Dennis-Kenji Kipker, Michael Walkusz

Hersteller- und Verkäuferpflichten bei softwarebezogenen IT-Sicherheitsupdates

Rechtsgrundlagen und Umfang

Tagtäglich werden neue Schwachstellen in der IT-Sicherheit entdeckt. Damit einhergehend stellt sich für Hersteller und Verkäufer von IT-Produkten die Frage, in welchen Fällen, in welchem Umfang und für wie lange sie ihren Kunden IT-sicherheitsbezogene Softwareupdates zur Verfügung stellen müssen. Der vorliegende Beitrag beleuchtet die gegenwärtige Situation im Vertrags- und Deliktsrecht für die nicht immer klar geregelten Updatepflichten im B2B-Bereich vor allem aus der Herstellerperspektive – insbesondere auch jenseits individuell vereinbarter Garantieverträge. Einbezogen werden dabei die drei möglichen Parteien Hersteller, (Zwischen-)Händler oder Intermediär und Kunde bzw. Nutzer.

1 Leistungsbeziehungen im Rahmen von Softwareherstellung und -vertrieb

Heutzutage zeichnen sich Softwareherstellung und entsprechende Vertriebswege dadurch aus, dass sie oftmals nicht linear verlaufen, sondern in einem komplexen Netzwerk und auf unterschiedliche Weise miteinander verkettet sind.[1] So ist es bspw. denkbar, dass die Grundkomponenten oder Bibliotheken eines Programms ursprünglich aus einer Open Source-Quelle stammen, und dann von entsprechenden Zulieferern erst an den Hersteller geliefert werden, der – das unter Umständen nach Kundenwünschen individualisierte – Produkt erstellt und an den Anwender oder Integrator (Systemhäuser/Zwischenhändler) ausliefert, die ihrerseits weitere Modifikationen vornehmen können. Hinzu kommt, dass Software vielfach nicht als selbstständiges Produkt hergestellt wird, sondern als Embedded System in ihren Funktionen untrennbar mit Hardwarekomponenten verbunden ist. Daraus folgt, dass die Bestimmung von rechtlichen Verantwortlichkeiten im Hinblick auf die Software mit erheblichen Herausforderungen verbunden ist, da die unterschiedlichen Pflichtenkreise und deren Umfang nicht immer leicht voneinander abgrenzbar sind.

Dr. Dennis-Kenji Kipker

ist Geschäftsführer der Certavo GmbH – international compliance management, wissenschaftlicher Geschäftsführer des IGMR an der Universität Bremen, Legal Advisor im VDE e.V. – Abteilung CERT@VDE – in Frankfurt a.M. und Mitglied des Vorstandes der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin.
E-Mail: kipker@uni-bremen.de

Michael Walkusz

ist studentischer Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen, Uni-Start-Tutor für das Fach Zivilrecht in Kooperation mit dem Projekt „ForstAIntegriert" (Forschendes Studieren von Anfang an) an der Universität Bremen.
E-Mail: mwalkusz@uni-bremen.de

2 Vertragstypologisierung und vertragliche Pflichtenkreise

Vertraglich muss der Hersteller unabhängig vom Vertragstypus eine mangelfreie Leistung erbringen.[2] Ob es sich bei dem Produkt um eine selbstständige Software oder um ein Embedded System handelt, spielt keine Rolle, da es im Ergebnis nur darauf ankommt, dass das Produkt dem geschuldeten Funktionsumfang

1 Dies wohl zu vereinfachend *Schrader/Engstler*, MMR 2018, 356, 357.
2 Vgl. §§ 433 Abs. 1 S. 2, 535 Abs. 1 S. 2, 633 Abs. 1 BGB.

entspricht, gleichgültig, ob hierdurch physische Prozesse stattfinden oder es zu einer ausschließlich digitalen Datenverarbeitung kommt. Die juristisch geführte Diskussion, ob Software eine Sache im rechtlichen Sinne ist, ist an dieser Stelle ebenfalls zu vernachlässigen, da dies im Ergebnis keine nennenswerten Auswirkungen hat: Denn selbst wenn die Sacheigenschaft der Software verneint wird, ist § 453 BGB anwendbar, der die Vorschriften des Sachkaufs für entsprechend anwendbar erklärt.[3] Für das Werkvertragsrecht spielt die körperliche Sacheigenschaft ebenfalls keine Rolle, da hier rechtlich keine Sache, sondern ein Erfolg geschuldet ist, der auch immaterieller Art sein kann.[4] Soweit die Sacheigenschaft bejaht wird, findet bei Überlassung einer Software auf Zeit das Mietrecht Anwendung,[5] bei verneinter Sacheigenschaft ist zwar Pachtrecht anzuwenden,[6] das aber in § 581 Abs. 2 BGB unter Vorbehalt spezieller Regelungen wiederum Rückgriff auf das Mietrecht nimmt.

2.1 Pflichten aus dem Kauf- und Werkvertragsrecht

Das Kauf- oder Werkvertragsrecht ist grds. dann anwendbar, wenn für das zu liefernde oder herzustellende Produkt auf einen punktuellen Leistungszeitpunkt abgestellt wird. Die Mangelhaftigkeit beurteilt sich kaufrechtlich nach § 434 BGB, im Werkvertragsrecht gem. § 633 BGB. Für Werklieferungsverträge gem. § 650 BGB ist das Kaufrecht anwendbar. Da, soweit keine besonderen vertraglichen Abreden bestehen, auch regelmäßig keine für den jeweiligen Vertrag vorausgesetzte Verwendung bestimmt ist, beurteilt sich die Frage des Mangels für das Kaufrecht nach § 434 Abs. 1 S. 2 Nr. 2 BGB, sowie für das Werkvertragsrecht nach § 633 Abs. 2 S. 2 Nr. 2 BGB. Demnach muss das Produkt eine Beschaffenheit aufweisen, die bei Sachen der gleichen Art üblich ist und die der Kunde nach der Art der Sache erwarten kann. Zur Auslegung dieser Bestimmungen ist der geltende Maßstab die Verkehrsauffassung eines durchschnittlichen Kunden.[7] Anhaltspunkte hierfür sind auch wesentliche Sicherheitsvorschriften.[8] Eine Legaldefinition zur Sicherheit in der Informationstechnik findet sich in § 2 Abs. 2 BSIG; hierunter ist demnach die Einhaltung bestimmter Sicherheitsstandards zu verstehen, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen. Dies kann durch Sicherheitsvorkehrungen in IT-Systemen, Komponenten oder Prozessen oder bei der Anwendung von IT-Systemen, Komponenten oder Prozessen gewährleistet werden. Dass es sich hierbei um eine Begriffsbestimmung handelt, die aus dem Anwendungsbereich Kritischer Infrastrukturen stammt, ist unschädlich, da die technisch-organisatorischen IT-Sicherheitsziele branchenübergreifend definiert werden.[9] Gleiches gilt auch für die Definition der IT-Sicherheitslücke gem. § 2 Abs. 6 BSIG: Eine solche liegt vor, wenn ein Programm Eigenschaften aufweist, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden IT-Systemen verschaffen oder die Funktion der IT-Systeme beeinflussen können. Aus den vorgenannten Definitionen lässt sich ableiten, dass eine Software bzw. ein diese enthaltendes Produkt in jedem Fall vor Fremdeinflüssen abzusichern ist.[10] Fehlt es an einer solchen Maßnahme, liegt eine Schwachstelle vor. Insbesondere enthält eine Software bereits dann eine mangelrelevante Sicherheitslücke, wenn diese einen Angriff durch Schad- oder Spähsoftware ermöglicht, obwohl dies vermeidbar gewesen ist,[11] denn auch bloße Risiken können einen diesbezüglichen Mangel begründen.[12]

Für die Beurteilung der Mangelhaftigkeit eines Produkts kommt es im Kaufrecht auf den Zeitpunkt der Übergabe, im Werkvertragsrecht auf denjenigen der Abnahme an.[13] Die rechtliche Situation ist unproblematisch, wenn der zuvor beschriebene Mangel bereits bei Leistung vorliegt, denn im Falle einer solchen Schlechtleistung besteht eine Pflicht zur Nachbesserung von IT-Sicherheitslücken durch fehlerhafte Software z. B. in der Form von Patches. Für die Praxis interessanter ist der Fall, dass das Produkt zum Zeitpunkt des Gefahrübergangs den zu dem Stand gängigen Anforderungen an die IT-Sicherheit entsprach, sich aber erst im weiteren Lauf der Zeit Vulnerabilitäten in der Softwaresicherheit (Schwachstellen) ergeben. Grds. findet das Mängelgewährleistungsrecht nur auf solche Mängel Anwendung, die schon bei Gefahrübergang vorhanden waren, sodass der Hersteller oder Verkäufer prinzipiell von einer Verantwortlichkeit für solche Mängel befreit ist, die nicht schon von Beginn an im Produkt angelegt waren.[14] Dies ist gerade auch im IT-Sicherheitsrecht häufig der Fall: So kann ein Produkt zum Zeitpunkt seines Inverkehrbringens den seinerzeit gängigen Verschlüsselungsstandards entsprochen haben, die aufgrund der technischen Weiterentwicklung nach einigen Monaten oder Jahren jedoch unsicher sind.[15]

Fraglich ist, ob sich für Produkte im IT-sicherheitsrelevanten Umfeld an dieser Stelle Ausnahmen ergeben können. Die Übergabe einer Software erfolgt durch Übergabe des Datenträgers bzw. Embedded Systems oder durch das elektronische Bereitstellen einer Kopie.[16] Ein zum Zeitpunkt der Übergabe zu erwartender zukünftiger Mangel müsste deshalb als gegenwärtiger Mangel qualifiziert werden. Dies ließe sich mit der Begründung annehmen, dass auch bei Inverkehrbringen für sich genommen mangelfreier Produkte – man denke an das vorgenannte Verschlüsselungsbeispiel – die technische Entwicklung mit hoher Wahrscheinlichkeit dazu führt, dass ein einmal entwickeltes Produkt zukünftig den an dieses anzulegenden Anforderungen nicht mehr genügt und IT-Sicherheitslücken damit durchaus schon zum Zeitpunkt des Inverkehrbringens vorhersehbar sind.[17] Trotz dieses auf den ersten Blick logisch erscheinenden Arguments ist aber eine zukünftige Mangelvorhersehbarkeit nicht mit dem Mangel zum Zeitpunkt der Übergabe gleichzusetzen,[18] denn die bloße Vermutung, dass ein Produkt zu einem späteren Zeitpunkt den an es anzulegenden Anforderungen nicht mehr genügen könnte,

3 *Stresemann* in: MüKoBGB, § 90, Rn. 25.
4 *Busche* in: MüKoBGB, § 631, Rn. 2.
5 BGH NJW 2007, 2394; *von dem Bussche/Schelinski*, Münchner Anwaltshandbuch zum IT-Recht, Rn. 340; *Redeker*, IT-Recht, Rn. 596.
6 *Roth-Neuschild* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 13, Rn. 21; *zur Megede,* NJW 1989, 2580, 2583.
7 Für die inhaltsgleiche Formulierung im Kaufrecht BGH NJW 2009, 2807; *Faust* in: BeckOKBGB, § 434, Rn. 66.
8 BGH NJW 1985, 1769, 1770; *Berger* in: Jauernig, BGB, § 434, Rn. 30.
9 BSI, Leitfaden Informationssicherheit, S. 4 ff., abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3 (Stand: 05.04.2019).
10 *Rockstroh/Kunkel*, MMR 2017, 77, 78.
11 *Redeker*, IT-Recht, Rn. 328.
12 BGH NJW 2017, 2817, 2818.
13 *Westermann* in: MüKoBGB, § 434, Rn. 50; *Sprau* in: Palandt, BGB, § 633, Rn. 3.
14 *Busche* in: MüKoBGB, § 644, Rn. 4 f.; *Faust* in: BeckOKBGB, § 446, Rn. 16; *Westermann* in: MüKoBGB, § 446, Rn. 10.
15 Vgl. *Schrader/Engstler*, MMR 2018, 356, 357.
16 *Kindl* in: BeckOKBGB, § 929, Rn. 7.
17 Vgl. *Schimmer*, DuD 2006, 616, 617.
18 *Eggert*, DS 2009, 247, 252.

stellt noch keinen klar umgrenzten Mangel im rechtlichen Sinne dar. Und auch in technischer Hinsicht wäre eine solche zukünftige IT-Sicherheitslücke nicht hinreichend konkret, um einen Handlungsbedarf in der Produktentwicklung bei Inverkehrbringen zu begründen. Die Rückbeziehbarkeit einer möglicherweise erst in Zukunft auftretenden IT-Sicherheitslücke auf den Zeitpunkt der Übergabe, um daraus eine Pflicht zur Mängelbeseitigung herzuleiten, ist somit nicht möglich. Mit einer ähnlichen Begründung muss letztlich auch die Argumentation abgelehnt werden, dass ein bloßer (technischer) Mangelverdacht zu einem Mangel im Rechtssinne führen kann, wenn hierdurch die weitere Verwendbarkeit des Produkts nicht unerheblich erschwert wird. Denn auch hier muss der Grund für den Mangelverdacht bereits bei Abnahme bzw. Gefahrübergang veranlagt sein,[19] sodass abstrakte, in die Zukunft gerichtete Umstände genau so wenig wie bloße Vermutungen, dass ein Produkt zu einem späteren Zeitpunkt IT-sicherheitsbezogene Mängel aufweisen könnte, ausreichend sind, um zur Bejahung einer Gewährleistungspflicht zu gelangen. Ein gegenteiliges Ergebnis hätte zur Folge, dass die mit den Vorteilen der Nutzung auch einhergehende Betriebsgefahr auf den Hersteller bzw. Verkäufer abgewälzt würde.

Unabhängig von dieser Feststellung wurde in der Rechtsprechung schon in den 1990er-Jahren eine „Wartungspflicht" von Software zur Sicherung ihrer reibungslosen Funktionsfähigkeit diskutiert, denn der Nutzer habe ein berechtigtes Interesse daran, das Produkt mit seinem Erwerb auch für einen gewöhnlichen und der Preisklasse des Produkts angemessenen Lebenszyklus nutzen zu können.[20] Fraglich ist, wie weit eine solche Wartungspflicht – als vertragliche Nebenpflicht verstanden – inhaltlich reicht und für welche Dauer sie einschlägig wäre. Fest steht, dass ein Hersteller verpflichtet ist, Ersatzteile für das von ihm vertriebene Produkt auch über den Zeitraum einer Verjährung der Gewährleistung hinaus zu produzieren[21] – insbesondere auch gesetzt den Fall, dass das Produkt keinen anfänglichen Mangel aufwies. Zwar handelt es sich bei IT-sicherheitsbezogenen Softwareupdates nicht um Ersatzteile im materiellen Sinn, allerdings besteht eine rechtlich vergleichbare Situation: Zweck von Ersatzteilen ist, defekte Teile eines Produkts zu ersetzen. Zwar ist ein Produkt mit nicht mehr zeitgemäßer und damit unsicherer Software nicht an sich defekt, da es im Rahmen seiner bestimmungsgemäßen Verwendung noch betrieben werden kann. Jedoch können erhebliche IT-Sicherheitsbedenken bei einem weiteren Betrieb des Produkts den Nutzer durchaus dazu zwingen, dieses nicht mehr zu verwenden, sodass das erhöhte Betriebsrisiko im Endeffekt einem nach Gefahrübergang bzw. Abnahme eingetretenen Defekt und somit einem Mangel gleichkommt.[22] Dieses Ergebnis führt jedoch nicht dazu, dass der Produktverantwortliche in jedem Falle auch die Kosten für IT-sicherheitsbezogene Softwareupdates zu tragen hat – schon deshalb, weil der Hersteller auch zur Bereitstellung von Ersatzteilen außerhalb der Gewährleistung grds. eine Vergütung verlangen kann.[23] Dies entspricht der damit verbundenen wirtschaftlichen Verteilung von Nutzen und Betriebsgefahr eines Produkts.

Fraglich ist, für welchen Zeitraum eine nebenvertragliche Wartungspflicht des Herstellers in Form von kostenpflichtigen Softwareupdates besteht. Für den Kauf eines „Verwaltungsprogramms" bspw. ist von einer Instandhaltungspflicht mindestens für den Zeitraum, innerhalb dessen die Software noch auf dem allgemein zugänglichen Markt angeboten wird, auszugehen. Darüber hinaus soll, damit auch der zeitlich letzte Erwerber eines Produkts, bevor es vom Markt genommen wird, einen angemessenen Nutzen aus seiner Investition ziehen kann, eine Wartungsfrist von weiteren fünf Jahren als interessengerecht gelten.[24] Grds. wird eine solche Frist auch für übrige softwarebetriebene Produkte angemessen sein. Dennoch ist, auch im Hinblick auf das Alter der Entscheidung von 1999, zu überlegen, ob diese Frist auszudehnen ist: Nicht nur, dass Software einen immer größeren Stellenwert in Betriebsabläufen einnimmt; auch die immer weitere Vernetzung sorgt für Vulnerabilitäten, die vor zwanzig Jahren noch nicht denkbar gewesen sind. Nicht zuletzt dürften hochpreisige Produkte wie z. B. industrielle Fertigungsanlagen oder medizinische Geräte und mittlerweile wohl auch das vernetzte Automobil eine physische Lebensdauer aufweisen, die weit über einer Softwarelebensdauer ohne Updates liegt.

2.2 Pflichten aus Dauerschuldverhältnissen, insbesondere dem Mietvertragsrecht

Moderne Vertriebskonzepte sehen mittlerweile immer weniger vor, dass Software als solche gekauft bzw. hergestellt und dem Kunden überlassen wird, sondern stellen die dauerhafte Nutzung eines Computerprogramms in Serviceverträge ein, die auch die regelmäßige Produktpflege umfassen. Dies gilt vor allem für komplexe eingebettete Systeme z. B. aus dem Bereich Industrie 4.0. Unabhängig von der Frage, wie die Vertragstypologisierung eines solchen Dauerschuldverhältnisses im Einzelfall aussieht – z. B. in der Form eines Miet- oder Pachtvertrages, oder eines typengemischten Vertrages, der unterschiedliche Vertragstypen und damit einhergehende Pflichten nach den in der jeweiligen Vereinbarung getroffenen Schwerpunkten bestimmt[25] – ist die Rechtslage für diesen Fall klarer als für das Kauf- oder Werkvertragsrecht.

Das Mietrecht als Ausgangspunkt genommen liegt ein Mangel gem. § 536 Abs. 1 BGB dann vor, wenn die Gebrauchstauglichkeit der Mietsache zur Zeit ihrer Überlassung aufgehoben oder gemindert ist. Selbiges gilt, wenn sich während der Mietzeit ein entsprechender Mangel zeigt. Ein Mangel ist jede nachteilige Abweichung des tatsächlichen Zustands von dem vertraglich vereinbarten Zustand.[26] Eine IT-Sicherheitslücke der gemieteten Software ist eine für den Mieter nachteilige Abweichung des tatsächlichen Zustands von dem vertraglich vereinbarten. Zwar ist es zumeist möglich, das Produkt trotz der Sicherheitslücke noch zu verwenden, sodass die eigentliche, hieraus resultierende Gebrauchsbeeinträchtigung erst bei einem durch die Sicherheitslücke kausal verursachten Angriff von außen auftritt. Jedoch lässt sich aus den mietvertraglichen Pflichten gem. § 535 Abs. 1 S. 2 BGB eine Instandhaltungspflicht ableiten, einen angemessenen Schutz vor von außen kommenden Störungen zu gewährleis-

19 BGH NJW 1972, 1462, 1462 f.; für eine Übertragbarkeit des Mangelverdachts auch auf das Werkvertragsrecht *Kleefisch/Durynek*, NJOZ 2018, 121, 131.

20 BGH NJW 1993, 3144, 3145; LG Köln NJW-RR 1999, 1285, 1286.

21 LG Köln NJW-RR 1999, 1285, 1286; AG Rüsselsheim DAR 2004, 280.

22 Zur Mangelhaftigkeit aufgrund fehlender Betriebssicherheit BGH NJW 2010, 2426, 2429.

23 Speziell für Software LG Köln NJW-RR 1999, 1285, 1286.

24 LG Köln NJW-RR 1999, 1285, 1286.

25 BGH NJW 2007, 2394, 2395; *Gehrlein* in: BeckOKBGB, § 311, Rn. 21.

26 Dazu BGH NJW 2000, 1714, 1715; BGH NJW 2005, 2152; BGH NJW 2010, 3152; BGH NJW 2011, 514, 515.

ten.[27] Dazu muss der Vermieter Vorsorgemaßnahmen treffen, um Eingriffe in die Rechte des Mieters zu vermeiden.[28] Während der Gebrauchsüberlassung eintretende IT-Sicherheitslücken sind im Dauerschuldverhältnis folglich durch entsprechende Updates zu beheben, unabhängig davon, ob die Software oder das Embedded System durch den Hersteller oder durch einen Intermediär gegen Zahlung eines Entgelts zum Gebrauch überlassen wird. Nichts anderes gilt auch dann, wenn zwischen den Parteien kein Miet-, sondern ein Dienstvertrag geschlossen wurde, der die Instandhaltung einer Software bzw. eines Embedded Systems zum Gegenstand hat: Eine normative Auslegung ergibt hier, dass der Kunde für diesen Fall auch konkludent von einer Aufrechterhaltung der (IT)-sicheren Nutzbarkeit des Produkts ausgehen kann, selbst wenn dies nicht vereinbart wurde.

2.3 Ausblick: EU-Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte

Mit dem Entwurf einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellungstellung digitaler Inhalte[29] greift die EU das Thema Softwareaktualisierung unter anderem auch zu Zwecken der IT-Sicherheit gesetzlich auf. Der Anwendungsbereich des Rechtsakts umfasst grds. Verbraucherverträge über die Bereitstellung digitaler Inhalte in Austausch einer Geldleistung. Zentraler Anknüpfungspunkt für die IT-Sicherheit der digitalen Inhalte, die auch Softwareprodukte umfassen können, sind die Art. 6 ff. des Entwurfs. So wird festgeschrieben, dass für das Produkt, um vertragskonform zu sein, Softwareupdates zur Verfügung zu stellen sind (Art. 7), und darüber hinaus, dass das Produkt den Anforderungen seines gewöhnlichen Einsatzzwecks und den damit verbundenen Verbrauchererwartungen genügen muss, hierbei wird auch auf technische Standards und auf die Sicherheit Bezug genommen (Art. 8). In diesem Zusammenhang ist sicherzustellen, dass dem Verbraucher IT-Sicherheitsupdates zur Verfügung gestellt werden. Der Richtlinienentwurf enthält ferner Aussagen zur Bereitstellungsdauer: Entweder ergibt sich diese bereits aus dem Vertrag, oder aber sie richtet sich nach den Umständen, die der Verbraucher vernünftigerweise erwarten kann. In den Art. 11 ff. finden sich schließlich umfassende Regelungen zur Verantwortlichkeit und auch zur Beweislastverteilung. Die vorliegenden Regelungsvorschläge betreffen zwar zunächst nur den Verbraucherschutz, in rechtspolitischer Hinsicht ist aber zumindest zu vermuten, dass sie mittelfristig auch den B2B-Bereich beeinflussen werden.

3 Deliktische Rahmenbedingungen

Soweit es um die Bereitstellung IT-sicherheitsbezogener Softwareupdates geht, sind auch die deliktischen Rahmenbedingungen zu beachten. Eine herstellerseitige Verantwortlichkeit gem. § 1 Abs. 1 ProdHaftG scheidet für den vorliegenden Fall zwar bereits mangels eine Fehlers gem. § 3 ProdHaftG aus, da die Software bei Inverkehrbringen dem Stand der Technik genügte. Jedoch könnte aus den Grundsätzen der deliktsrechtlichen Produzentenhaftung gem. § 823 Abs. 1 BGB eine Produktbeobachtungspflicht erwachsen, die nicht nur die Beobachtung auf seit Inverkehrgabe neu entstandene Schwachstellen umfasst, sondern auch deren Ausbesserung durch Bereitstellung entsprechender Softwareupdates beinhaltet.

Die Befolgung einer Pflicht zur Produktbeobachtung ist letztlich immer dann entscheidend, wenn Rechte oder Rechtsgüter i.S.d. § 823 Abs. 1 BGB (z. B. Leben, Gesundheit oder Eigentum) verletzt werden und festzustellen ist, ob gegen den Verantwortlichen ein Anspruch auf Schadensersatz besteht, er also rechtlich haftbar gemacht werden kann. Herleiten lässt sich die Produktbeobachtungspflicht aus der Tatsache, dass der Hersteller auch nach Inverkehrbringen eines Produkts weiterhin für dieses verantwortlich ist, da er auch die wirtschaftlichen Vorteile aus des-

27 LG Essen WuM 1998, 278; *Eisenschmid* in: Schmidt-Futterer, Mietrecht, § 535 BGB, Rn. 102.

28 BGH NJW 1987, 831, 833; *Hübner/Griesbach/Fuerst* in: Lindner-Figura/Oprée/Stellmann, Geschäftsraummiete, Rn. 93.

29 Die letzte Fassung des Gesetzentwurfs mit Stand vom 01.04.2019 ist abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7718_2019_INIT&from=EN (Stand: 05.04.2019).

sen Verbreitung zieht. Dementsprechend haftet er für Schäden, die bei IT-Sicherheitslücken kausal dadurch verursacht werden, dass Dritte (gezielt) in informatische Funktionsabläufe des Produkts eingreifen, wenn der Hersteller zumutbare Maßnahmen zum Schutz der Rechte und Rechtsgüter des Betroffenen unterlässt.[30]

In einem aktiven Sinne verstanden setzt die Produktbeobachtungspflicht voraus, dass sich der Hersteller über mögliche Gefahrenquellen umfassend[31] informiert.[32] Diese Pflicht ist auch auf solche Produkte anwendbar, die von vornherein fehlerfrei produziert wurden und sich erst im Laufe der Zeit durch neu eingetretene Umstände als potenziell gefährlich erweisen.[33] Gerade für die IT-Sicherheit gibt es für den Hersteller vielzählige Möglichkeiten, sich zu informieren, so z. B. durch Kundenbefragungen, Nutzerfeedback, Analysetools, Behördeninformationen, Newsletter, Mailinglisten, CERTs/PSIRTs, Herstellernetzwerke, Webrecherche, Konferenzen, Fachmagazine und eigenständige Überprüfungen.

Ebenso muss der Hersteller sämtliche zumutbaren Maßnahmen zur Verhinderung evtl. eintretender Gefahren ergreifen.[34] Die bloße Wirkungslosigkeit eines Produkts kann schon ausreichend sein.[35] Gerade für die IT-Sicherheit sind in diesem Zusammenhang konkretisierende rechtliche Vorgaben aber rar gesät, da es noch an der entsprechenden Rechtsprechung fehlt, die Leitlinien an die Hand gibt. Zumindest aber kann festgestellt werden, dass der Umfang der Produktbeobachtung von der Höhe des drohenden Schadens und der Zumutbarkeit der risikomindernden Maßnahmen durch den Hersteller abhängig ist.[36] Dabei gilt, dass je höher und wahrscheinlicher ein Schaden infolge der IT-Sicherheitslücke ist, umso eher eine schnelle und umfassende Reaktion des Herstellers zu empfehlen ist. Für die Bestimmung der Dauer einer Produktbeobachtung können zudem Parallelen zur vertraglichen Nebenpflicht gezogen werden, denn die Produktbeobachtung endet nicht mit dem Abschluss der Herstellung oder dem Vertrieb des Produkts, sondern kann bis zum Zeitpunkt seiner erwarteten Entsorgung fortgelten.[37] Auch hier gilt wieder: Professionell eingesetzte und hochwertige Produkte aus dem B2B-Bereich ziehen umfassende Produktbeobachtungspflichten des Herstellers auch für die IT-Sicherheit nach sich. Als Orientierungswert dürften hier die dem Hersteller vorliegenden Zahlen zur maximalen Lebensdauer seiner Produkte bei Kunden dienen.

Falls der Hersteller im Rahmen seiner Produktbeobachtungspflicht eine IT-Sicherheitslücke feststellt, steht ihm ein abgestufter Maßnahmenkatalog zur Verfügung: Zunächst trifft den Hersteller gegenüber Verkäufer und Nutzer eine Warnpflicht.[38] Ob darüber hinaus eine Pflicht zur Beseitigung des IT-Sicherheitsmangels besteht, ist einzelfallabhängig. Zwar ist der Hersteller gehalten, Gefahren effektiv zu beseitigen – das bedeutet jedoch nicht, dass (auch in Abgrenzung des vertraglichen Äquivalenz- vom deliktischen Integritätsinteresse) für jeden Fall das Produkt nachgebessert werden muss oder gar ein neues Produkt zu liefern ist. Eine Nachbesserungspflicht besteht vielmehr nur dann, wenn die Gefahr nicht auf anderem Wege beseitigt werden kann.[39] Gerade für den Fall von IT-Sicherheitslücken dürfte die herstellerseitige Warnung zur Gefahrbeseitigung allein oftmals nicht ausreichen, sodass hier im Rahmen der Produktbeobachtung regelmäßig von weiteren Maßnahmen auszugehen sein wird, die auch die Bereitstellung (nicht zwingend kostenloser) IT-sicherheitsbezogener Softwareupdates umfassen können.

4 Fazit

Auch wenn dies nicht immer deutlich aus dem Gesetz hervorgeht, unterliegen Hersteller und Anbieter von IT-Produkten umfassenden Verpflichtungen im Hinblick auf die Aufrechterhaltung der IT-Sicherheit. Soweit gesonderte vertragliche Vereinbarungen getroffen wurden, eine anfängliche Schwachstelle vorliegt oder aber das IT-Produkt im Rahmen eines Dauerschuldverhältnisses zur Verfügung gestellt wird, lässt sich eine IT-sicherheitsbezogene Pflicht zur Bereitstellung von Softwareupdates ohne weitere Probleme herleiten. Rechtlich schwieriger zu beurteilen ist der Fall, wenn die Schwachstelle bei einem Produkt, das bei seiner Inverkehrgabe einwandfrei war, erst infolge der weiteren technischen Entwicklung auftritt, da für diesen Fall die kauf- und werkvertraglichen Mängelgewährleistungspflichten nicht eingreifen. Über das Konstrukt einer vertraglichen Nebenpflicht lässt sich aber auch für diesen Fall eine Pflicht zur Bereitstellung kostenpflichtiger IT-Sicherheitsupdates durch den Hersteller ableiten. Zudem trifft den Hersteller auch außerhalb des vertraglichen Rahmens eine umfassende deliktische Produktbeobachtungspflicht im Hinblick auf die IT-Sicherheit, die die Bereitstellung IT-sicherheitsbezogener Softwareupdates umfassen kann.

Wo einerseits somit zumindest grundlegende rechtliche Klarheit über die Pflichtigkeit herrscht, stellt sich andererseits die Frage, wie weit deren jeweiliger Umfang zu bemessen ist. Da auch hier bei Fehlen gesonderter vertraglicher Absprachen keine gesetzlichen Klarstellungen vorhanden sind, ist die Reichweite der Pflichten durch Auslegung zu ermitteln. An dieser Stelle ergibt sich das Problem, dass es an einschlägiger Rechtsprechung und insbesondere an Präzedenzfällen zur IT-Sicherheit mangelt, sodass eine zweifelsfreie Bestimmung der jeweiligen Verantwortlichkeitsmaßstäbe nicht ohne Weiteres möglich ist. Herstellern und Anbietern von IT-Produkten ist zurzeit deshalb zu raten, soweit möglich Analogien zu vergleichbaren Produkten und Fällen zu ziehen, bis der Rechtsrahmen zum Umfang der softwarebezogenen IT-Sicherheitspflichtigkeit weiter konkretisiert wurde. Dass hiervon in absehbarer Zeit auszugehen ist, wird unter anderem auch durch die entsprechende Rechtsetzung auf EU-Ebene deutlich: Wo der Entwurf einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte zunächst nur auf den Verbraucherbereich zugeschnitten ist, werden mit dem EU Cybersecurity Act zeitgleich Vorgaben getroffen, die nicht nur branchenübergreifend sind, sondern zugleich auch unterschiedlichste Einsatzszenarien von IT berücksichtigen. Es ist somit nur eine Frage der Zeit, bis auch das Thema IT-Sicherheitsupdates im B2B-Segment juristisch aufgegriffen und weiter konkretisiert wird.

30 BGH NJW 1990, 1236, 1237.
31 BGH NJW 1981, 1606, 1608.
32 BGH NJW 1981, 1606, 1607 f.
33 BGH NJW 1981, 1606, 1607 f.; BGH GRUR 1987, 191, 192.
34 RGZ 163, 21, 26.
35 BGH NJW 1981, 1603, 1604.
36 *Förster* in: BeckOKBGB, § 823, Rn. 734; *Wagner* in: MüKoBGB, § 823, Rn. 838.
37 *Gesmann-Nuissl/Wenzel*, NJW 2004, 117, 118.
38 BGH NJW 1981, 1603, 1604; *Förster* in: BeckOKBGB, § 823, Rn. 740.
39 *Rockstroh/Kunkel*, MMR 2017, 77, 81; *Foerste* in: Foerste/Graf von Westphalen, Produkthaftungshandbuch, § 24, Rn. 340 ff.