fall steht aber nicht einem grundsätzlichen Absicherungsbedürfnis und einer grundsätzlichen Versicherbarkeit auf primärer Ebene entgegen.

In der **Vertragspraxis** decken Versicherer teilweise von vornherein keine Bußgelder. Auch die AVB Cyber sehen einen entsprechenden Risikoausschluss vor (A1-17.11). Einzelne Versicherer bieten Deckung „soweit dies rechtlich zulässig ist".[468] **293**

e) Cyberrisiken als systemisches Risiko und Kumulrisiko. Versicherer unterliegen aufsichtsrechtlichen Anforderungen an eine risikoadäquate Kapitalausstattung, insbes. durch die Solvabilität II-RL (vgl. auch → Rn. 638 ff.). Die risikoadäquate Kapitalausstattung erfordert eine Erfassung und Bewertung der vom Versicherungsunternehmen vertraglich übernommenen Risiken. In diesem Zusammenhang stellt die Versicherung und Rückversicherung von Cyberrisiken mit Blick auf Kumulrisiken[469] eine besondere Herausforderung dar. Schadenszenarien wie WannaCry verdeutlichen das globale Risiko systemischer Auswirkungen von Cyberrisiken. Nicht nur die hochgradige Vernetzung ist problematisch, sondern insbes. auch die systemische Abhängigkeit. Nutzt eine Schadsoftware eine Schwachstelle in einem global genutzten Betriebssystem, sind Zahl und Ausmaß möglicher Einzelschäden unübersehbar. Klassische Methoden der Einschätzung und Steuerung von Massenrisiken (zB bei Naturgefahren) basieren auf statistischen, historischen Daten und der geographischen Begrenzung der Risikosituation. Für Cyberrisiken entwickeln sich Datengrundlagen erst. Cyberrisiken sind zudem nicht geographisch begrenzt. Sie müssen über risikorelevante Parameter erfasst werden, die ein Kumulszenario begünstigen oder erschweren. Dazu gehören etwa die Art der Systeme und Software und die Schutzmechanismen.[470] Um den Anforderungen an den Bilanzschutz und die Bildung angemessener Rückstellungen zu entsprechen, ist die Entwicklung geeigneter Systeme zur strukturierten Erfassung und Steuerung des Kumulrisikos daher eine vordringliche Aufgabe der Versicherungsindustrie. Auf vertragsrechtlicher Ebene bedienen sich Versicherer zur Kumulbegrenzung Regelungen vor allem Risikoausschlüssen (zB A1-17.5 AVB Cyber für den Ausfall von Infrastrukturen sowie erweiterte Kriegsausschlüsse für „Cyberkrieg/cyber war" und „Cyperoperationen/cyber operations")[471] und Maximierungen. **294**

E. Haftpflicht für Informationssicherheitsverletzungen

I. Untersuchungsmaßstab

Dieser Teil soll einen **Überblick zur privatrechtlichen, gesetzlichen Haftpflicht für Informationssicherheitsverletzungen** geben. Gegenstand sind nicht nur vorsätzliches Handeln etwa in Form von Ein- und Angriffen, sondern **295**

[468] Malek/Schütz r+s 2019, 421 (429); Fortmann r+s 2019, 429 (432); Notthoff r+s 2022, 61 (64).

[469] Unter Kumulrisiko versteht man das Risiko eines Versicherers, dass durch den Eintritt ein und desselben zufälligen Ereignisses gleichzeitig bei mehreren oder vielen versicherten Einheiten Schäden ausgelöst werden, vgl. mit Bezug auf die Cyberversicherung Lohmann et al. BaFin-Perspektiven 1/2020, 76 (80 Fn. 3) (abrufbar unter bafin.de unter „Publikationen & Daten"; abgerufen am 25.5.2024).

[470] GDV-Erläuterungen Abschn. 5.5.

[471] Salm in HK-VVG AVB Cyber A.1-17 Rn. 9.

vor allem fahrlässige Pflichtverletzungen. Hierzu zählen etwa ungewollte Schädigungen Dritter durch Versicherungsnehmer bzw. mitversicherte Personen, deren Mitarbeiter, beauftragte (Sub-)Unternehmen und Produkte. Im Fokus stehen dabei mögliche Haftungsszenarien, denen kleine und mittelständische Unternehmen außerhalb kritischer Infrastruktur (Art. 4 Nr. 4, Art. 5 Abs. 2 RL (EU) 2016/1148, § 2 Abs. 10 BSIG iVm BSI-KritisV)[472] ausgesetzt sein können. Es gilt zu beachten, dass die **Zielgruppe der Cyber-Versicherung** nach den Musterbedingungen des GDV vor allem solche Unternehmen sind, deren Geschäftsmodell (überwiegend) die eigene Nutzung von Informations- und Kommunikationssystemen, nicht aber deren Produktion bzw. Dienstleistungen zu diesen vorsieht.[473] Dies schließt allerdings über die bloße Kommunikation hinausgehende haftungsträchtige Rollen wie den Betrieb einer Website, eines Webshops oder eines Mail-Servers, vor allem aber die Implementierung von Netzwerkfunktionalitäten in eigenen Produkten nicht aus. Es geht also um **Unternehmen mit IT, aber nicht um IT-Unternehmen,**[474] wobei die Übergänge fließend sind.[475] In das Cyber-Deckungskonzept können aber auch Versicherungsnehmer aufgenommen werden, die nach der Betriebsbeschreibung Komponenten produzieren oder Dienstleistungen erbringen, die (auch) der IT-Sicherheit dienen.

296 Im Zentrum der Betrachtung stehen **vertragliche und deliktische Ansprüche auf Schadenersatz** vor allem für Vermögensschäden nach deutschem Recht.[476] Ansprüche etwa auf Auskunft, Beseitigung, Widerruf oder Unterlassung sind nicht Gegenstand der Ausführungen.[477] Vertragserfüllung und Gewährleistung werden nur insoweit behandelt, wie sie für Schadenersatzansprüche relevant sind. Es wird auch auf Haftungsrisiken in besonderen Rollen etwa als Plattformbetreiber oder Provider hingewiesen, auch wenn diese für die Versicherungsnehmer der Zielgruppe nach der Betriebsbeschreibung höchstens ein Nebenrisiko darstellen dürften. Bestehen beim Versicherungsnehmer jedoch solche Risiken, werden sich Versicherungsnehmer, Makler und Versicherer insbes. bei Anfragen zur (gesonderten) Eindeckung auch mit entsprechenden Haftungsfragen auseinandersetzen müssen.

297 Als eine Art **Vorfilter bei Internetsachverhalten** sind ggf. Fragen des internationalen Privatrechts[478] und einschlägige Regelungen des TKG für

[472] Näher Voigt IT-SicherheitsR Rn. 243 ff. und nach dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz Kipker/Dittrich MMR 2023, 481. Durch den stärkeren Fokus auf die Zulieferer- und Dienstleisterkette werden die Unternehmen in dieser immer mehr vertraglichen Pflichten ausgesetzt sein, die denen der KRITIS-Betreiber entsprechen.

[473] Vgl. GDV-Erläuterungen Abschn. 1.3.3. Zur Abgrenzung von privater und geschäftsmäßiger Datenverarbeitung Hansen in Hornung/Schallbruch IT-SicherheitsR-HdB § 26 Rn. 18 ff.

[474] Heckmann MMR 2006, 280 (284).

[475] Fallenbeck/Eckert in Vogel/Heuser/Bauernhansl/Hompel, Handbuch Industrie 4.0, Bd. 4, 2020, S. 135.

[476] Vgl. Kosseff, Cybersecurity Law, 2. Aufl. 2019, S. 57 ff. (USA) und S. 385 ff. (weitere Länder); zur Produkthaftung in anderen Staaten Kullmann/Pfister/Stöhr/Spindler Produzentenhaftung Kz. 4500 ff.; Rödl & Partner, Handbuch internationale Produkthaftung, 3. Aufl. 2019, Teil 4.

[477] Vgl. hierzu etwa Damm/Rehbock, Widerruf, Unterlassung und Schadenersatz in den Medien, 3. Aufl. 2008, 3. Teil.

[478] Bestimmung des zuständigen Gerichts und des anwendbaren Rechts, hierzu Hoeren in Hoeren/Bensinger S. 89 ff. Zum anwendbaren Recht insbes. bei etwa Ransomware- und Cloud-Sachverhalten im Überblick Lesser S. 67 ff. mwN.

Telekommunikationsdienste und des TMG/TDDDG zu verschiedenen Provider-Rollen vor der Anwendung spezieller Haftungsregeln zu prüfen.[479] Dies sind der eigene Informationen Bereitstellende (Content-Provider; § 7 Abs. 1 TMG[480]), der Zugangsgewährende zu und Durchleiter von fremden Informationen (Access-Provider; §§ 8, 9 TMG[481]) sowie der fremde Informationen Bereitstellende (Host-Provider; § 10 TMG[482]). Weitere Provider-Rollen können sich nach dem ab dem 17.2.2024 zu beachten Digital Services Act (DSA) ergeben (VO (EU) 2022/2065[483]). Auch Unternehmen, die nicht dezidiert Internetservices anbieten,[484] können eine solche Rolle einnehmen, sei es über die Cloud-Anbindung ihrer Produkte, Angebote an Mitarbeiter oder bei der Bereitstellung an Lieferanten und Partner bei der Zusammenarbeit in Projekten. Es bestehen dann vor allem Schutzpflichten gegenüber dem Nutzerkreis ggf auch nach dem TDDDG, welches unter anderem das Speichern und Lesen (auch) von (nicht-personenbezogenen) Daten auf Endgeräten reguliert.[485] Eine weitere Haftungsquelle sind bereitgestellte oder abgerufene Inhalte, die aber vorliegend nur in einem IT-sicherheitstechnischen Kontext etwa als Gegenstand eines Datenabflusses oder einer ungewollten Änderung oder Löschung von Daten oder der Ausnutzung von Sicherheitslücken betrachtet werden (→ Rn. 310 ff.).[486]

---

[479] Hierzu und zum Folgenden Spindler in Hornung/Schallbruch IT-SicherheitsR-HdB § 12 Rn. 1 ff.; Hoeren in Hoeren/Bensinger S. 19 ff.; Sobola in Auer-Reinsdorff/Conrad IT- und DatenschutzR-HdB § 42 Rn. 73 ff.; Spindler MMR 2018, 48; zur Haftung von Plattformen Wagner GRUR 2020, 329 und GRUR 2020, 447. Zur Entstehung der Haftungsprivilegien für Fremdcontent im US-Recht kritisch Kosseff, The Twenty-Six Words that created the Internet, 2019, S. 3 ff. Zu den Auswirkungen des DSA Spindler MMR 2023, 73.

[480] Beispiel: eigene Homepage. Haftung nach den allgemeinen Regeln. Vertiefend für Website-Betreiber Bensinger/Zentner in Hoeren/Bensinger S. 293 ff.

[481] Beispiel: Betreiber eines Einwahlknotens oder (W)LAN für den Internetzugang. Grds. keine Verantwortung für die allein passiv, automatisiert durchgeleiteten Informationen, ggf. aber Sperr- und Auskunftspflichten (str.), vertiefend Brinkel/Osthaus in Hoeren/Bensinger S. 101 ff. und BVerfG NJW 2019, 755. Zur Störerhaftung der Zugangsprovider BGH GRUR 2018, 3779 (Dead Island); ZUM 2023, 137.

[482] Beispiel: Serverbetreiber, der Dritten Speicherplatz im Netz für deren Inhalte zur Verfügung stellt. Haftung nur bei Kenntnis von rechtswidrigen Inhalten, vertiefend Schwartmann/Polzin in Hoeren/Bensinger S. 353 ff. mwN; für das Haftungssystem der Plattformbetreiber nach der neuen EU-Urheberrechtsrichtlinie RL (EU) 2019/790 vgl. BGH MMR 2022, 947; MMR 2022, 870; Wandtke NJW 2019, 1841 (1845); nach dem NetzDG Sobola in Auer-Reinsdorff/Conrad IT- und DatenschutzR-HdB § 42 Rn. 92 ff.; BGH ZD 2021, 639 mAnm Hoeren/Pinelli.

[483] ausführlich Spindler MMR 2023, 73 (zur Kategorisierung einiger Dienste als Hilfsdienste wie das Content-Delivery-Network als Caching oder Domain Registrare als Access-Provider).

[484] Und damit nicht als Störer in Betracht kommen, vgl. Hoeren/Sieber/Holznagel MMR-HdB Teil 18.2 Rn. 17 ff.

[485] Vgl. insbes. § 25 TDDDG (etwa zur Konkurrenz mit der DS-GVO, Cookies und einer ggf. nötigen Einwilligung, vgl. Hanloser ZD 2021, 399). Zum TTDSG im Überblick Golland NJW 2021, 2238; Piltz CR 2021, 555; Voigt IT-SicherheitsR Rn. 169 ff.

[486] Hierzu ausführlich vor allem bzgl. gewerblicher Schutzrechte Bensinger/Zentner in Hoeren/Bensinger S. 304 ff.; Hoeren in Hoeren/Sieber/Holznagel MMR-HdB Teil 18.2 Rn. 46 ff.; Sobola in Auer-Reinsdorff/Conrad IT- und DatenschutzR-HdB § 42 Rn. 26 ff.

II. Vertragliche Haftung

298 **1. Mangelhafte Hauptleistung. a) IT-Sicherheit als Eigenschaft. IT-Sicherheit** kann **als Eigenschaft eines Produkts,** Werkes oder Mietobjekts bzw. auch Ziel eines Dienstes eine vertragliche Hauptleistung sein. Abseits bereits erfolgter Volldigitalisierung nimmt die Verzahnung des Digitalen mit dem Analogen durch eine Art Schleppnetzeffekt[487] weiter zu. Dabei haben vor allem die **Netzwerk- und Datenaustauschfunktionalitäten sowie Schnittstellen und deren Absicherung** Gewicht, wobei es nicht darauf ankommt, wie die Daten ausgetauscht werden.[488] Über die bloße Netzanbindung hinaus kommt es vor allem auf die bereitgestellten Dienste und deren Funktionalitäten an. Selbst etwa Küchengeräte, Beleuchtungsmittel und Handwerkzeuge sind heute in der Lage Daten zu erfassen, zu speichern und auszutauschen. Das Internet der Dinge breitet sich aus, was ein stetiges Zurückdrängen der Offline-Sphäre und eine zunehmende Kontrolle des Digitalen über das Analoge bedeutet.[489] Zugespitzt: Es vernetzt sich alles mit allem. Resultierend steigen die Gefahren sowohl für die digitale wie auch analoge Funktionsfähigkeit und das Bedürfnis nach IT-Sicherheit. Insbesondere Funktionen als Server tragen ein besonderes Missbrauchs- und Fehlfunktionsrisiko samt drohendem Dominoeffekt in sich. So können die Produkte etwa Bestandteil eines Bot-Netzes werden oder zu schützende Daten pflichtwidrig unverschlüsselt Nichtberechtigten zugänglich machen. Zwar sind die Netzwerkfähigkeiten häufig nützliches, aber nicht notwendiges Feature, ohne dass das Produkt trotzdem funktionieren würde.[490] Gerade das Marketing bewirbt aber digitale und internetbasierende Ausstattungsmerkmale auch, um Modernität zu betonen. Käufer nehmen die Vorlage der Werbung auf und empfinden den (vermeintlichen) Gewinn an Komfort oder Bedienungsfreundlichkeit als wichtig. Da die Funktionalitäten häufig in Firmware, dem Betriebssystem des Geräts und Apps integriert sind, stellen sie kein eigenständiges Produkt dar und werden immer mehr zu einer (subjektiv) essenziellen, aber schwer abgrenzbaren funktionalen Komponente.[491] Dabei defi-

[487] Faktischer Zwang zur Digitalisierung allein, weil vorausgehende oder aufbauende Prozesse digitalisiert worden sind.

[488] Einbindung und Datenaustausch über LAN, WLAN, Mobilfunk, Bluetooth oder Datenträger etc.

[489] Zur Risikoentstehung reicht die Verbindung mit anderen IoT-Geräten. Die Schnittstelle (LAN, WLAN, Bluetooth etc) ist dabei unerheblich. Die Verbindung aus oder in das Internet wirkt risikoerhöhend, eröffnet sie doch einen Angriffsweg durch Unbekannte, der sonst nur über das Eindringen ins interne Netz erreicht werden könnte; NISTIR 8228, Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, vom 25 6.2019, S. 3 ff. (abrufbar unter nist.gov; abgerufen am 17.11.2023).

[490] Häufig wird jedoch bei der Erstinbetriebnahme eine (Zwangs-)Registrierung beim Hersteller oder einem Dienstleister sowie die Zulassung der Erhebung von Telemetriedaten im laufenden Betrieb verlangt, ohne die das Produkt gar nicht oder nur eingeschränkt funktioniert. Gründe etwa: Verhinderung von Produktpiraterie; Erschwerung/Verhinderung des Weiterverkaufs; Erhebung von Daten zur Produkt- und Kundenbetreuung; Kundenbindung; Anomalieerkennung zum Schutz etwa vor der Kaperung für Botnetze; Updateverteilung; Support/Feedback-Anbindung; Werbeplatzierung; (Meta-)Datengewinnung zur Produktentwicklung oder zum Verkauf; Personalisierung; Verknüpfung mit Datenbeständen und Cloud-Diensten sowie Steuerung über andere Geräte bzw. Cloud-Dienste; Anbieten von (kostenpflichtigen) Zusatzdiensten; Kontrolle und Abschaltmöglichkeiten.

[491] Wenigstens gegenüber dem Endkunden ist bei ganzheitlicher Betrachtung im Zweifel auch keine Differenzierung angezeigt, vgl. Erwgr. 14 f. RL (EU) 2019/771.

niert Software (dynamisch) die Funktionen der Hardware. Da sich die Funktionalität aus dem Zusammenspiel einer Vielzahl von Hard- und Software-Elementen im und außerhalb des Produkts ergibt, handelt es sich auch bei der IT-Sicherheit um eine häufig nicht greifbare **virtuelle Eigenschaft.**

299 Produkte, die etwa der Verschlüsselung, dem Blockieren oder Filtern von Datenübertragungen dienen, versprechen meist eigene Sicherheit gepaart mit einer Steigerung der Sicherheit anderer Systeme. Fehlt eine von beiden, liegt ein Mangel vor. In der IT-Branche werden beispielsweise **typengemischte Verträge** für die Her- und Bereitstellung, den Betrieb, die Nutzung, Wartung und Pflege von IT-Infrastruktur (Hard- und Software,[492] aber auch (Cloud-)Services) abgeschlossen.[493] Es ist zu berücksichtigen, dass der Trend dahin geht im Kern **Gebrauchsvorteile und Nutzungsmöglichkeiten** (entgeltlich) einzuräumen, auch wenn vordergründig eine Sache verkauft wird.[494] Gerade IoT-Geräte sind häufige Hybride von Hard- und Software (zB Steuerung über Apps) mit Service-Elementen (zB Anbindung an Cloud-Dienste), die Unternehmen nach dem Kauf gerne als **Dauerschuldverhältnis etwa in Form eines Abonnements** am Markt platzieren, um kontinuierliche Einnahmen zu generieren.[495] Die Konturen von Kauf-, Werk-, Dienst-, Miet-, Pacht-, Leasing- oder Schenkungsvertrag verschwimmen dabei immer mehr (vgl. §§ 437 Nr. 3, 634 Nr. 4 BGB jeweils mit Verweis auf § 280 Abs. 1 BGB als allgemeiner Anspruchsgrundlage des Rechts der Schuldverhältnisse[496]). Prägend bleibt gerade bei Geschäften mit haptisch-fassbaren IoT-Produkten[497] das Kaufrecht. Der Kunde erwirbt regelmäßig vom Händler.[498] Einzig mit dem Verkäufer hat er eine vertragliche Beziehung,[499] auch wenn etwa hersteller- oder zuliefererseitige Clouddienste bei deren Nutzung Raum für Kontrakte mit den vorgelagerten Gliedern der Lieferkette eröffnen. Als **Regelfall** wird im Weiteren, wo nicht anders vermerkt, von einem **Kaufvertrag mit einem Händler** ausgegangen, der nicht gleichzeitig Hersteller des schadensstiftenden Produkts ist.[500]

---

[492] Zu den Begrifflichkeiten im juristischen Kontext Marly SoftwareR-HdB Rn. 1 ff.

[493] Vgl. Missling in Weitnauer/Mueller-Stöfen, Beck'sches Formularbuch IT-Recht, 5. Aufl. 2020, H. 7.

[494] Die Hardware fungiert dabei als Ermöglicher („Enabler") für den Zugriff auf Funktionen, die für die Dauer der Unterstützung durch den Hersteller mietähnlich genutzt werden. Ohne diese Funktionen ist die Hardware eine weitestgehend wertlose Hülle.

[495] Bräutigam in Bräutigam/Kraul, Internet of Things, 2021, S. 2 ff.; NIST Cybersecurity White Paper, Internet of Things (IoT) Trust Concerns, Stand 17.10.2018, S. 17 (abrufbar unter nist.gov; abgerufen am 24.7.2024).

[496] Hierzu Kaiser in Staudinger, Eckpfeiler des Zivilrechts, 6. Aufl. 2018, I. Rn. 152 ff. Die Trennschärfe zwischen den Vertragstypen nimmt bei zunehmender Komplexität, kurzfristigen Änderungsbedürfnissen, kürzeren Entwicklungszyklen und Projektorientierung in Mikroschritten immer weiter ab, vgl. etwa Schneider/Conrad in Auer-Reinsdorff/Conrad IT- und DatenschutzR-HdB § 10 Rn. 24 ff.; Marly SoftwareR-HdB Rn. 1202 ff. Vgl. für die Abgrenzung im IT-Vertragsrecht zwischen Werkvertrags- und Kaufrecht BGH NJW 2021, 53; NJW 2021, 1532 und die Anm. von Hoeren MMR 2021, 42.

[497] In Abgrenzung zu (reinen) Software-Produkten, vgl. Marly SoftwareR-HdB Rn. 1 ff.

[498] Gegebenenfalls auch vom Hersteller direkt, der dann eine Doppelrolle inne hat.

[499] Ausnahmen sind hier nicht weiter beleuchtete Garantievereinbarungen oder gesonderte Verträge zB für den Zugang zu Ressourcen (Rezepte, Medien, virtuelle Produktindividualisierungen etc).

[500] Zur (meist fehlenden) Haftung des bloßen Softwarelieferanten Röttgen ITRB 2017, 191.

300 **b) Fehlende IT-Sicherheit und Datenschutzkonformität als Mangel. aa) Abweichen von Beschaffenheitsvereinbarungen der Parteien. (1) Abweichung vom Soll.** Ein Mangel stellt eine **Abweichung des Ist- vom vertraglichen Soll-Zustand** dar.[501] Konkrete gesetzliche IT-Sicherheitsvorgaben für Produkte sind (noch) selten[502] und bei produktspezifischer bzw. sektoraler Regulierung zu finden.[503] Es kommt also im Übrigen auf die **Vereinbarungen der Vertragsparteien** an.[504] Öffentliche Äußerungen etwa in Dokumentation,[505] Katalogen, Werbematerialien[506] oder durch Kennzeichnung, auch wenn sie bekannt, zurechenbar oder unwidersprochen durch Dritte erfolgen, können den Soll-Zustand verbindlich definieren und konkretisieren.[507] Wirbt ein Online-Händler mit Garantiezusagen des Herstellers, muss umfassend über den Inhalt informiert werden.[508] Bei entsprechenden Äußerungen kommt es etwa auf die Definition und Benennung von **Schutzzielen** und des gewählten **Schutzniveaus** an.[509] In negativer Abgrenzung sind auch entsprechend kommunizierte und erst recht vereinbarte Verwendungseinschränkungen oder -ausschlüsse zu beachten.[510] Außer bei Soft- und Hardware, die dezidiert der Verbesserung der IT-Sicherheit dienen soll, oder in sicherheitssensiblen Branchen/Produktkategorien sind hinreichend **konkrete Festlegungen bzw. Zusicherungen von Sicherheitseigenschaften bzw. sicherer Funktionalitäten**

[501] Zum Folgenden vgl. Beckmann in Staudinger, Eckpfeiler des Zivilrechts, 6. Aufl. 2018, N Rn. 37 ff.

[502] Vgl. für besondere Kategorien von Funkanlagen ab 1.8.2024 Art. 3 Abs. 3 S. 1 lit. d–f RL (EU) 2014/53; VO (EU) 2022/30 (Beachtung technischer Standards wie ETSI/EN 303645 zur Konformität für das CE-Kennzeichen) dazu Dickmann ICLR 4 (2023), 21; und für Kalifornien Senate Bill 327 Information privacy: connected devices (abrufbar unter leginfo.legislature.ca.gov; abgerufen am 17.11.2023), in dem für IoT-Geräte vom Hersteller etwa die Vergabe von individuellen Passwörtern gefordert wird, vgl. auch Ritter MMR 2019, 3; zu Tendenzen etwa in China zumindest die Prüffähigkeit von Netzwerkprodukten im KRITIS-Sektor vorzuschreiben Kipker/Müller DSRITB 2018, 713.

[503] Produktspezifisch im Überblick Lenz, Produkthaftung, 2. Aufl. 2022, § 9 (allerdings beginnt sich der Fokus erst auf IT-Sicherheit als Faktor zu richten) und sektoral indirekt über Anforderungen der von Verpflichteten verwendeten Produkte/Dienstleistungen, ausführlich Hornung/Schallbruch IT-SicherheitsR-HdB § 21 ff.; Voigt IT-SicherheitsR S. 107 ff.; Kipker Cybersecurity-HdB Kap. 12.

[504] Zu Qualitätskriterien, Kundenerwartungen und Bewertung von Softwareprodukten vgl. etwa die Normenreihe ISO/IEC 250xx, Hoffmann, Software-Qualität, 2. Aufl. 2013, S. 9 f. und zu Modellen für die Einarbeitung, Messung und Prüfung von Sicherheit in Software Paulus, Basiswissen Sichere Software, 2011, S. 54 ff. sowie zur Erhebung und Formulierung von Sicherheitsanforderungen, S. 69 ff. Vgl. aus technischer Sicht zudem die vertraglich zu adressierenden möglichen Schwachstellen bei Rasner, Cybersecurity & Third-Party Risk, 2021, S. 339 ff.

[505] Etwa zur Sicherheitsarchitektur von Software und (vermeintlich) beachteten Design-Prinzipien, vgl. Paulus, Basiswissen Sichere Software, 2011, S. 127 ff.

[506] Vgl. OLG Hamburg BeckRS 2008, 1414; MMR 2003, 340.

[507] Dazu im Einzelnen Westermann in MüKoBGB BGB § 434 Rn. 27 ff.; Graf v. Westphalen in Foerste/Graf v. Westphalen ProdHaft-HdB § 1 Rn. 69 ff.

[508] EuGH NJW 2022, 1871 (UWG-Sache) mAnm Thalhofer/Purucker NJW 2022, 1851.

[509] Verfügbarkeit, Authentizität, Integrität, Zuverlässigkeit, Verbindlichkeit und Vertraulichkeit. Vgl. zum technischen Hintergrund und Definitionen → Rn. 4.

[510] Etwa generell für den Fahrzeugbau.

(noch) eher selten.[511] Zudem ist regelmäßig (insbes. bei nicht zugänglichem Quellcode) nicht nachweisbar, dass Software bestimmte Funktionen, aber auch Fehler nicht hat.[512] Bei einem entsprechenden negativen Interesse des Käufers hat dieser beweistechnisch einen schweren Stand.[513]

Neben der Funktionstüchtigkeit und Nutzungsmöglichkeit kommt es (auch) **301**
auf die **Sicherheit des Produkts im laufenden Betrieb** an. Haftungsseitig ist eingangs zu fragen, welche vertraglichen Leistungen konkret zu erbringen sind und wie die Risikosphären der Vertragsparteien (sowie ggf. auch zu Dritten) definiert und abgegrenzt werden.[514] Bei unklaren Vereinbarungen bestehen ggf. Hinweis-, Nachfrage- und Aufklärungspflichten.[515] Auch an (wirksame) haftungsausschließende und -begrenzende Regelungen[516] wie etwa eine Beschränkung auf den Auftragswert, Jahresmaximierungen, eine generelle Deckelung bei korrespondierender Versicherungspflicht und ein Ausschluss für entgangenen Gewinn als Schaden ist zu denken. Die Verletzung relevanter vertraglicher Pflichten und Obliegenheiten kann anspruchsmindernd oder -ausschließend wirken.[517] Pauschalisierte Schadenersatzpositionen[518] können bei Nachweis der Haftung dem Grunde nach die Abwicklung zur Höhe vereinfachen, andererseits aber insbes. ohne einen Mindestschadennachweis, Transparenz in der Berechnung, Angemessenheit und dem Recht, einen geringeren Schaden nachzuweisen, gar Vertragsstrafencharakter entwickeln. Dann entsprechen sie nicht mehr der gesetzlichen Haftung. Dies gilt ebenso für die Verlängerung von Gewährleistungs- und Verjährungsfristen. Bezüglich der Einbeziehung und Wirksamkeit entsprechender Klauseln ist insbes. das AGB-Recht nach §§ 305 ff. BGB zu beachten.[519] Schließlich

[511] Die Software-Industrie bleibt daher bei vielen Sicherheits-Features ihrer Produkte (insbes. bei Standard-Titeln) zB bewusst unkonkret, stellt die Ausgestaltung von Funktionalitäten einseitig zur jederzeitigen eigenen Disposition und Verweist auf das beim Betreiber/Nutzer liegende Interaktionsrisiko mit anderer Hard-/Software. Vgl. Kohnfelder, Designing Secure Software, 2022, S. 7.

[512] Die Übergänge vom Feature zum Bug sind fließend. So können etwa unzureichend abgesicherte und nicht dokumentierte Fernwartungsfunktionen bei Entdeckung durch Dritte zu einer Schwachstelle werden.

[513] Vgl. Lesser S. 99 ff. Ggf. modifizierbar durch Darlegungs- und Beweislastregelungen, denn trotz bekannt schlechter Softwarequalität im Allgemeinen besteht nach Gesetz und Rechtsprechung bislang keine anfängliche Vermutung dahingehend, dass ein (kausaler) Fehler im Quellcode vorliegt.

[514] Vgl. die Fallgruppenübersicht bei Voigt IT-SicherheitsR Rn. 615 f. Zur Bestimmbarkeit in AGB Pour Rafsendjani/Bomhard in Hornung/Schallbruch IT-SicherheitsR-HdB § 9 Rn. 32 ff.

[515] Vgl. für IT-Verträge mit dem Bund Nr. 7.1 EVB-IT Dienstleistungs-AGB, Version 2.1 vom 1.4.2018 (abrufbar unter cio.bund.de; abgerufen am 17.11.2023); hierzu Bischof/Intveen ITRB 2017, 119; auch vorvertraglich vgl. Hoeren/Pinelli, IT-Vertragsrecht, 3. Aufl. 2022, S. 154 ff.

[516] Zu den AGB-rechtlichen Implikationen Hoeren/Pinelli, IT-Vertragsrecht, 3. Aufl. 2022, S. 161 ff.

[517] Etwa die Erstellung von Backups sowie die richtige und vollständige Dokumentation der eigenen Systeme samt rechtzeitiger Übergabe an den Vertragspartner.

[518] Vgl. zur AGB-rechtlichen Wirksamkeit Hoeren/Pinelli, IT-Vertragsrecht, 3. Aufl. 2022, S. 186 ff.

[519] Hierzu ausführlich Thüsing in von Westphalen/Thüsing, Vertragsrecht und AGB-Klauselwerke, 48. EL März 2022, Schadenspauschalierungsklauseln Rn. 1 ff.; Habersack in Ulmer/Brandner/Hensen, AGB-Recht, 13. Aufl. 2022, BGB § 305 Rn. 101 ff.

muss von Anspruchstellerseite zuerst bewiesen werden, dass eine konkrete Pflichtverletzung auch kausal zum Schaden geführt hat. Dies kann gerade bei Fällen, in denen weder Täter noch Angriffsweg und Schadensumfang (vollständig) identifiziert und nachgewiesen sind, schwierig sein.

302 Bei Verletzung vertraglicher Hauptpflichten besteht in der Leistungsphase das **Primat der Nacherfüllung.** Können der resultierende Mangel und dessen Unwert durch Nachbesserung oder Nachlieferung ausgeräumt werden, ist dem Verkäufer hierzu (unter Fristsetzung) grundsätzlich Gelegenheit zu geben.[520] Bei **Unmöglichkeit**[521] der Leistungserbringung bzw. Nacherfüllung sowie bei **Unzumutbarkeit** für den Vertragspartner wandeln sich die Leistungsansprüche spätestens nach entsprechender Einrede in **Sekundäransprüche.**[522] Die im vorliegenden Zusammenhang relevanten **Begleit- und Folgeschäden** an anderen Rechtsgütern als dem Produkt bzw. Leistungsgegenstand unterliegen dem Vorrang nicht.

303 **(2) Datenschutzverstöße.** Gerade mit Blick auf die verschärfte Haftung nach der DS-GVO[523] kann die **Einhaltung von Vorgaben des Datenschutzes** (und damit indirekt die IT-Sicherheit der eigenen Systeme; vgl. Art. 32 DS-GVO) zu einer Hauptleistungspflicht erhoben werden.[524] Augenscheinlich eine Hauptpflicht ist die Einhaltung von Datenschutzrecht bei der Auftragsdatenverarbeitung (vgl. Art. 28 DS-GVO) oder bei der Bereitstellung von Testdatensätzen.[525] Dies gilt ebenso, wenn die Gewährleistung der datenschutzkonformen Nutzbarkeit eine wesentliche Eigenschaft darstellt.[526] Zwar verpflichtet Art. 25 DS-GVO nur den Verantwortlichen und nicht den Hersteller von Hard- und Software.[527] Die Pflichten zu datenschutzfreundlicher Technikgestaltung und Voreinstellungen[528] haben aber indirekt Auswirkungen auf die Herstellung und Beschaffung von Hard- und Software bis hin zur (selektiven) Löschbarkeit von Inhalts- und Metadaten (vgl. Art. 17 DS-GVO), auch wenn sich kein technisches Lastenheft des Verordnungsgebers findet.[529] Es besteht jedoch nicht zwangsläufig ein Automatismus hin zur Pflicht einer datenschutzkonformen Gestaltung von Produkten, die nicht an Endnutzer (Verbraucher) vertrieben werden, sondern es bedarf diesbezüglicher ver-

[520] Vgl. zur Ersatzlieferung eines Nachfolgemodells im Verbrauchsgüterkauf BGH NJW 2021, 2958; BeckRS 2021, 23312; BeckRS 2021, 23330 und die kritische Anm. von Jaensch jM 1/2022, 18. Für Digitalprodukte vgl. aber § 327e Abs. 5 BGB.

[521] Vgl. hierzu Pour Rafsendjani/Bomhard in Hornung/Schallbruch IT-SicherheitsR-HdB § 9 Rn. 11 ff. und zur Einrede höherer Gewalt Rn. 19 ff.

[522] Zum Komplex und der Einordnung von Schadenersatz statt und neben der Leistung Graf v. Westphalen in Foerste/Graf v. Westphalen ProdHaft-HdB § 9 Rn. 1 ff.

[523] Im Überblick Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 8 Rn. 1 ff.; zur zivilrechtlichen Haftung im Detail Dickmann r+s 2018, 345.

[524] Vgl. Dümeland K&R 2019, 22.

[525] Franz/Tremmel/Kruse, Basiswissen Testdatenmanagement, 2018, S. 27 ff. und 52 ff. (etwa – unberechtigte – Bereitstellung personenbezogener Daten in nicht anonymisierter Form oder von zu schützenden Produktivdaten samt Datenabfluss).

[526] Dazu näher Schuster/Hunzinger CR 2017, 141 und im Rahmen des § 327e BGB Schneider ZD 2021, 485.

[527] Hartung in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 12 f. Zum Begriff EuGH BeckRS 2023, 34702.

[528] Privacy by Design (Art. 25 Abs. 1 DS-GVO) und Privacy by Default (Art. 25 Abs. 2 DS-GVO).

[529] Hartung in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 8.