2. Produktsicherheit und IT-Sicherheit – Haftung für Schäden durch Cyber-Angriffe

Ein sensibler Punkt bei der außervertraglichen Haftung im Zusammenhang mit IoT und Industrie 4.0 ist das Einwirken von Dritten in Form eines **Cyber-Angriffs.** Einige der jüngsten Digital-Rechtsakte des EU-Gesetzgebers adressieren einzelne Aspekte der Verantwortung für solche Angriffe. Durch das verstärkte Ineinandergreifen von öffentlich-rechtlichen Anforderungen und zivilrechtlicher Haftung werden einige Szenarien zukünftig durch spezielle Vorschriften abgedeckt sein. Für Produkte, die vor dem jeweiligen Inkrafttreten der Rechtsakte in Verkehr gebracht werden, gilt allerdings die aktuelle Rechtlage. Daher soll in einem ersten Schritt die Diskussion innerhalb des aktuellen Rechtsrahmens dargestellt werden (a), bevor der Regelungsgehalt neuerer Vorschriften analysiert wird (b). **73**

a) Aktueller Rechtsrahmen

ZT wird in der juristischen Literatur der Cyber-Angriff ohne Zögern als eine der **neuen Gefahren** der digitalen Produktwelt genannt, gemeinsam mit anfänglichen Programmierfehlern, die insbesondere bei komplexer Software nicht vermeidbar seien.[92] Auch in der dogmatischen Betrachtung werden IT-Sicherheitslücken vielfach ohne weitere Begründung rechtlich als **Produktfehler** klassifiziert.[93] Diese Betrachtung greift aber deutlich zu kurz. Es ist vielmehr eine genaue Differenzierung erforderlich, die ua sehr sorgfältig herausarbeitet, durch welche schädigende Handlung ein Rechtsgut verletzt wurde[94]. Nach den Grundsätzen der Produkthaftung kommt eine Verantwortlichkeit des Herstellers für Cyber-Attacken auf seine vernetzten Produkte nur in Ausnahmefällen in Betracht: **74**

Zunächst ist festzuhalten, dass die Frage der IT-Sicherheit als Produktfehler kein grundsätzliches Thema von IoT Anwendungen ist. Vielmehr entsteht dieses Problem **ausschließlich bei vernetzten Produkten,** ganz unabhängig davon, ob sie automatisch, smart oder autonom sind. **75**

Grundsätzlich **endet die Verantwortlichkeit des Herstellers** dort, wo ein Dritter vorsätzlich und rechtswidrig missbräuchlich eingreift und es dadurch zum Schaden kommt.[95] Eine Ausnahme besteht nur, wenn der Benutzer berechtigterweise erwarten durfte, dass das Produkt gegen derartige Eingriffe gesichert ist. Wenn zusätzlich der Hersteller die Sicherheitslücke nach dem Stand von Wissenschaft und Technik hätte voraussehen müssen, kann er selbst ggf. in die Verantwortung genommen werden.[96] Hinsichtlich der Allgegenwärtigkeit von nicht zielgerichtet gesteuerten Computerviren, -würmern und Trojanern ist daher eine **intensive Beobachtung** der Weiterentwicklung solcher Schadsoftware durch den Hersteller vernetzter Produkte unerlässlich.[97] Diese Pflicht bezieht sich aber ausschließlich auf den Zeitpunkt des Inverkehrbringens. Davon nicht automatisch erfasst ist eine Pflicht zur Nachmarkt-Beobachtung im Hinblick auf neu entwickelte Cyber-Angriffe. **76**

Vor allem im Zusammenhang mit Industrie 4.0 ist IT-Sicherheit von besonderer Bedeutung. Nach einer Untersuchung des BSI aus dem Jahr 2014 ist schon jetzt die größte Bedrohung für Anlagenbetreiber die Infektion mit Schadsoftware über das Internet und Intranet.[98] Eine Legaldefinition des Begriffs IT-Sicherheit findet sich in § 2 Abs. 2 BSIG. Demnach bedeutet Sicherheit in der Informationstechnik die Einhaltung bestimmter **77**

[92] Schmid CR 2019, 141 (145); Wiebe NJW 2019, 625.
[93] Vgl. zB Oechsler NJW 2022, 2713 (2716).
[94] AA offenbar Schmid CR 2019, 141 (146).
[95] Grüneberg/Sprau ProdHaftG § 2 Rn. 1.
[96] Insofern zu pauschal Droste CCZ 2015, 105 (107); vgl. Spindler NJW 2004, 3145 (3146); grundlegend zur Haftung für die Wirkungslosigkeit von Sicherungsmitteln siehe BGH Urt. v. 17.3.1981 – VI ZR 191/79, BGHZ 80, 186 – Derosal und BGH Urt. v. 17.3.1981 – VI ZR 286/78, BGHZ 80, 199 – Benomyl; BGH Urt. v. 19.12.1989 – VI ZR 182/89, NJW 1990, 1236 (1237) zur Pflicht des Eigentümers und Vermieters eines Mehrfamilienhauses, Abdeckroste eines Lichtschachtes gegen unbefugtes Abheben zu sichern, wenn der Schacht sich über die volle Breite des Hauseingangs erstreckt.
[97] Ebenso Droste CCZ 2015, 105 (108); Spindler NJW 2004, 3145 (3147).
[98] BSI, Industrial Control Systems Security, 2014, S. 2; Rockstroh/Kunkel MMR 2017, 77 (78).

Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. Für die erforderliche Sabotagefestigkeit – also Resilienz – von Produkten sind vor allem die Verfügbarkeit und Unversehrtheit der Systeme von Bedeutung.[99] Dabei gilt durchweg ein relativer Sicherheitsmaßstab.[100] Die Anforderungen wachsen mit der Bedeutung des Systems für Wirtschaft und Versorgung. Das BSIG definiert auch den Begriff „Schwachstelle", der mit dem Begriff „Sicherheitslücke" wohl in etwa gleichgesetzt werden kann.

78 Allerdings ist nicht jede Sicherheitslücke in diesem Sinne zugleich ein produkthaftungsrechtlich relevanter Produktfehler. Vielmehr muss zunächst das Sicherheitsproblem der IT zum Sicherheitsproblem („Gefahr") für eines der in § 823 Abs. 1 BGB und § 1 ProdHaftG genannten Rechtsgüter werden.[101]

79 Schließlich ist auch genau zu trennen zwischen einer IT-Sicherheitslücke, die bereits **beim Inverkehrbringen** des Produktes bestand und ggf. – je nach aktuellem Stand von Wissenschaft und Technik – einen Konstruktionsfehler darstellen kann, und einer IT-Sicherheitslücke, die erst nach Inverkehrbringen des Produktes auftaucht, uU weil Hacker neue Möglichkeiten gefunden haben, Sicherungsfunktionen zu umgehen.[102]

80 **aa) Grundsätze zur Produkt-/Produzentenhaftung beim Dazwischentreten der Handlung eines Dritten.** Der Hersteller eines Produktes kann jedenfalls nicht für jeden Angriff eines Dritten auf sein Produkt zur Verantwortung gezogen werden. Die aktive, sicherheitsrelevante Veränderung eines Produktes unterbricht vielmehr grundsätzlich die für den Schadensersatzanspruch notwendige **Kausalität** zwischen Produktfehler und Rechtsgutsverletzung. Gleichzeitig bildet auch der bewusste Missbrauch eines Produktes – also zB die Manipulation eines Roboterarms dahingehend, dass er Menschen verletzt – die Grenze der Produkthaftung des Herstellers.[103]

81 Andererseits kennt die allgemeine Dogmatik der Verkehrssicherungspflichten in anderen Bereichen des Deliktsrechts durchaus die Pflicht zur Vornahme von **Sicherungsmaßnahmen,** die ein naheliegendes Fehlverhalten anderer Personen verhindern, das im Zusammenhang mit der vom Verkehrssicherungspflichtigen begründeten Gefahr das Schadensrisiko erhöht. Hiervon sind unter bestimmten Voraussetzungen auch Sicherheitsmaßnahmen gegen vorsätzliches Verhalten Unbefugter erfasst.[104] Für einen nur hypothetisch möglichen, praktisch aber fernliegenden Kausalverlauf soll der Verkehrssicherungspflichtige aber nicht mehr haften.[105]

82 Inwieweit diese Grundsätze zum einen produkthaftungsrechtlich überzeugend und zum anderen auf die Herstellerhaftung für IT-Sicherheitslücken übertragbar sind, ist im Einzelfall sehr sorgfältig zu prüfen. Hierbei ist zu berücksichtigen, dass das erforderliche Maß an IT-Sicherheit nur durch ein **Zusammenwirken** der Beteiligten, also Hersteller, Vertreiber und Anwender, erreicht werden kann.[106] Die Verantwortung für die IT-Sicherheit darf

---

99 Bräutigam/Klindt NJW 2015, 1137 (1241).

100 Vgl. nur Gesetzesbegründung zum BSIG, BR-Drs. 134/90, 16.

101 Rockstroh/Kunkel MMR 2017, 77 (78).

102 Differenzierend Raue NJW 2017, 1841 (1844).

103 Rockstroh/Kunkel MMR 2017, 77 (78 f.); Bräutigam/Klindt NJW 2015, 1137 (1142); vgl. hierzu auch BGH Urt. v. 12.11.1991 – VI ZR 7/91, NJW 1992, 560 – Kindertee; BGH Urt. v. 19.2.1975 – VIII ZR 144/73, NJW 1972, 2217 – Haartonicum; BGH Urt. v. 5.5.1992 – VI ZR 188/91, NJW 1992, 2016 (2018) – Kippsilo; BGH Urt. v. 19.5.1999 – VI ZR 192-98, NJW 1999, 2815 f. – Papierreißwolf.

104 BGH Urt. v. 19.12.1989 – VI ZR 182/89, NJW 1990, 1236 (1237); zur Pflicht des Hauseigentümers, Abdeckungen von Keller-Lichtschächten gegen Wegnahme zu sichern, da ansonsten Sturzgefahr begründet wird; anders OLG Karlsruhe Urt. v. 22.6.2005 – 7 U 104/04, NJW-RR 2005, 1264 f. bei einem Abdeckgitter, das 150 kg schwer war und dessen unberechtigte Entfernung daher nicht mehr als naheliegend bewertet wurde.

105 Vgl. hierzu Bamberger/Roth/Spindler BGB § 823 Rn. 328.

106 So auch ausdrücklich in der Gesetzesbegründung zum BSIG, BT-Drs. 11/7029.

daher nicht allein auf den Hersteller abgewälzt werden. Soweit es technische Regelwerke zur IT-Sicherheit der Software gibt oder der Hersteller einen Wissensvorsprung hat, sollten diese Erkenntnisse bei der Entwicklung jedenfalls berücksichtigt werden, um etwaige Haftungsrisiken so weit wie möglich zu reduzieren.

bb) Maßstab für vom Hersteller zu treffende Sicherheitsmaßnahmen. Vor dem Hintergrund des oben dargestellten Rechtsrahmens der deliktsrechtlichen Haftung für IT-Sicherheitslücken ist zu berücksichtigen, dass Maßstab der dem Hersteller auferlegten Verkehrssicherungs- und damit Sorgfaltspflichten stets der **aktuelle Stand von Wissenschaft und Technik** ist. Dieser Stand geht in vielen Fällen über den allgemeinen Stand der Technik oder Branchenüblichkeit hinaus, ist im Einzelfall aber oft schwierig zu bestimmen – ua weil es keine scharfe Definition des Begriffes gibt. Der BGH hat aber jedenfalls als Konkretisierung herausgearbeitet, dass der maßgebliche Stand der Wissenschaft und Technik nicht mit Branchenüblichkeit gleichgesetzt werden darf, da die in der jeweiligen Branche tatsächlich praktizierten Sicherheitsvorkehrungen durchaus hinter der technischen Entwicklung und damit hinter den rechtlich gebotenen Maßnahmen zurückbleiben können. Vielmehr soll es darauf ankommen, ob nach gesichertem Fachwissen der einschlägigen Fachkreise praktisch einsatzfähige Lösungen zur Verfügung stehen. Hiervon kann grundsätzlich erst dann ausgegangen werden, wenn eine sicherheitstechnisch überlegene Alternativkonstruktion zum Serieneinsatz reif ist. Der Hersteller ist dagegen nicht dazu verpflichtet, solche Sicherheitskonzepte umzusetzen, die bisher nur „auf dem Reißbrett erarbeitet" oder noch in der Erprobung befindlich sind.[107] **83**

Es besteht Einigkeit darüber, dass die Anforderungen aus **öffentlich-rechtlichen Sicherheitsvorschriften** und technischen Normen in dieser Hinsicht lediglich einen **Mindeststandard** darstellen.[108] Daher befreit die Einhaltung dieser Regelwerke nicht von der zivilrechtlichen Produzentenhaftung. Der aktuelle Stand von Wissenschaft und Technik kann vielmehr – gerade in einem sich schnell technisch weiterentwickelnden Bereich – darüber hinausgehen. Umgekehrt besteht aber bei Nichterfüllung dieser Regelwerke stets die nur schwer widerlegbare Vermutung, dass ein sicherheitsrelevanter Produktfehler gegeben ist.[109] Es liegt mithin in der Verantwortung des Herstellers, durch die Auswertung von Fachliteratur und anderen relevanten Quellen, die Teilnahme an Fachkonferenzen und schließlich auch die Beobachtung des Verhaltens der eigenen und auch Konkurrenzprodukte im Markt, den aktuellen Stand von Wissenschaft und Technik zu kennen und umzusetzen. **84**

Der Umfang der dabei zu ergreifenden Maßnahmen richtet sich zum einen nach der **Größe** und den **Kapazitäten** des jeweiligen Unternehmens. Maßgebliches Kriterium ist darüber hinaus die Art und der Grad der durch das jeweilige Produkt verursachten Gefahr.[110] **85**

In der juristischen Literatur wird vor diesem Hintergrund zT darauf hingewiesen, dass zB Software im medizinischen Bereich oder zur Flugsicherung, die eine **besondere Gefahrenquelle** für Leib, Leben und Gesundheit darstellt, einem strengeren Maßstab unterliege als Software in Bereichen, in denen solche Gefahren nicht existieren.[111] Zu berücksichtigen ist allerdings, dass sich diese rechtliche Analyse auf Softwarefehler im Allgemeinen bezieht, nicht hingegen auf Sicherheitslücken, die einen Zugriff von Dritten möglich machen, der **86**

[107] BGH Urt. v. 16.6.2009 – VI ZR 107/08, NJW 2009, 2952 (2954) – Airbag.

[108] Vgl. nur MüKoBGB/Wagner § 823 Rn. 1077 ff.; OLG Schleswig Urt. v. 19.10.2007 – 17 U 43/07, NJW-RR 2008, 691 – Geschirrspülmaschine; OLG Karlsruhe Urt. v. 10.10.2001 – 7 U 117/99, VersR 2003, 1584 (1585) – Buschholzhackmaschine; für Produkte, die nach dem Inkrafttreten der Cyberresilienz-VO in Verkehr gebracht werden, gilt aber jedenfalls im öffentlichen Produktrecht die Konformitätsvermutung des Art. 27 Cyberresilienz-VO.

[109] Grüneberg/Sprau BGB ProdHaftG § 3 Rn. 4; vgl. auch BGH Urt. v. 1.3.1988 – VI ZR 190/87, NJW 1988, 2667 zur Haftung des Trägers eines Kinderspielplatzes.

[110] BGH Urt. v. 16.6.2009 – VI ZR 107/08, NJW 2009, 2952 (2954) – Airbag; BGH Urt. v. 23.10.1984 – VI ZR 85/83, VersR 1985, 64 (65); Foerste/Graf v. Westphalen ProdHaft-HdB/Foerste § 24 Rn. 51.

[111] ZB Foerste/Graf v. Westphalen ProdHaft-HdB/Graf v. Westphalen § 24 Rn. 173, § 48 Rn. 45.

dann erst zu einer Gefährdung führen kann. Auf Sicherheitslücken ist dieser Ansatz überhaupt nur übertragbar, wenn ein Fall vorliegt, in dem die **IT-Sicherheit als Teil der Produktsicherheit** gesehen werden kann. Zudem ist produkthaftungsrechtlich strikt zu unterscheiden zwischen einem dem Produkt von Anfang an – möglicherweise unentdeckt – innewohnender Softwarefehler, der zu einer sicherheitsrelevanten Fehlfunktion der IoT-Anwendung führen kann und einer Software, die unbefugte Zugriffe von Dritten auf das System ermöglicht. Ein Ansatz für einen gesetzlichen Sicherheitsmaßstab zur Vermeidung des vorsätzlich-böswilligen Zugriffs Dritter findet sich in der **Cybersicherheits-VO** (EU) 2019/881.[112] Im Rahmen des mit der VO (EU) 2019/881 eingeführten europäischen Schemas für Cybersicherheit wird ein Konformitätsbewertungsverfahren für Hersteller aufgesetzt, das mit der Ausstellung einer EU-Konformitätserklärung endet. Mit Durchführungsverordnung (EU) 2024/482 hat die Europäische Kommission ein erstes Zertifizierungsschema veröffentlicht, das ab 27.2.2025 verfügbar sein soll.[113] Die **Cybersicherheitszertifizierung** und die damit einhergehende Ausstellung der EU-Konformitätserklärung ist allerdings bis auf Weiteres freiwillig. Sie stellt somit keine gesetzliche Anforderung für das Inverkehrbringen eines IKT Produktes dar. Dennoch wird – wenn das europäische Schema für die Cybersicherheitszertifizierung erst einmal erarbeitet und veröffentlicht ist – die Möglichkeit der Einordnung und Zertifizierung von Produkten in verschiedenen Vertrauenswürdigkeitsstufen Einfluss auf die **Verkehrssicherungspflichten** der Hersteller haben. Der Hersteller wird sich bei Auslobung einer bestimmten Vertrauenswürdigkeitsstufe daran messen lassen müssen, die Vorgaben des jeweiligen Schemas auch einzuhalten. Diese Vorgaben betreffen zunächst den Zeitpunkt des Inverkehrbringens eines solches IKT Produktes. Art. 55 VO (EU) 2019/881 geht aber darüber hinaus: Wenn der Hersteller ein zertifiziertes IKT Produkt anbietet, muss er der Öffentlichkeit ua Informationen darüber zugänglich machen, über welchen Zeitraum dem Endnutzer Sicherheitsunterstützung angeboten wird, insbesondere in Bezug auf die Verfügbarkeit von cybersicherheitsbezogenen Aktualisierungen.

87 Aufgrund der grundsätzlich anerkannten, erhöhten Fehleranfälligkeit von Software sowie der Schnelllebigkeit der technischen Weiterentwicklung im IT-Bereich und des „Wettrennens" von Software-Anbietern und Hackern ist die **Produktbeobachtungs- und Gefahrabwendungspflicht** in diesem Bereich von besonderer Bedeutung. Der Hersteller ist auch nach Inverkehrbringen seines Produktes verpflichtet, dieses auf seine Bewährung im Feld und sich ggf. zeigende Sicherheitsrisiken zu beobachten. In Anknüpfung hieran wird von der juristischen Literatur – soweit sie sich überhaupt mit dieser Frage eingehender beschäftigt – eine intensivierte Produktbeobachtungspflicht für Software hergeleitet.[114] Auch eine Gefahrabwendungspflicht in Form der Warnung oder regelmäßiger Sicherheitsupdates wird von der Literatur zT ohne Weiteres angenommen.[115] Dies scheint allerdings eine sehr starke Ausweitung der Herstellerpflichten, die grundsätzlich auf die Sicherheit des eigenen Produkts beschränkt sind. Die Rechtsprechung hatte noch keine Gelegenheit, hierzu Stellung zu nehmen. Der genaue Umfang der Produktbeobachtungspflicht des Software-Herstellers wird maßgeblich davon abhängen, wie sich die objektiv ermittelte Sicherheitserwartung des durchschnittlichen Benutzers und die Abgrenzung der Verantwortungsbereiche von Hersteller, Vertreiber und Anwender entwickeln.

88 **cc) Verantwortungszuweisung bei mehreren Wirtschaftsakteuren in der Wertschöpfungskette.** Zu berücksichtigen ist, dass es bei softwaregesteuerten Geräten in der Regel mehrere Verantwortliche in der Produktionskette gibt: Oft ist – wie auch in einigen

[112] Vgl. hierzu Klindt EuZW 2019, 665.

[113] Eine Kurzbeschreibung der Europäischen Kommission zur Zertifizierung ist hier zu finden: https://digital-strategy.ec.europa.eu/en/library/brand-book-european-common-criteria-based-cybersecurity-certification-scheme-eucc.

[114] Vgl. zB Spindler NJW 2004, 3145 (3147); Spindler CR 2015, 766 (769); Foerste/Graf v. Westphalen ProdHaft-HdB/Foerste § 24 Rn. 174.

[115] Foerste/Graf v. Westphalen ProdHaft-HdB/Foerste § 24 Rn. 175.

der hier zu Grunde zu legenden Konstellationen – der Hersteller des Gerätes ein anderer als der Hersteller der Software. In diesem Fall ist jeder der Beteiligten in gewissem Maße auch für sogenannte Kombinationsrisiken verantwortlich, die an der Schnittstelle seines eigenen Produkts zu einem fremden Produkt auftreten können.

Wie oben dargestellt, haftet der Hersteller grundsätzlich für Schäden, die durch sein fehlerhaftes Produkt verursacht werden. Die Rechtsprechung hat diese Produzentenhaftung – unter engen Voraussetzungen – ausgedehnt auf Schäden, die gerade durch das Zusammenwirken zweier Produkte verursacht werden (sog. **Kombinationsrisiken**). Im Hinblick auf solche Kombinationsrisiken kann dem Hersteller eine Produktbeobachtungs- und ggf. Gefahrabwendungspflicht obliegen.[116] Aus den Urteilsgründen dieser Rechtsprechung entnimmt ein großer Teil der sich damit auseinandersetzenden Literatur, dass eine Haftung für Kombinationsrisiken insbesondere dann in Betracht kommt, wenn ein Produkt notwendigerweise mit einem anderen kombiniert werden muss um funktionsfähig zu sein.[117] Diese Voraussetzungen werden gerade bei IoT Anwendungen, die nur durch Zusammenwirken von Hard- und Software ihre Funktionalität erfüllen können, in der Regel vorliegen. **89**

Vom Schadensersatzanspruch des § 823 Abs. 1 BGB sind nur Schäden erfasst, die durch Verletzung eines der in der Vorschrift abschließend aufgeführten Rechtsgüter verursacht werden, nämlich Eigentum, Leben, Körper, Gesundheit und Freiheit sowie sonstige Rechte – zB Besitz, allgemeines Persönlichkeitsrecht, eingerichteter und ausgeübter Gewerbebetrieb. Reine **Vermögensschäden** sind hingegen gem. § 823 Abs. 1 BGB nicht ersatzfähig.[118] Denkbare Schäden, die durch Sicherheitslücken in Software verursacht werden könnten, sind insbesondere Löschung oder Manipulation von Daten. Es ist umstritten, ob das Einwirken auf **Daten** an sich eine Eigentumsverletzung – und damit einen gem. § 823 Abs. 1 BGB zu ersetzenden Schaden – darstellt. Eigentum kann nämlich gem. §§ 903 ff. BGB nur an Sachen erlangt werden. Daten – und auch Software selbst – sind allerdings keine Sachen iSd § 90 BGB, sehr wohl aber die Verkörperung von Software auf einem Datenträger.[119] Ob vor diesem Hintergrund ein Löschen oder eine Manipulation von Daten eine von § 823 Abs. 1 BGB erfasste Rechtsgutsverletzung darstellt, ist umstritten. Eine Ansicht sieht in einem solchen Eingriff stets auch eine Veränderung des Datenträgers und bejaht in der Konsequenz die relevante Rechtsgutsverletzung.[120] Eine andere Ansicht lehnt hingegen bei Löschung oder Manipulation von Daten eine Eigentumsverletzung ab.[121] Es bleibt allerdings möglicherweise ein Schadensersatzanspruch gem. § 823 Abs. 2 BGB iVm mit den öffentlich-rechtlichen Anforderungen an Cybersicherheit. Hierfür ist jeweils sorgfältig zu prüfen, ob es sich um Schutzgesetze iSd § 823 Abs. 2 BGB handelt (→ Rn. 56). **90**

dd) Öffentlich-rechtliche Dimension. Auch eine öffentlich-rechtliche Verantwortung des Herstellers für Sicherheitslücken seiner vernetzten Produkte kommt in Betracht. Die inzwischen ausdifferenziert durch EU-Richtlinien und EU-Verordnungen geregelte **Product Compliance** findet Eingang in das deutsche Recht im Produktsicherheitsgesetz (ProdSG). Das ProdSG ist nach seinem § 1 anwendbar, wenn Produkte auf dem deutschen Markt bereitgestellt werden. Es stellt sich also auch hier die Frage, ob Software an sich unter diesen Produktbegriff gefasst werden kann. Dies wird unter Berücksichtigung des Wortlauts und der Systematik der Vorschrift abgelehnt.[122] Insbesondere spricht die Definition des **91**

[116] BGH Urt. v. 9.12.1986 – XVI ZR 65/86, NJW 1987, 1009 – Lenkerverkleidung.

[117] Foerste/Graf v. Westphalen ProdHaft-HdB/Foerste, § 25 Rn. 184; Helmig PHi 2004, 92 (100); MüKoBGB/Wagner § 823 Rn. 1099; aA Bamberger/Roth/Spindler § 823 Rn. 513.

[118] Reine Vermögensschäden sind nur über § 823 Abs. 2 BGB ersatzfähig, der die schuldhafte Verletzung eines Schutzgesetzes voraussetzt. Hierzu ausführlich → Rn.

[119] BGH Urt. v. 15.11.2006 – XII ZR 120/04, NJW 2007, 2394; Peschel/Rockstroh MMR 2014, 571 (572).

[120] MüKoBGB/Wagner § 823 Rn. 165.

[121] So wohl Bamberger/Roth/Fritzsche BGB § 90 Rn. 26; LG Konstanz Urt. v. 10.5.1996 – 1 S 292/95, NJW 1996, 2662.

[122] Sehr anschaulich unter Einbeziehung der Regelungssystematik des EU-Produktrechts und der Richtlinie 87/379/EWG Wiebe NJW 2019, 625 (626).

Begriffes „Produkt" in § 2 Nr. 22 ProdSG als „Waren, Stoffe oder Zubereitungen, die durch einen Fertigungsprozess hergestellt worden sind" gegen eine Erfassung von Software. Darüber hinaus bezieht zB die europäische Medizinprodukte-Verordnung VO (EU) 2017/745[123] in ihrem Art. 2 Nr. 1 ausdrücklich Software in den Anwendungsbereich ein. Aus einem Umkehrschluss lässt sich daraus herleiten, dass Software nicht unter den allgemeinen **Produktbegriff** des europäischen Produktrechts fällt. Allerdings bedeutet dies nur, dass reine Software nicht vom Anwendungsbereich des ProdSG umfasst ist. Vernetzte Produkte mit bereits integrierter Software („embedded Software") fallen ohne Weiteres darunter.

92 § 3 ProdSG schreibt vor, dass nur Produkte auf dem Markt bereitgestellt werden dürfen, die den einschlägigen rechtlichen Vorschriften entsprechen. Dabei ist im deutschen Recht zwischen dem sog. harmonisierten Bereich und dem nicht-harmonisierten Bereich zu unterscheiden.

93 Jedenfalls muss ein Produkt, das Software enthält – egal ob es vernetzt ist oder nicht – den zum Zeitpunkt des Inverkehrbringens geltenden Rechtsvorschriften entsprechen. Dies gilt auch für die integrierte Software. Wegen der gesetzlichen Implementierung einer Vermutungswirkung bestimmter technischer Normen empfiehlt es sich, die existierenden einschlägigen Normen für Cybersicherheit anzuwenden. Damit geht nämlich eine Privilegierung bei der Prüfung der Produkte durch Marktüberwachungsbehörden einher.

94 Für Verbraucherprodukte und Produkte, die einer bereits an den New Legislative Framework angepassten europäischen Richtlinie oder Verordnung unterfallen[124], sieht das öffentliche Recht zudem eine Pflicht des Herstellers vor, ein funktionierendes **Produktbeobachtungs- und Beschwerdemanagement-System** einzuführen sowie auch die bereits in Verkehr gebrachten Produkte tatsächlich auf ihr Verhalten im Feld zu beobachten.[125] Bei Erkenntnissen über eine vom Produkt ausgehende Gefahr im Feld ist der Hersteller verpflichtet, die erforderlichen Gefahrabwendungsmaßnahmen zu ergreifen und das Produktrisiko bei der zuständigen Marktüberwachungsbehörde zu notifizieren.

95 Im Rahmen der öffentlich-rechtlichen Produktbeobachtungspflicht greift die Argumentation im aktuellen juristischen Diskurs häufig zu kurz. Hier wird zT ohne eingehende Begründung darauf verwiesen, dass aufgrund des Vorsorgecharakters der Produktbeobachtungspflicht für Verbraucherprodukte aus § 6 Abs. 3 ProdSG im Rahmen der Stichprobendurchführung auch immer wieder die in Verbraucherprodukten verwendete Software auf bestehende Fehler überprüft werden müsse.[126] Dem kann in dieser Pauschalität nicht zugestimmt werden. Allerdings statuiert § 26 Abs. 2 ProdSG die Befugnis der Marktüberwachungsbehörden, Maßnahmen gegenüber dem verantwortlichen Wirtschaftsakteur anzuordnen, wenn der begründete Verdacht besteht, dass ein Produkt nicht den gesetzlichen Anforderungen entspricht. Zu dem **Maßnahmenkatalog** gehört auch die Anordnung eines Produktrückrufs als ultima ratio. Jedenfalls im Falle eines ernstes Risikos nach der von der Europäischen Kommission vorgegebenen Methodik der Risikobewertung muss die Behörde einen Produktrückruf anordnen.[127] Auch wenn der Produktrückruf die drastischste Maßnahme der Marktüberwachungsbehörde darstellt, kann nicht davon ausgegangen werden, dass andere produktbezogene Maßnahmen als Minus in dieser Befugnis enthalten sind. Zu berücksichtigen ist nämlich, dass der Produktrückruf allein darauf gerichtet ist, ein Risiko aus dem Feld zu beseitigen, nicht hingegen darauf, die bereits im

[123] Umgesetzt in deutsches Recht durch das Medizinproduktegesetz (MPG); zu den besonderen Regelungen des Medizinprodukterechts im Hinblick auf Update-Pflichten vgl. → § 15 Rn. 239 ff.

[124] Insbesondere elektrische Betriebsmittel im Anwendungsbereich der RL 2014/35/EU (im deutschen Recht umgesetzt durch die 1. Produktsicherheitsverordnung), Geräte mit Funkfunktion (einschließlich Bluetooth- und W-Lan-Funktionen) im Anwendungsbereich der RL 2014/53/EU (iim deutschen Recht umgesetzt durch das Funkanlagengesetz), Geräte im Anwendungsbereich der Richtlinie über die elektromagnetische Verträglichkeit 2014/30/EU (im deutschen Recht umgesetzt durch das Gesetz über die elektromagnetische Verträglichkeit).

[125] Vgl. zB Art. 83 VO (EU) 2017/745, Art. 10 VO (EU) 2023/1230.

[126] Wiebe NJW 2019, 625 (627).

[127] Vgl. hierzu ausführlicher Klindt/Wende NVwZ 2011, 602.

Feld befindlichen Produkte in einen Zustand zu versetzen, in dem sie sicher und vertragsgemäß benutzt werden können. Soweit in der Literatur eine Befugnis der Marktüberwachungsbehörden zur Anordnung eines **sicherheitsrelevanten Software-Updates** auf die Generalklausel des § 26 Abs. 2 S. 1 ProdSG unter Heranziehung der Vergleichbarkeit mit dem Regelbeispiel in § 26 Abs. 2 Nr. 5 ProdSG (Anbringung von Warnhinweisen) gestützt wird[128], kann dem nicht gefolgt werden. § 26 Abs. 2 Nr. 5 ProdSG bezieht sich nämlich auf Produkte, die gerade noch nicht in Verkehr gebracht wurden. Die rein technische Möglichkeit, mit Software-Updates auf bereits im Feld befindliche Produkte zuzugreifen darf nicht dazu führen, dass die für das Produktrecht wesentliche Differenzierung der Zeiträume und Pflichten vor und nach dem Inverkehrbringen verwaschen wird. Ohne Zweifel darf aber der verantwortliche Wirtschaftsakteur ein im Feld entdecktes Produktrisiko mittels eines Fern-Updates beseitigen.[129] Er kann damit ggf. die Anordnung eines Produktrückrufs durch die Marktüberwachungsbehörde verhindern, da die Behörde gem. § 26 Abs. 3 ProdSG effektive, freiwillige Maßnahmen des Produktverantwortlichen bei ihrer Entscheidungsfindung zu berücksichtigen hat. Allerdings ist auch im öffentlichen Produktrecht nicht jede Sicherheitslücke in einem vernetzten Produkt zwangsläufig als Produktrisiko zu werten. Vielmehr sind auch hier die Verantwortlichkeiten von Hersteller, Benutzer und angreifendem Dritten sorgfältig auszuloten.

ee) Verantwortung des Betreibers/Anwenders einer Industrie 4.0 oder IoT Anwendung. Der sich fragmentarisch entwickelnde Rechtsrahmen zu Cybersicherheits-Pflichten und einer Haftung für Schäden, die aus Sicherheitslücken resultieren, tendiert zum einen zu einer **weitgehenden Haftung** für **Hersteller** oder **Anbieter** solcher Systeme. Zu berücksichtigen sind allerdings auch Rechtsakte, die den **Betreiber** oder **Anwender** eines solchen Systems in die Pflicht nehmen. In der Dogmatik des Produkthaftungsrechts endet die Verantwortlichkeit des Herstellers an der Grenze seines Produktes. In bestimmten Bereichen sind noch Schnittstellen zu anderen Produkten erfasst. Das bewusste, auf Herbeiführung eines Schadens gerichtete Dazwischentreten eines Dritten unterbricht die Kausalkette, so dass der Eintritt des Schadens dem Hersteller nicht mehr zuzurechnen ist. Daher ist noch eine intensive rechtsdogmatische Diskussion zu erwarten, inwieweit die Absicherung vor Cybersicherheitsrisiken dem Hersteller obliegt, wenn und soweit durch derartige Eingriffe produkthaftungsrechtlich relevante Schäden (zB anderer Verkehrsteilnehmer) hervorgerufen werden können.[130] Dazu gehört auch die Frage, ob und in wessen Verantwortungsbereich IT-Sicherheit und Produktsicherheit zu einem gemeinsamen Schutzkonzept zu entwickeln sind.[131] **96**

Gleichzeitig treffen den **Benutzer** des Produktes auch Pflichten im Hinblick darauf, die IT-Sicherheit zu erhalten, zB durch regelmäßige Updates. Es ist noch nicht geklärt, wie genau die Grenze zwischen Hersteller- und Benutzerverantwortung gezogen wird. Durchaus denkbar ist, dass sich bei besonders sensiblen Produkten mit einer **lebensschützenden Funktion** eine Pflicht des Herstellers zur automatischen Installation von Sicherheitsupdates entwickelt. Jedenfalls zeigt die bisherige Rechtsprechung, insbesondere zur europäischen Produkthaftungs-RL 85/374/EEG, dass bei solchen Produkten von einer gesteigerten, berechtigten Sicherheitserwartung der Benutzer ausgegangen werden muss.[132] **97**

Sowohl das BSIG als auch technische Normen, wie zB IEC 62443 erlegen vor allem dem **Betreiber** die Verantwortung für die Sicherheit seiner Produktionsanlage auf.[133] Zu berücksichtigen ist dabei aber, dass der Maßstab der Sicherheit nach dem BSIG – selbst für kritische Infrastrukturen – hinter demjenigen des Produkthaftungsrechts zurückbleibt. Gemäß § 8a BSIG sind die Betreiber kritischer Infrastrukturen ua verpflichtet, angemessene **98**

[128] Wiebe NJW 2019, 625 (629).
[129] Zu rechtlichen Einschränkungen der Befugnis vgl. Wiesemann/Mattheis/Wende MMR 202.
[130] Hartmann DAR 2015, 122 (123).
[131] Vgl. auch Bräutigam/Klindt NJW 2015, 1137 (1240).
[132] ZB EuGH Urt. v. 5.3.2015 – C-503/13 und C-504/14, NJW 2015, 1163 – Herzschrittmacher.
[133] Kunkel/Rockstroh MMR 2017, 77 (80).

organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Integrität oder Vertraulichkeit ihrer informationstechnischen Systeme zu treffen. Dabei soll der Stand der Technik eingehalten werden. Das Produkthaftungsrecht verpflichtet den Hersteller hingegen zur Einhaltung des weitergehenden aktuellen Stands von Wissenschaft und Technik.[134]

99 Besondere Pflichten zur Cybersicherheit treffen denjenigen, der **personenbezogene Daten** verarbeitet. Der EuGH setzte sich erstmals mit der Verantwortlichkeit für Schäden aus Cyberangriffen im Zusammenhang mit einem Schadensersatzanspruch gem. Art. 82 Abs. 1 DS-GVO auseinander.[135] Anspruchsvoraussetzung ist zunächst ein Verstoß des in Anspruch genommenen Unternehmens gegen die Vorschriften der DS-GVO. Zwar enthält die DS-GVO keine ausdrücklichen Anforderungen an die Cybersicherheit, sie verpflichtet allerdings in Art. 24 und 32 Unternehmen, geeignete technische und organisatorische Maßnahmen zu ergreifen, um personenbezogene Daten bei der Verarbeitung angemessen zu schützen.

100 Bei Lücken oder Schwachstellen der Cybersicherheit, die beim Inverkehrbringen des jeweiligen Produktes objektiv nicht erkennbar waren, taucht regelmäßig die Frage auf, ob ein sog. **Entwicklungsfehler** vorliegt, der sowohl die Produkthaftung als auch die deliktsrechtliche Produzentenhaftung ausschließt. Hierbei ist allerdings zu berücksichtigen, dass der haftungsbefreiende Entwicklungsfehler von der Rechtsprechung sehr **eng ausgelegt** wird. Es soll nicht darauf ankommen, ob ein spezifischer Fehler am konkreten Produkt erkennbar war.[136] Vielmehr kann sich der Hersteller nicht auf den Entwicklungsfehler berufen, sobald eine bestimmte Fehleranfälligkeit des Produktes erkennbar war. Es ist daher damit zu rechnen, dass die Gerichte einen Entwicklungsfehler ablehnen werden, da die Problematik der fehlenden IT-Sicherheit bei entsprechenden Schwachstellen bekannt ist. Dies wäre eine konsequente Fortführung der ständigen Rechtsprechung, zB im Hinblick auf die Erkennbarkeit von Haarrissen in Mineralwasserflaschen[137] oder die grundsätzliche Kenntnis der Gefahr von Fehlauslösungen von Airbags[138].

b) Weitere Ausgestaltung der Haftung für Schwachstellen in der Cybersicherheit

101 Die haftungsrechtliche Verantwortung für Schäden, die durch Cyberangriffe auf vernetzte Systeme und damit auf die darin befindlichen Daten, Software oder KI verursacht werden, wird durch verschiedene **EU-Rechtsakte** konkretisiert, die in nächster Zeit in Kraft treten. Die Vorschriften sind nach der deutschen Dogmatik teilweise dem öffentlichen Recht, teilweise dem Zivilrecht zuzuordnen. Da das EU-Recht auch im Hinblick auf die Methodik autonom vom nationalen Recht ist und die Rechtsakte zT eine Verschränkung der öffentlich-rechtlichen Anforderungen mit zivilrechtlichen Haftungstatbeständen vorsehen[139] oder das nationale Zivilrecht als ggf. notwendigen Baustein der nationalen Rechtsdurchsetzung unter Berücksichtigung des effet utile voraussetzen, werden die Anforderungen im Folgenden nicht dogmatisch getrennt, sondern thematisch gebündelt dargestellt. Konsequenzen der dogmatischen Einordnung werden jeweils an den relevanten Stellen aufgezeigt.

102 Art. 7 Abs. 2 lit. f **EU-ProdHaftRL** regelt ausdrücklich, dass „sicherheitsrelevante Cybersicherheitsanforderungen" als Anforderungen an die **Produktsicherheit** für die Bewertung des haftungsbegründenden Produktfehlers berücksichtigt werden müssen. Damit wird die Cybersicherheit dem Verantwortungsbereich des **Herstellers** eines vernetzten Produktes zugeordnet. Damit ist aber noch nicht die Frage beantwortet, ob der Hersteller über

[134] Vgl. hierzu zB Foerste/Graf v. Westphalen ProdHaft-HdB/Foerste § 24 Rn. 23.
[135] EuGH Urt. v. 14.12.2023 – C-340/21, EuZW 2024, 234; hierzu eingehend: Stegemann/Schumacher EuZW 2024, 209 (210).
[136] So bereits BGH Urt. v. 17.3.1981 – VI ZR 191/79, BGHZ 80, 186 – Derosal.
[137] BGH Urt. v. 9.5.1995 – VI ZR 158/94, NJW 1995, 2162 – Mineralwasserflaschen.
[138] BGH Urt. v. 16.6.2009 – VI ZR 107/08, NJW 2009, 2952 – Airbag.
[139] Hierzu eingehend Krüger/Wagner ZfPC 2023, 124 (125 f.).