Aktenzeichen: Pet 4-19-07-2263-002532

Der Deutsche Bundestag hat die Petition am 01.12.2022 abschließend beraten und beschlossen:

Das Petitionsverfahren abzuschließen,
- weil dem Anliegen teilweise entsprochen worden ist.

Begründung

Mit der Petition wird gefordert, die Gewährleistung für vernetzte elektronische Geräte so auszuweiten, dass Hersteller (nicht Verkäufer) verpflichtet sind, mindestens fünf Jahre ab Markteinführung eines Modells und mindestens zwei Jahre ab Erstverkauf des Gerätes alle Geräte dieses Typs unentgeltlich und regelmäßig mit Sicherheitsupdates auf dem aktuellen Stand der Technik zu versorgen.
Zur Begründung der Petition wird im Wesentlichen vorgetragen, dass immer mehr technische Geräte nicht nur Chips enthielten, die sie zu Minicomputern machten, sondern auch Kommunikationsschnittstellen, über die sie mit anderen Geräten und Netzwerken verbunden werden könnten. Viele Geräte benötigten sogar eine gelegentliche oder ständige Internetverbindung, um nutzbar zu sein. Dies diene zunehmend der Koordination und Steuerung von Geräten untereinander, d. h. sie bilden das sogenannte „Internet of Things“.
Jedes derart vernetzte Gerät sei der potentiellen Gefahr ausgesetzt, von außerhalb nicht nur kontaktiert, sondern angegriffen zu werden. Viele Angriffe erfolgten automatisiert. Dabei nutzten praktisch alle Angriffe Schwachstellen im Design oder der Implementierung der Betriebssoftware, seltener der Hardware. Sobald diese bekannt und dokumentiert seien, könnten Hersteller bzw. deren Zulieferer in nahezu allen Fällen zeitnah mit zumutbarem Aufwand Gegenmaßnahmen entwickeln. Im eigenen Interesse täten sie dies in der Regel auch, verwendeten die Lösungen allerdings häufig nur für zukünftige Produkte, die auf derselben Technik aufbauten.

Die meisten vernetzten Geräte würden als Einmalinvestition beworben und verkauft, also auch keine Pflege durch die Hersteller erhalten. Das verringere für diese die Kosten und die Attraktivität von Nachfolgemodellen. Ein Hersteller, der aktive Produktpflege betreibe, riskiere also zumindest kurz- bis mittelfristig einen Wettbewerbsnachteil. Daher sei der Gesetzgeber gefordert, regulierend einzugreifen. Die Petition solle einen Beitrag zu besserem Datenschutz und mehr persönlicher und öffentlicher Sicherheit leisten.

Die Eingabe wurde als öffentliche Petition auf der Internetseite des Deutschen Bundestages eingestellt und dort diskutiert. Sie wurde durch 125 Mitzeichnungen unterstützt. Außerdem gingen 12 Diskussionsbeiträge ein.

Der Petitionsausschuss hat der Bundesregierung Gelegenheit gegeben, ihre Haltung zu der Eingabe darzulegen. Darüber hinaus hat der Petitionsausschuss in der 19. Wahlperiode nach § 109 Absatz 1 Satz 2 der Geschäftsordnung des Deutschen Bundestages eine Stellungnahme des Ausschuss für Inneres und Heimat des Deutschen Bundestages eingeholt, dem die Anträge der Fraktion der FDP „Smart Germany – Bundesministerium für Digitalisierung etablieren“ (Bundestags-Drucksache 19/9929) und „Digitalisierung ernst nehmen – IT-Sicherheit stärken“ (Bundestags-Drucksache 19/7698) sowie der Antrag der Fraktion von BÜNDNIS 90/DIE GRÜNEN „Offen für die Zukunft – Offene Standards für eine gerechte und gemeinwohlorientierte Gestaltung der Digitalisierung nutzen“ (Bundestags-Drucksache 19/7589) vorlagen. Der Ausschuss für Inneres und Heimat hat die Petition in seine Beratungen einbezogen. Nach der Beschlussempfehlung und des Berichts des Ausschusses (Bundestags-Drucksache 19/13601) sind die Anträge mehrheitlich abgelehnt worden.

Das Ergebnis der parlamentarischen Prüfung lässt sich unter Einbeziehung der seitens der Bundesregierung sowie des zuständigen Fachausschusses angeführten Aspekte wie folgt zusammenfassen:

Der Ausschuss weist zunächst darauf hin, dass bereits nach geltendem Kaufvertragsrecht ein Gewährleistungsanspruch des Käufers gegen den Verkäufer bestehen kann, wenn beim Kauf eines vernetzten elektronischen Geräts die darauf installierte Software Sicherheitslücken aufweist. Zu den vertragstypischen Pflichten bei einem Kaufvertrag gehört es, dass der Verkäufer dem Käufer die Sache frei von Sach und Rechtsmängeln überträgt (vgl. § 433 Absatz 1 Satz 2 des Bürgerlichen Gesetzbuches [BGB]). Eine Sache

ist dann (sach-)mangelhaft, wenn sie bei Gefahrübergang nicht die vereinbarte Beschaffenheit hat oder aber – wenn keine Vereinbarungen getroffen wurden – sich nicht für die gewöhnliche Verwendung eignet oder nicht die für Sachen dieser Art übliche Beschaffenheit aufweist (vgl. § 434 Absatz 1 BGB).

Die Rechtsprechung nimmt einen Sachmangel unter anderem dann an, wenn die Kaufsache die Anforderungen der maßgeblichen Sicherheitsbestimmungen nicht einhält oder wenn, gemessen am jeweiligen Entwicklungsstand des Produkts, der Zustand der Kaufsache nicht dem Stand der Technik entspricht. Ein Mangel am Software-Produkt kann auch im Bestehen vermeidbarer Sicherheitslücken liegen, die etwa einen Virenbefall ermöglichen.

Maßgeblicher Zeitpunkt für die Pflicht des Verkäufers, dem Käufer die Kaufsache frei von Mängeln zu verschaffen, ist der Gefahrübergang (vgl. § 434 Absatz 1 Satz 1 BGB). Dies ist in der Regel der Zeitpunkt, in dem die Kaufsache an den Käufer übergeben wird (vgl. § 446 Absatz 1 BGB). Ist die Software eines gekauften Geräts bei Gefahrübergang mangelhaft, stehen dem Käufer gegen den Verkäufer vertragliche Ansprüche (Gewährleistungsrechte) zu. Diese sind in erster Linie auf die Beseitigung des Mangels gerichtet und umfassen auch Schadensersatz für den Fall, dass der Verkäufer den Mangel verschuldet hat (vgl. §§ 437, 439, 440, 441, 323, 280, 281, 276 BGB). Die Ansprüche auf Gewährleistung unterliegen grundsätzlich einer zweijährigen Verjährungsfrist, die mit der Ablieferung der Kaufsache an den Käufer zu laufen beginnt.

Mit dem Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags vom 25. Juni 2021 und dem Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 25. Juni 2021 sind Aktualisierungspflichten für Verträge über den Verkauf von Waren mit digitalen Elementen und für Verträge über die Bereitstellung digitaler Produkte eingeführt worden. Seit dem 1. Januar 2022 haben danach Verbraucher, die von einem Unternehmer/Verkäufer eine Ware mit digitalen Elementen (beispielsweise ein Notebook, Smartphone oder intelligente Haustechnik) oder ein digitales Produkt (etwa eine App oder sonstige Software) erwerben, einen Anspruch auf die Bereitstellung von Software-Aktualisierungen, die für den Erhalt der

Vertragsmäßigkeit der Ware/des digitalen Produkts erforderlich sind (§§ 327f, 475b Absatz 4 BGB).

Von der Aktualisierungsverpflichtung sind insbesondere auch Sicherheitsaktualisierungen umfasst. Der Unternehmer/Verkäufer ist verpflichtet, die Schutzmaßnahmen zu treffen oder treffen zu lassen, die nach dem Stand der Technik geeignet und erforderlich sind, um die digitalen Elemente vor einem unberechtigten Zugriff Dritter auf Daten oder Funktionen zu schützen (vgl. Entwurf der Bundesregierung für ein Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags, Bundestagsdrucksache 19/27424, Seite 33). Die Updateverpflichtung besteht für den Zeitraum, in dem die Verbraucherin oder der Verbraucher Aktualisierungen aufgrund der Art und des Zwecks der Ware oder des digitalen Produkts und unter Berücksichtigung der Umstände erwarten kann (§ 327f Absatz 1 Satz 3 Nummer 2, 475b Absatz 4 Nummer 2 BGB).

Adressat der Verpflichtung zur Bereitstellung ist der Unternehmer, der dem Verbraucher die Ware mit digitalen Elementen oder das digitale Produkt verkauft oder sonst bereitgestellt hat. Die Aktualisierung muss der Unternehmer/Verkäufer dabei aber nicht selbst bereitstellen, sondern diese kann gemäß § 267 BGB grundsätzlich auch durch einen Dritten wie zum Beispiel den Hersteller geleistet werden.

Kommt ein Verkäufer einer bestehenden Aktualisierungsverpflichtung nicht nach, stellt dies einen Sachmangel/Produktmangel in Sinne von § 475b BGB/§ 327e BGB dar und der Verbraucher kann seine gesetzlichen Gewährleistungsrechte gegenüber dem Verkäufer geltend machen (das sind der primäre Anspruch auf Nacherfüllung in Gestalt der Nachbesserung/Reparatur oder der Ersatzlieferung sowie die sekundären Ansprüche auf Minderung, Rücktritt und Schadensersatz, vgl. § 437 BGB/§ 327i BGB).

Da der Verbraucher sein Recht auf Bereitstellung von Aktualisierungen gegenüber seinem Vertragspartner (Unternehmer/Verkäufer) im Rahmen der Ausübung seiner Gewährleistungsrechte geltend machen kann, erscheint ein zusätzlicher Anspruch gegen den Hersteller im Rahmen der Gewährleistung aus Sicht des Petitionsausschusses nicht erforderlich. Ansprüche auf Gewährleistung, die eine verschuldensunabhängige Einstandspflicht begründen, sieht das deutsche Recht zudem bisher nur gegenüber dem jeweiligen Vertragspartner vor. Die Einführung eines Gewährleistungsanspruchs gegen

den Hersteller, zu dem seitens des Verbrauchers grundsätzlich keine Vertragsbeziehung besteht, wäre daher im deutschen Recht systemfremd.
Gleichwohl ist der Endnutzer auch im Verhältnis zum Hersteller eines vernetzten elektronischen Gerätes nach geltendem Recht geschützt: Unabhängig von der Vertragsbeziehung zwischen dem Käufer und dem Verkäufer der Software können deliktische Ansprüche des Endnutzers gegen den Softwarehersteller bestehen, wenn ein Produktfehler im Sinne des Produkthaftungsgesetzes (ProdHaftG) vorliegt bzw. der Hersteller bestimmte Verkehrssicherungspflichten schuldhaft verletzt hat.
Das ProdHaftG setzt die europäische Richtlinie 85/374/EWG vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (Produkthaftungsrichtlinie) um. Es normiert die verschuldensunabhängige Haftung des Herstellers für Produktfehler.
Nach allgemeiner Auffassung gilt auch Software grundsätzlich als Produkt im Sinne des ProdHaftG, wenn Sie auf einem Datenträger, d. h. CD-ROM, Computerfestplatte etc., verkörpert ist. Dies dürfte selbst dann gelten, wenn die Software über das Internet (etwa mittels Smartphone-App) heruntergeladen wird, da es auch insoweit zu einer Verkörperung auf dem Endgerät kommt. Die Software ist fehlerhaft, wenn sie nicht die Sicherheit gewährleistet, die berechtigterweise erwartet werden kann (vgl. § 3 ProdHaftG). Der gebotene Sicherheitsstandard richtet sich objektiv nach der herrschenden Verkehrsauffassung. Wird bei der Softwareherstellung bereits konzeptionell der Stand von Wissenschaft und Technik (also das realisierbare Ergebnis wissenschaftlicher Forschung) nicht beachtet, z. B. indem erkennbare Sicherheitslücken bestehen, liegt ein Produktfehler vor. Derzeit ist die Haftung nach dem ProdHaftG allerdings ausgeschlossen, wenn die Fehlerhaftigkeit des Produkts im Zeitpunkt der Inverkehrgabe nach Stand von Wissenschaft und Technik nicht erkannt werden konnte (§ 1 Abs. 2 Nr. 5 ProdHaftG, sog. Entwicklungsfehler). Insoweit bestehen keine Unterschiede zur Haftung für analoge Produkte.
Ist die Software fehlerhaft im Sinne des ProdHaftG, haftet der Hersteller grundsätzlich bei Tötung, Körper- oder Gesundheitsverletzung und Sachbeschädigung. Bei der Sachbeschädigung ist zu beachten, dass nur solche Schäden zu ersetzen sind, die nicht am fehlerhaften Produkt selbst, sondern an sonstigen privaten Sachen des Endnutzers

entstanden sind. Daher kann ein Schadensersatzanspruch unter Umständen auch dann gegeben sein, wenn virenverseuchte oder sonst fehlerhafte Software Hardwarekomponenten beschädigt oder zu einem Datenverlust führt.
Die Produkthaftungsrichtlinie regelt den Gestaltungsspielraum des nationalen Gesetzgebers abschließend; die Richtlinie ist hinsichtlich der Gefährdungshaftung des Herstellers vollharmonisierend. Anpassungen des Produkthaftungsregimes sind daher grundsätzlich nur auf europäischer Ebene möglich.
In diesem Zusammenhang weist der Petitionsausschuss darauf hin, dass die Europäische Kommission im Rahmen ihrer Initiative „Zivilrechtliche Haftung – Anpassung der Haftungsregeln an das digitale Zeitalter und an die Entwicklungen im Bereich der künstlichen Intelligenz“ angekündigt hat, im dritten Quartal 2022 einen Vorschlag zur Revision der Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (Produkthaftungsrichtlinie) sowie einen Vorschlag über die Einführung eines neuen Rechtsakts zur Haftung bei Künstlicher Intelligenz zu unterbreiten. In diesem Kontext hat die Bundesregierung gegenüber der Europäischen Kommission die Auffassung vertreten, dass Hersteller während der üblichen Nutzungszeit Updates bereitstellen sollten, es aber noch weiterer Prüfungen bedürfe, welches der geeignete unionsrechtliche Regelungsstandort für eine solche Verpflichtung sei.
Die Rechtsprechung hat bereits jetzt den Herstellern über die sog. Produzentenhaftung hinaus weitere (Sorgfalts-)Pflichten auferlegt. Die Produzentenhaftung knüpft an die schuldhafte Verletzung von Verkehrssicherungspflichten an: Der Hersteller ist verpflichtet, im Rahmen des ihm Zumutbaren alle Gefahren abzuwenden, die sich bei der Benutzung seines Produktes, d.h. vorliegend der Software, ergeben können. Verkehrssicherungspflichtverletzungen sind denkbar bei der Konstruktion (fehlerhafte Programmierung), bei der Fabrikation (z.B. fehlerhafte Virenprüfung; fehlerhafte Übertragung) und bei der Produktbeobachtung (unterlassene Marktbeobachtung bzw. Warnhinweise/Rückrufe).
Einerseits muss der Hersteller sicherstellen, dass bei der Programmierung der Stand von Wissenschaft und Technik beachtet wird. Es ist zu fragen, ob unter Berücksichtigung dieses Standes der Hersteller bei Inverkehrbringen des Programms z. B. Sicherheitslücken

hätte kennen müssen. Anderseits muss der Hersteller sein Produkt auch aktiv auf dem Markt und im täglichen Einsatz beobachten (sog. Produktbeobachtungspflicht). Die Anforderungen an die Produktbeobachtungspflicht steigen u.a. mit dem Gefährdungspotential sowie mit der Komplexität des Produktes und der damit einhergehenden Fehleranfälligkeit. D.h., je schadensträchtiger die Software ist, desto höher sind grundsätzlich die Verkehrssicherungspflichten des Herstellers. Neben eigenen Erkenntnissen und Tests muss der Hersteller etwa auch mediale Berichte beachten, Hinweisen von externen Experten nachgehen und vor etwaigen Sicherheitslücken in Softwareprogrammen warnen. Verstößt der Hersteller schuldhaft gegen die o. g. Verkehrssicherungspflichten, haftet er.

Ob sich aus diesen Grundsätzen für den Hersteller auch die Pflicht ergeben kann, Sicherheitsupdates bereitzustellen, ist anhand der Umstände des konkreten Einzelfalls zu entscheiden. In aller Regel dürfte der Hersteller aber bereits ein eigenes wirtschaftliches Interesse an derartigen Updates haben, um möglichen Haftungsansprüchen aufgrund von Sicherheitslücken vorzubeugen.

Darüber hinaus hat die Bundesregierung in den vergangenen Jahren die Hersteller bereits im Rahmen der IT-Sicherheitsgesetzgebung kontinuierlich weiter in die Pflicht genommen. So wurde etwa mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes in § 7 Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geregelt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Erfüllung seiner Aufgaben unter Nennung der Bezeichnung des Herstellers vor Sicherheitslücken in informationstechnischen Produkten oder Diensten warnen kann. Im Rahmen des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - Bundesgesetzblatt Teil I 2015 Nr. 31 24.07.2015 S. 1324) wurde in § 8b Absatz 6 BSIG geregelt, dass das BSI zum Schutz von Kritischen Infrastrukturen von Herstellern informationstechnischer Produkte und Systeme die Mitwirkung an der Störungsbeseitigung und -vermeidung verlangen kann. Eine vergleichbare Regelung enthält auch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (Bundesgesetzblatt Teil I 2017 Nr. 40

29.06.2017 S. 1885) in § 5a Absatz 6 BSIG. Danach kann das BSI im Rahmen eines Einsatzes der „Mobile Incident Response Teams“ (MIRTs) von Herstellern die Mitwirkung an der Wiederherstellung der IT Sicherheit oder Funktionsfähigkeit ihrer Produkte und Systeme verlangen.

Der Petitionsausschuss weist ergänzend darauf hin, dass sich die Koalitionsparteien des Deutschen Bundestages in dem Koalitionsvertrag für die 20. Legislaturperiode darauf verständigt haben, die digitalen Bürgerrechte und die IT-Sicherheit zu stärken. Danach ist u. a. beabsichtigt, dass Hersteller für Schäden haften, die fahrlässig durch IT Sicherheitslücken in ihren Produkten verursacht werden. (vgl. Koalitionsvertrag Rn. 435 ff.).

Unabhängig hiervon stellt der Ausschuss fest, dass nach der geltenden Rechtslage Verbraucher insbesondere einen Anspruch auf die Bereitstellung von Software-Aktualisierungen, die für den Erhalt der Vertragsmäßigkeit der Ware/des digitalen Produkts erforderlich sind, haben. Der mit der Petition vorgetragenen Forderung wird hierdurch bereits teilweise entsprochen. Ein darüber hinausgehender gesetzgeberischer Handlungsbedarf besteht nach Ansicht des Ausschusses nicht.

Der Petitionsausschuss empfiehlt deshalb, das Petitionsverfahren abzuschließen, weil dem Anliegen teilweise entsprochen worden ist.