Juni 2021
9. Jahrg.
84364
Seite 57–120

InTeR

Zeitschrift zum Innovations- und Technikrecht

2

dfv Mediengruppe · Frankfurt am Main

Dr. Gerhard Wiebe, Berlin*

IT-sicherheitsbezogene Pflichten von Herstellern smarter Produkte

Die Gesetzgebung reagiert auf die zunehmende Digitalisierung der Produktwelt – wenn auch zögerlich. Entsprechend gemächlich setzen sich die Hersteller smarter Produkte mit IT-Sicherheitspflichten auseinander. Für Verhaltenheit besteht jedoch kein Anlass: Sie treffen bereits de lege lata (mittelbare) IT-sicherheitsbezogene Herstellerpflichten, die dieser Beitrag in den Fokus rückt.

I. Einführung

Smarte Produkte finden unterbrochenen Einzug in den privaten Konsum, etwa als IoT-Verbraucherprodukte, ebenso wie in die gewerbliche Verwendung in Gestalt von vernetzten Maschinen im Rahmen der „Industrie 4.0". Schätzungsweise sollen mittlerweile über 40 Mrd. solcher integrierten Systeme im EU-Binnenmarkt im Umlauf sein.[1] Mit den neuen Eigenschaften dieser intelligenten, vernetzten Produkte gehen auch neue Risiken einher – namentlich Gefahren aufgrund von IT-Sicherheitslücken, wie beispielsweise Cyberangriffe. Bei diesen Produkten spielt folglich die IT-Sicherheit ebenso eine Rolle, wobei sie nicht mit der Produktsicherheit im klassischen Sinn gleichzusetzen ist.[2] Aufgrund dessen hat sich zur Unterscheidung das Wortpaar „Security" als Ausdruck für die IT-Sicherheit und „Safety" als Bezeichnung der Produktsicherheit etabliert.

Wie so häufig hinkt die Gesetzgebung bei der Adressierung neuer Gefahrenlagen hinterher. Doch die in Herstellerkreisen häufig anzutreffende Einschätzung, aus der aktuellen Rechtslage ließen sich keine IT-Sicherheitsanforderungen an smarte Produkte ableiten, erweist sich als Fehlannahme. Richtig ist: Eine allgemeine Herstellerpflicht zur Gewährleistung von IT-Sicherheit in Bezug auf smarte Produkte besteht (noch) nicht. Bei genauer Betrachtung ergeben sich aus dem bestehenden Produktsicherheits- und Produkthaftungsregime gleichwohl (mittelbare) IT-Sicherheitsvorgaben.

Der Beitrag zeichnet die im öffentlichen Produktsicherheitsrecht bestehenden, an Hersteller gerichteten IT-Sicherheitsanforderungen an smarte Produkte nach (IV.) und deckt etwaige Risiken bei auftretenden IT-Sicherheitslücken unter produkthaftungsrechtlichen Gesichtspunkten auf (V.). In gebotener Kürze soll vorab der Begriff „IT-Sicherheit" im rechtlichen Sinne konturiert (II.) und Software als Bezugspunkt für IT-Sicherheit im Anwendungsbereich des Produktrechts verortet werden (III.). Der Beitrag endet schließlich mit einem Ausblick und Fazit (VI.).

II. IT-Sicherheit im rechtlichen Sinne

Eine Legaldefinition des Begriffs IT-Sicherheit findet sich in § 2 Abs. 2 BSIG. Sie bedeutet die Einhaltung bestimmter 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. Zu den Schutzgütern der IT-Sicherheit gehören die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme sowie der dort vorgehaltenen Daten.[3] IT-Sicherheit ist daher nicht identisch mit der Produktsicherheit, auch wenn die IT-Sicherheit, wie zu zeigen ist, die Produktsicherheit zu beeinflussen vermag.

III. Software als Bestandteil vernetzter Produkte

Lange Zeit war umstritten, ob Software den Rechtsbegriff des Produkts erfüllt und damit vom Anwendungsbereich des Produktrechts erfasst wird. Jedenfalls unterfällt sog. embedded Software bzw. Firmware als integraler Bestandteil eines körperlichen Gegenstandes dem Produktbegriff des § 2 Nr. 22 ProdSG und des § 2 ProdHaftG.[4] Derweil ist unter Verweis auf den Bericht der EU-Kommission über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung[5] eine Tendenz zu vernehmen, wonach auch unverkörperte „stand alone" Software als Produkt einzustufen ist.[6] Ungeachtet einer Verkörperung besitzt Software als Bezugspunkt für IT-Sicherheit(-slücken) und Einfallstor für Cyberangriffe mithin produkt(haftungs)rechtliche Relevanz.

IV. IT-Sicherheitsanforderungen im Maschinen- und Niederspannungsrecht

Im Folgenden gilt es, unmittelbare (1.) oder indirekte (2.) IT-Sicherheitsanforderungen im Maschinen- und Niederspannungsrecht zu identifizieren. Diese beiden Teilgebiete des öffentlichen Produktsicherheitsrechts bilden nämlich den Rechtsrahmen für eine Vielzahl smarter Produkte.

1. Ausdrückliche IT-Sicherheitsanforderungen

Die Suche nach ausdrücklichen IT-Sicherheitsanforderungen im Maschinen- und Niederspannungsrecht erweist sich als vergeblich. Schließlich zählt die IT-Sicherheit nicht zu den Schutzzielen der Maschinen-[7] bzw. Niederspannungsrichtlinie[8]. Sie bezwecken vielmehr primär den Schutz von Leben und Gesundheit.[9] Gleiches gilt für die allgemeine Produktsicherheitsrichtlinie[10] bzw. das ProdSG und die Funkanlagenrichtlinie[11] resp. das FuAG als horizontale Rechtsakte. Die Funkanlagenrichtlinie richtet im Zusam-

---

* Mehr über den Autor erfahren Sie auf Seite III.

1 KOM (2007) 243 final, 15.

2 *Bräutigam/Klindt,* NJW 2015, 1137, 1141 f.

3 *Rockstroh/Kunkel,* MMR 2017, 77, 78.

4 *Wiebe,* NJW 2019, 625, 626; *Joggerst/Wendt,* InTeR 2021, 13, 14.

5 COM (2020) 64 final, 17.

6 *Wittbrodt,* InTeR 2020, 74, 76; *Joggerst/Wendt,* InTeR 2021, 13, 14.

7 Richtlinie 2006/42/EG.

8 Richtlinie 2014/35/EU.

9 Vgl. Art. 1 der Richtlinie 2014/35/EU und Erwägungsgrund (28) der Richtlinie 2006/42/EG.

10 Richtlinie 2001/95/EG.

11 Richtlinie 2014/53/EU.

menhang mit (eigenständiger) Software Vorgaben an den Hersteller (Art. 10 Abs. 8; Anhang V). Es handelt sich dabei jedoch nur um Informationspflichten, die keine materiellen IT-Sicherheitsanforderungen setzen.

2. Mittelbare IT-Sicherheitsanforderungen: Produktsicherheit durch IT-Sicherheit

IT-Sicherheitslücken, die eine in einem Produkt integrierte Software aufweist, können zu Lebens- und Gesundheitsgefährdungen führen. Beispielsweise kann ein Softwarefehler selbst eine gefährdende Produktfunktion auslösen oder ein unbefugter Dritter kann, eine IT-Sicherheitslücke ausnutzend, Zugriff über das Produkt erlangen und es lebens- bzw. gesundheitsgefährdend manipulieren. Die Herstellerpflicht, die Produktsicherheit zu gewährleisten, umfasst auch die Verpflichtung, dafür Sorge zu tragen, dass das Produkt aufgrund von IT-Sicherheitslücken nicht unsicher, d.h. lebens- bzw. gesundheitsgefährdend ist. Diese Herstellerpflicht gilt unabhängig von dem Kausalverlauf einer produktbezogenen Lebens- oder Gesundheitsgefährdung; auch durch Zwischenursachen, etwa in Form von Cyberangriffen, vermittelte Gefährdungen werden erfasst.[12] Daher müssen Hersteller ebenso mittelbare, IT-bedingte Gefährdungen für Leben und Gesundheit bei der Produktkonstruktion in den Blick nehmen. Diese Maßgabe zeigt sich etwa in der Maschinenrichtlinie, wenn dort im Anhang I Nr. 1.2.1. auf Fremdeinflüsse und den Defekt der Steuerungssoftware als mögliche Gefahrenauslöser Bezug genommen wird. In der Niederspannungsrichtlinie ließe sich dieses Verständnis etwa im Anhang I Nr. 3 verankern; diese Ziffer beschäftigt sich nämlich mit dem Schutz vor Gefahren, die durch äußere Einwirkungen auf elektrische Betriebsmittel entstehen können. Im Übrigen geht auch die EU-Kommission in dem oben erwähnten Bericht davon aus, dass sich das unionale Produktsicherheitskonzept jedenfalls mittelbar auf IT-Sicherheitsaspekte erstreckt.[13]

Im nicht harmonisierten Bereich lässt sich der mittelbare IT-Sicherheitsbezug aus § 3 Abs. 2 S. 2 Nr. 1 ProdSG herleiten. Danach ist die Eigenschaft des Produkts, wozu unter anderem die IT-Komponenten und die Internetfähigkeit zählen, bei der Beurteilung, ob das Produkt den Sicherheitsanforderungen entspricht, zu berücksichtigen. Zudem qualifiziert auch die zentrale Bundesoberbehörde für das Produktsicherheitsrecht, die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, mangelhafte Software als ernstliches Gefährdungsmerkmal bei Produkten.[14]

Aufgrund dessen müssen Hersteller trotz fehlender expliziter Anforderungen die IT-Sicherheit im Zuge des Konstruierens, bei der Gestaltung technischer Sicherheitsmaßnahmen und beim Instruieren zwecks Gewährleistung der Produktsicherheit beachten. Eine entsprechende Orientierungshilfe für die Einhaltung des Stands der Technik bieten etwa DIN SPEC 27072 „Informationstechnik – IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit", der europäische Standard ETSI EN 303 645 für IoT-Verbraucherprodukte oder die „Guidelines for Securing the Internet of Things" der Agentur der Europäischen Union für Cybersicherheit. Ferner können die Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits-(Cybersicherheits-)Aspekte (ISO/TR 22100-4) herangezogen werden.

V. IT-Sicherheitsanforderungen des Haftungsrechts: Herstellerpflichten und Haftungsrisiken

Ausdrückliche Haftungsregelungen für vernetzte Produkte wegen Cyberrisiken existieren (noch) nicht. Nichtsdestotrotz lassen sich aus dem allgemeinen zivilrechtlichen Haftungsregime, insbesondere aus der Produkthaftungsrichtlinie[15] bzw. dem ProdHaftG und der Produzentenhaftung gemäß § 823 Abs. 1 BGB IT-Sicherheitsanforderungen an smarte Produkte ableiten (3.). Eine eins-zu-eins Übertragung der produkthaftungsrechtlichen Grundsätze auf die Herstellerhaftung für IT-Sicherheitslücken kann dennoch nicht angenommen werden: Denn hinsichtlich der IT-Sicherheit als Schutzrichtung des Haftungsrechts (1.) und der genauen Grenzen der Herstellerverantwortung für Cyberangriffe (2.) herrscht noch keine abschließende rechtliche Klarheit.

1. IT-Sicherheit als Schutzrichtung des Haftungsrechts?

Der Hersteller haftet nur, wenn es zu Schäden an einem geschützten Rechtsgut, wie etwa Leib, Leben und Gesundheit sowie Eigentum, kommt. Dass eine IT-Sicherheitslücke bzw. ein Cyberangriff zu Schäden an einem dieser Rechtsgüter führen können, ist unschwer vorstellbar. So kann ein Dritter mittels einer Hackerattacke die Steuerung einer Maschine oder eines vernetzten Produkts an sich reißen und aufgrund manipulierter Funktionen den Maschinenführer bzw. den Produktverwender verletzen.[16] Auch das Eigentum des Inhabers der gekaperten Maschine kann beschädigt werden. Beispielsweise vermag ein Hackerangriff Schäden an anderen vernetzten Maschinen oder der von der Maschine hergestellten Produkte[17] auszulösen. Der durch einen Hackerangriff verursachte bloße Nutzungsausfall[18] oder die Beschädigung der kompromittierten Maschine selbst stellt lediglich unter engen Voraussetzungen (Stichwort „Weiterfresserschaden")[19] eine Eigentumsverletzung dar. Aus dem Blickwinkel des ProdHaftG kann eine Eigentumsverletzung im Übrigen nur angenommen werden, wenn es sich bei der geschädigten Sache um eine solche handelt, die nicht für gewerbliche Zwecke bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist (§ 1 Abs. 1 S. 2 ProdHaftG).

Uneinigkeit besteht bislang darüber, ob die Schutzgüter der IT-Sicherheit im oben unter II. genannten Sinn zu den Rechtsgütern des Haftungsrechts gehören. Einen Anknüpfungspunkt für die Erfassung der IT-Sicherheit bietet das Rechtsgut „Eigentum" in Gestalt des Datenträgers. Im rechtswissenschaftlichen Diskurs wird teilweise vertreten, dass ein Löschen oder eine Manipulation von Daten stets eine relevante Veränderung des Datenträgers selbst ist und damit eine Rechtsgutsverletzung darstellt.[20] Eine andere Ansicht verneint die Löschung und Manipulation von Daten als Eigentumsverletzung.[21] Die Rechtsprechung hat hierzu noch keine dezidierte Stellung bezogen.

12 *Bauer,* Das Recht des technischen Produkts, 2018, Rn. 342.
13 COM (2020) 64 final, 8.
14 Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Gefährliche Produkte 2018, 26.
15 Richtlinie 85/374/EWG.
16 *Raue,* NJW 2017, 1841 f.; *Wiebe,* NJW 2019, 625 f.; *Reusch,* BB 2019, 904 f.
17 Vgl. *Wagner,* in: MüKo, BGB, 8. Aufl. 2020, § 823 Rn. 287 ff.
18 *Wagner,* in: MüKo (Fn. 17), § 823 Rn. 279.
19 *Wagner,* in: MüKo (Fn. 17), § 823 Rn. 281 ff.
20 *Wagner,* in: MüKo (Fn. 17), § 823 Rn. 165.

2. Herstellerverantwortung trotz unmittelbarer Verursachung durch Dritte?

Mit der Frage, ob und inwieweit Hersteller für durch Cyberangriffe verursachte Schäden haften, hat sich die Rechtsprechung ebenso wenig befasst. Diesem Szenario liegt ein vorsätzlicher Missbrauch eines Produkts unter Ausnutzung von IT-Sicherheitslücken durch Dritte zugrunde. Prima vista mag man an dieser Stelle, d. h. beim Dazwischentreten eines missbräuchlichen Verhaltens eines Dritten, die Grenze der Herstellerverantwortung ziehen.[22] Bei genauerer Betrachtung lässt sich eine Herstellerverantwortung jedoch auch in der Situation nicht per se ausschließen. Denn das Deliktsrecht verlangt unter bestimmten Bedingungen ebenso das Ergreifen von Sicherheitsvorkehrungen gegen vorsätzliches Missbrauchsverhalten Dritter.[23] Dieses Erfordernis kann man im Produzenten- bzw. Produkthaftungsrecht insbesondere an zwei Stellen festmachen: Zum einen muss der Hersteller im Rahmen seiner Verkehrssicherungspflicht auch vorhersehbare Fehlanwendungen des Produkts im Zuge der Konstruktion berücksichtigen und entsprechende Sicherheitsmaßnahmen treffen, obgleich dies primär aus Sicht des befugten Produktverwenders zu geschehen hat.[24] Zum anderen bilden die „berechtigten Sicherheitserwartungen" den vom Hersteller zu erfüllenden Maßstab. Bei digitalen Produkten erstrecken sich die „berechtigten Sicherheitserwartungen" regelmäßig ebenso auf die IT-Sicherheit, da Vorkehrungen zur Resistenz gegen Cyberangriffe, die Schäden an geschützten Rechtsgütern verursachen können, aus Sicht eines Durchschnittsverwenders erwartet werden.[25] Schließlich eröffnen Hersteller mit der Inverkehrgabe von digitalen Produkten, denen solche Gefährdungsszenarien immanent sind, eine Gefahrenquelle, die Dritte ausnutzen können. Herstellern ist daher dringend zu raten, (Mindest-)Schutzmaßnahmen zur Abwehr von potenziell schadensstiftenden Hackerattacken vorzunehmen. Die Abwesenheit von jeglichen Vorkehrungen käme einem „Einladen" zur Vornahme von Sabotageakten gleich, sodass sich der Hersteller eine auf diesem Exponieren beruhende Schadensverursachung zurechnen lassen müsste.

Betreiber von „smart factories", in denen vernetzte Maschinen zum Einsatz kommen, werden freilich ebenfalls aufgrund arbeitsschutzrechtlicher Maßgaben (insb. auf Grundlage der BetrSichV) in die Pflicht genommen, um (IT-bedingte) Rechtsgutsverletzungen bei ihren Arbeitnehmern zu vermeiden. Es obliegt ihnen, einen Beitrag für die IT-Sicherheit der Maschinen und die cybersichere Nutzung zu leisten. So müssen sie etwa vom Hersteller zur Verfügung gestellte IT-Sicherheitsinformationen weiterleiten bzw. beachten sowie Software-Updates durchführen. Aufgrund dessen bietet es sich an, klare Risiko- und Verantwortungssphären zwischen Hersteller und Betreiber vertraglich festzulegen, um Streitigkeiten im Regressfall vorzubeugen. Flankierend lässt sich auch der Abschluss eines Software-Pflegevertrages für IT-Wartungsleistungen durch den Hersteller, sofern er solche erbringt, empfehlen.

3. Haftungsrechtliches Anforderungsprofil unter dem Aspekt der IT-Sicherheit

Trotz der angedeuteten Rechtsunsicherheiten in der haftungsrechtlichen Bewertung von Cyberattacken und den darin wurzelnden Rechtsgutsverletzungen tun Hersteller gut daran, IT-Sicherheit vorsorglich mitzudenken, um Haftungsrisiken von vornherein auszuschließen. Anforderungen an die IT-Sicherheit lassen sich im haftungsrechtlichen Pflichtenkanon, d. h. im Zuge der Konstruktion und Fabrikation (a), Instruktion (b) sowie bei der Produktbeobachtung und Gefahrabwendung (c), ausmachen.

a) IT-Sicherheit im Rahmen der Konstruktion und Fabrikation

Im Rahmen der Konstruktion und Fabrikation herrscht der Anforderungsmaßstab des Stands von Wissenschaft und Technik. Diesem strengen Maßstab unterfallen ebenfalls vernetzte Produkte bzw. Firmware. Wie oben angedeutet, sind digitale Produkte bzw. Firmware unter Beachtung dieses Maßstabs so zu designen und (Schutz-)Maßnahmen zu ergreifen, dass unberechtigte Einflussnahme durch Dritte und dadurch entstehende Gefährdungen für Leib, Leben und Eigentum verhindert werden können. Insoweit ist die Rede von „Security by Design". Zu etwaigen Maßnahmen gehört beispielsweise die Updatefähigkeit eines digitalen Produkts, um IT-Sicherheitslücken mittels nachträglicher Firmware-Updates beheben zu können.[26] Bei der Bestimmung des geltenden Sicherheitsmaßstabs gilt es, die bestehenden Vorgaben des IT-Sicherheitsrechts sowie die einschlägigen technischen Regelwerke, wie die oben unter IV. angeführten, zu beachten.

Der konkrete Umfang der Herstellerpflichten hinsichtlich der IT-Sicherheit zwecks Abwehr von Hackerangriffen hängt vom Einzelfall ab. Lenkende Kriterien für die Konturierung des Umfangs sind unter anderem das IT-sicherheitsbedingte Gefahrenpotenzial des vernetzten Produkts, die technische Realisierbarkeit und Zumutbarkeit, um IT-Sicherheitslücken (insb. unter Hinzuziehung technischer Regelwerke) zu schließen. Auch sind der Benutzerkreis und die Möglichkeit der Inpflichtnahme der Nutzer zu berücksichtigen; beim gewerblichen Gebrauch durch Fachleute darf der Hersteller eine größere Erfahrung und Kenntnis hinsichtlich IT-Eigenschutz verlangen als bei Endverbrauchern.[27] Ein hohes Sicherheitsniveau ist bei Maschinen zu fordern, die ihre Verwendung in sog. Kritischen Infrastrukturen[28] finden, weil dieses Einsatzfeld eine besondere Attraktivität für Cyberangriffe bietet, eine verstärkte Kritikalität aufweist und ein erhöhtes Schadenspotenzial besitzt. Eine absolute Sicherheit vor Fehlfunktionen infolge von Sabotageakten Dritter ist indes technisch weder dar-

21 Vgl. *Fritzsche,* in: BeckOK BGB, Hau/Poseck, § 90 Rn. 26.

22 *Rockstroh/Kunkel,* MMR 2017, 77, 78 f.; *Bräutigam/Klindt,* NJW 2015, 1137, 1142.

23 *Wittbrodt,* InTeR 2020, 74, 78; vgl. auch BGH, 19.12.1989 – VI ZR 182/89, NJW 1990, 1236, 1237; BGH, 6.3.1990 – VI ZR 246/89, NJW-RR 1990, 789, 790; *Wagner,* in: MüKo (Fn. 17), § 823 Rn. 432.

24 Siehe etwa *Wagner,* in: MüKo (Fn. 17), § 823 Rn. 485 f.; *Förster,* in: BeckOK BGB (Fn. 21), § 823 Rn. 332.

25 Konferenz der Justizministerinnen und Justizminister der Länder, Arbeitsgruppe „Digitaler Neustart", Bericht vom 15.4.2019, S. 192; *Wagner,* in: MüKo (Fn. 17), § 3 ProdHaftG Rn. 34.

26 *Reusch,* BB 2019, 904, 906 f.; *Wittbrodt,* InTeR 2020, 74, 79.

27 *Rockstroh/Kunkel,* MMR 2017, 77, 80.

28 Zu Kritischen Infrastrukturen gehören Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (vgl. § 2 Abs. 10 BSIG).

stellbar noch rechtlich geboten.[29] Daher dürfte der Hersteller für Schäden, die aufgrund theoretisch möglicher, aber de facto abwegiger Geschehensverläufe im Zusammenhang mit Hackerangriffen entstehen, nicht haften.[30]

Kauft der Hersteller des Endprodukts „Maschine" oder eines anderen vernetzten Produkts die Firmware hinzu, treffen den Zulieferer als Teilproduktehersteller die produkthaftungsrechtlichen Herstellerpflichten. Der Zulieferer kommt insofern auch als Haftungspflichtiger in Betracht. Dies gilt jedoch insoweit eingeschränkt, als erst der Endprodukthersteller die Verwendung der Software sowie das Zusammenwirken mit der Hardware und damit das Gefahrenpotenzial überblicken bzw. letztlich beeinflussen kann. Aufgrund dessen müssen zwischen Endhersteller und Zulieferer hinsichtlich der Firmware klare technische Spezifikationen unter Beachtung des geltenden Sicherheitsmaßstabs auch mit Blick auf den Schutz vor Cyberattacken vereinbart werden.

b) IT-Sicherheit durch Instruktion

Obgleich Konstruktion und Fabrikation gegenüber Instruktion Vorrang genießen, kommt der Instruktion im Rahmen der Gewährleistung der IT-Sicherheit und der Abwehr schadensstiftender Cyberangriffe eine starke Bedeutung zu. Denn mit der Zunahme der Komplexität von (embedded) Software lassen sich IT-Sicherheitslücken nicht in Gänze ausschließen. Diesen Restrisiken kann mit entsprechenden Verwenderinformationen begegnet werden. Dies gilt umso mehr, als einerseits die Angreifbarkeit und die Ausnutzungsmöglichkeit von IT-Sicherheitslücken in besonderem Maß vom Produktnutzerverhalten abhängig sind. Andererseits bedarf der Nutzer aufgrund der zuweilen hohen Komplexität der IT-Elemente eine besondere Anweisung. Warnhinweise sowie Gebrauchsanleitungen müssen für IT-Sicherheitsgefahren sensibilisieren und eine cybergerechte Nutzung sicherstellen sowie zum Aufspielen allfälliger sicherheitsrelevanter Software-Updates anhalten und etwaige updatebedingte Nutzungsmodifikationen erläutern.

c) Produktbeobachtungs- und Gefahrabwendungspflicht

Im Gegensatz zum ProdHaftG folgt aus der deliktischen Haftung gem. § 823 Abs. 1 BGB eine zusätzliche Produktbeobachtungs- und Gefahrabwendungspflicht. Hersteller müssen Beschwerden und Gefahrenhinweise entgegennehmen, sich proaktiv über die Gefahrenlagen ihrer Produkte im Feld informieren sowie erforderlichenfalls Maßnahmen zur Abwehr festgestellter Gefahren ergreifen.[31] Aufgrund der dargestellten Gefahrträchtigkeit von IT-Sicherheitslücken bzw. Hackerangriffen bezieht sich diese Pflicht ebenso auf Cybergefahren; nachfolgend werden die Besonderheiten in diesem Zusammenhang erörtert.

aa) Remote-Produktbeobachtung und automatische Datenerhebung

Zunächst bestehen Überlegungen, die Durchführung einer integrierten, smarten Produktbeobachtung zu fordern, auf Grundlage derer Daten des vernetzten Produkts an den Hersteller übertragen und von ihm anschließend ausgewertet werden. Diese Art der Produktbeobachtung ist nur ein gangbarer Weg, wenn zuvor ein entsprechendes Einverständnis des Produktnutzers eingeholt wird.[32] Andernfalls sprechen datenschutzrechtliche Gründe gegen eine automatische Datenerhebung und -auswertung.

bb) Fremdhergestellte nachrüstbare IT-Elemente

Die Produktbeobachtungspflicht erstreckt sich auch auf Zubehörteile von Fremdherstellern und deren Zusammenwirken mit dem eigenen Produkt. Diese Pflicht betrifft daher auch Hersteller von analogen Maschinen bzw. Produkten in Bezug auf fremdhergestellte IT-Elemente, mit denen ihr Produkt nachträglich aufgerüstet werden kann, wodurch es zum vernetzten Produkt avanciert.

cc)Pflicht zum Firmware-Update

Weisen im Feld befindliche Produkte IT-Sicherheitslücken auf, wird darüber diskutiert, ob den Hersteller im Rahmen seiner Gefahrenabwendungspflicht eine Verpflichtung zur Programmierung sowie kostenfreien Bereitstellung und sogar zum automatischen Aufspielen von Firmware-Updates trifft.[33] Teilweise wird eine solche Verpflichtung abgelehnt, weil dies einer dem Haftungsrecht grundsätzlich fremden kostenfreien Nachrüstung gleichkäme.[34] Da diese Frage von der Rechtsprechung noch nicht entschieden wurde, sollte der Hersteller zur Vermeidung von Haftungsrisiken jedenfalls sicherheitsrelevante Firmware-Updates bereitstellen, sofern dies technisch möglich sowie wirtschaftlich zumutbar ist und andere Maßnahmen geringere Wirksamkeit versprechen.[35] So kann etwa die Effektivität von Warnungen als alternative Maßnahme bei B2C-Produkten bezweifelt werden, da bei Verbrauchern häufig ein geringeres Gefahrenverständnis als bei gewerblichen Nutzern vorherrscht,[36] sodass ein Firmware-Update vor allem bei IoT-Verbraucherprodukten in Frage kommt. Die Zumutbarkeit richtet sich nach dem Gefahrenpotenzial der IT-Sicherheitslücke und dem nötigen Programmierungs- und Bereitstellungsaufwand. Zumindest letzterer dürfte sich in Grenzen halten, wenn das Firmware-Update problemlos über das Internet durchführbar ist.[37] Selbstredend darf das Update seinerseits zu keinen Gefahren führen und erfordert eventuell eine erneute Nutzerinstruktion.

Die Entscheidung über die tatsächliche Durchführung des Updates verbleibt jedoch bei dem Nutzer. Nur in absoluten Ausnahmefällen, etwa bei sehr ernsten Cybergefahren, die nicht nur den Nutzer, sondern auch unbeteiligte Dritte betreffen, kann der Hersteller das Firmware-Update ohne das Wissen oder gar gegen den Willen des Nutzers aufspielen.[38] Insofern genügt es regelmäßig, wenn der Hersteller den Nutzern ein Update andient und dessen Verfügbarkeit anzeigt sowie über mögliche Folgen einer unterlassenen Update-Durchführung aufklärt.

dd) Sicherheitswarnungen

Eine Sicherheitswarnung stellt eine weitere denkbare Maßnahme zur Abwehr von Cybergefahren dar – entweder flankierend zu einem Firmware-Update oder anstelle eines

29 *Wagner,* in: MüKo (Fn. 17), § 3 ProdHaftG Rn. 34.
30 Vgl. *Förster,* in: BeckOK BGB, (Fn. 21) § 823 Rn. 332.
31 *Förster,* in: BeckOK BGB, (Fn. 21), § 823 Rn. 731 f.
32 *Böck/Theurer,* BB 2021, 520, 524.
33 Aus Sicht des Produktsicherheitsrechts siehe *Wiebe,* NJW 2019, 625 ff.
34 So etwa *Wiesemann/Mattheis/Wende,* MMR 2020, 139, 140; siehe auch *Reusch,* BB 2019, 904, 905 f.; *Raue,* NJW 2017, 1841, 1844 f.
35 Konferenz der Justizministerinnen und Justizminister der Länder, Arbeitsgruppe „Digitaler Neustart", Bericht vom 15.4.2019, S. 192; *Wagner,* in: MüKo (Fn. 17), § 823 Rn. 1008 ff.; *Wiebe,* NJW 2019, 625, 629.
36 Vgl. BGH, 16.12.2008 – VI ZR 170/07, NJW 2009, 1080, 1081 f.
37 *Wiebe,* NJW 2019, 625, 629.
38 *Wiesemann/Mattheis/Wende,* MMR 2020, 139, 141.

Updates, wenn dieses unverhältnismäßig erscheint. Im letzteren Fall sollte die Warnung mit einer Empfehlung zur Stilllegung des Produkts oder Deaktivierung der IT-Schnittstelle verbunden werden. Nach Möglichkeit gilt es, Warnungen hinsichtlich bestehender IT-Sicherheitslücken direkt an die Nutzer zu adressieren und auf öffentlichkeitswirksame Warnkampagnen zu verzichten, um Cyberattacken nicht zu provozieren.[39]

VI. Ausblick und Fazit

Zweifelsohne werden IT-Sicherheitsanforderungen an smarte Produkte und Maschinen in naher Zukunft ausdrücklich gesetzlich fundiert. Abgesehen von der EU-seitigen Überprüfung des bestehenden gesetzlichen Produktsicherheits- und Produkthaftungsrahmens unter dem Aspekt der Cybersecurity[40] existiert eine Vielzahl von konkreten (Gesetzes-)Initiativen. Auf Ebene der EU ist etwa der sog. EU Cybersecurity Act[41] zu nennen, der die Maßgabe „Security by Design" aufgreift und einen Rahmen für freiwillige Zertifizierungen bieten soll. Ferner sehen die EU-Warenverkaufsrichtlinie[42] und darauf fußend der Entwurf des deutschen Umsetzungsrechtsakts eine Sicherheitsaktualisierungspflicht für Verbraucherprodukte mit digitalen Elementen vor. Zudem fordert das DIN[43] und bitkom[44] die Unterwerfung der Cybersecurity unter den New Legislative Framework und die Schaffung einer entsprechenden horizontalen CE-Richtlinie. Aus deutschrechtlicher Perspektive kann das geplante IT-Sicherheitsgesetz 2.0 erwähnt werden, das produktbezogene Herstellerpflichten zur IT-Sicherheit formuliert (§ 8h BSIG-E). Zudem legt es einen weiteren Schwerpunkt auf den Verbraucherschutz, indem es parallel zum EU Cybersecurity Act ein freiwilliges IT-Sicherheitskennzeichen für IT-Produkte etabliert (§ 9a BSIG-E).[45]

Obwohl diese Bemühungen noch im Fluss sind, ein klarer Gesetzesrahmen noch nicht besteht und die genannten Rechtsunsicherheiten durch die Rechtsprechung noch nicht ausgeräumt wurden, treffen den Hersteller bereits jetzt IT-sicherheitsbezogene Pflichten in Bezug auf vernetzte Produkte bzw. Maschinen. Daher sind Hersteller zur Vermeidung von Haftungsrisiken gut beraten, proaktiv ein Mindestmaß an IT-Sicherheit zu gewährleisten; zumal unklar ist, ob Produkthaftpflichtversicherungen eine Gefahrenrealisierung aufgrund von IT-Sicherheitslücken abdecken. Die Hersteller sind insbesondere angehalten, die IT-Sicherheit im Rahmen der Konstruktion und Fabrikation sowie in die entsprechende Risikobeurteilung einzubeziehen, Informationen über mögliche Cybergefahren und IT-Sicherheitslücken bereitzustellen sowie eine genaue Produktbeobachtung und ggfs. Gefahrabwehrmaßnahmen unter dem Gesichtspunkt der IT-Sicherheit durchzuführen.

39 *Raue,* NJW 2017, 1841, 1843 f.; *Wiebe,* NJW 2019, 625, 629.
40 SWD (2018) 161 final; COM (2020) 64 final.
41 Verordnung (EU) 2019/881.
42 Art. 7 Abs. 3 Richtlinie (EU) 2019/771.
43 Positionspapier zum IT-Sicherheitsgesetz 2.0. Das geplante IT-Sicherheitskennzeichen muss auf internationalen und europäischen Normen und Standards basieren; abrufbar unter: https://www.dke.de/resource/blob/1977870/6780b24839e06c1fd1525fc112fbac4e/positionspapier-zum-it-sicherheitsgeset--pdf-data.pdf (zuletzt abgerufen am 5.4 2021).
44 Positionspapier: Anforderungen an eine kohärente Regulierung der Cybersicherheit vom 7.6.2019; abrufbar unter: https://www.bitkom.org/sites/default/files/2019-06/20190606_anforderungen_an_eine_koharante_regulierung_der_cybersicherheit.pdf. (zuletzt abgerufen am 5. 4 2021).
45 Hierzu näher *Kipker/Scholz,* MMR 2019, 431, 434 f.

Dr. Dr. Fabian Teichmann, LL.M. und Jan Koch, St. Gallen*

Wirtschaftsstrafrecht und Digitalisierung – Chancen und Herausforderungen

Die zunehmende Digitalisierung im Bereich der Wirtschaft und des Rechtsmarkts eröffnet nicht nur Kriminellen alternative Vorgehensweisen, sondern bietet auch neue Chancen zur Bekämpfung der Wirtschaftskriminalität. Anhand ausgewählter Herausforderungen im Zusammenhang mit der Wirtschaftskriminalität werden konkrete Chancen der Digitalisierung im Bereich der Compliance sowie der Kriminalitätsbekämpfung und -prävention aufgezeigt.

I. Einleitung

Zwischen 2018 und 2020 wurde knapp die Hälfte aller deutschen Unternehmen Opfer von Wirtschaftskriminalität.[1] Dabei wurden gut 50 % aller Fälle nur per Zufall entdeckt,[2] was auf eine große Anzahl weiterer, unentdeckt gebliebener Fälle hindeutet. Von Seiten der Strafverfolgungsbehörden wird die Anzahl an unentdeckt gebliebenen Fällen im Bereich der Wirtschaftskriminalität ebenfalls als hoch eingeschätzt.[3] Da ein großer Anteil deutscher Unternehmen bereits zum Opfer von Wirtschaftskriminalität wurde, liegt es nahe, dass neben der Strafverfolgung auch weitere präventive Maßnahmen notwendig sind. Eine solche Ergänzung kann die Digitalisierung im Compliance-Bereich bieten. Dies wird auch von den Unternehmen so gesehen: Über 70 % erwarten durch die weitere Digitalisie-

* Mehr über die Autoren erfahren Sie auf Seite III.
1 pwc, Wirtschaftskriminalität – Ein niemals endender Kampf, 2020, verfügbar unter: https://www.pwc.de/de/consulting/forensic-services/wirtschaftskriminalitaet-ein-niemals-endender-kampf.pdf (zuletzt abgerufen am 2.4.2021).
2 *Reuter, Blees,* KPMG-Studie: Wirtschaftskriminalität in Deutschland 2020, Berlin 2020, verfügbar unter: https://home.kpmg/de/de/home/media/press-releases/2020/08/kpmg-studie-wirtschaftskriminalitaet-in-deutschland-2020.html (zuletzt abgerufen am 2.4.2021).
3 Bundeskriminalamt, Wirtschaftskriminalität – Bundeslagebild 2018, Wiesbaden 2019, verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2018.html?nn=28030 (zuletzt abgerufen am 2.4.2021).