (Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen) und zum anderen nach der hohen Bedeutung für das Funktionieren des Gemeinwesens, da durch den Ausfall oder die Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (Nr. 2).

Die ursprünglich am 03. Mai 2016 in Kraft getretene Rechtsverordnung zur näheren Bestimmung der Kritischen Infrastrukturen nach §§ 2 Abs. 10 S. 2, 10 Abs. 1 BSIG enthielt in ihrer ursprünglichen Fassung lediglich Bestimmungen zu den Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung. Die Bestimmungen zu den Sektoren Transport, Verkehr, Gesundheit sowie Finanz- und Versicherungswesen wurden nachgelagert mit dem „2. Korb“ der BSI-KritisV verabschiedet. Das IT-Sicherheitsgesetz 2.0 hat zuletzt die Siedlungsabfallentsorgung aufgenommen.

Für Anbieter digitaler Dienste (§ 2 Abs. 11 und 12 BSIG) gilt § 8c BSIG. Diese sind durch das Gesetz zur Umsetzung der NIS-RL näher definiert, das am 18. Oktober 2024 außer Kraft tritt. Spätestens im Oktober 2024 muss der deutsche Gesetzgeber auch das Gesetz zur Umsetzung der NIS-2-Richtlinie vorgelegt haben.[65]

§ 2 Abs. 11 BSIG

(11) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 09. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17. September 2015, S. 1), und die

1. es Verbrauchern oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18. Juni 2013, S. 63) ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Webseite dieser Dienste oder auf der Webseite eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste verwendet, abzuschließen (Online-Marktplätze);
2. es Nutzern ermöglichen, Suchen grundsätzlich auf allen Webseiten oder auf Webseiten in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können (Online-Suchmaschinen);
3. den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen (Cloud-Computing-Dienste),

und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden.

§ 2 Abs. 12 BSIG

(12) „Anbieter digitaler Dienste“ im Sinne dieses Gesetzes ist eine juristische Person, die einen digitalen Dienst anbietet.

[65] Die bisherigen Referentenentwürfe können hier abgerufen werden https://ag.kritis.info/2023/07/19/referentenentwurf-des-bmi-nis-2-umsetzungs-und-cybersicherheitsstaerkungsgesetz-nis2umsucg/. Zum nationalen Referentenentwurf vgl. Kipker/Dittrich, MMR 2023, 481.

2.3 Haftungsrisiken und Folgen bei IT-Unsicherheit

Trotz der teils noch unklaren Rechtslage in Bezug auf das Recht der IT-Sicherheit, der verstreuten Regelungspraxis und der vielfach ausfüllungsbedürftigen Vorbehalte der Erforderlichkeit und Zumutbarkeit stellen sich bei Verletzungen von IT-sicherheitsrechtlichen Vorgaben weitreichende Haftungsfragen.

2.3.1 Sorgfaltspflichten

Zum einen gibt es Standards, die verpflichtend eingehalten werden müssen, z. B. im Bereich der Verwaltung (vgl. Art. 43 BayDiG, § 10 EGovG). Auch das BSIG kennt verpflichtende Standards (vgl. § 8 Abs. 1 BSIG). Teilweise wird in Rechtsverordnungen auf Standards Bezug genommen (§ 5 OZG). Sie können aber auch zwischen den Parteien vereinbart werden und sind so auf eine vertragliche Grundlage gestellt. Die Vorgaben können auch in einem Vergabeverfahren Berücksichtigung finden.

Zum anderen können auch vermeintlich „unverbindliche“ Standards (vor allem die ISO-Standards) bei ihrer Missachtung Folgen hervorrufen („soft law“). Im Falle einer Cyber-attacke mit Schäden können die üblichen technischen Standards zusammen mit dem Stand der Technik als Sorgfaltsmaßstab (vertragliche Rücksichtnahmepflicht, Begründung eines Sachmangels oder aber auch als deliktische Verkehrssicherungspflicht) herangezogen werden. Auch sind Branchenstandards und technische Normen ein wesentlicher Maßstab im Rahmen des Produkthaftungsrechts, sodass bei Missachtung ein Haftungsfall vorliegen kann. Standards begründen in der Regel nur Mindestanforderungen, sodass Gerichte andere und vor allem strengere Vorgaben verlangen können (was in der Praxis aber nur ausnahmsweise geschieht). So sind etwa schutzwürdige Verkehrskreise besonders zu berücksichtigen, was bei Standards nicht immer der Fall ist. Es ist hingegen nicht ausgeschlossen, dass durch alternative Methoden für ein gleichartiges Niveau an IT-Sicherheit gesorgt wird. In diesem Fall scheidet eine Haftung aus, auch wenn die Standards nicht beachtet werden.

Da Zertifizierungen von Standards nur eine Momentaufnahme sind, kann aus diesen nicht per se die Einhaltung des Sorgfaltsmaßstabs folgen. Darüber hinaus spiegelt sich in diesen auch nur der genannte „Mindeststandard“ wider.

Grundsätzlich übernimmt die Leitungsebene die Verantwortung für die IT-Sicherheit und muss die allgemeinen Anforderungen zur IT-Sicherheit beachten, vgl. § 43 Abs. 1 GmbHG, § 93 Abs. 1 AktG, § 91 Abs. 2 AktG.

Nach § 93 Abs. 1 S. 1 AktG hat der Vorstand bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Vorstandsmitglieder, die ihre Pflichten verletzen, sind gem. § 93 Abs. 2 AktG der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast. An dieser Stelle entfalten Standards die oben genannte Wirkung. Zu beachten bleibt jedoch, dass der Vorstand die Aufgabe zwar delegieren darf, aber die Leitung und

regelmäßige Überwachung gewährleistet bleiben muss. Streitig ist, ob sich ein weitgehendes Informationssicherheitsmanagementsystem aus den §§ 91, 93 AktG herleiten lässt. Nach dem Wortlaut der Normen sind nur Früherkennungssysteme für bestandsgefährdende Risiken erforderlich. Das kann bei IT-Sicherheitsrisiken nicht immer angenommen werden.

Für Geschäftsführer einer GmbH soll sich das aus § 43 Abs. 1 GmbHG, § 347 Abs. 1 HGB ergeben („dort aber weniger explizit geregelt"). Nach § 43 Abs. 1 GmbHG haben die Geschäftsführer in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes (vgl. § 347 Abs. 1 HGB: „ordentlicher Kaufmann") anzuwenden. Werden diese missachtet, haftet der Vorstand als Gesamtschuldner, § 43 Abs. 2 GmbHG.

2.3.2 Schadensersatzpflicht

2.3.2.1 Deliktische Haftung

Die deliktische Haftung für IT-sicherheitsrechtliche Verstöße folgt in erster Linie aus § 823 Abs. 1 BGB oder § 823 Abs. 2 BGB i. V. m. der Verletzung von Schutzgesetzen.

Vielfach wird kein positives Handeln als Verletzungshandlung vorliegen, sondern lediglich der Verstoß gegen Verkehrssicherungspflichten. Verkehrssicherungspflichten ergeben sich zumeist aus der Herrschaft über Gefahrenquellen. Derjenige, der eine Gefahrenquelle betreibt, ist verpflichtet, die notwendigen und zumutbaren Vorkehrungen zu treffen, um Schädigungen anderer zu vermeiden. Verkehrssicherungspflichten werden insbesondere auch durch technische Standards konkretisiert, sie werden also mittelbar im Rahmen des § 823 BGB relevant.

Beispiel

Die Kontrolle über den Zugang zu IT-Systemen stellt eine Gefahrenquelle dar, die zu Verkehrssicherungspflichten hinsichtlich dieser Gefahrenquelle führt. So kann sich eine Haftung des IT-Verwenders ergeben, wenn dieser seine Gefahrenquelle „IT-System" nicht durch aktuell verfügbare Sicherheitsmaßnahmen, etwa Anti-Viren-Programme und Passwörter, schützt und sich infolgedessen ausgehend von seinen IT-Systemen Malware auf andere Systeme verbreitet und dadurch Schäden entstehen.

Unabhängig davon ist natürlich die Haftung des Malware-Schöpfers, die sich ebenso aus Delikt ergibt.

Die verschuldensabhängige deliktische Haftung des § 823 BGB setzt zumindest fahrlässiges Handeln des Verletzers voraus (vgl. § 823 Abs. 1, 2 S. 2 BGB). Fahrlässig handelt, wer die im

Verkehr erforderliche Sorgfalt außer Acht lässt (vgl. § 276 Abs. 2 BGB). Es handelt sich also nicht um eine Gefährdungshaftung.

Die Bestimmung der erforderlichen Sorgfalt kann im Einzelfall erhebliche Schwierigkeiten bereiten.

Anerkannt ist zumindest, dass Unmögliches nicht eingefordert werden kann. Damit beschränkt sich die Sorgfalt auf vermeidbare Risiken und erfasst nicht auch noch unvermeidbare Risiken.

Rückschlüsse auf die zu fordernde Sorgfalt können sich aus dem Rechtsrahmen des IT-Sicherheitsrechts ergeben. Problematisch ist nur, dass die zu fordernden IT-sicherheitsrechtlichen Anforderungen vielfach den Vorbehalten des technisch Möglichen und wirtschaftlich Zumutbaren unterliegen und damit keine allgemeingültigen Aussagen getroffen werden können.

Trotz dieser Unsicherheiten lassen sich einige IT-sicherheitsrechtliche Verstöße als fahrlässig, wenn nicht gar grob fahrlässig einordnen.

Beispiele für fahrlässiges Verhalten

- Fehlen eines hinreichenden IT-Sicherheitskonzepts
- Einsatz veralteter Hardware und Software, die nicht mehr aktualisiert wird
- Versäumen von Sicherheitsupdates
- Nicht-Verwendung handelsüblicher Security-Lösungen
- Verwendung unzureichender Zugangshürden (Passwörter etc.)
- Fehlende oder unzureichende Schulung der Mitarbeiter
- Sorgloser Umgang mit mobilen Endgeräten

Aus spezifischen IT-sicherheitsrechtlichen Bestimmungen, etwa den Regelungen des IT-Sicherheitsgesetzes, können sich erweiterte Anforderungen an die IT-Sicherheit ergeben. So werden je nach Adressatenkreis des IT-Sicherheitsgesetzes erhöhte Anforderungen an die im Verkehr erforderliche Sorgfalt gestellt.

Nicht außer Acht zu lassen sind etwaige Mithaftungsquoten des in eigenen Rechtsgütern Verletzten, die zu einer eingeschränkten Liquidierbarkeit von Schäden führen können. Nach § 254 BGB muss sich der Verletzte eigenes Verschulden bei der Entstehung oder Vertiefung des Schadens zurechnen lassen. Soweit also der Verletzte selbst IT-sicherheitsrechtliche Verpflichtungen verletzt hat, kann dies zu einer lediglich anteiligen Haftung des Verletzers bis hin zu einem Ausschluss der Haftung führen.

Beispiel: OLG Hamm, MMR 2004, 487

Ein Reisebüro hatte einen Computer-Reparaturdienst damit beauftragt, die Ursachen für eine Fehlermeldung des IT-Systems zu finden. Bei der Suche kam es zum Serverabsturz, woraufhin zahlreiche Geschäftsdaten teils unwiederbringlich gelöscht wurden, da das Reisebüro nicht einmal monatlich eine Datensicherung durchführte. Daraufhin machte das Reisebüro Schadensersatz gegen den Reparaturdienst geltend, da sich dieser über den Stand der vorgenommenen Datensicherung hätte informieren müssen. Das OLG Hamm nahm jedoch ein überwiegendes Mitverschulden des Reisebüros i. S. d. § 254 BGB an, da die Gewährleistung einer zuverlässigen, zeitnahen und umfassenden Routine zur Datensicherung zu den im gewerblichen Bereich vorauszusetzenden Selbstverständlichkeiten gehört.

Denkbar sind auch Ansprüche des Unternehmens selbst gegen eigene Mitarbeiter aus Delikt. Allerdings wären die allgemein geltenden Grundsätze des innerbetrieblichen Schadensausgleichs zu berücksichtigen, die vielfach zu einem Entfallen der Haftung des Mitarbeiters führen würden.

Für die Hersteller von IT-Produkten und IT-Systemen kann eine Haftung nach den Grundsätzen der Produzentenhaftung i. V. m. § 823 Abs. 1 BGB in Frage kommen. Daneben gilt das Produkthaftungsgesetz, das in § 1 Abs. 1 ProdHaftG einen Anspruch gegen den Hersteller statuiert und im Unterschied zu den §§ 823 Abs. 1, Abs. 2, 826 BGB verschuldensunabhängig ausgestaltet ist.

Zudem können in bestimmten Fällen deliktische Haftungstatbestände aus Spezialgesetzen nach § 823 Abs. 2 BGB in Frage kommen.

Beispielsweise kann eine deliktische Haftungsverpflichtung eines Telekommunikations-unternehmers nach §§ 44, 44a TKG gegenüber Wettbewerbern und Endverbrauchern im Falle der Missachtung der Benachrichtigungs- und Störungsbeseitigungsverpflichtung nach § 109a Abs. 4 TKG bestehen.

Im datenschutzrechtlichen Bereich kann sich eine Verpflichtung zum Schadensersatz aus Art. 82 DS-GVO ergeben. Hiernach hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, grundsätzlich einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Künftig wird auch das Produkthaftungsgesetz Software unter den Produktbegriff fassen und mangelnde IT-Sicherheitsvorkehrungen als Produktfehler aufgreifen (vgl. 2.1.1.3.8.).

2.3.2.2 Vertragliche Haftung

Soweit vertragliche Beziehungen zwischen dem Geschädigten und dem Verletzer bestehen, können vertragliche Haftungsansprüche aufgrund von IT-sicherheitsrechtlichen

Verstößen in Betracht kommen. Die vertragliche Haftung unterliegt – wie die deliktische Haftung – dem Verschuldensprinzip. Demnach muss der haftende Vertragspartner die Pflichtverletzung zu vertreten haben (vgl. § 280 Abs. 1 S. 2 BGB). Zu vertreten hat der Vertragspartner Fahrlässigkeit und Vorsatz. Die zentrale Fragestellung bei der vertraglichen Haftung ist damit die Einhaltung der im Verkehr erforderlichen Sorgfalt. Anhaltspunkte für die Bestimmung der erforderlichen Sorgfalt finden sich wiederum im Recht der IT-Sicherheit. Darüber hinaus können die Vertragsparteien selbstredend zusätzliche IT-sicherheitsrechtliche Pflichten vereinbaren.

Das konkrete Haftungsregime richtet sich nach dem zugrundeliegenden Vertragstyp. Denkbar ist im Falle einer Verletzung IT-sicherheitsrechtlicher Pflichten im Falle eines Kaufvertrags das Vorliegen eines Sachmangels nach § 434 BGB, ggfs. über § 650 BGB im Falle eines Werklieferungsvertrags.

Inzwischen ist auch der neue Vertragstypus des Vertrags über digitale Inhalte gem. § 327 ff. BGB zu beachten. Durch das Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 25. Juni 2021 (BGBl. I 2021 S. 2123 ff.) wurde dieser in das BGB aufgenommen. Auch der Vertrag über digitale Inhalte hat sein eigenes Haftungsregime erhalten, das es ggfs. zu beachten gilt. Ein Produktmangel nach § 327e BGB liegt beispielsweise vor, wenn das digitale Produkt nicht den Sicherheitsanforderungen entspricht (§ 327e Abs. 3 Nr. 2 BGB). Auch eine Updatepflicht ist in § 327f BGB vorgesehen.

Auch im Rahmen der vertraglichen Haftung können sich Beschränkungen aus dem Gesichtspunkt anzurechnenden Mitverschuldens nach § 254 BGB ergeben.

Ein aktuelles Urteil des OLG Karlsruhe (Urteil vom 27. Juli 2023 – Az. 19 U 83/22)[66] zeigt das Risiko, wenn man zu sehr auf elektronische Kommunikation vertraut.

In dem Rechtsstreit ging es um einen Kaufpreisanspruch. Die Beklagte weigerte sich zu zahlen, da sie eine gefälschte Rechnung erhalten und diese dann beglichen hatte. Sie wollte nicht „erneut“ zahlen und warf der Klägerin vor, unzureichende Sicherheitsvorkehrungen getroffen zu haben. Die Klägerin ihrerseits argumentierte, dass ihre E-Mail-Kommunikation gehackt worden sei und sie deshalb nicht für die gefälschte Rechnung verantwortlich gemacht werden könne.

Vor diesem Hintergrund war das OLG Karlsruhe mit zwei zentralen Fragestellungen konfrontiert. Erstens, inwiefern eine Zahlung an einen unbekannten Dritten gemäß § 362 BGB Erfüllungswirkung entfalten könnte. Zweitens, welche angemessenen Sicherheitsvorkehrungen im Kontext geschäftlicher E-Mail-Korrespondenz zu treffen sind und von der Klägerin möglicherweise zu treffen gewesen wären.

Das OLG Karlsruhe gab der Klägerin Recht, dass ihr Zahlungsanspruch durch die Zahlung der gefälschten Rechnung durch die Beklagte nicht erloschen sei. Im Fokus des Urteils

[66] https://lrbw.juris.de/cgi-bin/laender_rechtsprechung/document.py?Gericht=bw&nr=39004.

steht die Frage, ob die Klägerin ausreichende Sicherheitsmaßnahmen ergriffen hat, um solche Vorfälle zu verhindern, und ob sie deshalb für den erlittenen Schaden haftbar gemacht werden kann. Ein mögliches Fehlverhalten der Klägerin, das dazu führte, dass ein Dritter die gefälschte Rechnung mit veränderten Kontodaten der Beklagten senden konnte und so eine Täuschung über die Zahlung auslöste, könnte Schadensersatzansprüche der Beklagten gemäß § 280 Abs. 1 BGB wegen Verletzung vertraglicher Nebenpflichten begründen.

Das Gericht analysierte die Pflichten der Klägerin im Zusammenhang mit der E-Mail-Sicherheit. Es kommt zu dem Schluss, dass keine konkreten gesetzlichen oder branchenüblichen Verpflichtungen für die Anwendung bestimmter Verschlüsselungsverfahren im Geschäftsverkehr bestehen. Es existieren keine eindeutigen Vorschriften für Sicherheitsmaßnahmen bei E-Mails im geschäftlichen Kontext. Insbesondere sei der sachliche Anwendungsbereich der Datenschutz-Grundverordnung im Streitfall nicht eröffnet, da diese nur für die Verarbeitung von Informationen gilt, die sich auf eine natürliche Person beziehen (vgl. Art. 2 Abs. 1, Art. 4 Nr. 1 DS-GVO). Auch eine ausdrückliche Vereinbarung zwischen den Parteien fand nicht statt. Daher könne der Klägerin keine Pflichtverletzung im Zusammenhang mit der Vernachlässigung spezifischer Sicherheitsverfahren vorgeworfen werden.

Die Beklagte argumentiert weiterhin, dass die Klägerin durch den Verzicht auf bestimmte Sicherheitsmaßnahmen wie das SPF-Verfahren oder die Verschlüsselung von PDF-Dateien fahrlässig gehandelt habe. Das Gericht weist jedoch darauf hin, dass die Beklagte keine ausreichenden Gründe vorlegt, warum diese Maßnahmen in der spezifischen Geschäftsbeziehung zwischen den Parteien erwartet werden sollten. Das Gericht betont zudem, dass die Beklagte ihrerseits keine ausreichenden Sicherheitsvorkehrungen getroffen hat. Auffällige Unstimmigkeiten in der gefälschten Rechnung wurden von der Beklagten nicht ausreichend hinterfragt. Das Gericht argumentiert, dass die Klägerin keine ausreichende Kausalität zwischen ihren angeblichen Pflichtverletzungen und dem erlittenen Schaden nachgewiesen wurde. Insgesamt zeigt das Urteil, dass im E-Mail-Verkehr zwischen Unternehmen keine klaren gesetzlichen Anforderungen für Sicherheitsmaßnahmen gelten. Die Beklagte wird für ihre mangelnde Achtsamkeit hinsichtlich verdächtiger Rechnungen kritisiert und kann keinen ausreichenden Zusammenhang zwischen den behaupteten Pflichtverletzungen der Klägerin und dem erlittenen Schaden herstellen. Dies führt auch zu einer deutlichen Reduktion eines möglichen Schadensersatzanspruches der Beklagten nach § 254 BGB. Das Gericht unterstreicht, dass es im vorliegenden Fall nicht überzeugend nachgewiesen wurde, dass der Angriff in der kontrollierbaren Sphäre der Klägerin stattgefunden hat.

2.3.3 Ordnungswidrigkeiten

Die Nichterfüllung IT-sicherheitsrechtlicher Vorgaben kann auch zur Verhängung von Bußgeldern durch staatliche Stellen führen.

Grundvoraussetzung ist ein vorsätzlicher oder fahrlässiger Verstoß gegen die bußgeld-bewehrten IT-sicherheitsrechtlichen Vorschriften.

Überblick über ausgewählte Bußgeldtatbestände[67]

Art. 83 Abs. 4 lit. a DS-GVO	Bei Verstößen gegen Art. 25, 32 ff. DS-GVO
Art. 83 Abs. 5 lit. a DS-GVO	Bei Verstößen gegen Art. 5 Abs. 1 lit. f DS-GVO („Integrität und Vertraulichkeit“)
§ 228 Abs. 2 Nr. 38 TKG	Verstoß gegen die rechtzeitige Erstellung eines Sicherheitskonzepts
§ 228 Abs. 2 Nr. 39 TKG	Unterlassene Meldung eines Sicherheitsvorfalls
§ 64 Abs. 3 Nr. 15 ZAG	Unrichtige oder unvollständige Unterrichtung der BaFin über Vorfälle

Eine für die Praxis erhebliche Frage wird derzeit vor dem EuGH verhandelt: Muss ein Unternehmen auch dann ein Bußgeld zahlen, wenn ein Verstoß gegen die DSGVO (zum Beispiel auch ein Verstoß gegen Pflichten zur Gewährleistung von Datensicherheit nach Art. 25, 32 DSGVO) vorliegt, dem Unternehmen aber kein Verschulden (Vorsatz oder Fahrlässigkeit) vorgeworfen werden kann (Prinzip der „strict liability“).

Während zwei Generalanwälte am EuGH in den Vorlageverfahren das Prinzip der verschuldensunabhängigen Haftung ablehnen[68], hat sich die Datenschutzkonferenz der Vertreter der Aufsichtsbehörden von Bund und Ländern in Deutschland (kurz vor der mündlichen Verhandlung beim EuGH im Fall Deutsche Wohnen) im Januar 2023 dahingehend positioniert, dass Bußgelder nach Art. 83 DSGVO auch verschuldensunabhängig verhängt werden dürften.[69] Ein Blick in die juristische Literatur zur DSGVO zeigt ein gegenüber der Rechtsauffassung der DSK konträres Bild. Dort wird eine verschuldensunabhängige Bußgeldhaftung nach Art. 83 DSGVO weitgehend abgelehnt.[70] Dieser herrschenden Lehre ist im Ergebnis zuzustimmen.

Wenn man „strict liability“ im Kontext des Rechtsstaatsprinzips betrachtet, scheidet eine verschuldensunabhängige Haftung – zumal im Datenschutzrecht – aus. So ist das Verschuldensprinzip ein Bestandteil der Rechtsstaatlichkeit (Art. 2 EU-Vertrag), die auch für den DSGVO-Gesetzgeber nicht zur Disposition steht. Es lässt sich insbesondere als Ausfluss des Verhältnismäßigkeitsgrundsatzes begreifen. Dieser wiederum wird in Art. 83 Abs. 1 S. 1 DGSVO ausdrücklich genannt, wonach Bußgelder „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend“ sein müssen. Das wird unterstrichen durch den Grundsatz „ultra posse nemo obligatur“ – niemand muss etwas Unmögliches leisten. Diesen Grundsatz zugrundegelegt, lässt sich die Verhängung eines Bußgeldes trotz fehlenden Verschuldens nicht rechtfertigen. Bekanntlich ist Fahrlässigkeit das „Außerachtlassen der erforderlichen Sorgfalt“. Wollte man also verschuldensunabhängige Sanktionen zulassen, müsste auch

[67] Weitere Bußgeldtatbestände wird der Cyber Resilience Act regeln (siehe Art. 53 CRA-E).
[68] EuGH Gerichtsmitteilung v. 21.12.2021 – C-807/21, BeckEuRS 2021, 750343; BeckRS 2023, 8604; EuGH Gerichtsmitteilung v. 12.11.2021 – C-683/21, BeckEuRS 2021, 749200 BeckRS 2023, 8983.
[69] https://www.datenschutzzentrum.de/uploads/dsk/20230118-Stellungnahme-DSK.pdf.
[70] Vgl. nur Gola, in: Gola/Heckmann, DSGVO Art. 83 Rn. 3; Paal/Pauly/Frenzel DS-GVO Art. 83 Rn. 8; Klaas/Momsen/Wybitul DatenschutzsanktionenR-HdB, § 3 Rn. 38 ff. m.w.N.; Popp, in: Sydow/Marsch DS-GVO/BDSG, Art. 83 DSGVO Rn. 12.

derjenige „bestraft“ werden können, der in seinem Verhalten (vor dem Hintergrund einer sehr detailreich regelnden DSGVO) sämtliche Sorgfaltsanforderungen erfüllt hat. Jede verschuldensunabhängige Verhängung eines Bußgeldes in dieser Situation eines „non liquet“ wäre zugleich ein Grundrechtseingriff, der nicht nur rechtfertigungsbedürftig ist, sondern zugleich einer expliziten gesetzlichen Grundlage bedarf: Eingegriffen wird nicht nur in das Recht zur unternehmerischen Entfaltung, sondern auch in all jene Grundrechte, deren Gewährleistung ihrerseits der Datenverarbeitung bedarf. Für einen solchen Grundrechtseingriff findet sich unterdessen keine taugliche Rechtsgrundlage. Eine solche müsste – um hinreichend bestimmt zu sein – ausdrücklich regeln, dass ein Bußgeld bereits immer dann verhängt werden darf, wenn das Unternehmen bestimmte datenschutzrechtliche Vorschriften nach Auffassung der Aufsichtsbehörde verletzt. Art. 83 DSGVO bildet hierfür gerade keine ausreichende Rechtsgrundlage.

Wie problematisch letztlich eine Haftung nach dem Grundsatz „strict liability“ ist, sieht man auch daran, dass eine verschuldensunabhängige Haftung ein Innovationshemmnis darstellt. Informationstechnische Innovationen gehen regelmäßig mit bestimmten Risiken einher, die auch aus der Abwägung von Datenschutz und Datennutzung herrühren. Wollte man ein hohes Haftungsrisiko vermeiden, wird man sich regelmäßig gegen die Innovation entscheiden.

2.3.4 Straftaten

Haftungsfolgen aus dem StGB können sich für die Unternehmensleitung, den IT-Sicherheitsbeauftragten oder ggf. Compliance-Beauftragten aus verschiedenen Straftatbeständen des StGB ergeben.

2.3.4.1 § 266 Abs. 1 StGB Untreue

Eine Verletzung der Vermögensbetreuungspflicht kann unter bestimmten Umständen zu einer strafrechtlichen Haftung führen. Voraussetzung für eine Vermögensbetreuungspflicht ist eine gewisse Selbstständigkeit in der Aufgabenerfüllung beziehungsweise ein Handlungsspielraum der betroffenen Person, um die Haftung nicht über Gebühr auszudehnen. Die weiträumigen Entscheidungsbefugnisse und die oftmals fehlende Kontrolle seitens der Unternehmensleitung sprechen für das Bestehen einer Vermögensbetreuungspflicht von IT-Sicherheitsbeauftragten beziehungsweise Compliance-Beauftragten neben der Unternehmensleitung.[71]

Die erforderliche Verletzung dieser Pflicht kann sich nicht nur aus einem positiven Tun, sondern auch aus einem Unterlassen ergeben. Im Bereich der IT-Sicherheit kann damit die Nichtvornahme IT-sicherheitsrechtlich notwendiger Schutzvorkehrungen zu einer Verletzung der Vermögensbetreuungspflicht führen.

[71] Vgl. Schmidl, in: Hauschka/Moosmayer/Lösler, Corporate Compliance, 3. Aufl. 2016, § 28 Rn. 151 ff.

Einer Strafbarkeit wegen Untreue wird aber im Bereich der IT-Sicherheit oftmals der fehlende Nachweis des Vorsatzes entgegenstehen.

2.3.4.2 § 203 StGB Verletzung von Privatgeheimnissen

Der Straftatbestand der Verletzung von Privatgeheimnissen kann auch durch das Unterlassen von IT-Sicherheitsmaßnahmen begangen werden. Insbesondere die Herstellung sicherer Kommunikationswege ist von entscheidender Bedeutung, um eine Haftung nach § 203 StGB zu vermeiden. So sind der Einsatz von Verschlüsselungstechnik und Firewalls für die Übermittlung von Daten i. S. v. § 203 StGB erforderlich.

Ähnlich ist eine mögliche Haftung nach § 17 UWG für den Verrat von Geschäfts- und Betriebsgeheimnissen zu beurteilen.

2.3.4.3 § 106 UrhG Unerlaubte Verwertung urheberrechtlich geschützter Werke

Eine möglicherweise drohende Strafbarkeit nach § 106 UrhG kann durch Speicher-Quotas (Rationierung von Speichermengen) oder die regelmäßige Überprüfung der laufenden Serverprogramme und der Netzwerkauslastungen vermieden werden.

2.3.4.4 § 27 JuSchG Jugendgefährdende Medien

Der Arbeitgeber muss Abwehrmaßnahmen gegen jugendgefährdende Medien ergreifen, die von den Auszubildenden in den Systemen des Arbeitgebers gespeichert oder dort ausgetauscht werden. Falls der Arbeitgeber gegen derartige Tätigkeiten der Auszubildenden keine Maßnahmen ergreift sieht er sich gegebenenfalls dem Vorwurf des Zugänglichmachens jugendgefährdender Medien ausgesetzt. Insbesondere droht auch bei bloß fahrlässigem Zugänglichmachen bereits eine Haftung.

2.3.5 Meldepflichten infolge von IT-Unsicherheit

Für spezifische IT-sicherheitsrechtliche Pannen sieht die Rechtsordnung in verschiedenen Gesetzen Meldepflichten für die betroffenen Unternehmen vor. In der Regel enthalten diese Rechtsnormen eine Pflicht zur Meldung der Sicherheitsvorfälle gegenüber der zuständigen staatlichen Stelle und unter besonderen Umständen die verpflichtende Benachrichtigung der von den Sicherheitsvorfällen Betroffenen (z. B. Kunden).

Art. 33, 34 DS-GVO enthalten für datenschutzrechtlich relevante Sicherheitsvorfälle eine Meldepflicht. Eine ähnliche Regelung findet sich in § 168 TKG für den Telekommunikationsbereich. Auch das IT-Sicherheitsgesetz hat in § 8b Abs. 4 BSIG eine Meldepflicht für Betreiber Kritischer Infrastrukturen und in § 8c Abs. 3 BSIG für Anbieter digitaler Dienste geschaffen.

Auch aus spezialgesetzlichen Grundlagen können sich weitere Meldepflichten ergeben. Beispielsweise im Gesundheitssektor besteht eine Meldepflicht im Rahmen der Telematikinfrastruktur nach § 291b Abs. 6 S. 2 SGB V. Zahlungsdienstleister sind nach § 54 Abs. 1 S. 1 ZAG zu einer Meldung an die BaFin verpflichtet.

Bei Verlust von personenbezogenen Daten können gem. Art 33, 34 DS-GVO datenschutzrechtliche Anzeigepflichten gegenüber der Datenschutzaufsichtsbehörde und den betroffenen Datenberechtigten bestehen.

Grundsätzlich muss das verantwortliche Unternehmen der Aufsichtsbehörde jede Datenschutzverletzung unverzüglich und möglichst innerhalb von 72 Stunden melden, nachdem dem Verantwortlichen die Verletzung bekannt wurde. Ausnahmsweise besteht dann keine Pflicht zur Meldung bei der Datenschutzaufsichtsbehörde, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen führt. Hierfür ist aber das verantwortliche Unternehmen beweispflichtig.

Hat eine Datenschutzverletzung darüber hinaus voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge (z. B. Identitätsdiebstahl, Rufschädigung, materieller oder immaterieller Schaden), muss das verantwortliche Unternehmen grundsätzlich die hiervon betroffenen Personen ohne unangemessene Verzögerung benachrichtigen. Ausnahmsweise kann von der Benachrichtigung abgesehen werden, wenn das verantwortliche Unternehmen Risiken für die betroffenen Personen durch geeignete technische und organisatorische Schutzmaßnahmen ausgeschlossen hat.

Durch die neue IT-Sicherheitsgesetzgebung kommen neue Meldungspflichten hinzu: So müssen etwa Hersteller nach Art. 11 Abs. 1 CRA-E aktiv ausgenutzte Schwachstellen innerhalb 24 Stunden nach Kenntnis an ENISA melden. Art. 23 Abs. 1 NIS-2-RL schreibt vor: wesentliche und wichtige Einrichtungen melden unverzüglich jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste gemäß Absatz 3 (erheblicher Sicherheitsvorfall) hat. Aufgrund des gesteigerten Anwendungsbereichs durch NIS-2 hat dies nun auch größere Bedeutung für die Wirtschaft.

2.3.6 Sonstige Haftungsrisiken

Neben den direkt aus den jeweiligen Gesetzen folgenden Haftungsfragen bestehen noch weitere – oftmals indirekt wirkende – Haftungsrisiken.

2.3.6.1 Störungen des Betriebs und Umsatzeinbußen

Die Störungen des Betriebs durch IT-sicherheitsrechtliche Vorfälle stellen nicht nur ein technisches Ärgernis dar, das behoben werden muss, sondern führen oftmals auch zum Abfluss beziehungsweise Verlust wichtiger unternehmerischer Daten – oftmals gar von Betriebs- und Geschäftsgeheimnissen – und damit letztendlich zu Umsatzeinbußen und Wettbewerbsnachteilen.

2.3.6.2 Reputationsverlust

Wenn IT-sicherheitsrechtliche Verstöße publik werden – sei es durch gesetzliche Meldeverpflichtungen oder durch Whistleblower – drohen dem betroffenen Unternehmen immense Reputationsschäden.

Der konkret eintretende, schwerlich messbare Reputationsverlust wird im Einzelfall von der Reichweite des IT-sicherheitsrechtlichen Vorfalls und dessen Vermeidbarkeit bestimmt. Infolge derartiger Reputationsverluste drohen weitere ideelle Schäden, etwa sinkendes Vertrauen der Kunden in die Produkte, aber auch materielle Schäden in Form von rückläufigen Umsatzzahlen. Nachdem Vertrauen in die IT-Sicherheit in der digitalen Welt eine zentrale Rolle einnimmt, kann der Verlust des Vertrauens zu spürbaren bis zu existenzgefährdenden Umsatzeinbußen führen.

Die vorstehenden Ausführungen zu den Umsatzeinbußen gelten nur eingeschränkt für Monopole und monopolähnliche Unternehmen, da deren Dienste häufig nicht ersetzt werden können.

2.3.6.3 Vergaberecht

Das Vergaberecht weist zwei Anknüpfungspunkte für die Vorgaben der IT-Sicherheit auf. Einerseits kann bereits im Rahmen der Leistungs- und Aufgabenbeschreibung Bezug auf die Anforderungen an die IT-Sicherheit genommen werden. Dadurch kann bereits bei der Beschreibung – soweit diese in nichtdiskriminierender Weise erfolgt – Einfluss auf die Anforderungen an die IT-Sicherheit genommen werden.

Andererseits können bei der Wertung der eingegangenen Angebote durch den öffentlichen Auftraggeber IT-sicherheitsrechtliche Anforderungen berücksichtigt werden.

2.3.6.4 Versicherungsrecht

Im versicherungsrechtlichen Bereich können sich bei IT-sicherheitsrechtlichen Verstößen gleich zwei Hürden für IT-unsichere Unternehmen ergeben.

Zum einen sieht § 81 Abs. 2 VVG eine Kürzung von Versicherungsleistungen für die Fälle des grob fahrlässigen Herbeiführens von Versicherungsfällen vor. Diese Regelung wird insbesondere bei auf Cyber-Risiken zugeschnittenen Versicherungsprodukten eine Rolle spielen.

Beispiel

Unternehmer A versichert seinen Webshop gegen Cyberrisiken bei Versicherer V. Für den vom Unternehmer A selbst betriebenen Webshop versendet A aus Versehen eine Liste mit den Zugangsdaten und Kennwörter aller Mitarbeiter über einen unsicheren

Kommunikationsweg. Selbst als er auf diesen Fehler aufmerksam gemacht wird, veranlasst er keine Änderung der Zugangsdaten. Als ihm durch diese Schwachstelle diverse Bestellungen von Kunden verloren gehen, will er den Schaden von der Versicherung ersetzt haben.

Einer Leistung der Versicherung an den Unternehmer A steht im vorliegenden Fall § 81 Abs. 2 VVG entgegen, da der Versicherungsnehmer den Versicherungsfall grob fahrlässig herbeigeführt hat.

Zum anderen sieht Solvency II vor, dass Versicherungsgeber Kriterien – wie sie auch Basel II für Kreditgeber vorsieht – vor der Vergabe von Versicherungen zu berücksichtigen haben. Damit kann eine Verletzung der IT-sicherheitsrechtlichen Vorgaben eine niedrigere Einstufung der Versicherungsfähigkeit von Unternehmen und damit eine erschwerte Versicherung unternehmerischer Risiken, zumindest aber schlechteren Konditionen zur Folge haben.

Von großer Praxisbedeutung ist das Urteil des LG Tübingen vom 26. Mai 2023 (Az. 4 O 193/21, das als erstes deutsches Urteil zur Cyberversicherung gilt: Es betrifft die vorvertragliche Anzeigepflicht bestehender Risiken auf Nachfrage durch Versicherer. Wird hier „gelogen“, greift § 19 VVG und der Versicherer hat ein Rücktrittsrecht. Das Gericht bejaht eine Gefahrerhöhung nach § 23 VVG, wenn etwa angekündigte Sicherheitsmaßnahmen nach Vertragsschluss doch nicht durchgeführt werden.

Leitsätze des LG Tübingen, Urteil vom 26. Mai 2023, Az. 4 O 193/21

---

1. Gelingt es, dass bei einem sog. "Pass-the-Hash"-Cyber-Angriff unter Ausnutzung einer bekannten Schwachstelle des Betriebssystems von Microsoft Administratorenrechte für alle Server des geschädigten Unternehmens erbeutet werden, lässt der Umstand, dass nicht alle Server mit den aktuellen Sicherheits-Updates ausgestattet waren, einen Leistungsanspruch gegen den Versicherer unberührt, weil eine mögliche Verletzung einer diesbezüglichen Anzeigeobliegenheit weder für den Eintritt oder die Feststellung des Versicherungsfalles noch für Feststellung oder den Umfang der Leistungspflicht ursächlich ist, es sei denn, der Versicherungsnehmer hat arglistig gehandelt.
2. Der Anwendungsbereich von § 81 Abs. 2 VVG ist dann nicht eröffnet, wenn die betreffende Gefahrenlage - hier: fehlende Sicherheitsmaßnahmen zur Vermeidung eines Cyber-Angriffs, die über den Einsatz einer Firewall und eines Anti-Viren-Scanners hinausgehen - bereits bei Vertragsschluss bestand und Grundlage der Risikoprüfung des Versicherers war bzw. hätte sein können.

2.3.6.5 Kreditwirtschaft – Basel II

Auch im Bereich des Kreditwesens drohen indirekte Haftungsrisiken, wenn die Vorgaben der IT-Sicherheit nicht eingehalten werden.

Wie bereits oben dargestellt spielt die IT-Sicherheit nach dem Basel II-Abkommen eine zentrale Rolle bei der Bewertung der Bonität des kreditbegehrenden Unternehmens. Damit kann eine Verletzung der IT-sicherheitsrechtlichen Vorgaben zu einer niedrigeren Einstufung der Bonität und damit zu einem geringeren Kreditvolumen oder zu höheren Zinsen führen.

2.3.6.6 Aufsichtsrechtliche Maßnahmen, insbesondere Gewerbeaufsicht

Die Vernachlässigung von IT-sicherheitsrechtlichen Anforderungen kann ein Einschreiten der zuständigen Aufsichtsbehörden nach sich ziehen. Denkbar sind Maßnahmen der Gewerbeaufsicht bei IT-Sicherheitsvorfällen. Die zuständigen Aufsichtsbehörden können in Einzelfällen die Entziehung der Gewerbeerlaubnis aufgrund von Unzuverlässigkeit anordnen.[72]

Auch das BSI hat entsprechende Befugnisse, die betroffenen Unternehmen zur Abhilfe zu Verpflichten vgl. §§ 7c, 7d, 8a Abs. 3 S. 5, 8c Abs. 4, 9b BSIG.

Im datenschutzrechtlichen Bereich können die Datenschutzaufsichtsbehörden Maßnahmen erlassen, um die Beseitigung von technischen oder organisatorischen Mängeln zu erreichen und als ultima ratio sogar die Datenverarbeitungen untersagen (vgl. zu privaten Stellen Art. 58 Abs. 2 DS-GVO).

2.4 Zusammenfassung zum IT-Sicherheitsrecht

Das IT-Sicherheitsrecht zeichnet sich durch ein verstreutes Regelungskonzept aus, das zwei große Regelungsregime anknüpfend an die Qualifikation als Kritische Infrastruktur/Anbieter digitaler Dienste/Unternehmen im besonderen öffentlichen Interesse oder Sonstiges enthält. Überschneidungen von Regelungen sind denkbar (z. B. im Hinblick auf Meldepflichten).

Die IT-sicherheitsrechtlichen Vorgaben enthalten vielfach den Vorbehalt des technisch Möglichen und wirtschaftlich Zumutbaren und eröffnen dadurch aus Verhältnismäßigkeitsgesichtspunkten notwendige Spielräume, die aber zugleich zu Rechtsunsicherheit auf Seiten der Verpflichteten führen können.

Dem nicht konsistenten IT-Sicherheitsrecht steht ein vielfältiges und umfassendes Haftungsregime gegenüber. Dieses knüpft an altbekannte Regelungen an und eröffnet über deren unbestimmte Rechtsbegriffe ein Einfließen der Wertungen des IT-Sicherheitsrechts.

[72] Vgl. Heckmann, MMR 2006, 280, 283.

3 Gefährdungsszenarien der IT-Sicherheit in Unternehmen

Erhöhtes Risiko durch fortschreitende Digitalisierung

Die IT-Sicherheitslage in Unternehmen hat sich in den letzten Jahren durch die zunehmende Professionalisierung der Angriffe und die fortschreitende Digitalisierung der Arbeitswelt verschärft, wenn auch zugleich der Markt für Sicherheitslösungen an Bedeutung gewonnen hat.

Der BSI Lagebericht für die IT-Sicherheit im Jahr 2022 sieht die Lage der IT-Sicherheit in Deutschland im Berichtszeitraum als im Verhältnis zur bereits zuvor angespannten Lage weiter zugespitzt: „Die Bedrohung im Cyber-Raum ist damit so hoch wie nie. Im Berichtszeitraum wurde – wie schon im Vorjahr – eine hohe Bedrohung durch Cybercrime beobachtet. Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine."

Abbildung 10
Top 3-Bedrohungen je Zielgruppe

Quelle: BSI

So führt das BSI weiter aus: „Ransomware blieb die Hauptbedrohung besonders für Unternehmen. Die im vergangenen Berichtszeitraum beobachtete Ausweitung von Methoden der Erpressungsmethoden im Cyber-Raum hat sich im aktuellen Berichtszeitraum fortgesetzt.[73] Insbesondere das sogenannte Big Game Hunting, also die Erpressung

[73] Vgl. hierzu auch BayWiDI Briefing 2023/1, S. 2 ff.

umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, hat weiter zugenommen. Sowohl die von IT-Sicherheitsdienstleistern berichteten Lösegeld- und Schweigegeld-Zahlungen als auch die Anzahl der Opfer, deren Daten etwa wegen ausbleibender Zahlungen auf Leak-Seiten veröffentlicht wurden, sind weiter gestiegen. Das nicht nur Unternehmen Ziel von Ransomware-Angriffen sind, zeigt eindrücklich der folgenschwere Angriff auf eine Landkreisverwaltung in Sachsen-Anhalt: Erstmals wurde wegen eines Cyber-Angriffs der Katastrophenfall ausgerufen. Bürgernahe Dienstleistungen waren über 207 Tage lang nicht oder nur eingeschränkt verfügbar."

Im mittlerweile vorherrschenden Spannungsfeld von Innovation, Globalisierung und Komplexität kommt die IT-Sicherheit oftmals zu kurz. Viel zu oft noch wird die Gewährleistung von IT-Sicherheit im Unternehmen lediglich als Kostenfaktor und nicht als Marktvorteil angesehen.

Die Gefährdungsszenarien der IT-Sicherheit in Unternehmen lassen sich auf vielfältige Art und Weise differenzieren. Im Folgenden wird nach den Schwachstellen, die als „Einfallstore" für IT-Sicherheitsvorfälle dienen, unterschieden.

Als Schwachstellen lassen sich die Faktoren Mensch, Technik und Organisation definieren. Diese Schwachstellen stehen aber keineswegs isoliert nebeneinander, sondern bedingen sich oftmals gegenseitig und verstärken die IT-Unsicherheit bei Nichteinhaltung IT-sicherheitsrechtlicher Vorgaben. Es bestehen mithin vielfach Wechselwirkungen zwischen den einzelnen Schwachstellen.

So ist es beispielsweise möglich, durch eine restriktive Technikgestaltung, etwa durch die Sperrung des Internetzugangs auf bestimmten Rechnern, von vornherein die Schwachstelle Mensch abzumildern. Ebenso ist es denkbar durch organisatorische Maßnahmen, etwa die Implementierung eines gestuften Rollen- und Rechtemanagements, wiederum menschliches Fehlverhalten, das zu IT-Sicherheitsvorfällen führen kann, zu reduzieren.

3.1 Schwachstelle Mensch

Die Schwachstelle Mensch zeichnet sich als die am schwierigsten regulierbare und zugleich in der Regel am stärksten ausgeprägte Schwachstelle im Unternehmen aus. Der Mensch fungiert als Schnittstelle zwischen der Unternehmens-IT und den Risiken für die IT im Internet. Menschliches Verhalten zeichnet sich gerade auch dadurch aus, dass unterschiedliche Bewertungsmaßstäbe an den Tag gelegt werden und Fehler im alltäglichen Arbeitsalltag unterlaufen. Damit bietet der Faktor Mensch im Unternehmen zahlreiche Anknüpfungspunkte für IT-sicherheitsrechtliche Problemstellungen.

IT-Sicherheitsrisiken können sich bei der Schwachstelle Mensch aus ihrem sorglosen Umgang mit IT-Systemen ergeben.

Der sorglose Umgang mit IT kann sich darin zeigen, dass Mitarbeiter auf unsicheren Seiten im World Wide Web surfen oder unsichere Dateien herunterladen und ausführen. Damit

kann Angreifern oder automatisch ausführender Schadsoftware der Zugang zu den IT-Systemen des Unternehmens ermöglicht werden.

Nicht nur der sorglose Umgang mit Passwörtern an sich, das heißt das Notieren an gut für Dritte erkennbaren Stellen, sondern auch die einfache Gestaltung von Passwörtern können für Cyber-Attacken ausgenutzt werden. Soweit Passwörter keinen Mindestanforderungen – etwa Groß- und Kleinschreibung, Verwendung von Zahlen, Sonderzeichen – genügen, stellen sie kein wirksames Hindernis für den Zugriff auf die IT-Systeme dar. Besonders wichtig ist, dass für verschiedene Dienste verschiedene Passwörter verwendet werden. Wird nämlich eines der Passwörter bekannt, berührt das nicht die übrigen Dienste.

Auch die sorglose Verwendung von mobilen Speichern (Beispiel: USB-Sticks) kann zu IT-Sicherheitsproblemen führen. Nicht nur manipulierte USB-Sticks, die auf Parkplätzen oder Messen ausgelegt werden, sondern auch von zu Hause mitgebrachte am eigenen Rechner verwendete Speichermedien können IT-unsicher sein und damit zu Schäden führen.

Besonders problematisch ist auch das Konzept „bring your own device“, also die Nutzung privater IT (z. B. Laptops oder Smartphones) im Unternehmenskontext. Durch die Einbindung zahlreicher verschiedener Hard- und Software ist eine wirksame Kontrolle der IT-Sicherheit kaum mehr möglich.

Der sorglose Umgang mit IT durch den Menschen kann sich im Falle von Manipulationen dahingehend wandeln, dass es zu einem vorsätzlichen Unterlassen oder Ausschalten von IT-Sicherheitsmaßnahmen kommt und dadurch Lücken in der IT-Sicherheit des Unternehmens entstehen. Die Ursachen hierfür können stark divergieren. Von Industriespionage bis hin zur Frustration am Arbeitsplatz oder mangelnder „Usability“ sind vielfältige Beweggründe denkbar.

Besondere Bedeutung im Zusammenhang mit der Schwachstelle Mensch kommt dem zunehmenden Phänomen des sog. Social Engineering zu.

Social Engineering als Methode meint die gezielte und professionelle Manipulation von Menschen zur Erlangung von Informationen. Damit wird also die Schwachstelle Mensch bewusst ausgenutzt.

Vielfach geschieht die Kontaktaufnahme in sozialen Netzwerken. Aber nicht nur in den sozialen Netzwerken, sondern auch über andere Telekommunikationsmedien, wie das Telefon, wird Social Engineering eingeleitet beziehungsweise durchgeführt.

Je mehr Informationen im Vorfeld über den Betroffenen Mitarbeiter und dessen Umfeld bekannt sind, desto effektiver kann der Angreifer das Vertrauen des Mitarbeiters erlangen. Diese Angriffsmethode macht sich damit den Mitarbeiter des Unternehmens zu Nutze und versucht über diesen Zugriff auf die IT-Systeme des Unternehmens zu erlangen. Der Zugriff auf die IT-Systeme kann mit Hilfe der Herausgabe von Passwörtern, von Unternehmensdaten oder auch Mitteilung interner Schwachstellen erfolgen.

Social Engineering ist oftmals lediglich Begleitmaßnahme von Angriffen auf die IT-Systeme von Unternehmen. So kann bei gezielten Angriffen Social Engineering eingesetzt werden, um mit dem erlangten persönlichen Wissen in der Folge Passwörter zu erraten (sog. Brute-Force-Angriff). Im Rahmen von sog. Social Hacking, dem Erlangen vertraulicher Informationen, kann Social Engineering eine bedeutende Rolle spielen. Social Engineering kann auch bei spezifizierten Phishing-Angriffen Relevanz zukommen. Indem der Angreifer erst über Social Engineering Informationen über den Mitarbeiter sammelt, kann er diesem in der Folge eine spezifizierte Phishing-Mail zusenden (sog. Spear-Phishing-Angriff).

In einem engen Zusammenhang mit der Schwachstelle Mensch steht die elektronische Kommunikation im Unternehmen, da diese von Menschen betrieben wird. Nachdem die einfache E-Mail mit über 280 Milliarden[74] täglich verschickten Nachrichten zu einem weltweit verbreiteten, umfassend im privaten wie geschäftlichen Rechtsverkehr genutzten Kommunikationsmedium avanciert ist, bietet sie auch zahlreiche Angriffsflächen. Der Einsatz der E-Mail ohne flankierende Sicherheitsvorkehrungen begegnet durchgreifenden Bedenken. So wird die E-Mail vielfach mit der Postkarte, die auch von jedermann eingesehen werden kann, verglichen. Einfache E-Mails können während des Übertragungsvorgangs abgefangen, gelesen oder gar verändert werden (sog. „Sniffing“), so dass die Vertraulichkeit, Integrität und Authentizität der E-Mail in Mitleidenschaft gezogen werden. Außerdem kann auch die Absenderadresse einer E-Mail verändert werden und damit eine in Wirklichkeit nicht bestehende Identität vorgetäuscht werden (sog. „Phishing“).

Beispiel

Die herkömmliche Begehungsform des Phishings besteht darin, dass ein Angreifer eine getarnte E-Mail an den Betroffenen sendet, die ihrer Gestaltung nach von der Bank des Betroffenen zu stammen scheint, und den Empfänger dazu veranlasst, einem in der E-Mail enthaltenem Link zu folgen. Auf einer der Bank des Betroffenen nachgestellten Seite wird der Betroffene nun aufgefordert seine Zugangsdaten einzugeben. Mit Hilfe dieser Daten kann der Angreifer vom Konto des Betroffenen Geld abgehen.

Im Unternehmensbereich spielen die Bankdaten der Mitarbeiter keine herausragende Rolle, dafür umso mehr die Zugangsdaten zur IT des Unternehmens. Phishing-Attacken können sich im unternehmerischen Bereich damit auf Zugangsdaten des Mitarbeiters zu den IT-Systemen des Unternehmens richten.

Im Dezember 2022 lag der Anteil der Spam-Mails am gesamten E-Mail-Verkehr weltweit bei rund 45,2 Prozent. Mit knapp 30 Prozent kam der Großteil der Spam-Mails im Jahr 2022 aus Russland, rund fünf Prozent stammten aus Deutschland.[75]

[74] https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/.
[75] https://de.statista.com/statistik/daten/studie/872986/umfrage/anteil-der-spam-mails-am-gesamten-e-mail-verkehr-weltweit/.

Ein nicht unerheblicher Anteil dieser Spam-Mails ist an E-Mail-Adressen von Unternehmen und deren Mitarbeiter gerichtet. Vielfach enthalten Spam-Mails Schadsoftware und können bei einem sorglosen Umgang mit den Dateianhängen oder versandten Links für gravierende IT-Sicherheitsvorfälle verantwortlich sein.

3.2 Schwachstelle Technik

Die IT-Systeme selbst sind trotz ihrer hochtechnisierten Grundlagen und Ausgestaltung selbst auch Anknüpfungspunkt für IT-Risiken und damit Schwachstelle für die IT-Sicherheit.

Im Rahmen der Schwachstelle Technik kommt dem Einsatz von Schadsoftware eine herausragende Bedeutung zu.

Die Ausgestaltungen von Schadsoftware selbst variieren stark. Neben Viren, Würmern kommen trojanische Pferde, Spyware und Adware zum Einsatz. Insbesondere unter dem Schlagwort „Cybercrime-as-a-Service“ hat sich ein regelrechter Markt für Schadsoftware im sog. Darknet gebildet, der es auch unerfahrenen Angreifern erlaubt, sich mit hochwertiger Schadsoftware auszurüsten. So heißt es im aktuellen Lagebericht des BKA[76]:

„Die Underground Economy (UE) ist primärer Umschlagplatz für illegale Waren und unrechtmäßig erlangte Daten, wie kompromittierte Zahlungs- und Zugangsdaten, sowie für verschiedenste Cybercrime-as-a-Service-Angebote (Zergliederung und Spezialisierung einzelner „Teiltatbeiträge“ des Phänomenbereichs Cybercrime). Die Angebote der UE besitzen auch weiterhin eine hohe Bedeutung für den Cyber-Bereich, da sie vielfach Ausgangspunkt für die Begehung weiterer Cybercrime-Delikte sind. Auch der Ausbau des arbeitsteiligen Cybercrime-as-a-Service-Modells setzte sich 2022 weiter fort.“

Aber nicht nur die Ausgestaltung variiert, auch die Verbreitungswege der Schadsoftware stellen sich als vielfältig dar. Drive-by-Exploits, Spam-Mail oder Verlinkungen auf Schadprogramme sind nur drei der möglichen Wege der Infizierung mit Schadsoftware.

Ausgehend von diesen Verbreitungswegen der Schadsoftware stellt sich die Frage, wie diese letztendlich in die unternehmenseigene IT gelangt. Oftmals dient die Schwachstelle Mensch mit Hilfe von Spam-Mails oder durch Ausnutzen des sorglosen Umgangs der Mitarbeiter mit der IT als Angriffspunkt. Diese Attacken lassen sich meist mit Ausnahme derjenigen, die Social Engineering als Begleitmaßnahme nutzen, als wenig gezielt und wahllos charakterisieren.

Es ist aber auch eine Zunahme gezielter Angriffe – sog. Advanced Persistant Threats (ATP) – zu verzeichnen. Diese sind nicht durch Ziel- und Wahllosigkeit charakterisiert, sondern durch die Verfolgung langfristiger Ziele. Der Verwender dieser Angriffsmethode verfügt in der Regel über entsprechende Ressourcen und Informationen. Oftmals können zwischen der Infektion des Systems mit der Schadsoftware und der Entdeckung der

[76] BKA, Bundeslagebild Cybercrime 2022, S. 11 ff.

Sicherheitspanne lange Zeiträume liegen. Social Engineering wird bei diesen gezielten Angriffen oft als Begleitmaßnahme genutzt. Die Folgen dieser Angriffe sind weitreichend und lassen sich nur schwerlich beseitigen. Der Ausfall gesamter IT-Systeme ist oftmals die Folge von sog. Distributed Denial-of-Service Angriffen (DDoS-Angriffe). Hier braucht das Unternehmen gar nicht letztendliches Ziel des Angriffs zu sein, sondern wird im Rahmen der Attacke als Verstärker für den Angriff missbraucht. Die Schäden treten damit nicht nur beim eigentlich betroffenen Unternehmen ein, sondern auch bei den „benutzten" IT-Systemen anderer Unternehmen. Die Schadsoftware für den späteren DDoS-Angriff gelangt oftmals durch Spam-Mail auf die Rechner der später benutzten IT-Systeme.

Infolge von DDoS-Attacken sind Webseiten nicht mehr erreichbar und die IT-Systeme stehen nicht mehr für die eigentlichen Arbeitsabläufe zur Verfügung.

DDoS-Attacken werden oftmals auch genutzt, um andere Angriffe auf die IT-Systeme des Betroffenen zu verschleiern. Die DDoS-Attacke soll damit lediglich zu einer Bindung der Ressourcen führen, um im Schatten des Angriffs weitere Schäden verursachen zu können.

Beispiel

So fanden im Jahr 2020 weltweit 50 Millionen DDoS-Angriffe statt, woraus sich eine Steigerung um 98 Prozent während der Corona-Pandemie errechnet.[77] Das BKA resümiert: „Die Corona-Pandemie zeigt den opportunistischen Charakter von Cyber-Kriminellen: Es werden jene angegriffen, welche für die Gesellschaft einen hohen Stellenwert besitzen."[78]

Der Einsatz veralteter Technik öffnet IT-Sicherheitsrisiken Tür und Tor. Nicht mehr dem Stand der Technik entsprechende Hard- und Software, die nicht mehr mit Sicherheitsupdates versorgt wird, stellt ein immenses IT-Sicherheitsrisiko dar.

Veraltete Technik ist nicht nur wirtschaftlich gesehen nachteilhaft wegen der verminderten Leistungsfähigkeit der Systeme, sondern kann vor allem den Zugang von Schadsoftware in die eigene IT erleichtern und deren Ausbreitung begünstigen.

Der Einsatz veralteter Technik beinhaltet gleichsam den Einsatz veralteter Sicherheitstechnik. So kann sich der Unternehmer nicht in Sicherheit wiegen, nur weil er beispielsweise Anti-Viren-Programme installiert hat, wenn er diese nicht regelmäßig aktualisiert. Aber selbst dann ist es nicht unwahrscheinlich, dass das Programm die Schadsoftware nicht erkennt oder es mehrere Wochen oder gar Monate dauert, bis ein Update für das Programm bereitsteht. Auch kann die fehlende Reaktion auf bekannte Schwachstellen, wie Backdoors in weit verbreiteter Technik, zu IT-Sicherheitsrisiken führen. Vor allem im Bereich der IoT- oder mobilen Geräte ist die Hardware-Lebensdauer weit über die Updateperiode.

[77] BKA, Bundeslagebild Cybercrime 2020, S. 27. Zu den aktuellen Zahlen vgl. BKA, Bundeslagebild Cybercrime 2022, S. 19 ff.
[78] BKA, Bundeslagebild Cybercrime 2020, S. 39.

Beispiele

Die Verwendung des Betriebssystems Windows XP auf IT-Systemen von Unternehmen stellt seit der Einstellung der Sicherheitsupdates am 08. April 2014 durch Windows eine nicht tragbare IT-Sicherheitslücke dar.

Die Sicherheitslücke „Heartbleed“ in OpenSSL-Versionen betraf Millionen von Nutzer. Vielfach verwendeten auch E-Mail-Plattformen großer Anbieter diese Version der Zugangsverschlüsselung. Mit Hilfe dieser Schwachstelle konnten Teile des Hauptspeichers eines betroffenen Systems ausgelesen werden und vor allem der private Schlüssel des Servers konnte auf diese Art und Weise erlangt werden. Die Beseitigung dieser Schwachstelle erforderte die Installation aktueller Sicherheitsupdates.

Vergleichbar problematisch wie das Einsetzen veralteter Hardware ist der Einsatz von Hardware, die bereits veraltet auf den Markt kommt und erst gar nicht aktualisiert wird. Bekannt wurde dieses Problem vor allem durch die entsprechenden IoT-Geräte.[79] Hier kann auch das Auseinanderfallen von Verantwortung und Schaden beobachtet werden. Funktioniert das Gerät trotz vorhandener Sicherheitslücken, bemerkt der Anwender eine Kompromittierung nicht oder hat kein Interesse, die Benutzung einzustellen.

Zur Schwachstelle Technik kann auch die Missachtung allgemein erforderlicher Sicherheitsanforderungen gezählt werden. So müssen die IT-Systeme auch gegen physische, naturbedingte Gefahren in Form von Feuer oder Wasser geschützt werden. Daneben sind auch weitere Aspekte der Gebäudesicherheit, wie das Verschließen von Serverräumen, zu berücksichtigen.

Beispiele

Die Unterbringung der Serverräume im Keller von Unternehmensgebäuden in Hochwassergebieten stellt eine Missachtung allgemein erforderlicher Sicherheitsanforderungen an die IT-Sicherheit dar.

Auch die fehlende Anbringung von Rauch- und Feuermeldern in Serverräumen ist als technische Schwachstelle im Rahmen der IT-Sicherheit anzusehen.

Die IT-Sicherheitsbedrohungslage wird durch den Einsatz von Künstlicher Intelligenz weiter verschärft. Entsprechende intelligente selbstlernende Algorithmen können Sicherheitslücken effizient aufspüren und in großem Umfang angreifen. Der Einsatz von

[79] BSI, Die Lage der IT-Sicherheit in Deutschland 2018, S. 20 f. Vgl. auch https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartCity/Handlungsempfehlungen_Smart_City.pdf?__blob=publicationFile&v=3

entsprechenden Tools ermöglicht es Angreifern mit weniger Ressourcen, die IT-Systeme von Unternehmen anzugreifen. Mithilfe von KI können beispielsweise auch adaptive Schadprogramme entwickelt werden, die sich ihrer Umgebung anpassen und von herkömmlicher Sicherheitssoftware nicht erkannt werden. Auch Bots, die mithilfe einer KI gesteuert werden, können große Schäden anrichten.

Gleichzeitig können mithilfe von KI-Software-Lösungen realistisch anmutende Audio- und Video-Deepfakes erstellt werden, die technische Sicherheitsvorkehrungen umgehen bzw. Mitarbeiter dazu veranlassen können, Schritte zu unternehmen, die dem Betrieb schaden.[80] Ferner können Cyberkriminelle inzwischen mithilfe von ChatGPT immer bessere Texte verfassen und damit glaubwürdigere gefälschte Webseite oder Phishing-E-Mails verfassen.[81]

Beispiele

Im Rahmen einer Videokonferenz wird ein Video des Geschäftsführers eingespielt, der darum bittet, Gelder vom Unternehmenskonto auf ein anderes Konto zu überweisen.

Eine Person ruft im Unternehmen an und sagt mit der Stimme des Geschäftsführers, dass eine E-Mail sicher sei und man den Link anklicken dürfe.

In Wirklichkeit kann es sich dabei auch um Deep-Fakes, d. h. Videos oder Audioaufnahmen handeln, die mithilfe einer intelligenten Software erstellt wurden. Es gibt beispielsweise Softwareprogramme, die eine Stimme oder eine Bildaufnahme aufgrund vorheriger Aufnahmen synthetisch nachbilden können. Daneben gibt es Softwarelösungen, die einen sog. face oder audio swap ermöglichen. Dabei wird die gewünschte Tonlage bzw. das gewünschte Gesicht in einem Video eingeblendet, während vor der Kamera bzw. dem Mikrophon in Wirklichkeit eine andere Person diese Aussage tätigt.

Umgekehrt können solche Tools auch zur Verbesserung der eigenen IT-Sicherheit eingesetzt werden. Durch die großen Datenmengen, die entsprechende Systeme analysieren können, können leichter Anomalien erkannt und Angreifer im System erkannt werden.

3.3 Schwachstelle Organisation

Neben den Schwachstellen Mensch und Technik spielt die Schwachstelle Organisation eine bedeutende Rolle. IT-Sicherheit ist Pflichtaufgabe der Unternehmensleitung und bedarf hinreichender organisatorischer Vorkehrungen.

[80] Beispiele für Deep Fake -Videos können unter dem folgenden Link angesehen werden: https://www.dw.com/de/faktencheck-wie-erkenne-ich-deepfakes/a-60192155.
[81] Zu den IT-Sicherheitsrisiken durch ChatGPT vgl. BayWiDI Briefing 2023/2, S. 2 ff.

Die schwerwiegendste organisatorische Verfehlung im Rahmen der IT-Sicherheit kann der völlig planlose und unstrukturierte Versuch sein, IT-Sicherheit im Unternehmen herzustellen. IT-Sicherheit „ins Blaue hinein“ – also IT-Sicherheit ohne erforderliches Know-how – führt zwangsläufig zu immensen Sicherheitslücken in der unternehmenseigenen IT.

Nicht nur das Fehlen eines IT-Sicherheitskonzepts, sondern auch die wahllose Verwendung sich ggf. behindernder IT-sicherheitsrechtlicher Maßnahmen kann zu Angriffsflächen für Hacker und Schadsoftware führen.

Fehlende klare Aufgabenzuweisungen im Rahmen der IT-Sicherheit, die mangelnde Implementierung eines Meldesystems für IT-Sicherheitsvorfälle im Unternehmen und die unzureichende beziehungsweise nicht stattfindende Schulung der Mitarbeiter können IT-Sicherheitslücken großen Ausmaßes erst ermöglichen oder gar hervorrufen.

IT-Sicherheit „ins Blaue hinein“ ist damit zwar überwiegend im Bereich der Organisation anzusiedeln, schlägt sich aber vor allem in der Schwachstelle Mensch nieder.

Ohne klare Meldevorgaben, ohne hinreichende Schulungen der Mitarbeiter wird die Schwachstelle Mensch nicht reguliert, sondern sogar noch verstärkt. Auch eine fehlende Aufgabenzuweisung von IT-sicherheitsrechtlich vorzunehmenden Sicherheitsvorkehrungen schlägt sich sowohl im Faktor Mensch als auch im Faktor Technik nieder, wenn beispielsweise keine Updates mehr eingepflegt werden oder auf Sicherheitslücken im bestehenden System nicht hingewiesen wird.

Die Schwachstelle des fehlenden Know-hows in Unternehmensleitungen und zuständigen Stellen weist damit zwangsläufige Wechselwirkungen mit den anderen beiden Schwachstellen Mensch und Technik auf und potenziert damit die IT-Unsicherheit.

Die nachhaltige Datensicherung stellt eine zentrale Aufgabe im Rahmen der IT-Sicherheit dar. Eine aktive, regelmäßige Datensicherung ist unabdingbar. Selbst ein nur temporärer Verlust von Daten kann zu schwerwiegenden Einschränkungen des Betriebs führen und damit gravierende wirtschaftliche Schäden verursachen. Der vollständige Verlust von Daten kann gegebenenfalls bei datenbasierten Unternehmen die Existenz des Unternehmens bedrohen.

Die Sicherung unternehmenswichtiger Daten fördert nicht nur isoliert die Schutzkomponente der Verfügbarkeit der Informationen. Vielmehr können auch die übrigen Schutzziele – Integrität, Vertraulichkeit und Authentizität – keine Wirkung mehr entfalten, wenn die Daten verloren gehen.

Die Gründe für Datenverluste können vielfältiger Natur sein. Nicht nur Beschädigungen der Speichermedien durch Erschütterungen oder Verschleiß, sondern vor allem durch Schadsoftware sind vielfach verantwortlich für den Verlust unternehmenswichtiger Daten. Aber auch durch die falsche Bedienung durch Mitarbeiter, Diebstahl der Hardware oder anderweitige externe Einflüsse können Datenverluste auftreten. Die Datensicherung stellt sich

damit als Querschnittsmaterie aus den Schwachstellen der Organisation, Technik und Mensch dar; ihr Schwerpunkt ist aber im Bereich der Organisation zu verorten.

Beispiele

Der Verschlüsselungstrojaner „Locky“ schlug im Frühjahr 2016 hohe Wellen, als durch seinen Einsatz vielfach Daten auf den Rechnern der Opfer verschlüsselt und erst gegen Zahlung eines „Lösegeldes“ wieder entschlüsselt wurden. Die Erpresser-Software infizierte alleine an einem Tag deutschlandweit über 17.000 Rechner.

Der Verschlüsselungstrojaner gelangte zwar nicht zwangsläufig durch fehlende organisatorische Maßnahmen auf die Rechner, denn er verbreitete sich vielfach durch rechnungsähnlich gestaltete Dateianhänge. Verschärft wurde die Problematik allerdings oftmals durch fehlende hinreichende Backups der Daten und damit durch Versäumnisse im organisatorischen Bereich der IT-Sicherheit.

Eine nicht zu vernachlässigende Schwachstelle in der IT-Sicherheitsinfrastruktur von Unternehmen stellen mobile Endgeräte dar. Insbesondere im Rahmen von Bring Your Own Device (BOYD), dem Einsatz privater IT-Systeme zur dienstlichen Nutzung, als organisatorischer Entscheidung spielen mobile Endgeräte eine herausragende Rolle. Mobile Endgeräte, etwa Smartphones, weisen durch ihre leichte Portabilität ein erhöhtes Gefährdungspotenzial auf. Zu den allgemein für die IT bestehenden Risiken der Infizierung mit Schadsoftware, kommen noch die Probleme des physischen Verlusts der mobilen Endgeräte. Der damit verbundene Datenverlust stellt eine große Gefährdung für die IT-Sicherheit dar. Auch die diversen Schnittstellen mobiler Endgeräte – USB, WLAN und Bluetooth – können bei Verbindung mit ungesicherten Netzwerken den Verlust von Daten oder die Infizierung mit Schadsoftware zur Folge haben.

Die Sicherheit von Apps stellt einen maßgeblichen Faktor der IT-Unsicherheit mobiler Endgeräte dar. Apps, die mehr als die eigentlich für den Betrieb der App erforderlichen Rechteeinräumung erfordern, sind keine Seltenheit auf dem Markt. Der ungeprüfte Einsatz von Apps auf den für Unternehmenszwecken genutzten Smartphones kann damit zu einem unbemerkten Zugriff auf die mobil gespeicherten Daten führen.

Die Schwachstelle der mobilen Endgeräte stellt sich als klassische Schnittstelle zwischen Organisation, Technik und Mensch dar. Nicht nur organisatorische Verfehlungen, sondern gerade auch technische – etwa der Einsatz veralteter Systeme – und menschliche Versäumnisse – etwa die wahllose Installation von Apps – können die Schutzlücke in der IT-Sicherheitsinfrastruktur vergrößern.

4 Maßnahmen zur IT-Sicherheitsgewährleistung

Umsetzung im Unternehmen

4.1 IT-Sicherheitskonzept

4.1.1 Gesetzliche oder faktische Verpflichtung

Bevor auf die Bestandteile eines IT-Sicherheitskonzepts eingegangen werden kann, muss zunächst geklärt werden, ob für Unternehmen überhaupt eine Verpflichtung zur Erstellung eines IT-Sicherheitskonzepts besteht.

Zwar sehen die Grundsätze der Logik eine – zumindest gedankliche – Durchführung einer Risikoanalyse und darauffolgend eines IT-Sicherheitskonzepts vor, weil IT-Sicherheitsmaßnahmen, zu denen ein Unternehmen schon nach Art. 32 DS-GVO verpflichtet ist, sonst keine Grundlage hätten bzw. nicht rational und planmäßig, sondern eher situativ und zufällig erfolgen. Dennoch ist nicht klar, ob sich aus dem geltenden IT-Sicherheitsrecht eine allgemeine Verpflichtung ergibt.

Im speziellen Bereich des TKG besteht nach § 166 Abs. 1 Nr. 3, Abs. 2 TKG die Verpflichtung zur Erstellung eines IT-Sicherheitskonzepts. Flankiert wird die Regelung im TKG von der Sanktionierung beim Betreiben eines öffentlichen Telekommunikationsnetzes in Form eines Ordnungswidrigkeitstatbestands nach § 228 Abs. 2 Nr. 38 TKG. Auch im GlüStV 2021 mit Wirkung zum 01. Juli 2021 findet sich nunmehr in § 6f GlüStV eine Verpflichtung zur Schaffung eines IT-Sicherheitskonzeptes für die Betreibung eines Online-Casinos.

Selbst in den IT-sicherheitsrechtlichen Bestrebungen im Hinblick auf den Schutz Kritischer Infrastrukturen hat die Pflicht zur Erstellung eines IT-Sicherheitskonzepts keinen Eingang in das Gesetz gefunden. Lediglich in der Gesetzesbegründung zum IT-Sicherheitsgesetz findet sich der Hinweis, dass es „sachgerecht“ sei, wenn die Betreiber von Kritischen Infrastrukturen die Umsetzung der Mindestanforderungen nach § 8a Abs. 1 BSIG in entsprechenden Sicherheits- und Notfallkonzepten dokumentieren.[82] Das IT-Sicherheitsgesetz 2.0 schafft nunmehr besondere Regelungen für Unternehmen im besonderen öffentlichen Interesse in Form des § 8f BSIG. Nach § 8f Abs. 1 BSIG müssen diese ihr IT-Sicherheitskonzept beim Bundesamt vorlegen.

In den allgemeinen Bereichen, in denen etwa das KonTraG die Maßnahmen der IT-Sicherheit bedingen, findet sich im Wortlaut der Vorschriften selbst keine Verpflichtung zur

[82] BT-Drs. 18/4096, S. 26.

Erstellung eines IT-Sicherheitskonzepts. Dennoch kann man in das KonTraG, welches im AktG und im HGB Niederschlag gefunden hat die Grundvoraussetzung der Erstellung eines IT-Sicherheitskonzepts hineinlesen.

Anders sieht es mittlerweile im Datenschutzrecht aus. So sieht Art. 32 Abs. 1 lit. d DS-GVO (auch) als Maßnahme der IT-Sicherheit vor, dass ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vorgehalten werden. Hierdurch wird ausdrücklich ein Sicherheitsmanagement gefordert. Daneben verpflichtet Art 30 Abs. 1 lit g DS-GVO dazu, dass die Verantwortlichen, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 in das Verarbeitungsverzeichnis aufnehmen. Auch das zwingt die Verantwortlichen zumindest dazu, sich Gedanken über den status quo zu machen. Ein weitgehendes „Outsourcing“ der Verpflichtungen im Rahmen der Auftragsverarbeitung ist möglich (vgl. Art 28 Abs.3 S. 2 lit. e DS-GVO). Gleiches gilt im Rahmen einer gemeinsamen Verantwortlichkeit (vgl. Art. 26 Abs. 1 S. 2 DS-GVO).

Außerdem kann aus einer Gesamtbetrachtung der allgemeinen wie besonderen Vorgaben des IT-Sicherheitsrechts und der drohenden Haftungsrisiken eine – wenigstens faktische – Verpflichtung zur Erstellung eines IT-Sicherheitskonzepts im Sinne einer Obliegenheit zur Vermeidung von Haftungsrisiken abgeleitet werden.

4.1.2 Vorgehensweise

Vorgehensweise

1. Risikoanalyse
2. Beachtung spezieller rechtlicher Anforderungen
3. Definition der IT-Sicherheitsleitlinie / des IT-Sicherheitsziels
4. Konkrete Erstellung des IT-Sicherheitskonzepts
5. Tatsächliche Umsetzung des IT-Sicherheitskonzepts
6. Kontrolle des IT-Sicherheitskonzepts

Der eigentlichen Erstellung eines IT-Sicherheitskonzepts durch den IT-Sicherheitsbeauftragten sind drei wesentliche Schritte vorgelagert.

4.1.2.1 Risikoanalyse

Zuerst muss das Unternehmen eine Risikoanalyse beziehungsweise sog. SWOT-Analyse durchführen. Das Unternehmen muss seinen individuellen Schutzbedarf ermitteln, um überhaupt die Erforderlichkeit von Maßnahmen einschätzen zu können.

Dazu muss es analysieren, welche konkreten Gefährdungen beziehungsweise Risiken für das Unternehmen infolge unzulänglicher IT-Sicherheit bestehen würden. Die Analyse der Risiken kann beispielsweise anhand der Schwachstellen im Unternehmen – Mensch, Organisation und Technik – vorgenommen werden.

Mögliche Schäden durch die Beeinträchtigung der IT-Sicherheit sind zu identifizieren. Bei den Schäden sind vor dem Hintergrund des dargestellten Haftungsregimes [B. IT-Sicherheitsrecht] nicht nur direkt eintretende Schäden in die Betrachtung mit einzubeziehen, sondern auch Folgeschäden, etwa die keinesfalls zu vernachlässigenden Reputationsschäden, entsprechend zu gewichten.

Letztlich sind auch die potenziellen Auswirkungen auf den ordnungsgemäßen Geschäftsablauf und die Aufgabenerfüllung durch Sicherheitsvorfälle zu analysieren und zu bewerten.

Die Risikoanalyse dient dazu, Risiken überhaupt zu erkennen, Schwachstellen zu identifizieren und diese einer Gewichtung zuzuführen. Anhand dieser Analyse kann das Unternehmen den konkreten Schutzbedarf für bestimmte Bereiche des Unternehmens bestimmen.

4.1.2.2 Beachtung spezieller rechtlicher Anforderungen

Nach der Analyse der drohenden Risiken ist eine Beachtung spezieller rechtlicher Anforderungen an die IT-Sicherheit geboten. Gegebenenfalls unterfällt das Unternehmen besonderen IT-sicherheitsrechtlichen Vorschriften und muss dadurch in bestimmten Bereichen – unabhängig vom konkret festgestellten Schutzbedarf – erhöhten Sicherheitsanforderungen genügen.

Beispielsweise unterliegen Betreiber Kritischer Infrastrukturen besonderen Mindestanforderungen an die IT-Sicherheit nach § 8a BSIG, die sie einhalten müssen.

4.1.2.3 Definition der IT-Sicherheitsleitlinie / der IT-Sicherheitsziele

Nach der Analyse der drohenden Risiken sowie der damit einhergehenden Einstufung des Schutzbedarfs der IT-Systeme des Unternehmens und der Betrachtung spezieller rechtlicher Anforderungen muss das jeweilige Unternehmen seine individuelle IT-Sicherheitsleitlinie beziehungsweise IT-Sicherheitsziele definieren.

Diese IT-Sicherheitsleitlinie bestimmt anhand des ermittelten Schutzbedarfs welche konkreten IT-Sicherheitslevels im Unternehmen einzuhalten sind, um den reibungslosen Betrieb des Unternehmens zu gewährleisten.

So wird beispielsweise ein E-Commerce-Unternehmen die dauerhafte Erreichbarkeit der Homepage höher einstufen als ein Unternehmen, dessen Vertrieb noch überwiegend im analogen Bereich funktioniert.

Die Definition der IT-Sicherheitsziele dient als Grundlage für die Erstellung des Sicherheitskonzepts, da es eine Wertung bestimmter zu gewährleistender IT-Sicherheitsbereiche vorgibt und damit bestimmte Maßnahmen beziehungsweise Kategorien von Maßnahmen zwingend voraussetzt.

4.1.2.4 Erstellung des IT-Sicherheitskonzepts

Aus den zuvor im Rahmen der Risikoanalyse ermittelten Schutzbedarfsstufen, gesetzlichen Vorgaben und individualisierten IT-Sicherheitszielen müssen sich die konkret zu treffenden IT-sicherheitsrechtlichen Schutzvorkehrungen ableiten.

4.1.2.5 Tatsächliche Umsetzung des IT-Sicherheitskonzepts

Ohne eine Umsetzung des IT-Sicherheitskonzepts in die Unternehmenswirklichkeit bleibt es nichts weiter als bloßer Programmsatz. Die tatsächliche Umsetzung und Etablierung der im IT-Sicherheitskonzept vorgeschriebenen Schutzvorkehrungen ist unabdingbare Voraussetzung für die Erreichung der gesetzten IT-Sicherheitsziele im Unternehmen.

4.1.2.6 Kontrolle des IT-Sicherheitskonzepts

Selbst nach der Umsetzung des IT-Sicherheitskonzepts bedarf dieses sowohl einer Überprüfung im Normalbetrieb als auch steter Kontrolle hinsichtlich der Einhaltung der Vorgaben. Flankieren kann die Kontrolle die Etablierung eines Sanktionensystems für die Nichteinhaltung wesentlicher IT-sicherheitsrechtlicher Schutzvorkehrungen.

4.1.3 Bestandteile eines IT-Sicherheitskonzepts

Die drei wesentlichen Schritte der Risikoanalyse, Beachtung spezieller gesetzlicher Bestimmungen und Definition individualisierter IT-Sicherheitsziele stellen die Basis des IT-Sicherheitskonzepts dar.

Nachdem IT-Sicherheit nicht durch isolierte Einzelmaßnahmen erreicht werden kann, muss ein spezifisch auf die Bedürfnisse des Unternehmens zugeschnittenes Konzept, das auf einer Vielzahl von Maßnahmen beruht, erstellt werden. Erforderlich ist demnach eine Maßnahmenplanung. Zu beachten ist aber im Rahmen der Planung der einzelnen Maßnahmen, dass diese gegebenenfalls nicht kompatibel miteinander sind oder sich gar gegenseitig behindern. Bei der Erstellung des IT-Sicherheitskonzepts müssen mithin die einzelnen Maßnahmen konsolidiert werden.

Orientierungshilfen für die einzeln zu ergreifenden und möglichen Maßnahmen finden sich beispielsweise in den IT-Grundschutz-Kompendium des BSI sowie in ISIS12 für kleine und mittelständische Unternehmen (KMU).

Im Folgenden werden einige unabdingbare Bestandteile eines IT-Sicherheitskonzepts beschrieben, die unerlässlich sind, um zu einem angemessenen IT-Sicherheitsniveau zu gelangen.

4.1.3.1 Implementierung wesentlicher Schutzvorkehrungen

Wesentliche, geschäftsübliche Schutzvorkehrungen – etwa Anti-Viren-Programme, Spam-Filter, Firewalls – müssen Bestandteil jedes IT-Sicherheitskonzepts sein. Ein weiterer zwingender Bestandteil eines IT-Sicherheitskonzepts sind Vorgaben zur Datensicherung im Unternehmen.

4.1.3.2 Festlegung klarer Zuständigkeiten

Die Festlegung klarer Zuständigkeiten im Rahmen der IT-Sicherheit kann die Gefährdungslagen der IT-Sicherheit „ins Blaue hinein“ minimieren. Nur wenn im Unternehmen klar ist, wer für welche Bereiche der IT-Sicherheit verantwortlich ist, werden die diesbezüglich zu treffenden Schutzvorkehrungen auch tatsächlich umgesetzt werden.

Es empfiehlt sich, die Zuständigkeiten nicht nur im IT-Sicherheitskonzept festzulegen, sondern auch für das gesamte Unternehmen in Form einer Kompetenzmatrix publik zu machen. Diese muss Angaben über Verantwortliche und Stellvertreter für folgende Stellen enthalten: IT-Sicherheitsbeauftragter, Datenschutzbeauftragter, Brandschutzbeauftragter sowie Notfallbeauftragter.

4.1.3.3 Organisatorische Maßnahmen bezüglich der Schwachstelle Mensch

Die Analyse der Bedrohungslagen (C. Gefährdungsszenarien) hat ergeben, dass der Mensch eine wesentliche Schwachstelle der IT-Sicherheit darstellt. Um diese Schwachstelle zumindest einzugrenzen, muss das IT-Sicherheitskonzept diesbezüglich organisatorische Vorgaben enthalten.

Das IT-Sicherheitskonzept muss die Vornahme von Schulungen der Mitarbeiter, die Festlegung unternehmensinterner Richtlinien für IT-Anwender sowie ein Rechte- und Rollenmanagement vorschreiben.

Von wesentlicher Bedeutung ist auch die Etablierung eines unternehmensinternen Meldesystems für IT-Sicherheitsvorfälle. Dieses ist klar von den gesetzlichen Meldepflichten nach DS-GVO, TKG und BSIG zu unterscheiden.

4.1.3.4 Dokumentation

Der Dokumentation der getroffenen Maßnahmen kann für Haftungsfragen eine maßgebliche Bedeutung zukommen. Auch im Rahmen von späteren Revisionen kommt der Dokumentation der IT-Sicherheitsmaßnahmen Relevanz zu.

4.1.3.5 Etablierung eines Kontrollsystems, Zeitvorgaben

Die Etablierung eines Kontrollsystems zur Einhaltung der Vorgaben des IT-Sicherheitskonzepts ist von Nöten, um zu verhindern, dass das Konzept zu einem bloßen Programmsatz verkommt.

Die Festlegung von Zeitplänen zur Umsetzung der IT-Sicherheitsvorkehrungen geht in dieselbe Richtung und soll die Wirkungslosigkeit des Konzepts verhindern.

4.1.3.6 Notfallkonzept [ggf. auch als eigenes Konzept]

Alle bisher genannten Maßnahmen beschäftigten sich mit der Sicherstellung des zuvor definierten IT-Sicherheitsniveaus. Um aber auch für Notfälle, also das Versagen einzelner IT-sicherheitsrechtlicher Schutzvorkehrungen, gewappnet zu sein, muss das IT-Sicherheitskonzept entweder ein Notfallkonzept beinhalten oder ein solches muss explizit als eigenständiges Konzept erstellt werden.

Ein solches Notfallkonzept muss zunächst den Begriff des Notfalls definieren, um seinen Anwendungsbereich klar abzustecken. Dieses Konzept muss weiter Vorgaben zur Einschätzung des Notfalls und zur Reaktion auf den Notfall enthalten.

Zentrale Bausteine der Reaktion sind eine Zuordnung der Verantwortlichkeiten im Notfall und die Etablierung eines Alarmierungsplans. Abhängig von der konkreten Einstufung des Notfalls müssen die Vorgehensweisen definiert werden. Die Erstellung von Wiederherstellungsdateien, die redundante Vorhaltung wesentlicher IT-Infrastrukturen und die Priorisierung wichtiger Dienste sind wesentliche Bestandteile des Vorgehens bei Notfällen.

Auch die Erstellung eines Notfallhandbuchs für die IT-Sicherheit kann helfen, das Notfallkonzept bei allen Mitarbeitern präsent zu machen und das Vorgehen im Notfall zu erleichtern.

Der Notfallplan muss von der Durchführung von Notfallübungen beziehungsweise der Simulation von Notfällen flankiert werden, um im Ernstfall adäquate Ergebnisse erzielen zu können.

Hinweise zum Vorgehen im Falle eines Notfalls finden Sie im Anhang 3.

4.2 IT-Sicherheitsbeauftragter

Eine gesetzliche Pflicht zur Bestellung eines IT-Sicherheitsbeauftragten findet sich lediglich in § 166 Abs. 1 Nr. 1 TKG. Die übrigen Gesetze – selbst das spezielle IT-Sicherheitsgesetz – dagegen schweigen sich zur verpflichtenden Bestellung eines IT-Sicherheitsbeauftragten aus.

Trotz der fehlenden ausdrücklichen gesetzlichen Verpflichtung ergibt eine Gesamtbetrachtung des anwendbaren IT-Sicherheitsrechts und des Haftungsregimes zumindest eine faktische Pflicht zur Bestellung eines IT-Sicherheitsbeauftragten, um das Haftungsrisiko zu reduzieren. Auch eine mittelbare Pflicht aus § 91 Abs. 2 AktG beziehungsweise § 43 Abs. 1 GmbHG im Falle einer AG beziehungsweise GmbH erscheint konstruierbar.[83]

Hinsichtlich der Anforderungen, die an die Person des IT-Sicherheitsbeauftragten zu stellen sind, kann auf die Grundsätze der Bestellung von Datenschutzbeauftragten in Unternehmen zurückgegriffen werden. Demnach werden auch hier Fachkunde und Zuverlässigkeit wesentliche Kriterien bei der Bestellung darstellen.

4.3 Grundlegende Anforderungen an IT-Sicherheitsmaßnahmen

Die Darstellung des IT-sicherheitsrechtlichen Rechtsrahmens hat gezeigt, dass vielfach keine expliziten Sicherheitsvorkehrungen im Gesetz genannt werden, sondern lediglich auf technische und organisatorische Schutzvorkehrungen abgestellt wird. Diese stehen aus Verhältnismäßigkeitsgesichtspunkten unter dem allgemeinen Vorbehalt des technisch Möglichen und wirtschaftlich Zumutbaren. Oftmals wird noch ausdrücklich eine Orientierung der Schutzvorkehrungen am Stand der Technik vom Gesetzgeber eingefordert.

Die Gesichtspunkte zur Bestimmung des technisch Möglichen und wirtschaftlich Zumutbaren ergeben sich stets aus dem konkreten Einzelfall. Maßgeblich ist hierfür eine Güterabwägung, in welche die betroffenen Positionen einzustellen sind. Hilfreich ist hierfür eine Qualifizierung der IT-Sicherheitsrisiken anhand von Schutzbedarfsstufen, die im Rahmen der Risikoanalyse vorgenommen wird.

4.4 Konkrete Handlungsempfehlungen

Ausgehend von den oben dargestellten Gefährdungsszenarien (C. Gefährdungsszenarien) soll im Rahmen der organisatorischen und technischen Handlungsempfehlungen jeweils Bezug darauf genommen werden, welche Schwachstellen durch diese Maßnahmen vermindert werden.

[83] Schmidl/Tannen, in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 8 Corporate Governance und Compliance Rn. 38.

4.4.1 Organisatorische Handlungsempfehlungen

Überblick

- Schulungen
- IT-Sicherheitsrichtlinien
- Klare Zuständigkeitsverteilung und Rechtemanagement
- Internes Meldesystem
- Passwortschutz
- Schutzvorkehrungen für mobile Endgeräte
- Datensicherungen
- Zugangs- und Zutrittskontrollen
- Qualifizierter Notfallplan
- Gewährleistung nachhaltiger IT-Sicherheit

Um die Schwachstelle Mensch mittels organisatorischer Schutzvorkehrungen einzudämmen, kommen insbesondere Schulungen der Mitarbeiter und Erlass von IT-Sicherheitsrichtlinien im Unternehmen in Frage.

Der sichere Umgang mit IT setzt die Kenntnisse bestimmter Grundlagen der IT voraus, die den Mitarbeitern durch Schulungen vermittelt werden müssen. Außerdem kann in den Schulungen auch auf besondere Gefährdungslagen eingegangen werden. Die Schulungen sind in regelmäßigen Zeitabständen zu wiederholen, um das Sicherheitsbewusstsein der Mitarbeiter nachhaltig zu fördern und zu sensibilisieren. Durch Newsletter oder andere aktuelle Informationen sind die Mitarbeiter über aktuell bestehende Bedrohungslagen zu informieren.

Vor dem Hintergrund der aktuellen Bedrohungslagen durch Social Engineering müssen sich IT-Sicherheitsschulungen auch vermehrt mit dem Thema Vertrauen im World Wide Web und den sozialen Netzwerken auseinandersetzen.

Beispiel

Im Zeitraum der höchsten Aktivität des Verschlüsselungstrojaners „Locky“ war es unabdingbar, Mitarbeiter durch explizite Warnungen für diese Bedrohung zu sensibilisieren.

IT-Sicherheitsrichtlinien stellen unverzichtbare Verhaltensanweisungen und -empfehlungen für die Mitarbeiter im Umgang mit IT dar. Diese Richtlinien können vielfältige Vorgaben zur Nutzung der IT durch die Mitarbeiter enthalten. Darin sind etwa das ordnungsgemäße Verhalten der Mitarbeiter im World Wide Web und Verbote hinsichtlich des

Downloads von Software festzuschreiben. So kann auch das Verbot der privaten Nutzung der IT-Systeme des Unternehmens in den Sicherheitsrichtlinien vorgesehen werden.

Außerdem sind die Sicherheitsrichtlinien an aktuelle Entwicklungen in der IT anzupassen. So sind beispielsweise mobile Endgeräte aufgrund ihrer zunehmenden Verbreitung im Arbeitsalltag mittlerweile zwingender Bestandteil von IT-Sicherheitsrichtlinien.

Die klare Verteilung von Zuständigkeiten und ein eingeschränktes Rechte- und Rollen-management können dazu beitragen, dass der sorglose Umgang der Einzelnen mit der IT verhindert wird.

Die Veröffentlichung einer Zuständigkeitsmatrix der relevanten Stellen im Unternehmen kann dazu beitragen, dass die Verteilung der Zuständigkeiten im gesamten Unternehmen klar hervortritt.

Im Rahmen eines eingeschränkten Rechte- und Rollenmanagements soll dem einzelnen Mitarbeiter nur insoweit Zugriff auf die IT-Systeme zugestanden werden, wie er auch tatsächlich für seine Aufgabenerfüllung im Unternehmen benötigt. Damit können sowohl versehentliche Löschungen von Datenbeständen, das Einschleppen von Schadsoftware in sensible Bereiche als auch die bewusste Manipulation der IT-Systeme vermieden werden.

Sowohl das Verbot der Installation von Software durch die Mitarbeiter als auch die Verpflichtung zu Durchführung von Updates seitens der IT-Verantwortlichen sind organisatorische Maßnahmen, die aber zugleich auf die Schwachstellen Mensch und Technik Einfluss nehmen und deren Gefährdungspotenziale reduzieren.

Die Etablierung eines internen Meldesystems für IT-Sicherheitsvorfälle stellt einen wesentlichen Baustein im Rahmen der IT-Sicherheitsinfrastruktur dar. Nur wenn einzelne betroffene Mitarbeiter wissen, an wen sie sich in IT-Sicherheitsvorfällen oder bei Bedrohungen der IT-Sicherheit wenden können, ist die Gewährleistung der IT-Sicherheit im gesamten Unternehmen möglich.

Für die Passwortsicherheit von Bedeutung ist vor allem, dass unterschiedliche Passwörter für verschiedene Dienste genutzt werden. Das mildert die Folgen der Offenlegung eines einzelnen Passworts ab. Darüber hinaus kann eine Zwei-Faktor-Authentisierung sinnvoll sein, da dann selbst mit Kenntnis des Passworts kein Zugriff erfolgen kann. Häufige Passwortwechsel sind entgegen einem häufigen Missverständnis kontraproduktiv.[84]

Flankiert werden muss die Passwortsicherheit durch entsprechende Regelungen in den IT-Sicherheitsrichtlinien. Die Weitergabe des Passworts an unbefugte Dritte muss klar untersagt werden.

[84] https://www.heise.de/newsticker/meldung/Wider-den-Zwang-zur-Passwort-Aenderung-3176493.html; https://www.heise.de/ix/meldung/Bitkom-Stress-mit-der-Passwort-Flut-3171943.html.

In Zeiten von BYOD und mobilen Endgeräten ist es von essenzieller Bedeutung, dass Unternehmen ein zwingendes Meldesystem für den Verlust von mobilen Endgeräten, auf denen Daten des Unternehmens gespeichert sind, zu etablieren. Von vornherein sollten mobile Geräte nur verschlüsselt genutzt werden.

Aber nicht nur die Meldung des Verlusts an sich, sondern auch die Fernsperrung oder gar Fernlöschung der Daten müssen organisatorisch sichergestellt werden.

Im Rahmen der Schulungen und der Sicherheitsrichtlinien ist diesem gegenwärtigen Phänomen der mobilen Endgeräte ebenfalls Bedeutung beizumessen. Um hier Gefährdungen auszuschließen kann von Vornherein die private Nutzung mobiler Endgeräte des Unternehmens verboten werden.

Die Installation von Apps auf den mobilen Endgeräten kann anhand von Corporate App Stores IT-sicherer gestaltet werden. Listen mit zugelassenen Apps (sog. White Lists) können ebenfalls wirksame Instrumente sein.

Alternativ zu BYOD können Unternehmen auf Choose Your Own Device (CYOD) setzen und damit lediglich IT-sichere mobile Endgeräte von Seiten des Unternehmens an die Mitarbeiter ausgeben. CYOD kann damit als IT-sicherere Alternative zu BYOD verstanden werden.

Eine aktive, kontinuierliche Datensicherung ist für Unternehmen unerlässlich. Die Ausführung der Datensicherung kann durch verschiedene Konzepte bewerkstelligt werden.

Der benötigte Backup-Umfang, die Backup-Strategie, der Zeitplan sowie die örtliche Aufbewahrung der Backups bestimmen letztendlich die individuell zu wählende Backup-Strategie. Keinesfalls dürfen Backups aber auf demselben Medium gesichert werden, auf dem die zu sichernden Dateien liegen. Vielmehr sind Backups auf externen Laufwerken oder Unternehmensservern zu verorten.

Die Erstellung qualifizierter Notfallpläne ist unabdingbare Voraussetzung, um beim Versagen der IT-Sicherheitsvorkehrungen den Schaden eindämmen und möglichst schnell wieder in den Normalbetrieb zurückkehren zu können. Bestandteile eines qualifizierten Notfallplans sind die Benennung von Verantwortlichen, die Erstellung von Wiederherstellungsdateien, die redundante Vorhaltung wesentlicher IT-Infrastrukturen und die Priorisierung wichtiger Dienste.

Das Schlagwort der Nachhaltigkeit kann auch in die IT-Sicherheit Eingang finden. Die IT-Sicherheitslage zeichnet sich gerade durch ihren innovativen, schnelllebigen Wandel aus. Daher ist ein ständiges Reagieren auf aktuelle Bedrohungslagen, die Anpassung der Sicherheitskonzepte und -vorkehrungen von Nöten, um zu adäquaten Lösungen zu gelangen. Nachhaltigkeit kann auch dadurch gewährleistet werden, dass Kostenaspekte bei der Beschaffung von IT-Sicherheitsvorkehrungen nicht in den Vordergrund treten, sondern der Sicherheit der Vorrang eingeräumt wird. Insbesondere darf nicht außer Acht gelassen werden, dass bei fehlender IT-Sicherheit vielfältige Haftungsrisiken drohen. (siehe 2. IT-Sicherheitsrecht)

4.4.2 Technische Handlungsempfehlungen

Überblick

- Sichere elektronische Kommunikation
- Prävention vor unberechtigten Zugriffen und Malware
- Wartung und Aktualisierung
- Gebäudesicherheit

Der Schutz der elektronischen Kommunikation ist vor dem Hintergrund ihrer weiträumigen Verbreitung und der bestehenden Risiken eine wesentlich technisch zu bewältigende Problematik.

Durch den Einsatz angemessener kryptographischer Verfahren können die Schutzziele der Authentizität, Integrität und Vertraulichkeit im Rahmen der elektronischen Kommunikation gestärkt werden. Bei der Verschlüsselung ist eine sog. Ende-zu-Ende-Verschlüsselung für besonders vertrauliche Kommunikation vorzuziehen. Das Verschlüsselungsniveau kann natürlich abhängig vom Schutzbedarf der jeweiligen Kommunikation variieren.

Auch die Verwendung digitaler Signaturen im Rahmen der unternehmensinternen Kommunikation kann beispielsweise Phishing-Attacken im unternehmerischen Bereich eindämmen. Fortgeschrittene oder qualifizierte elektronische Signaturen stärken hierbei die Authentizität und Integrität der elektronischen Kommunikation.

Die Prävention vor unberechtigten Zugriffen und vor Malware kann überwiegend durch den Einsatz handelsüblicher IT-Schutzvorkehrungen erreicht werden. Die Einrichtung von Viren-/Malwarescannern und die Einrichtung von Spamfiltern sind wesentliche Bausteine einer ordnungsgemäßen IT-Infrastruktur. Die Spam-Filter haben wiederum Einfluss auf den Faktor Mensch, der letztendlich durch die Spam-Filter vor übermäßigen Spam-Aufkommen in Schutz genommen wird und damit der sorglose Umgang mit Spam-Mails zumindest in weiten Bereichen verhindert wird.

Die Einrichtung von Browser Plug-Ins zur Erkennung gefährlicher Webseiten stellt zwar eine technische Maßnahme dar, die aber überwiegend das Gefahrenpotenzial sorglosen Umgangs mit der IT durch die Mitarbeiter betrifft. Daneben ist zu überlegen, ob nicht Adblocker und Scriptblocker im Browser genutzt werden müssen. Das vermindert die Angriffsfläche für Angriffe über Browser stark.

Die restriktivere Handhabung der IT kann auch die Sperrung bestimmter Webseiten abhängig von den konkreten Arbeitsplätzen beinhalten. Dadurch werden diesbezüglich bestehende Schwachstellen infolge Fehlverhaltens der Mitarbeiter nahezu komplett ausgeschlossen.

Eine beständige Wartung und Aktualisierung der unternehmenseigenen Hard- und Software ist notwendig, um bestehenden IT-Risiken zu begegnen.

Ein nicht zu vernachlässigender Faktor im Rahmen der technischen Schutzvorkehrungen ist die Sicherstellung der allgemeinen Gebäudesicherheit. Eine räumliche Trennung wichtiger Speichermedien, die Verschließbarkeit von Räumen mit Serveranlagen sowie Vorkehrungen zum Brandschutz sind nur einige der zu treffenden Maßnahmen.

Die allgemeine Gebäudesicherheit kann auch Eingang in die IT-Sicherheitsrichtlinien des Unternehmens finden, indem Mitarbeitern aufgegeben wird, die Arbeitsräume beim Verlassen zu verschließen, um damit dem Verlust von unternehmenswichtigen Informationen und Produktionsmitteln vorzubeugen.

4.5 Zusammenfassung

Sowohl die Erstellung eines IT-Sicherheitskonzepts als auch die Bestellung eines IT-Sicherheitsbeauftragten sind faktisch zwingende und wesentliche Elemente zur Gewährleistung der IT-Sicherheit.

Die Darstellung der organisatorischen und technischen Maßnahmen, die Bestandteile des IT-Sicherheitskonzepts sind, hat deutlich gemacht, dass IT-Sicherheitsmaßnahmen niemals isoliert betrachtet werden dürfen. Selbst wenn die Maßnahmen aus organisatorischen oder technischen Gründen getroffen werden, so haben sie Auswirkungen auf diverse Schwachstellen im Unternehmen. Deshalb ist für jedes Unternehmen ein spezifisch an die jeweiligen Bedürfnisse angepasstes Konzept erforderlich.

Nur die Einbeziehung aller sog. Schwachstellen im Unternehmen kann dazu beitragen, ein nachhaltiges und wirksames IT-Sicherheitskonzept zu gestalten, das in seiner tatsächlichen Umsetzung zur adäquaten Gewährleistung der IT-Sicherheit beiträgt.

5 IT-Sicherheit in der Praxis

Informationsquellen

5.1 Umfragen, Gutachten, Handlungsempfehlungen

Umfragen zur IT-Sicherheit

- IT-Sicherheit: Verfassungsschutz fordert mehr Engagement von Unternehmen
  https://www.heise.de/news/IT-Sicherheit-Verfassungsschutz-fordert-mehr-Engagement-von-Unternehmen-9292914.html

- Bitkom-Umfrage 2023: Mehr als 200 Milliarden Euro Schaden für die deutsche Wirtschaft in diesem Jahr
  https://www.deutschlandfunk.de/bitkom-umfrage-mehr-als-200-milliarden-euro-schaden-fuer-die-deutsche-wirtschaft-in-diesem-jahr-100.html

- Bitkom und BKA zum Cyberlagebild 2022
  https://www.bitkom.org/Presse/Presseinformation/Bitkom-und-BKA-zum-Cyberlagebild-2022

- BSI Cyber-Sicherheits-Umfragen
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/cyber-sicherheitsumfrage_node.html

Gutachten/Studien/Handlungsempfehlungen

- BSI: Die Lage der IT-Sicherheit in Deutschland 2022
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6

- Europol: Internet Organised Crime Threat Assessement 2023
  https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

- BSI: Anforderungskatalog Cloud Computing (C5) 2020
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

- Deloitte Future of Cyber Security 2030
  https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Deloitte-European-Cyber-Defense-Report-Part-2.pdf

- Teletrust: Handreichung zum „Stand der Technik“
  https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

- Bitkom: Spionage, Sabotage und Datendiebstal – Wirtschaftsschutz in der Industrie
  https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

- Bundesdruckerei: Digitalisierung und IT-Sicherheit in deutschen Unternehmen
  https://www.bundesdruckerei.de/de/loesungen/it-sicherheit

- BSI: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2

- BMWi: Plattform Industrie 4.0 Fortschrittsbericht 2023
  https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/2023-fortschrittsbericht.html

- Standard-Datenschutzmodell der Konferenz der unabhängigen Datenschutzbehörden
  https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
  - Das SDM soll eine systematische Planung, Umsetzung und Überwachung der Datenschutzvorgaben ermöglichen
  - Es soll ein einheitliches, transparentes, nachvollziehbares Gesamturteil über ein Verfahren erlauben
  - Die Bausteine sind momentan bruchstückhaft, sollen aber sukzessive ausgebaut werden

- BayStMI/BayStMFH: Bericht zur Cybersicherheit in Bayern 2022
  https://www.stmi.bayern.de/assets/stmi/sus/datensicherheit/broschüre_cybersicherheit_in_bayern_2022.pdf

- Bitkom: Wirtschaftsschutz 2022
  https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf

- BSI: Die Lage der IT-Sicherheit in Deutschland 2022
  https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

- ENISA: NIS Investments 2022
  https://www.enisa.europa.eu/publications/nis-investments-2022

- BSI: Große Sprachmodelle – Chancen und Risiken für Industrie und Behörden,
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Grosse_KI_Sprachmodelle.html

- BKA: Bundeslagebild Cybercrime 2022
  https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

5.2 Sonstige Vorhaben in der Politik zur IT-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Modernisierter IT-Grundschutz:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

Strategie Künstliche Intelligenz der Bundesregierung vom November 2018

- https://www.ki-strategie-deutschland.de/home.html
- „Wir wollen sicherstellen, dass IT-Systeme, die KI nutzen und zur Anwendung bringen, ein hohes Niveau an IT-Sicherheit gewährleisten, damit Manipulation, Missbrauch und Risiken für die öffentliche Sicherheit dieser sensiblen Technologie bestmöglich verhindert werden." (Seite 8, lit. g)
- „Wir werden die Angriffssicherheit von KI-Systemen steigern und KI als Grundlage für die allgemeine IT-Sicherheit weiter ausbauen." (S. 18).
- „Aufgrund der zunehmenden Durchdringung von KI und der damit einhergehenden Intensivierung von Mensch-Maschine-Interaktion erfordern die Entwicklung und
- Anwendung von KI die Einhaltung höchster Sicherheitsstandards. Die Gewährleistung von IT-Sicherheit ist eine zentrale Voraussetzung für die Produktsicherheit von KI-Anwendungen beziehungsweise von Produkten, die KI nutzen. Die heutige Fokussierung auf Betreiber kritischer IT-Infrastrukturen etwa im IT-, Gesundheits- oder Energiebereich reicht nicht mehr aus. Daher ist eine adäquate Verpflichtung für Hard- und Softwarehersteller anzustreben, die das Prinzip Security by Design fördert." (S. 38)
- Beschluss des Bundeskabinetts zur Fortschreibung der KI-Strategie der Bundesregierung bis 2025:
  https://www.bmbf.de/bmbf/shareddocs/pressemitteilungen/de/kabinett-beschliesst-fortschre--strategie-der-bundesregierung.html#:~:text=Kabinett%20beschließt%20Fortschreibung%20der%20KI%20Strategie%20der%20Bundesregierung%2002.12.2020,auf%20fünf%20Milliarden%20Euro%20erhöht
- KI-Aktionsplan des BMBF 2023:
  https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/kuenstliche-intelligenz/kuenstliche-intelligenz_node.html

Strategien der Länder:

- Cybersicherheitsstrategie des Freistaates Bayern als Teil des 2023 verabschiedeten Digitalplans (https://digitalplan.bayern/bayern/de/flexPrjList/57903/project/205;jsessionid=4B2CCC8E84F19D2B7CDD4AF1B3B37D9D.liveWorker2)
- Zu den Cybersicherheitsstrategien der Bundesländer vgl. https://background.tagesspiegel.de/cybersecurity/welche-bundeslaender-haben-eine-cybersicherheitsstrategie

Aktionspläne

- FinTech-Aktionsplan der EU-Kommission (https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0003.02/DOC_1&format=PDF)

- Umsetzung der Leitlinie des IT-Planungsrats zur Informationssicherheit (https://www.it-planungsrat.de/projekte/umsetzung-der-leitlinie-fuer-informationssicherheit)
  - Der Umsetzungsplan zur Leitlinie schreibt die stufenweise Umsetzung der Vorgaben vor. Für 2022 ist z. B. die flächendeckende Erstellung der Sicherheitskonzepte für geschäftskritische oder für OZG-Verfahren als Ziel vorgegeben. Parallel dazu wird jährlich die Fortbildung der Informationssicherheitsbeauftragten und die Durchführung von Sensibilisierungsveranstaltungen für die Beschäftigten durch den IT-Planungsrat gefördert. Die Förderung wird im Rahmen der ständigen Arbeitsgruppe Informationssicherheit des IT-Planungsrates zwischen Bund und Ländern abgestimmt.

- BMVI: Digitalisierung und Künstliche Intelligenz in der Mobilität (https://www.bmvi.de/SharedDocs/DE/Anlage/DG/aktionsplan-ki.pdf?__blob=publicationFile)
  - „Die Gewährleistung von IT-Sicherheit und Datenschutz sind integrale Bestandteile der ‘digitalen Mobilität‘.“

- BMI: Cybersicherheitsagenda und Cybersicherheitsstrategie der Bundesregierung von September 2021 https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cybersicherheitspolitik/cybersicherheitspolitik-node.html
  - Die Cybersicherheitsstrategie 2021 definiert vier übergreifende Leitlinien:
    - Cybersicherheit als gemeinsame Aufgabe von Staat, Wirtschaft, Gesellschaft und Wissenschaft etablieren
    - Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken
    - Digitalisierung sicher gestalten und Ziele messbar und transparent ausgestalten

- BMI: Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4)

Literaturverzeichnis

Auer-Reinsdorff/Conrad:
Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019

Bronner/Ziegler:
DSGVO-Schadensersatz nach Hacker-Angriff, BayWiDI-Briefing 2023/3, S. 6 f.

Denkhaus/Richter/Bostelmann:
Onlinezugangsgesetz, 2019

Djeffal, C.:
Neue Sicherungspflicht für Telemediendiensteanbieter. Webseitensicherheit jetzt Pflicht nach dem IT-Sicherheitsgesetz, MMR 2015, 716

Dittrich/Heinelt, Die Europäische DORA, RDi 2023, 164

Gola/Heckmann:
DSGVO BDSG, 3. Aufl. 2022

Hauschka/Moosmayer/Lösler:
Corporate Compliance, 3. Auflage, 2016

Heckmann, D.:
Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, MMR 2006, 280

Heckmann D./Paschke A.:
jurisPraxiskommentar Internetrecht, 7. Aufl. 2021

Hornung, G./Schallbruch, M.:
IT-Sicherheitsrecht, 2021

Kipker, D.:
Cybersecurity, 2. Aufl. 2023

Kipker/Birreck/Niewöhner/Schnorr:
NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie, MMR 2021, 214

Köhler/Bornkamm:
GeschGehG, 39. Aufl. 2021

Köstner/Nonn:
Das Cybersecurity Law der VR China, MMR 2020, 591

Paal/Pauly:
DS-GVO, 3. Aufl. 2021

Scherer, H.:
Good Governance und ganzheitliches strategisches und operatives Management, CCZ 2012, 201

Scholtyssek/Judis/Krause:
Das neue Geschäftsgeheimnisgesetz – Risiken, Chancen und konkreter Handlungsbedarf für Unternehmen, CCZ 2020, 23

Wagner, F.:
Datenschutz und die VR China – ein Widerspruch? Sozialkreditsystem und Personal Information Security Specification, ZD 2020, 140

Ziegler, N.:
Digitale Produktsicherheit: Der Vorschlag des Cyber Resilience Acts der EU-Kommission. jurisPR-ITR (2/2023 Anm. 2)

Anhang

Kapitelübersicht

A.1 Standards – Überblick nach Inhalten

3.3 Zuordnung der Einzelstandards

Im Folgenden werden die grundlegenden Standards zum IT-Sicherheits- und Risikomanagement den oben dargestellten Gruppen zugeordnet

Privacy- und Identity Management

ISO/IEC 29100	Privacy framework
ISO/IEC 29101	Privacy architecture framework
ISO/IEC 24760	A framework for Identity management
ISO/IEC 29115	Entity authentication assurance framework

Biometrie

ISO/IEC 19784	Biometric application programming interface Biometrische Anwendungs-programmier-Schnittstelle(BioAPI)
ISO/IEC 19785	Common Biometric Exchange Formats Framework Rahmenbedingungen gemeinsamer biometrischer Austauschformate
ISO/IEC 19794	Biometric data interchange formats Biometrische Datenaustauschformate
ISO/IEC 30107	Presentation attack detection Presentation Attack Detection

Informationssicherheits-Managementsysteme (ISMS)

ISO/IEC 27001	Information security management systems – Requirements Informationssicherheits-Managementsysteme– Anforderungen
ISO/IEC 27002	Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement

Risikomanagement

ISO/IEC 27005	Information security risk management Informationssicherheits-Risiko-management
ISO/IEC 27014	Governance of information security Governance von Informationssicherheit

Vorschriften

BDSG	Bundesdatenschutzgesetz

Evaluierung von IT-Sicherheit

Common Criteria

ISO/IEC 15408 (CC)	Evaluation criteria for IT security (Common Criteria) Evaluationskriterien für IT-Sicherheit
ISO/IEC TR 15443	A framework for IT security assurance Rahmenrichtlinien für Sicherung von IT-Sicherheit

■ ISO/IEC 18045	Methodology for IT security evaluation Methodik zur Evaluation von IT-Sicherheit
■ ISO/IEC 21827 (SSE-CMM)	System Security Engineering – Capability Maturity Model Modell der Ablaufstauglichkeit (auch ISO 21827)
■ BSI-TR-03125	Technische Richtlinie für Beweiswerterhaltung kryptographisch signierter Dokumente

Schutzprofile

■ ISO/IEC TR 15446	Guide on the production of protection profiles and security targets Leitfaden zum Erstellen von Schutzprofilen und Sicherheitsvorgaben

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

■ ISO/IEC 18033	Encryption algorithms Verschlüsselungsalgorithmen
■ ISO/IEC 10116	Modes of operation for an n-bit block cipher Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
■ ISO/IEC 19772	Data encapsulation mechanisms Daten verkapselnde Mechanismen
■ ISO/IEC 29192	Lightweight cryptography Leichtgewichtige Kryptographie

Digitale Signaturen

■ ISO/IEC 9796	Digital signature schemes giving message recovery Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht
■ ISO/IEC 14888	Digital signatures with appendix Digitale Signaturen mit Anhang
■ ISO/IEC 15946	Cryptographic techniques based on elliptic curves Auf elliptischen Kurven aufbauende kryptographische Techniken

Hash-Funktionen und andere Hilfsfunktionen

■ ISO/IEC 10118	Hash functions Hash-Funktionen
■ ISO/IEC 18031	Random bit generation Erzeugung von Zufallszahlen
■ ISO/IEC 18032	Prime number generation Primzahlerzeugung

Authentifizierung

■ ISO/IEC 9798	Entity authentication Authentisierung von Instanzen
■ ISO/IEC 9797	Message Authentication Codes (MACs) Nachrichten-Authentisierungscodes (MACs)

PKI-Dienste

■ ISO/IEC 15945	Specification of TTP services to support the application of digital signatures Spezifizierung der Dienste eines vertrauenswürdigen Drittens zur Unterstützung der Anwendung von digitalen Signaturen
■ ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party Services Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

Schlüsselmanagement

■ ISO/IEC 11770	Key management Schlüsselmanagement

Kommunikationsnachweise

■ ISO/IEC 13888	Non-repudiation Nicht-Abstreitbarkeit

Zeitstempeldienste

■ ISO/IEC 18014	Time-stamping services Zeitstempeldienste

A.2 Standards – Überblick nach Institutionen

- **Konsortialstandards**

Bezeichnung	Inhalt	Nachweise
PCI DSS Payment Card Industry Data Security Standard v 1.2	„Der Payment Card Industry Data Security Standard (PCI DSS) stellt ein Sicherheitsrahmenwerk dar und enthält eine umfassende Anforderungsliste an die Kontrollen der Bereiche physikalische und logische Sicherheit. Das Ziel des Standards ist die Verbesserung der Sicherheit von Kreditkartendaten und des Online-Zahlungsverkehrs, sofern dieser über Kreditkartenzahlungen abgewickelt wird.“	„Einzelhändler oder Dienstleister, die **mehr als 1.000.000** Transaktionen pro Jahr ausführen müssen ihre **Netzwerksicherheit** von einem Approved Scanning Vendor (ASV) **prüfen lassen**. Die Experten eines ASV führen einen Schwachstellenscan des Netzwerks durch. Die Einhaltung der **weiteren Anforderungen** des Standards wird durch externe Parteien (sogenannte **Qualified Security Assessor** (QSA)) geprüft und bescheinigt. Zur Aufrechterhaltung des Zertifikats muss der Schwachstellenscan quartalsweise wiederholt und die Erfüllung der weiteren gestellten Anforderungen jährlich durch einen Assessor bescheinigt werden. Unternehmen mit **weniger als 1.000.000** Transaktionen müssen die Anforderungen durch ein **jährliches Selbsttestat** und einen **vierteljährlichen Schwachstellenscan** durch einen ASV bestätigen.“
Richtlinie VDI/VDE2182 Informationssicherheit in der industriellen Automatisierung	„Die Richtlinie beschreibt, wie die Informationssicherheit von Automatisierungsgeräten sowie automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Maßnahmen erreicht werden kann.“	Es ist ein regelmäßiges Audit notwendig.
Cobit Control Objectives for Information and Related Technology	„Die Cobit umfasst eine Sammlung international akzeptierter und allgemein einsetzbarer Kontrollziele“, zum IT-Einsatz von der Planung bis zum Betrieb und Entsorgung“.	Es kann eine Personenzertifizierung erfolgen.

ITIL **Information** Technology Infrastructure Library	„Die Information Technology Infrastructure Library (ITIL) ist ein Best Practice Referenzmodell für IT-Servicemanagement (ITSM) und sieht als solches Sicherheitsaspekte als unverzichtbare Bestandteile eines ordnungsgemäßen IT-Betriebs an. Durch konkrete Empfehlungen für die Gestaltung von Unternehmensprozessen werden die Planung, Erbringung und Optimierung von IT-Serviceleistungen mit Blick auf den Nutzen für die unternehmerischen Ziele unterstützt.“	Es kann die Teilnahme an der ITIL-Schulung zertifiziert werden.

- **BSI-Standards**

Bezeichnung	Inhalt	Nachweise
IT-Grundschutz-Standards	„BSI-Standard **200-1** definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS).“ „Der BSI-Standard **200-2** bildet die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS).“ „Der BSI-Standard **200-3** beinhaltet erstmals gebündelt alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.“	Zertifizierung von Kern- bzw. Standardabsicherung. Die Kernabsicherung betrifft nur den Schutz der wichtigsten Geschäfts- bzw. Fachaufgaben. Es erfolgt eine ISO 27001 Zertifizierung auf Basis von IT-Grundschutz durch einen BSI-zertifizierten Auditor, der die Referenzdokumente überprüft und auch Prüfungen vor Ort vornimmt. Der Auditbericht wird an das BSI weitergeleitet.
Branchenspezifische Standards nach § 8a Abs. 2 BSIG	Erreichung der Vorgaben des § 8a Abs. 1 BSIG für Betreiber kritischer Infrastrukturen erforderlich.	Regelmäßiger Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen notwendig. Das BSI kann Anforderungen an die prüfende Stelle stellen, vgl. § 8a Abs. 5 BSIG.

		BSI muss die Branchenstandards **anerkennen**.
Technische Richtlinien des BSI[1] (Sicherheitsstandards)	„Technische Richtlinien haben originär Empfehlungscharakter. Ihre Verbindlichkeit entsteht erst durch individuelle Vorgabe des Bedarfsträgers." Es existieren z.B. Richtlinien für kryptografische Verfahren, sicherer RFID-Einsatz etc.	Einhaltung der Anforderungen wird durch ein Zertifikat bestätigt. Eine vom BSI anerkannte Prüfstelle übernimmt hierbei die Prüfung.
BSI Mindeststandards für die Sicherheit der Informationstechnik des Bundes nach § 8 Abs. 1 BSIG	Die Standards richten sich an alle Stellen des Bundes. Es gibt zahlreiche verschiedene Standards: - Externe Cloud-Dienste - Externe Cloud-Dienste - Mobile Device Management - Protokollierung und Detektion - Schnittstellenkontrollen - Sichere Web-Browser - SSL/TLS-Protokoll	
BSI Anforderungskatalog C5	„Der Anforderungskatalog fasst aus Sicht des BSI Anforderungen zusammen, die Cloud-Anbieter unabhängig von Anwendungskontext erfüllen sollten, um ein **Mindestmaß an Sicherheit ihrer Cloud-Dienste** gegenüber Ihrer Kunden zu gewährleisten. Beim Anforderungskatalog handelt es sich um einen Prüfstandard. Er beinhaltet daher **nur prüfbare Anforderungen** und schreibt nicht vor, durch welche Maßnahmen diese zu erfüllen sind. Damit unterscheidet sich der Anforderungskatalog grundlegend von anderen Katalogen, wie z. B. den IT-Grundschutz-Katalogen, die konkrete Maßnahmen zur Umsetzung beinhalten."	Testat nach BSI C5 durch zertifizierte Wirtschaftsprüfer

- **DIN EN-Standards**

Bezeichnung	**Inhalt**
DIN 18095 **Rauchschutz**abschlüsse	„Ziel des Standards ist die Etablierung und Aufrechterhaltung eines IT Continuity Managements."

[1] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/Technische_Richtlinien/Technische_Richtlinien_node.html.

DIN EN 1143-1 Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl – Teil1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume	„Zweck von DIN 18095 ist es, die notwendigen Anforderungen an Rauchschutztüren und -abschlüsse zu definieren und Prüfverfahren zur Bestimmung unter anderem der Dichtheit festzulegen.“
DIN EN 60529 **Schutzarten durch Gehäuse** - IP-Code	„Auf Grundlage dieser Europäischen Norm werden freistehende Wertschutzschränke, Einbauschränke (Boden und Wand), Wertschutzschränke für Geldautomaten (ATM-Safes) und ATM-Sockel, Wertschutzraumtüren sowie Wertschutzräume (mit oder ohne Tür) gemäß ihrem Widerstandswert gegen Einbruchdiebstahl geprüft und klassifiziert.“
DIN V ENV 1627 Fenster, Türen, Abschlüsse - **Einbruchhemmung** - Anforderungen und Klassifizierung	Die Norm soll Begriffe und Anforderungen für den Schutz durch Gehäuse von elektrischen Betriebsmitteln vor Gefahren bei menschlichem Kontakt sowie dem Eindringen von festen Gegenständen und Wasser festlegen.

- **ISO/IEC-Standards**

Die meisten internationalen Standards zu diesem Themengebieten stammen vom ISO-Subkomitee 27 „IT-Security Techniques“. Zur Wirkungsweise dieser Standards siehe die allgemeinen Ausführungen.

Bezeichnung	Inhalt	Nachweise
ISO/IEC 27001	„ISO/IEC 27001 legt [in generischer Weise] die Anforderungen für die Errichtung, Einführung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheits-Managementsystems fest.“	Ein Nachweis kann durch eine akkreditierte Stelle vorgenommen werden (z.B. TÜV Süd) und muss regelmäßig wiederholt werden. Die ISO 27001-Zertifizierung auf Basis IT-Grundschutz ist ebenfalls möglich aber umfangreicher (s.o.).
ISO/IEC 15408 (bekannt als „Common Criteria“)	„Die Norm definiert ein Kriterienwerk für die Sicherheitsevaluierung von IT-Produkten und IT-Systemen.“	Die Zertifizierung kann durch Prüfstellen, Zertifizierungsstellen und die nationalen Behörden (BSI) durchgeführt werden.

ISO/IEC 27017 **Code of practice for information security controls based on ISO/IEC 27002 for cloud services**	„Der Standard (…) erweitert ISO/IEC 27002 um eine Reihe von „Good Practices“ für Kunden und Anbieter, die bei einer **sicheren Nutzung bzw. Implementierung von Cloud Diensten** helfen sollen. Zusätzlich enthält der Standard weitere Anforderungen, die speziell das Thema Cloud Computing betreffen. Die Anforderungen behandeln z. B. die besondere Beziehung zwischen Cloud-Nutzern und Cloud-Anbietern, spezielle Anforderungen zum operativen Betrieb von Cloud Diensten, sowie Anforderungen an Zugriffskontrollen in geteilten Umgebungen, an Logging und Monitoring, sowie an das Netzsicherheitsmanagement.“	
ISO/IEC 27018 **Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**	Der Standard „befasst sich mit dem **Schutz personenbezogener Daten im Cloud Computing**. Er lehnt sich stark an den europäischen Datenschutz an, besitzt aber keinen normativen Charakter. Da der Anforderungskatalog sich nicht mit dem Datenschutz befasst, kann ISO/IEC 27018 als sehr hilfreiche Ergänzung zum Datenschutz herangezogen werden.“	
ISO/IEC 10116	Der Standard befasst sich mit der Verschlüsselung von Computern und Netzwerken.	
ISO/IEC 20009	Spezifizierung von anonymen digitalen Signaturen zur „Geheimhaltung der Identität eines Kommunikationspartners bei gleichzeitiger Verifikation seiner Authentizität“.	
ISO/IEC 27002	„Ziel von ISO/IEC 27002 ist es, Informationssicherheit als Gesamtaufgabe darzustellen“ und zu strukturieren. Der Standard umfasst alle „Bereiche der Organisation: Erhebung, Verarbeitung, Speicherung, Löschung von Informationen“.	

ISO/IEC TR 15443	Der technische Bericht 15443 soll eine Hilfestellung bei der Entscheidung geben, nach welchen Kriterien und mit welchen Methoden man die Vertrauenswürdigkeit in die Sicherheit von IT-Produkten, -Systemen oder –Dienstleistungen bewertet.	
ISO/IEC 19772	„Dieses Dokument legt sechs Methoden der authentisierten Verschlüsselung fest, das heißt vorgegebene Wege zur Verarbeitung eines Datenstroms mit den Sicherheitszielen Datenvertraulichkeit, Datenintegrität, Datenursprungsauthentisierung.“	
ISO/IEC 27003	„ISO/IEC 27003:2010 beleuchtet erfolgsrelevante Aspekte beim Design und der Implementierung eines **Informationssicherheits-Managementsystems** (ISMS) nach ISO/IEC 27001:2005. Der Standard beschreibt den Weg zu einer ISMS Spezifikation und gibt Hilfestellung bei der Umsetzung eines ISMS Projekts.“	
ISO/IEC 9796	„Das Ziel der Normenreihe ist die Festlegung von Digitalen Unterschriftsmechanismen, die eine teilweise oder vollständige Wiederherstellung von Nachrichten bei verringertem Speicher- und Übertragungsaufwand ermöglichen.“	
Die ISO/IEC 29134:2017	„Die ISO/IEC 29134:2017 beschreibt detailliert den Ablauf einer **Datenschutzfolgenabschätzung** von der Vorbereitungs- über die Durchführungs- bis hin zur Nachbereitungs- und Report-Phase.“	
ISO/IEC TR 19791	„Der technische Bericht 19791 dient dazu, die Methoden des Standards 15408 auch auf die Evaluierung von in Betrieb befindlichen IT-Systemen inklusive der organisatorischen Sicherheitsmassnahmen anwendbar zu machen.“	

ISO/IEC 14888	„Ziel dieser Normenreihe ist die Festlegung von Mechanismen für **Digitale Signaturen** mit Anhang für Nachrichten beliebiger Länge.“	
ISO/IEC 27007	„ISO/IEC 27007:2017 gibt Hilfestellung speziell bezüglich der **Auditierung eines Informationssicherheits-Managementsystems (ISMS)** und ergänzt damit den Leitfaden ISO 19011 Leitfaden zur Auditierung von Managementsystemen.“	
ISO/IEC 19790 (FIPS 140-2)	„Das Dokument dient der Evaluierung von **Kryptomodulen** und ist daher für Hersteller und Evaluatoren solcher Module interessant […].“ „Die in der Norm detailliert spezifizierten Sicherheitsanforderungen adressieren insgesamt elf Teilbereiche des Designs und der Implementierung derartiger Produkte.“	
ISO/IEC 15946	„ISO/IEC 15946 behandelt auf elliptischen Kurven aufbauende **kryptographische Verfahren** für öffentliche Schlüssel. Diese schließen die Etablierung von Schlüsseln für Systeme geheimer Schlüssel und Mechanismen für Digitale Signaturen mit ein.“	
ISO/IEC 24759	„Der Standard 24759 dient dazu, den Anforderungen des Standards 19790 an kryptographische Module spezifische Testanforderungen zuzuordnen, anhand derer die Erfüllung dieser Anforderungen geprüft werden kann.“	
ISO/IEC 10118	„Der Standard ISO/IEC 10118 beschreibt Aufbau und Anwendung von **Hash-Funktionen**.“	
ISO/IEC 27013	„ISO/IEC 27013:2012 ist ein Leitfaden für Organisationen, die eine integrierte Implementierung von sowohl **ISO/IEC 27001** als auch ISO/IEC 20000-1 anstreben.“	
ISO/IEC 19792	„Der in Erarbeitung befindliche Standard ISO/IEC 19792 dient dazu, grundlegende Aussagen zur	

	Evaluierung **biometrischer Produkte** und Systeme zu machen.“	
ISO/IEC 18031	„Dieses Dokument legt ein konzeptionelles Modell eines Zufallszahlengenerators für kryptographische Zwecke mit seinen Elementen fest.“	
ISO/IEC 27011	„Der textgleich als ITU-T Recommendation X.1051 veröffentlichte internationale Standard ISO/IEC 27011 spezifiziert **ISMS-Leitlinien für Telekommunikationsunternehmen**.“	
ISO/IEC 18032	„Dieses Dokument behandelt die Erzeugung von Primzahlen, wie sie für kryptographische Protokolle und Algorithmen gebraucht werden. Es legt Methoden fest, mit denen Zahlen darauf getestet werden können, ob sie Primzahlen sind, und zeigt die Anwendung dieser Methoden zur Primzahlenerzeugung und -prüfung.“	
ISO/IEC 27019	„Der Standard ISO/IEC 27019 […] stellt Leitlinien für ein **Informationssicherheitsmanagementsystems** (ISMS) für Prozessleitsysteme und Automatisierungstechnik in der Energieversorgungsindustrie vor. Im Fokus des Standards stehen Systeme und Netzwerke zur Steuerung, Regelung und Überwachung von Gewinnung oder Erzeugung, Übertragung, Speicherung und Verteilung von [**kritischer Infrastruktur**:] elektrischer Energie, Gas, Öl und Wärme. Dazu gehören Steuerungs- und Automatisierungssysteme, Schutz- und Sicherheits- sowie Messsysteme inklusive der Kommunikationstechnik. Der Standard fasst diese als Prozessleittechnik zusammen.“	
ISO/IEC 9798	„Die Normenreihe legt informationstechnische **Mechanismen zur Authentisierung** von Instanzen fest. Diese werden zur Bestätigung	

	eingesetzt, dass eine Instanz tatsächlich die ist, die sie vorgibt zu sein. Eine zu authentisierende Instanz beweist ihre Identität, indem sie zeigt, dass sie einen geheimen Authentisierungsschlüssel kennt. Die Mechanismen sind für den technischen Austausch von Informationen zwischen Instanzen und, wo notwendig, mit einem vertrauenswürdigen Dritten (Trusted Third Party, TTP) gedacht.“	
ISO/IEC 29101	„ISO/IEC 29101 bietet ein Rahmenwerk für Datenschutzarchitekturen.“ „[Die Norm] spezifiziert technische Aspekte des Datenschutzes, die bei Informations- und Kommunikationstechnologie bei der Verarbeitung personenbezogener Daten – zu beachten sind, […] listet Komponenten für die Implementierung datenschutzfreundlicher Systeme auf[, etc.].“	
ISO/IEC 9797	„Die Normenreihe legt Algorithmen für Nachrichten-Authentisierungscodes (Message Authentication Code, MAC) das heißt Datenvollständigkeitsmechanismen fest, die eine kurze Zeichenkette (den MAC) als eine komplexe Funktion aus jedem Datenbit und einem geheimen Schlüssel erzeugen.“ „[…] Zweck [solcher Algorithmen] ist die Entdeckung jeder unautorisierten Veränderung der Daten wie Löschen, Einfügen oder Transportieren von Objekten innerhalb der Daten.“	
ISO/IEC 18043	„Ziel des Standards ist es, die Auswahl, Entwicklung und den Betrieb eines IDS [intrusion detection system, Anm.] im Unternehmen zu beschreiben. Im ausführlichen Anhang werden grundlegende Konzepte der Erkennung von Angriffen respektive des Eindringens in Netze und Systeme dargestellt.“	

ISO/IEC 24760	Der Standard behandelt Fragen des Identitätsmanagements	
ISO/IEC 15945	„Dieser Standard definiert technische Dienste für einen vertrauenswürdigen Dritten (Trusted Third Parties – TTP, in der Regel Trust Center), die im Zusammenhang mit digitalen Signaturen notwendig sind. Beispiele solcher Dienste sind Registrierung, Zertifizierung, Schlüsselerzeugung und Gegen-Zertifizierung.“	
ISO/IEC 24762	„Die ISO/IEC 24762 definiert Anforderungen und gute Praktiken an Dienste zur Wiederherstellung (**Disaster recovery services**) von Informations- und Kommunikationstechnologien wie bspw. Notfall-Arbeitsplätze oder Ausweich-Rechenzentren.“	
ISO/IEC 29115	„Die Norm ISO/IEC 29115 bietet ein Rahmenwerk zur **Authentifizierung beliebiger Entitäten**. Insbesondere spezifiziert sie vier Assurance Levels (LoA) für Authentifizierung und die Kriterien und Richtlinien zur Erreichung jedes der vier Niveaus.“	
ISO/IEC TR 14516	„Dieser Leitfaden behandelt Fragen des Managements und der Nutzung eines vertrauenswürdigen Dritten (in der Regel Trust Center) im Rahmen einer Public-Key Infrastruktur (PKI).“ „Das Dokument legt verschiedene Kategorien wie Zeitstempeldienste, Unleugbarkeit, Schlüsselverwaltung, Zertifikatsverwaltung und elektronische Beurkundung fest […].“	
ISO/IEC 27033	„Ziel dieses Standards ist es, **Netzwerksicherheit** mittels verschiedener Richtlinien detailliert für unterschiedliche Zielgruppen in einer Organisation zu adressieren. Dabei werden Sicherheitsaspekte bei Umgang, Wartung und Betrieb von IT-Netzwerken und	

	deren Beziehung, auch Außenverbindungen, betrachtet.“	
ISO/IEC 29191	„Die Norm ISO/IEC 29191 bietet ein Rahmenwerk für das Gebiet der teilweise anonymen, teilweise unverkettbaren **Authentisierung** und beschreibt die einschlägigen Anforderungen. In vielen Fällen wird eine Entität, etwa ein Nutzer, bei einer Authentisierung so umfassend identifiziert, dass diese Entität bei anderen Authentisierungen gegenüber anderen Partnern als dieselbe Entität wiedererkannt werden kann, Diese Verknüpfbarkeit zweier Aktivitäten einer Entität stellt ein erhebliches Risiko für Privatsphäre und Datenschutz dar […].“	
ISO/IEC 11770	„Der Zweck des Schlüsselmanagements ist die Bereitstellung von Verfahren zum Umgang mit **kryptographischem Verschlüsselungsmaterial**, das nach den gültigen Sicherheitsbestimmungen in symmetrischen oder asymmetrischen kryptographischen Algorithmen eingesetzt wird.“	
ISO/IEC 27031	„Ziel des Standards ist die Etablierung und Aufrechterhaltung eines **IT Continuity Managements [=Notfallvorsorge]**. Er beschreibt die einzelnen Aktivitäten, die durchzuführen sind.“	
ISO/IEC 24745	„ISO/IEC 24745 liefert Hinweise zum Schutz **biometrischer Informationen** bezüglich verschiedener Anforderungen nach Vertraulichkeit, Integrität, Erneuerbarkeit und Rückrufbarkeit während der Speicherung und dem Transfer dieser Informationen Zusätzlich enthält ISO/IEC 24745 Anforderungen und Hinweise für das sichere und	

	datenschutzkonforme Verwaltung und Verarbeitung biometrischer Information.“	
ISO/IEC 13888	„Der Zweck von **Nicht-Abstreitbarkeitsdiensten** ist das Erstellen, Sammeln, Erhalten, Verfügbar-machen und Prüfen von **technischen Beweisen** zu geforderten Ereignissen oder Aktionen um Streitfälle über das Auftreten oder Wegbleiben dieser Ereignisse oder Aktionen lösen zu können.“	
ISO/IEC 27005	„Der Standard enthält Leitlinien für ein systematisches und prozessorientiertes **Risikomanagement**, das gegebenenfalls auch die Einhaltung der Anforderungen an das Risikomanagements nach ISO/IEC 27001 unterstützt.“	
ISO/IEC 7064	„Das Dokument zielt auf die Verhinderung **von Fehlern beim Eingeben oder Kopieren von Daten** durch den Einsatz von festgelegten reinen oder hybriden Prüfsummensysteme, die vor allem einfache und doppelte Ersetzungs-, Umstellungs- und Verschiebungsfehler erfassen.“	
ISO/IEC 18014	„In der Normenreihe werden Mechanismen und Protokolle für **vertrauenswürdige Zeitstempel** spezifiziert.“	
ISO/IEC 27014	„Der Standard ISO/IEC 27014 bildet die Schnittstelle zwischen der Organisation, der Geschäftsleitung sowie den Verantwortlichen für die Umsetzung und den Betrieb eines Information Security Management Systems. […] Der Standard beschreibt, wie **Maßnahmen zur Informationssicherheit in der gesamten Organisation** umgesetzt werden sowie IT-Sicherheitsberichte in einem geschäftlichen Kontext zurück an die Geschäftsleitung gelangen.“	

ISO/IEC 18033	„Der Standard ISO/IEC 18033 beschreibt die **Anwendung von Verschlüsselungsalgorithmen**.“	
ISO/IEC 20008	„**Anonyme Signaturen sind digitale Signaturen** mit speziellen Eigenschaften. Bei anonymen digitalen Signaturen kann man zwar die Echtheit einer Signatur überprüfen, jedoch bleibt die Identität des Signaturerzeugers anonym. Eine wichtige Anwendung für anonyme digitale Signaturen sind anonyme Authentifizierungsmechanismen, wie sie etwa in ISO/IEC 20009 spezifiziert sind.“	

A.3 Notfallplan IT-Sicherheit

Der deutschen Wirtschaft ist im Jahr 2022 ein Schaden von rund 203 Milliarden Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage entstanden. Nach dem aktuellen Bericht des Bundesamtes für Sicherheit in der Informationstechnik ist die Bedrohung im Cyber-Raum so hoch wie nie. Im Falle einer Attacke aus dem Internet müssen die Betroffenen unverzüglich handeln.

1 Vorgehen im Notfall

Oft ist das Schadensausmaß eines Datenverlusts davon abhängig, wie schnell und offen Schwierigkeiten kommuniziert werden. Es ist daher sinnvoll, einen unternehmensinternen Notfallplan zu erstellen, der im Fall der Fälle abgearbeitet werden kann. Der Notfallplan sollte mindestens Alarmierungspläne, Meldewege, Wiederanlauf-, Wiederherstellungs- und Geschäftsfortführungspläne, sowie alle wichtigen Informationen und Aufgabenzuordnungen der Mitglieder des Notfallteams enthalten. Es sollte ein Notfallbeauftragter benannt werden, der den Notfallmanagement-Prozess steuert und koordiniert.

1.1 Sachverhaltserfassung und Benachrichtigung der zuständigen Personen

Zunächst muss geprüft werden, ob es sich bei einer Störungsmeldung tatsächlich um einen Notfall handelt.

Können gespeicherte Dateien und Dokumente nicht geöffnet oder wiedergefunden werden, muss der IT-Sicherheitsbeauftragte des Unternehmens kontaktiert werden, ohne selbst Datenrettungsversuche zu unternehmen. Sobald der Beauftragte die Situation analysiert hat, kann er Maßnahmen zur Datenrettung einleiten. Zudem sollten die betroffenen Mitarbeiter informiert werden.

Wenn starke Indizien darauf hinweisen, dass Wirtschaftsspionage vorliegt, müssen schnellstmöglich alle Internetverbindungen der im Netzwerk befindlichen PCs gekappt werden, um einen weiteren Zugriff durch Kriminelle zu verhindern.

1.2 Systemüberprüfung

Bevor versucht wird, verlorene oder beschädigte Dateien zu retten, muss zunächst eine Überprüfung des gesamten Systems durch ein geeignetes und aktuelles Antiviren-Programm durchgeführt werden (vor Neustart des PCs!). Schlägt dieses Alarm und werden Schadprogramme wie Viren oder Trojaner gefunden, muss versucht werden, diese mit Hilfe des Programms zu beseitigen.

Anschließend müssen alle persönlichen und unternehmensinternen Daten auf einem externen Medium gesichert werden, um die aktuellen und virengeprüften Dateien später wieder zurückspielen zu können. Da man nach dem Fund von Schadprogrammen nicht weiß, welcher Schaden am System angerichtet wurde, ist das Einspielen einer kompletten Datensicherung oder eine Neuinstallation des Systems und die Änderung sämtlicher Passwörter für diesen PC zwingend erforderlich. Andernfalls läuft man Gefahr, dass die erkannten Schadprogramme zwar restlos entfernt worden sind, aber zwischenzeitlich das System so verändert haben, dass Dritte nun unbemerkt Zugang zum System erlangen können.

1.3 Einsatz von Datenrettungssoftware

Ist es nicht möglich, die benötigten Dateien über Datensicherungen wieder zu gewinnen, besteht die Option, spezielle Datenrettungs-Software einzusetzen. Hierbei ist zu beachten, dass sowohl kostenlose, als auch kostenpflichtige Software generell nur dann eingesetzt werden darf, wenn sie von einem seriösen Hersteller stammt und den richtigen Funktionsumfang aufweist. Zudem ist eine Datenrettungs-Software nicht für jeden Anwender sinnvoll.

Bei Auswahl und Einsatz der Software sollte ein IT-Fachmann zu Rate gezogen werden, da ein großes Risiko besteht, die Situation der Festplatte durch Softwareeingriffe dieser Art weiter zu verschlimmern, so dass spätere professionelle Datenrettungsversuche durch Dienstleistungsunternehmen nicht weiterhelfen.

Datenrettungsversuche sollten nie auf dem Original-Datenträger, sondern auf einer Kopie der Festplatte durchgeführt werden.

1.4 Einschalten von Spezialisten

In manchen Fällen hilft nur noch die professionelle Hilfe eines seriösen Datenrettungs-Unternehmens. Wichtig ist, vorher unbedingt ein Abbild des auf der Festplatte enthaltenen Inhalts zu erstellen. Auch hierbei helfen die auf Datenrettung spezialisierten Unternehmen.

Zudem sollte die Einschaltung von IT-Forensikern in Betracht gezogen werden, um die eventuelle Geltendmachung von Schadensersatzansprüchen gegen den Angreifer und ggf. den eigenen IT-Sicherheitsdienstleister abzusichern (ohne auf etwaige behördliche Ermittlungen angewiesen zu sein).

2 Fragenkatalog

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Fragenkatalog entwickelt. Die in den zwölf als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung:

- Wurden erste Bewertungen des Vorfalls durchgeführt, um festzustellen, ob es sich um einen Cyber-Angriff oder lediglich um einen technischen Defekt handelt?
- Haben Sie kontinuierlich Ihre Maßnahmen abgestimmt, dokumentiert und an alle relevanten Personen und Verantwortlichen kommuniziert?
- Wurden System-Protokolle, Log-Dateien, Notizen, Fotos von Bildschirminhalten, Datenträger und andere digitale Informationen forensisch gesichert?
- Haben Sie stets die besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus gehabt?
- Wurden betroffene Systeme vom Netzwerk getrennt? Wurden Internetverbindungen zu den betroffenen Systemen getrennt? Wurden alle unautorisierten Zugriffe unterbunden?
- Wurden Backups gestoppt und vor möglichen weiteren Einwirkungen geschützt? Wurden Maßnahmen unternommen, um das gesamte Maß der Ausbreitung festzustellen?
- Wurden alle angegriffenen Systeme identifiziert?
- Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-)Prozessen durch relevante Maßnahmen adressiert und behoben?
- Wurden, nach Abstimmung, die Polizei oder relevante Behörden (Datenschutz, Meldepflichten, etc.) benachrichtigt?
- Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z. B. neue Passwörter, 2FA)?
- Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien fest zustellen?
- Wurden die betroffenen Daten und Systeme wiederhergestellt oder neu aufgebaut?

3 Melde- und Anzeigepflichten

Gegebenenfalls muss kurzfristig reagiert werden mit Blick auf folgende Pflichten und Obliegenheiten:

- Bei Verlust von personenbezogenen Daten können gem. Art 33, 34 DS-GVO datenschutzrechtliche Anzeigepflichten gegenüber der Datenschutzaufsichtsbehörde und den betroffenen Datenberechtigten bestehen.

  Grundsätzlich muss das verantwortliche Unternehmen der Aufsichtsbehörde jede Datenschutz-verletzung unverzüglich und möglichst innerhalb von 72 Stunden melden, nachdem dem Verantwortlichen die Verletzung bekannt wurde. Ausnahmsweise besteht dann keine Pflicht zur Meldung bei der Datenschutzaufsichtsbehörde, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten der von der Datenschutzverletzung betroffenen Personen führt. Hierfür ist aber das verantwortliche Unternehmen beweispflichtig.

  Hat eine Datenschutzverletzung darüber hinaus voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge (z. B. Identitätsdiebstahl, Rufschädigung, materieller oder immaterieller Schaden), muss das

verantwortliche Unternehmen grundsätzlich die hiervon betroffenen Personen ohne unangemessene Verzögerung benachrichtigen. Ausnahmsweise kann von der Benachrichtigung abgesehen werden, wenn das verantwortliche Unternehmen Risiken für die betroffenen Personen durch geeignete technische und organisatorische Schutzmaßnahmen ausgeschlossen hat.

- Gehört das angegriffene Unternehmen zu einer so genannten kritischen Infrastruktur (KRITIS-Unternehmen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden), müssen die folgenden Störungen unverzüglich an das BSI gemeldet werden (BSI – KRITIS-FAQ (bund.de)):

  - Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen geführt haben;
  - erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen führen können.

- Soll für den eingetretenen Schaden Versicherungsschutz in Anspruch genommen werden, obliegt es dem Unternehmen, eine unverzügliche (erste) Schadensanzeige an die Versicherung zu richten.

4 Institutionen und Ansprechpartner

Besteht Bedarf an externer Unterstützung, können Sie sich an nachfolgende Institutionen wenden.

4.1 Bayerisches Landeskriminalamt Zentrale Ansprechstelle Cybercrime (ZAC)

Wenn Sie Opfer eines Cyberangriffs geworden sind, sollten Sie sich zuerst an die Zentrale Ansprechstelle Cybercrime beim Bayerischen LKA wenden. Es wird aber nicht nur dann tätig, wenn es zu Betrugsversuchen oder sogar wirtschaftlichen Schäden gekommen ist, sondern auch im Bereich der Prävention. Es steht daher bayerischen Unternehmen generell als Ansprechpartner für Sicherheits-fragen zur Verfügung. Die ZAC ist verpflichtet, die zur Kenntnis gelangten Informationen vertraulich zu behandeln. Allerdings ist die ZAC als Strafverfolgungsbehörde verpflichtet, bei Verdacht einer Straftat von Amts wegen, somit

auch ohne einer entsprechenden Anzeige des Betroffenen, Ermittlungsmaßnahmen einzuleiten.

Kontakt

Die Zentrale Ansprechstelle Cybercrime erreichen Sie unter
(089) 1212-3300 oder E-Mail: zac@polizei.bayern.de.

Weitergehende Informationen finden Sie unter:
Die Bayerische Polizei - Zentrale Ansprechstelle Cybercrime für die Wirtschaft in Bayern

4.2 Das Cyber-Allianz-Zentrum Bayern (CAZ)

Besteht der Verdacht auf Wirtschaftsspionage, sollten Sie sich zunächst an das Cyber-Allianz-Zentrum Bayern des Bayerischen Landesamtes für Verfassungsschutz (LfV) wenden. Neben Ermittlungen im forensischen Bereich unterstützt auch das CAZ in Bayern ansässige Unternehmen bei der Prävention und Abwehr von elektronischen Angriffen. Alle Anfragen werden absolut vertraulich behandelt.

Im Unterschied zur ZAK ist das Landesamt für Verfassungsschutz nicht an das strafprozessuale Verfolgungsprinzip gebunden und somit nicht verpflichtet, im Falle der Kenntniserlangung von einem strafrechtlich relevanten Sachverhalt Strafverfolgungsbehörden einzuschalten bzw. eine entsprechende Strafanzeige zu erstatten.

Im Schadensfall stehen beim CAZ die drei Säulen „Kommunikation“, „Forensik“ und „Bewertung“ zur Unterstützung des betroffenen Unternehmens bereit:

- Kommunikation nimmt die Meldung des Betroffenen auf, kommuniziert nach innen, gibt ein Feedback der Bewertung an den Betroffenen, führt eine Abschlussbesprechung durch und gibt Handlungsempfehlungen.
- Forensik analysiert den Schadcode.
- Bewertung interpretiert den Angriff im Kontext des aktuellen nachrichtendienstlichen Lagebildes, reichert das Lagebild mit den bereits vorliegenden Parametern an, anonymisiert den Sachverhalt vor Veröffentlichung und gibt gegebenenfalls Warnmeldungen heraus.

Kontakt

Die Erstbewertung des Sachverhalts erfolgt telefonisch. Hierzu hat das CAZ eine Hotline eingerichtet:
Tel.: (089) 31201-222
E-Mail: caz@lfv.bayern.de

Warnmeldungen des CAZ und weitergehende Informationen finden Sie unter:
http://www.verfassungsschutz.bayern.de/spionageabwehr/cyber_allianz_zentrum/index.html

4.3 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Als zusätzliche weitere Behörde steht das BSI als bundesweit tätige, unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit zur Verfügung. Es schützt nicht nur die Netze des Bundes, sondern unterstützt auch gewerbliche und private Anbieter sowie Nutzer von Informationstechnik. Ein besonderes Augenmerk liegt auf dem Schutz Kritischer Infrastrukturen nach dem 2015 verabschiedeten IT-Sicherheitsgesetz, weshalb dem BSI dortige IT-Sicherheitsvorfälle gemeldet werden müssen (s. o. 3.).

Das BSI berät bei der Findung ausgewogener Lösungsstrategien in Fragen der Informationssicherheit, koordiniert Beratungsanfragen und führt grundlegende Ausbildungen in diesem Umfeld durch. Hierzu gehören auch Online-Schulungen.

Die Sicherheitsberatung beim BSI ist zentrale Anlaufstelle für Unternehmen zur Unterstützung bei Fragen zur Informationssicherheit. Zu beachten ist aber, dass das BSI wegen der Melde- und Weitergabefunktion keine Vertraulichkeit hinsichtlich der Vorfälle in Unternehmen zusichern kann.

Cyber-Sicherheitsnetzwerk (CSN)

Seit September 2021 gibt es das beim BSI angesiedelte Cyber-Sicherheitsnetzwerk. Dies ist ein freiwilliger Zusammenschluss von qualifizierten Experten für eine Vorfallbearbeitung, die ihre individuelle Expertise zur Behebung von IT-Sicherheitsvorfällen zur Verfügung stellen. Durch die Übernahme reaktiver Tätigkeiten sollen Vorfälle erkannt und analysiert werden, um das Schadensausmaß zu begrenzen und weitere Schäden abzuwenden. Dabei erfolgt die Unterstützung vorfall- und zielgruppenspezifisch.

Das Cyber-Sicherheitsnetzwerk bildet die zentrale erste Anlaufstelle sowohl für Betroffene als auch für Experten. Die Geschäftsstelle des CSN nimmt die Registrierungen vor und beantwortet alle prozessualen und organisatorischen Fragen.

Kontakt

Die Informationssicherheitsberatung erreichen Sie unter:
Telefon: (0228) 99 9582-333
FAX: (0228) 99 109582-333
E-Mail: Sicherheitsberatung@bsi.bund.de

Weitergehende Informationen finden Sie unter:
BSI – Unternehmen (bund.de)
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

4.3 Bundesamt für Verfassungsschutz (BfV)

Das BfV unterstützt Unternehmen bei der Prävention. Unter dem Stichwort Wirtschaftsschutz sollen deutsche Wirtschaftsunternehmen vor Wirtschaftsspionage, Sabotage und den damit einhergehenden Wettbewerbsnachteilen bewahrt werden. Das BfV steht den deutschen Unternehmen als Ansprechpartner für Sicherheitsfragen zur Verfügung.

Kontakt

Kontakt zum Referat für Wirtschaftsschutz im BfV:
Telefon: (0221) 792-3322
E-Mail: wirtschaftsschutz@bfv.bund.de

Weitergehende Informationen finden Sie unter:
Bundesamt für Verfassungsschutz - Wirtschafts-/ Wissenschaftsschutz

4.5 Allianz für Cyber-Sicherheit (ACS)

Außerhalb des rein behördlichen Bereichs gibt es weitere Anlaufstellen, die Unterstützung im Bereich IT-Sicherheit bieten. Die durch BSI und BITKOM initiierte Allianz für Cyber-Sicherheit hat sich das Ziel gesetzt, die Sicherheit des Standortes Deutschland zu stärken. Dazu stellt die Initiative ein umfang-reiches Informationsangebot mit Empfehlungen für die Wirtschaft und andere professionelle Bedarfsträger bereit. Die ACS bietet neben dem thematisch geordneten Einstieg in die Materie weitergehende Informationen und Angebote. Unter anderem wird ein Cyber-Sicherheitscheck zum Stand der Cyber-Sicherheit im Unternehmen angeboten sowie eine Liste qualifizierter Dienstleister.

Ein weiterer wesentlicher Bestandteil der ACS ist der Erfahrungsaustausch unter den über 5.000 Teilnehmern. Registrierte Teilnehmer erhalten Zugriff auf ein erweitertes Informationsangebot, insbesondere zur Sicherheitslage durch monatliche Lageberichte, Warnmeldungen sowie weitergehenden Hintergrundinformationen. Aufgrund der teilweise vertraulichen Natur dieser Informationen muss die Weitergabe dieser Inhalte restriktiv gehandhabt werden. Die Teilnahme an der Allianz steht grundsätzlich allen Institutionen mit Standort in Deutschland offen. Die Teilnahme ist kostenlos und kann jederzeit beendet werden.

Kontakt

Die Geschäftsstelle Allianz für Cyber-Sicherheit erreichen Sie unter:
Telefon: (0800) 2741000
E-Mail: info@cyber-allianz.de

Weitergehende Informationen finden Sie unter:
ACS – Allianz für Cyber-Sicherheit – ACS (allianz-fuer-cybersicherheit.de)

4.6 Initiative Wirtschaftsschutz

Im April 2016 wurde auf Bundesebene die "Initiative Wirtschaftsschutz" als gemeinsame Einrichtung von Wirtschaft und Staat gestartet. Sie bündelt die jeweilige Expertise und hat sich zum Ziel gesetzt, zentrale Unternehmenswerte für Deutschland und seine Wirtschaft besser zu schützen. Dazu arbeiten mehrere Akteure von Wirtschaft und Staat, koordiniert vom Bundesministerium des Innern, zusammen:

- Bundesverband der Deutschen Industrie (BDI)
- Deutscher Industrie- und Handelskammertag (DIHK)
- Allianz für Sicherheit in der Wirtschaft (ASW Bundesverband)
- Bundesverband der Sicherheitswirtschaft (BDSW)
- Bundesamt für Verfassungsschutz (BfV)
- Bundeskriminalamt (BKA)
- Bundesnachrichtendienst (BND)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die Initiative hat u. a. ein umfassendes Schutzkonzept entwickelt, das Maßnahmen und Projekte für einen verbesserten Wirtschaftsschutz enthält.

Weitere Informationen

Weitergehende Informationen finden Sie unter:
https://www.wirtschaftsschutz.info/DE/Home/home_node.html

Ansprechpartner/Impressum

Dr. Frank Rahmstorf
Grundsatzabteilung Recht

Telefon 089-551 78-230
frank.rahmstorf@vbw-bayern.de

Impressum

Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

Autor

Prof. Dr. Dirk Heckmann
Lehrstuhl für Recht und Sicherheit
der Digitalisierung
Technische Universität München

Telefon 089-907793-301
heckmann@mein-jura.de