Dialog für Cyber-Sicherheit

Ergebnisbericht Workstream „Digitales Mindesthaltbarkeits-datum“

Mit Cyber-Sicherheit zu mehr Nachhaltigkeit im Internet der Dinge – Lösungsansätze und Handlungsempfehlungen

„Dialog für Cyber-Sicherheit“

Ein Projekt im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Informationen zum Produkt

Dieser Bericht wurde im Rahmen des Projekts „Dialog für Cyber-Sicherheit“ von Juli 2021 bis März 2022 erarbeitet.

Ideengeber des Workstreams war: Nikolas Becker - Gesellschaft für Informatik (GI) e.V.

Mitwirkende Teilnehmer:innen des Workstreams waren: Nikolas Becker - Gesellschaft für Informatik (GI) e.V., Dr. Daniel Guagnin - Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., Robert Hoyer - BSI, Bettina Kloppig - Bundesarbeitsgemeinschaft der Seniorenorganisationen (BAGSO), Nadja Menz - Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Dr. Ayten Öksüz - Verbraucherzentrale Nordrhein-Westfalen e.V., Steffen Waurick - BSI

Beteiligte Mitarbeiter:innen der Geschäftsstelle am nexus Institut waren: Fabian Dantscher, Franziska Detsch

Unterauftragnehmer war: Prof. Dr. Maximilian von Grafenstein

Der Dialog für Cyber-Sicherheit ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das vom Think Tank iRights.Lab und dem nexus Institut durchgeführt wird. Die Auftragnehmer haben dazu eine Geschäftsstelle eingerichtet.

Der Workstream „Digitales Mindesthaltbarkeitsdatum“, in dem dieser Bericht entstanden ist, wurde im Rahmen eines partizipativen und offenen Austauschs von der Geschäftsstelle und interessierten Dialogpartner:innen (s.o. Ideengeber:innen und mitwirkende Teilnehmer:Innen) durchgeführt. Die Dialogpartner:innen haben das Thema aus dem Bereich Cyber-Sicherheit für den Workstream selbst gewählt.

Das vorliegende Bericht wurde von der Geschäftsstelle und den Workstream-Teilnehmer:innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. jedes einzelnen Teilnehmenden wider. Das BSI verfolgt mit dem Projekt das Ziel, einen offenen gesellschaftlichen Diskurs zum Thema IT-/Cyber-Sicherheit sowie damit verwandter gesellschaftlicher Themen zu ermöglichen. Das Projekt soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cyber-Sicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Weitere Informationen zum „Dialog für Cyber-Sicherheit“:
www.dialog-cybersicherheit.de
Kontakt Geschäftsstelle (iRights.Lab und nexus Institut):
kontakt@dialog-cybersicherheit.de

Stand: April 2022

Ein Projekt im Auftrag des:

iRights.Lab
Think Tank für die digitale Welt

nexus

Bundesamt für Sicherheit in der Informationstechnik

Zusammenfassung

Der vorliegende Bericht fasst die Ergebnisse des Workstreams „Digitales Mindesthaltbarkeitsdatum“ zusammen, der im Rahmen des Projekts „Dialog für Cyber-Sicherheit“ durchgeführt wurde.

Das Ziel des Workstreams war es, den Zusammenhang zwischen mangelhafter Cyber-Sicherheit bei Consumer-IoT-Geräten und ökologischer Nachhaltigkeit aufzuzeigen und konkrete Lösungsansätze und Handlungsempfehlungen zu entwickeln, die zur Verlängerung der Nutzungsdauer von IoT-Geräten unter Berücksichtigung der Cyber-Sicherheit beitragen.

Die Ergebnisse des Workstreams zeigen, dass **Informationssicherheit und ökologische Nachhaltigkeit im Internet der Dinge untrennbar miteinander verbunden sind**. Die häufig unzureichende Updatefähigkeit und Cyber-Sicherheit bei IoT-Geräten hat direkte negative Auswirkungen auf die Umweltbilanz der Produkte. Gleichzeitig wird den ökologischen Folgen einer mangelhaften Cyber-Sicherheit im IoT-Bereich jedoch von Politik, Industrie und Wissenschaft wenig Aufmerksamkeit geschenkt.

Vor diesem Hintergrund wurden im Rahmen des Workstreams insgesamt **19 Lösungsansätze zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT-Geräten** identifiziert und entwickelt. Diese lassen sich in vier Bereiche unterteilen: Regulierung & Transparenz, Sensibilisierung der Verbraucher:innen, Sensibilisierung der Hersteller:innen, und technische Lösungsansätze. Aus den verschiedenen Lösungsansätzen kristallisierten sich in den gemeinsamen Diskussionen der Dialogpartner:innen sowie in der Auseinandersetzung mit verschiedenen Expert:innenmeinungen zwei Ansätze heraus, die als **priorisierte Handlungsempfehlungen** tiefergehend ausformuliert wurden.

Im Konkreten empfiehlt die Arbeitsgruppe, dass **Hersteller:innen von Consumer-IoT-Geräten** dazu verpflichtet werden,

1. **Aktualisierungen für die Geräte bereitzustellen** und
2. **Angaben zur erwartbaren Nutzungsdauer der Geräte** und zum **Bereitstellungszeitraum von Updates** zu machen.

Grundsätzlich sieht die Arbeitsgruppe jedoch Handlungsbedarf auf allen Ebenen, wie die Vielzahl der gesammelten Lösungsansätze aufzeigt: Die Gewährleistung von Cyber-Sicherheit bei IoT-Geräten und die Verlängerung der sicheren Nutzungsdauer der Produkte ist eine gesamtgesellschaftliche Aufgabe, bei der insbesondere die Politik und Industrie, aber auch die Verbraucher:innen zusammenarbeiten und miteinbezogen werden müssen.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Hintergrund des Workstreams

Das Internet der Dinge – oder Internet of Things (IoT) – spielt eine zentrale Rolle bei der digitalen Transformation sowohl in der Industrie und bei Unternehmen als auch im Alltag der Verbraucher:innen. So stieg im Laufe der letzten Jahre die Zahl der vernetzten Geräte, die in Haushalten und von Individuen genutzt werden (Consumer-IoT), kontinuierlich an. Für das Jahr 2020 wurde die Zahl der Consumer-IoT-Geräte weltweit auf ungefähr 12,9 Milliarden geschätzt.[1] Im selben Jahr verwendeten sieben von zehn Konsument:innen in Deutschland mindestens ein Endgerät aus der Welt des Internets der Dinge.[2]

Mit der steigenden Anzahl an vernetzten Produkten nimmt auch das Risiko für IT-Sicherheitsvorfälle zu. Wie von Verbraucherschutzorganisationen und Cyber-Sicherheitsexpert:innen vielfach aufgezeigt, fehlt es Consumer-IoT-Geräten häufig an grundlegenden Sicherheitseigenschaften und sie sind anfällig für eine Vielzahl unterschiedlicher Arten von Cyberangriffen.[3] So können auf der einen Seite IoT-Geräte direkt angegriffen werden, um die Kontrolle über die Produkte zu übernehmen, sie zu beschädigen oder sensible persönliche Informationen abzugreifen. Auf der anderen Seite können vernetzte Geräte als Instrument für Angriffe auf Dritte missbraucht werden. Beispiel hierfür sind sogenannte Distributed-Denial-of-Service (DDoS) Attacken, bei der die Nichtverfügbarkeit eines Internetdienstes durch eine Vielzahl von gezielten Anfragen mutwillig herbeigeführt wird.

Ein großes Problem stellt in diesem Zusammenhang dar, dass IoT-Geräte nicht oder nur unzureichend mit Sicherheitsupdates versorgt werden bzw. die Updates von den Hersteller:innen nur für einen kurzen Zeitraum nach Markstart bereitgestellt werden.[4] Unter dem Gesichtspunkt der Cyber-Sicherheit sollten diese Geräte daher nur verhältnismäßig kurz genutzt werden und müssten regelmäßig ausgetauscht werden, was zum unnötigen Verbrauch wertvoller Ressourcen und zur Erzeugung von vermeidbarem Müll führt. So steigt die Menge des Elektroschrotts jährlich um 3 bis 5 Prozent, wobei Deutschland umgerechnet auf den Pro-Kopf-Anteil eine Spitzenposition einnimmt.[5] Gleichzeitig wächst ein Gebrauchtmarkt von IoT-Geräten, die nicht mehr sicher genutzt werden können.

---

[1] Statista (2017): Anzahl der vernetzten Geräte im Internet der Dinge (IoT) weltweit bis 2020. https://de.statista.com/statistik/daten/studie/537093/umfrage/anzahl-der-vernetzten-geraete-im-internet-der-dinge-iot-weltweit/

[2] Deloitte & BVDW (2021): Faktencheck Consumer IoT - Consumer IoT Marktstudie. https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/consumer-iot-studie.html

[3] ENISA Advisory Group (2019): Opinion Consumers and IoT Security. https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

[4] Knips, J.; Gries, C.; Wernick, C. (2020): Consumer-IoT in Deutschland - Anwendungsbereiche und möglicher Regelungsbedarf, WIK Diskussionsbeitrag, No. 471, WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honnef. https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_471.pdf

[5] BR (2020): Globaler E-Waste-Monitor 2020: Viel mehr Elektroschrott weltweit. https://www.br.de/nachrichten/wissen/globaler-e-waste-monitor-2020-viel-mehr-elektroschrott-weltweit,S3ZvJab

Diese Dynamiken zeigen, wie sich das Internet der Dinge im Spannungsfeld zwischen Cyber-Sicherheit und Nachhaltigkeit bewegt – mit oft signifikanten Auswirkungen für Umwelt, Verbraucher:innen und Gesellschaft. Den ökologischen Folgen einer unzureichenden Cyber-Sicherheit bei Consumer-IoT wird bisher jedoch von Politik, Industrie und Wissenschaft keine oder nur wenig Aufmerksamkeit geschenkt.[6]

Diese Thematik war Ausgangspunkt für die Arbeit des Workstreams „Digitales Mindesthaltbarkeitsdatum“, der im Rahmen der „Denkwerkstatt Sichere Informationsgesellschaft“ 2021 von mehreren zivilgesellschaftlichen Stakeholdern ins Leben gerufen und von Juli 2021 bis März 2022 als eines von fünf Teilprojekten im „Dialog für Cyber-Sicherheit“ durchgeführt wurde. Der Dialog für Cyber-Sicherheit ist ein Projekt im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das vom Think Tank iRights.Lab und dem nexus Institut umgesetzt wird.

1.2 Zielsetzung des Workstreams

Vor diesem in Kapitel 1.1 ausgeführten Hintergrund ist es das Ziel des Workstreams „Digitales Mindesthaltbarkeitsdatum“, die Themen Cyber-Sicherheit und Nachhaltigkeit im Kontext des IoT zu verknüpfen. Konkret wurde in der Arbeitsgruppe der Frage nachgegangen, wie die sichere Nutzungsdauer von Consumer-IoT-Geräten als Beitrag für mehr ökologische Nachhaltigkeit verlängert werden kann. Zu diesem Zweck wurden in einem ersten Schritt mögliche Ursachen und ökologische Auswirkungen einer kurzen Nutzungsdauer vernetzter Geräte sowie relevante rechtliche Rahmenbedingungen, Standards, Normen und Zertifizierungssysteme identifiziert. Darüber hinaus wurde die Perspektive der Verbraucher:innen und der Hersteller:innen von IoT-Produkten erfasst und analysiert. Auf der Grundlage dieser Daten wurden anschließend konkrete Maßnahmen, die die Nutzungsdauer von Consumer-IoT verlängern helfen, erarbeitet.

Es ist der Arbeitsgruppe ein Anliegen, mit diesem Bericht einen Beitrag zur gesellschaftlichen und politischen Debatte über die häufig nur kurze Nutzungsdauer und unzureichende Updatefähigkeit von IoT-Produkten zu leisten: Es sollen die Zusammenhänge und Auswirkungen von mangelhafter Cyber-Sicherheit bei Consumer-IoT in Bezug auf ökologische Nachhaltigkeit aufgezeigt und mögliche Handlungsempfehlungen in diesem Kontext formuliert werden.

1.3 Methodisches Vorgehen

Die Ergebnisse dieses Berichts basieren auf einer umfassenden Literaturrecherche, Expert:inneninterviews und -workshops, dem fachlichen Austausch der Workstream-Teilnehmenden untereinander sowie der Beratung durch einen Rechtswissenschaftler bei der Ausarbeitung der Handlungsempfehlungen.

Im Rahmen der Literaturrecherche wurden wissenschaftliche Studien, Berichte von Behörden und der Agentur der Europäischen Union für Cybersicherheit (ENISA) sowie Veröffentlichungen von Verbraucherschutzorganisationen erfasst. Insgesamt wurden rund 50 Dokumente und (Online-)Quellen in Bezug auf die Zielstellung des Workstreams ausgewertet. Ergänzend dazu wurden zwischen September und Dezember 2021 neun leitfadengestützte Interviews

[6] vgl. Janicke, H.; Abuadbba, S.; Nepal, S. (2020): "Security and Privacy for a Sustainable Internet of Things." Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). https://ieeexplore.ieee.org/document/9325365

mit Expert:innen aus unterschiedlichen Bereichen geführt: Dazu gehörten Vertreter:innen von IoT-Herstellern, Industrie-Verbänden, technischen Prüforganisationen und Verbraucherschutzorganisationen sowie IT-Sicherheits- und Rechtsexpert:innen.

Auf Basis der in der Bestandsaufnahme und den Interviews gesammelten Daten und Erkenntnisse identifizierten die Workstream-Teilnehmenden in einem zweiten Schritt mögliche Lösungsansätze zur Verlängerung der sicheren Nutzungsdauer von IoT-Geräten, die in einem Workshop gemeinsam konkretisiert wurden. Zwei der Ansätze wurden anschließend ausgewählt und im Austausch mit einem Rechtswissenschaftler mit Fokus auf Internettechnologie und der Regulierung von Innovationen tiefergehend ausgearbeitet. In Workshops mit Expert:innen aus den Bereichen Wirtschaft, Recht und Verbraucherschutz sowie vom BSI wurden die erarbeiteten Ergebnisse diskutiert, kommentiert und validiert.

Das methodische Vorgehen im Workstream wird in Abbildung 1 schematisch dargestellt. Die Mitwirkung der ehrenamtlichen Stakeholder:innen wird durch die roten Pfeile abgebildet:

Abbildung 1: Methodisches Vorgehen im Workstream "Digitales Mindesthaltbarkeitsdatum"

2 Betrachtungsgegenstand: Consumer-IoT

2.1 Charakterisierung von Consumer-IoT

Der Begriff „Consumer-IoT“ ist nicht eindeutig definiert und wird von Akteuren aus der Politik und Industrie und innerhalb der Fachöffentlichkeit teilweise unterschiedlich verwendet. Im Rahmen des vorliegenden Berichts bezieht sich Consumer-IoT auf alle „von Verbrauchern genutzte[n] Produkte und Dienstleistungen, die mit einem Netzwerk verbunden sind und aus der Ferne (zum Beispiel über einen Sprachassistenten oder ein Mobilgerät) gesteuert werden können“[7] – eine Begriffsdefinition, die so auch die Europäische Kommission teilt.[8]

Die Produktgruppe umfasst damit insbesondere Geräte aus den vier Bereichen Smart Home, Entertainment, Tracking und Monitoring sowie Wearables und erstreckt sich über Produkte wie intelligente Beleuchtungs- und Heizsysteme, vernetzte Saugroboter und Kühlschränke, Smart TVs und Fitness-Tracker.[9] Die folgende Abbildung des WIK – Wissenschaftliches Institut für Infrastruktur spiegelt die relevanten Anwendungsfelder im gegenwärtigen Consumer-IoT wider.

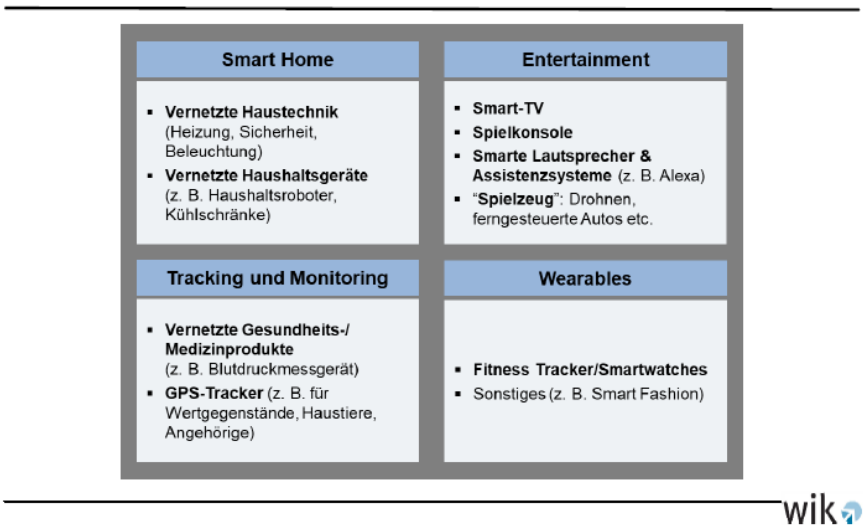

Abbildung 2: Consumer IoT: Relevante Anwendungsfelder (Quelle: WIK)

2.2 Nutzung von Consumer-IoT und Marktentwicklung

Der Consumer-IoT-Markt entwickelt sich in den letzten Jahren mit hoher Dynamik und die Zahl der intelligenten Geräte für Verbraucher:innen nimmt stark zu. Für das Jahr 2020 wurde die Zahl der verbraucherbezogenen IoT-Geräte weltweit auf ungefähr 12,9 Milliarden geschätzt.

[7] Knips, J.; Gries, C.; Wernick, C. (2020): Consumer-IoT in Deutschland - Anwendungsbereiche und möglicher Regelungsbedarf, WIK Diskussionsbeitrag, No. 471, WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honnef. https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_471.pdf
[8] https://ec.europa.eu/commission/presscorner/detail/de/IP_20_1326
[9] Consumer-IoT-Geräte werden häufig auch in Unternehmenskontexten verwendet. Diese Produkte werden gemeinhin ebenso als Consumer-IoT-Geräte eingestuft.

Zwei Jahre zuvor lag dieser Wert noch bei rund 7 Milliarden.[10] Zugleich wächst auch die Anzahl der Nutzer:innen solcher Geräte, wenngleich zumindest im deutschen Raum ungleich schwächer als die Zahl der Geräte selbst. Laut einer Studie stieg der Anteil der Konsument:innen in Deutschland, die mindestens ein IoT-Gerät verwenden, von 65 Prozent im Jahr 2018 auf 70 Prozent in 2020.[11] Die Untersuchungen zeigen, dass der Gerätebestand auf dem deutschen Markt vornehmlich innerhalb der bestehenden Nutzer:innengruppe anwächst. Das heißt, dass neue IoT-Geräte insbesondere von Verbraucher:innen erworben werden, die bereits Geräte aus dem Internet der Dinge verwenden.

2.3 Consumer-IoT und Cyber-Sicherheit

Mit der steigenden Zahl der vernetzten Geräte wächst auch das Risiko für IT-Sicherheitsvorfälle. Produkte, die aus der Ferne gesteuert werden können und nicht nur lokal im Netzwerk oder über Bluetooth ansteuerbar sind, sind grundsätzlich anfälliger für Angriffe von außen. Wie von Verbraucherschutzorganisationen und IT-Sicherheitsexpert:innen vielfach aufgezeigt, fehlt es Consumer-IoT-Geräten jedoch häufig auch bereits an den elementarsten Sicherheitseigenschaften.[12] So werden viele IoT-Geräte mit universellen Standard-Benutzernamen und -Passwörtern verkauft, bei denen fälschlicherweise davon ausgegangen wird, dass diese von den Verbraucher:innen geändert werden.[13] Des Weiteren sind für viele IoT-Geräte keine oder nur unzureichende Sicherheitsupdates erhältlich bzw. sie werden nur für einen kurzen Zeitraum nach Markteinführung bereitgestellt.[14] Diese systemischen Anfälligkeiten im Internet der Dinge in Kombination mit der großen Zahl und ständigen Konnektivität der Geräte hat das Feld Consumer-IoT zu einem attraktiven Ziel für Hacker:innen werden lassen.

Studien zeigen, dass Consumer-IoT-Geräte dabei für eine Vielzahl unterschiedlicher Angriffe anfällig sind.[15] Es kann hierbei zwischen zwei grundsätzlich unterschiedlichen Angriffsarten unterschieden werden: Auf der einen Seite können IoT-Geräte direkt angegriffen werden, um Schäden auf dem infizierten System selbst herbeizuführen – mit teilweise unmittelbaren Folgen für die Nutzer:innen. So können beispielsweise Kriminelle vernetzte Heizsysteme im Winter ausschalten oder sich bei nicht ausreichend gesicherten smarten Türschlössern physischen

[10] Statista (2017): Anzahl der vernetzten Geräte im Internet der Dinge (IoT) weltweit bis 2020. https://de.statista.com/statistik/daten/studie/537093/umfrage/anzahl-der-vernetzten-geraete-im-internet-der-dinge-iot-weltweit/

[11] Deloitte & BVDW (2021): Faktencheck Consumer IoT - Consumer IoT Marktstudie. https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/consumer-iot-studie.html. Abgefragt wurde Hardware aus den Bereichen Connected Entertainment, Smart Speakers, Wearables und Smart Homes. Ausdrücklich nicht eingerechnet sind Consumer-Geräte mit primärem Kommunikationsfokus wie Smartphones, Tablets und PCs/Laptops.

[12] ENISA Advisory Group (2019): Opinion Consumers and IoT Security. https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective-09.2019

[13] DCMS (2018): Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973926/Secure_by_Design_Report__V2.pdf

[14] Knips, J.; Gries, C.; Wernick, C. (2020): Consumer-IoT in Deutschland - Anwendungsbereiche und möglicher Regelungsbedarf, WIK Diskussionsbeitrag, No. 471, WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honnef. https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_471.pdf

[15] Blythe, J.; Johnson, S. (2019): A systematic review of crime facilitated by the consumer Internet of Things. Security Journal. https://doi.org/10.1057/s41284-019-00211-8

Zutritt zu Wohnungen verschaffen.[16] Geräte mit Mikrofon oder Kamera können verwendet werden, um Personen auszuspähen und sensible persönliche Informationen zu sammeln, die veröffentlicht oder für Erpressung und Missbrauch verwendet werden können.[17]

Auf der anderen Seite können vernetzte Geräte jedoch auch als Instrument für Angriffe auf Dritte missbraucht werden. Beispiel hierfür sind sogenannte Distributed-Denial-of-Service (DDoS) Attacken, bei denen ein Zusammenschluss aus kompromittierten IoT-Geräten (Botnetz) genutzt wird, um einen Überlastungsangriff auf Internetdienste durchzuführen. So wurde im Jahr 2016 ein Verbund aus Zehntausenden vernetzten Geräten für einen Angriff auf einen DNS-Dienstleister benutzt, durch den Websites und Services vieler internationaler Konzerne für eine längere Zeit nicht erreichbar waren.[18] Ebenso haben solche Attacken das Potenzial, einen Ausfall kritischer Infrastruktur zu verursachen und können dementsprechend eine Gefahr für Leib und Leben darstellen.[19] Die Zahl der DDoS-Angriffe stieg dabei in den letzten Jahren steil an und im Jahr 2020 wurden zum ersten Mal mehr als 10 Millionen solcher Attacken registriert.[20]

2.4 Consumer-IoT und Nachhaltigkeit

Wie die meisten modernen Elektronikgeräte haben Consumer-IoT-Geräte sowohl bei der Produktion als auch der Entsorgung erhebliche Umweltauswirkungen. Allein in Deutschland fallen jährlich etwa 1,6 Millionen Tonnen Elektroschrott an. Pro Kopf pro Jahr sind dies 19,4 Kilogramm ausrangierte Elektronikgeräte.[21] Dabei wächst die Menge an Elektromüll jährlich um 3 bis 5 Prozent.[22] Ein zentraler Treiber dieser Entwicklung ist, dass bei einer wachsenden Zahl an Geräten die Nutzungsdauer zunehmend kürzer wird, was insbesondere auf Consumer-IoT-Produkte zutrifft, bei denen Software über die Nutzungsdauer, Funktionalität und Zuverlässigkeit entscheidet.[23] Bei diesen Geräten ist das Grundproblem, dass sie eigentlich eine wesentlich längere Lebensdauer hätten, als die meisten Hersteller:innen Software-Updates bereitstellen. Ein Kühlschrank mit Internetanschluss müsste beispielsweise im Durchschnitt über 10 bis 15 Jahre mit Updates versorgt werden. Dabei kämen Unternehmen bei der Bereitstellung von Updates und Patches bei solch langen Laufzeiten jedoch schnell an die Grenzen des Machbaren, so die Interviewaussage eines Vertreters eines IoT-Herstellers. Vor dem Hintergrund

---

[16] DCMS (2018): Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973926/Secure_by_Design_Report__V2.pdf

[17] BBC (2017): Children's messages in CloudPets data breach. https://www.bbc.com/news/technology-39115001

[18] Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. (2017): DDoS in the IoT: Mirai and Other Botnets. Computer 50(7), 80–84

[19] Al-Hadhrami, Y.; Hussain, F. K. (2021): DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*, *24*(3), 971-1001

[20] BSI (2021): Die Lage der IT-Sicherheit in Deutschland 2021. S.32. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf?__blob=publicationFile&v=3#%5B%7B%22num%22%3A168%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22FitR%22%7D%2C-396%2C-2%2C991%2C844%5D

[21] Statista (2020): Die zehn Länder mit dem größten Elektroschrott-Aufkommen 2019. https://de.statista.com/infografik/12272/die-zehn-laender-mit-dem-groessen-elektroschrott-aufkommen/

[22] Vzbv (2020): Faktenblatt zur Langlebigkeit von Produkten. https://www.vzbv.de/sites/default/files/downloads/2021/01/12/2020_vzbv_faktenblatt_langlebigkeit_von_produkten_002.pdf

[23] Vgl. das Forschungsprojekt „Analyse der software-basierten Einflussnahme auf eine verkürzte Nutzungsdauer von Produkten“ im Auftrag des Umweltbundesamts: https://www.tne.tu-berlin.de/fileadmin/fg368/Flyer_Software-Obsoleszenz.pdf

der Umweltauswirkungen, die bei der Produktion und Entsorgung solcher Geräte erzeugt werden, wird gleichwohl klar: Je länger die Geräte genutzt werden, desto eher rechtfertigen sich deren ökologischen Kosten.

Überraschenderweise wird den ökologischen Auswirkungen des Consumer-IoT Markts jedoch von der Politik, Wissenschaft und Industrie bisher wenig Aufmerksamkeit geschenkt. Zwar hat sich die Bundesregierung in ihrem aktuellen Koalitionsvertrag dem Ziel verschrieben, „Nachhaltigkeit by design zum Standard bei Produkten“ zu machen. [24] Es bleibt jedoch abzuwarten, inwieweit die angestrebte Prüfung der „Erleichterung der Nutzbarkeit“ von Geräten durch Updates und ein Recht auf Reparatur in diesem Kontext Potential entfalten wird. Darüber hinaus gibt es auch mehr und mehr Studien zu der Fragestellung, wie das Internet der Dinge Nachhaltigkeit positiv beeinflussen kann. Dabei wird untersucht, wie das IoT für das Erreichen von Nachhaltigkeitszielen wie zum Beispiel die Senkung des Energie- und Wasserverbrauchs oder die Optimierung der Abfallwirtschaft genutzt werden kann – eine Sichtweise, die als *IoT for sustainability* bezeichnet wird.[25] Im Gegensatz dazu gibt es bisher sehr wenige Forschungsvorhaben zur Analyse der Lebenszyklen von IoT-Geräten und deren nachhaltiger Entwicklung, Nutzung und Wiederverwendung, also der Frage, wie die negativen Auswirkungen der Produktion und des Betriebs von IoT-Geräten auf die Umwelt verringert werden können. Erste vorliegende Studien zu diesem Bereich des sogenannten *sustainable IoT* weisen jedoch darauf hin, dass eine nachhaltige Produktion und Nutzung von IoT-Geräten nur in Kombination mit der Umsetzung von Security-by-Design-Prinzipien im gesamten Produktlebenszyklus zu erzielen ist.[26] Da die Gewährleistung einer hohen Cyber-Sicherheit gleichwohl häufig zu unerwünschten Nebeneffekten wie beispielsweise einer verkürzten Nutzungsdauer führt, zeigt sich, wie sehr sich das Internet der Dinge im Spannungsfeld zwischen Nachhaltigkeit und Cyber-Sicherheit bewegt.

[24] Auszug aus dem aktuellen Koalitionsvertrag: "Wir wollen Nachhaltigkeit by design zum Standard bei Produkten machen. Die Lebensdauer und Reparierbarkeit eines Produktes machen wir zum erkennbaren Merkmal der Produkteigenschaft (Recht auf Reparatur). Wir stellen den Zugang zu Ersatzteilen und Reparaturanleitungen sicher. Herstellerinnen und Hersteller müssen während der üblichen Nutzungszeit Updates bereitstellen. Wir prüfen Lösungen zur Erleichterung der Nutzbarkeit solcher Geräte über die Nutzungszeit hinaus. Für langlebige Güter führen wir eine flexible Gewährleistungsdauer ein, die sich an der vom Hersteller oder der Herstellerin bestimmten jeweiligen Lebensdauer orientiert." https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1

[25] Janicke, H.; Abuadbba, S.; Nepal, S. (2020): "Security and Privacy for a Sustainable Internet of Things." Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). https://ieeexplore.ieee.org/document/9325365

[26] Janicke, H.; Abuadbba, S.; Nepal, S. (2020): "Security and Privacy for a Sustainable Internet of Things." Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). https://ieeexplore.ieee.org/document/9325365

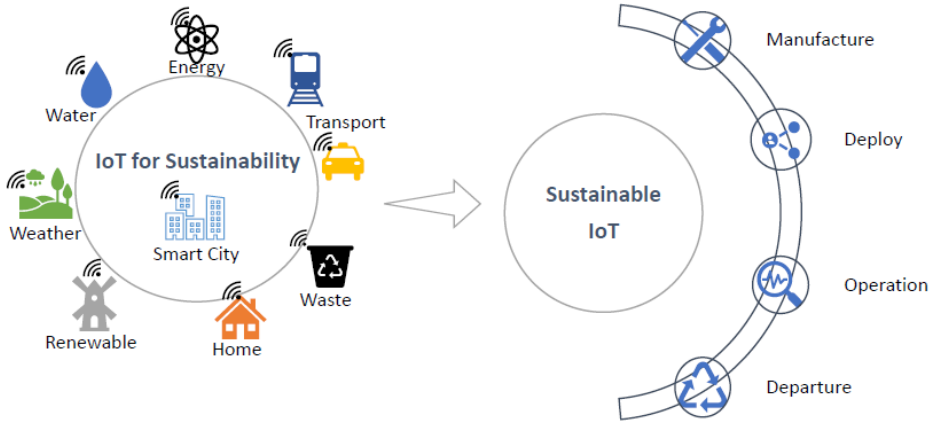

Abbildung 3: Darstellung zweier zentraler Sichtweisen auf das IoT im Zusammenhang mit Nachhaltigkeit: ‚IoT for sustainability' versus ‚sustainable IoT' (Quelle: Janicke et al.)

3 Perspektive der Verbraucher:innen

Im Rahmen der Literaturrecherche und der Expert:inneninterviews wurde unter anderem die Perspektive der Verbraucher:innen in Bezug auf die Nutzung von IoT-Geräten erfasst und analysiert. Dabei zeigte sich, dass insbesondere in Großbritannien im Zusammenhang mit der Entwicklung einer Gesetzgebung zur Gewährleistung von Cyber-Sicherheit bei Consumer IoT-Geräten[27] umfangreiche Verbraucherstudien durchgeführt wurden, deren Ergebnisse auch für Deutschland aufschlussreich sind.

Gewünschte Lebensdauer von Elektronikgeräten

Verbraucher:innen wünschen sich, dass Elektronikgeräte länger halten: Untersuchungen zeigen, dass die gewünschte Lebensdauer elektronischer Geräten je nach Produktkategorie um das 1,9- bis 3,6-fache höher liegt als die momentane tatsächliche Gebrauchsdauer.[28] Darüber hinaus halten viele Menschen die Langlebigkeit von Produkten für einen wichtigen gesellschaftlichen Wert an sich und sind sich bewusst, dass sie durch eine lange Nutzung der Geräte die Umweltbelastungen reduzieren können.[29] Aus Gründen der Informationssicherheitssicherheit macht aber ein Auslaufen der Geräteunterstützung und damit verbundenen Sicherheitsupdates eine Nutzung trotz technischer Funktionsfähigkeit unsicher.

Fähigkeit zur Risikoeinschätzung und Erwartungshaltung an integrierte Sicherheitsfunktionen bei IoT-Geräten

Laut den Interviewaussagen eines Vertreters einer Verbraucherschutzorganisation ist sich der Großteil der Verbraucher:innen nicht bewusst, dass IoT-Geräte gehackt und ggf. persönliche Daten abgegriffen werden können. Darüber hinaus könne nur ein Bruchteil der Nutzer:innen überhaupt erkennen, welche Geräte sicher sind. Verbraucher:innen würden sich am liebsten nicht um Cyber-Sicherheit kümmern müssen. „98 Prozent wollen ‚Security out of the box'", so die Aussage des Experten für Verbraucherschutz. Diese Einschätzungen decken sich auch mit den Ergebnissen einer repräsentativen Umfrage, die in Großbritannien durchgeführt wurde. Dort gaben 9 von 10 der Befragten an, dass IoT-Geräte über grundlegende integrierte Funktionen zum Schutz der Privatsphäre und der Sicherheit der Nutzer:innen verfügen sollten. Mehr als 80 Prozent der Verbraucher:innen waren der Meinung, dass die Händler:innen und Hersteller:innen dafür verantwortlich seien, sicherzustellen, dass IoT-Geräte über elementare Sicherheitsfunktionen verfügen, bevor sie verkauft werden dürfen.

Benutzung von IoT-Geräten nach Ablauf der Unterstützungsdauer

Die selbe Studie zeigt jedoch ebenfalls, dass eine große Zahl der Verbraucher:innen vernetzte Geräte auch nach Ablauf des Zeitraums, für den die Produkte Software-Updates erhalten, wei-

[27] https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation

[28] Wieser, H.; Tröger, N. (2015): Die Nutzungsdauer und Obsoleszenz von Gebrauchsgütern im Zeitalter der Beschleunigung: Eine empirische Untersuchung in österreichischen Haushalten. S. 40. https://www.arbeiterkammer.at/infopool/wien/Bericht_Produktnutzungsdauer.pdf

[29] https://challengeobsolescence.info/befragung-2019/

ter nutzen. So gaben 36 Prozent der Befragten an, IoT-Geräte nach Ablauf der Unterstützungsdauer auf die gleiche Art zu nutzen wie davor, während jede:r Fünfte das Gerät als Backup oder Ersatzgerät behält.[30]

Rolle der Mindestunterstützungsdauer bzw. Softwareupdates bei der Kaufentscheidung von IoT-Geräten

Laut der in Großbritannien durchgeführten Studie prüfen 20 Prozent der Konsument:innen beim Kauf eines vernetzten Geräts den Mindestunterstützungszeitraum (die Zeitspanne, in der das Produkt Updates erhält). Dabei achten die jüngeren Verbraucher:innen zwischen 16 und 24 Jahre am ehesten auf diese Information (46 Prozent).[31] Wie bereits erwähnt, sind Verbraucher:innen jedoch gegenwärtig meist nicht in der Lage, das Sicherheitslevel eines IoT-Produktes zu bewerten. Weitere Untersuchungen zeigen, dass Sicherheitsupdate-Labels geeignet sind, diesbezüglich Abhilfe zu schaffen und einen wesentlichen Einfluss auf die Kaufentscheidung der Konsument:innen haben können.[32]

Zahlungsbereitschaft für mehr Cyber-Sicherheit bzw. ein Sicherheitslabel bei IoT-Geräten

Weitere Studien zeigen, dass die Mehrheit der Verbraucher:innen bereit ist, für IoT-Geräte mit höherer Cyber-Sicherheit mehr zu zahlen: So sind laut einer Untersuchung aus Großbritannien Konsument:innen gewillt, für mehr Sicherheit bei SmartWatches, intelligenten Sicherheitskameras und Routern zwischen 32 und 63 Prozent mehr Geld auszugeben.[33] Eine weitere Studie im Auftrag der britischen Regierung zeigt, dass 60 Prozent der Verbraucher:innen bereit sind, für ein IoT-Gerät mit Sicherheitslabel einen Aufschlag von 5 Prozent gegenüber einem gleichwertigen Produkt ohne Label zu zahlen.[34]

[30] Ipsos MORI (2020): Consumer Attitudes Towards IoT Security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

[31] Ipsos MORI (2020): Consumer Attitudes Towards IoT Security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

[32] Morgner, P.; Mai, C.; Koschate-Fischer, N.; Freiling, F.; Benenson, Z. (2020, May): Security update labels: establishing economic incentives for security patching of IoT consumer products. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 429-446). IEEE.

[33] Blythe, J.M.; Johnson, S.D.; Manning, M. (2020): What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices, Crime Sci (2020) 9:1.

[34] Harris Interactive. (2019). Consumer Internet of Things Security Labelling Survey Research Findings. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950429/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report_V2.pdf

4 Perspektive der Hersteller:innen

Neben den Erwartungen und Sichtweisen der Verbaucher:innen wurde auch die Perspektive der herstellenden Unternehmen in Bezug auf die Cyber-Sicherheit bei IoT-Geräten erfasst. Die folgenden Aussagen beruhen dabei insbesondere auf den geführten Interviews mit einem IT-Sicherheitsexperten sowie drei Vertretern der Industrie. Da es sich um die Einschätzung einzelner Akteure handelt, stellen diese keine abschließende und repräsentative Betrachtung der Perspektive der Hersteller:innen dar.

Umsetzung von Cyber-Sicherheitsanforderungen bei der Entwicklung von Consumer-IoT-Geräten

Laut den Aussagen eines Experten, der Unternehmen seit Jahren zur Umsetzung von IT-Sicherheit und Datenschutz berät, würden etablierte Standards und Leitfäden für Cyber-Sicherheit bei der Entwicklung von IoT-Geräten von den Hersteller:innen häufig nicht berücksichtigt oder nur im Nachgang einbezogen. Vielmehr seien diese Standards den Unternehmen oftmals unbekannt und Cyber-Sicherheit sei in der Praxis selten ein relevantes Design-Ziel. Dies deckt sich mit den Aussagen eines Vertreters eines Industrie-Verbands, der beobachtet, dass Hersteller:innen sich nur notgedrungen für Normen und Standards interessieren und möglichst billig produzieren wollen würden. Unverbindliche Normen würden aus seiner Sicht jedoch „eigentlich nichts“ bewirken. Die meisten Interviewpartner:innen sind sich einig, dass es für Hersteller:innen zurzeit häufig nicht ökonomisch sinnvoll sei, Geld in die Entwicklung besserer Sicherheitsfunktionen zu investieren, da die Verbraucher:innen beim Kauf vor allem auf niedrige Preise und Leistungsfähigkeit achten würden und sie Geräte mit starken Sicherheitseigenschaften nicht von Produkten mit unzureichenden Sicherheitsmechanismen unterscheiden könnten.

Die Vertreter von zwei IoT-Herstellern gaben im Rahmen der Interviews jedoch an, dass in ihren Unternehmen die relevanten Standards sehr wohl bekannt seien. Man habe in den Gremien, in denen der neue ETSI Standard EN 303 645[35] diskutiert wurde, mitgewirkt und es sei insbesondere dieser Standard, der bei der Entwicklung der IoT-Geräte Anwendung finden würde. Die Gewährleistung von IT-Sicherheit sei Teil des Qualitätsanspruchs der Unternehmen und habe zur Reputation beigetragen, die man sich aufgebaut habe. Günstigen Anbietern könne man nur mit einer attraktiven Marke und einem hohen Qualitätsanspruch etwas entgegensetzten.

Auch für den Vertreter des Industrie-Verbandes und den Berater für IT-Sicherheit und Datenschutz ist der Dreh- und Angelpunkt der Markenwert eines Unternehmens. Aus ihrer Sicht würden die meisten Unternehmen Security-by-Design-Ansätze bei der Entwicklung von IoT-Geräten erst umsetzen, wenn ein hoher Leidensdruck vorhanden sei oder ein Imageverlust drohe. Wenn ein IoT-Unternehmen aufgrund von Sicherheitsvorfällen in negative Schlagzeilen gerate, habe dies oft schwerwiegende Folgen für die Geschäftsentwicklung. „Wenn sie als Hersteller einmal durch die Presse gehechelt wurden, weil sie nachbessern mussten, wollen sie das nicht noch einmal durchmachen“, so die Aussage aus einem Expert:inneninterview.

[35] siehe Kapitel 5.2

Herausforderungen bei der Gewährleistung von Cyber-Sicherheit bei IoT-Geräten

Sowohl die Vertreter der Industrie als auch der externe IT-Sicherheitsberater sind sich darin einig, dass die langfristige Gewährleistung von Cyber-Sicherheit bei IoT-Geräten mit großen Herausforderungen verbunden sei. Um die Cyber-Sicherheit eines vernetzten Geräts sicherzustellen, müsse von den Hersteller:innen die gesamte Lieferkette miteinbezogen werden. Selbst wenn ein Unternehmen Vernetzungsmodule für IoT-Geräte selbst herstelle, würden stets Teile der Module von Zulieferfirmen eingekauft. Die Vertragsbedingungen zwischen Hersteller:innen und zuliefernden Unternehmen müssten dann jeweils so gestaltet sein, dass die Zulieferfirmen Anpassungen der Softwarebibliotheken liefern, sobald Sicherheitslücken festgestellt werden. In einigen Fällen seien jedoch nicht die Hersteller:innen die bestimmenden Akteure, sondern die Zulieferfirmen hätten die größere Marktmacht und könnten die Vertragsdetails festlegen. Ein Vertreter eines IoT-Herstellers formulierte es folgendermaßen: „Man muss beachten, dass in den Lieferketten die Zulieferer häufig nicht kleine Unternehmen sind, denen man sagen kann, wie sie das machen sollen, sondern dass die Verhältnisse genau umgekehrt sind. Die Zulieferer sind teilweise sehr groß und die Hersteller der Folgeprodukte sind sehr klein, sodass sie dem Diktat der Zulieferer ausgeliefert sind.“ Recherchen der Verbraucherzentrale Rheinland-Pfalz verdeutlichen jedoch, dass die Abhängigkeiten zwischen Zulieferfirmen und Hersteller:innen auch anders geartet sein können und Zulieferer in einigen Fällen in großem Maße von den Herstellerfirmen abhängig sind.[36]

Laut den Aussagen des Vertreters eines IoT-Herstellers sei ferner ein Problem, dass die Hersteller:innen seit einigen Monaten aufgrund des Chipmangels in manchen Fällen nicht die Chips einbauen könnten, die ursprünglich vorgesehen waren. Dies führe zu einer Varianz in den Serienmodellen und stelle eine zusätzliche Schwierigkeit bei der Bereitstellung von Sicherheitsupdates bei IoT-Geräten dar.

Vor dem Hintergrund der vielfältigen Herausforderungen, mit denen Unternehmen bei der langfristigen Gewährleistung von Cyber-Sicherheit bei IoT-Geräten konfrontiert sind, geht der interviewte IT-Sicherheitsexperte davon aus, dass die Kosten für die Instandhaltung von IoT-Geräten um das 5- bis 10-fache steigen würden, wenn Sicherheitsanforderungen vollumfänglich umgesetzt würden.

[36] Verbraucherzentrale Rheinland-Pfalz (2021): Smart Surfer – Fit im digitalen Alltag. Lernhilfe für aktive Onliner:innen. https://smart-surfer.net/asset/61e7d9322a32ed01ec50f8c6/download

5 Bestandsaufnahme relevanter rechtlicher Rahmenbedingungen, Normen & Standards und Zertifizierungssysteme & Kennzeichen

Im Zuge der Bestandsaufnahme wurden rechtliche Rahmenbedingungen, Normen, Standards, Zertifizierungssysteme und Kennzeichen identifiziert und analysiert, die im Kontext der Cyber-Sicherheit bei Consumer-IoT-Geräten eine Rolle spielen. Die zentralen Ergebnisse sind im Folgenden in einer tabellarischen Übersicht dargestellt.

5.1 Rechtliche Rahmenbedingungen

Gesetz/Richtlinie	Beschreibung

Warenkauf-Richtlinie und Digitale-Inhalte-Richtlinie (2019/771/EU und 2019/770/EU)
Nationale Umsetzung:
Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags
und
Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen
	• Umsetzung der beiden Richtlinien in nationales Recht mit Wirkung zum 1. Januar 2022
	• enthalten Aktualisierungspflicht für Waren mit digitalen Elementen und digitale Produkte (beinhaltet Consumer-IoT und ggf. verbundene Cloud-Dienste)
	• Verkäufer:innen und Unternehmer müssen demnach die Funktionsfähigkeit und Cyber-Sicherheit der Geräte und Dienstleistungen auch nach ihrer Übergabe bzw. Zurverfügungstellung gewährleisten
	• der maßgebliche Zeitraum, in dem Aktualisierungen bereitgestellt werden müssen, wird nicht abschließend konkretisiert
	  ○ bei einem Vertrag über die dauerhafte Bereitstellung eines digitalen Produkts ist der maßgebliche Zeitraum der (vereinbarte) Bereitstellungszeitraum[37]
	  ○ in allen anderen Fällen ist der maßgebliche Zeitraum derjenige, den die Verbraucher:innen „aufgrund der Art und des Zwecks der Ware und ihrer digitalen Elemente sowie unter Berücksichtigung der Umstände und der Art des Vertrags erwarten [können]“[38]

Funkanlagenrichtlinie (RED) (2014/53/EU) *Nationale Umsetzung:* *Gesetz über die Bereitstellung von Funkanlagen auf*	• formuliert Anforderungen zur Beschaffenheit von Software und Informationen, die von Hersteller:innen beim Inverkehrbringen von Funkanlagen (Router, Smartphones, etc.) für einen bestimmungsmäßigen und EU-konformen Betrieb bereitgestellt werden müssen → umfasst auch Softwareänderungen

[37] § 327 f. BGB.
[38] § 327 f, § 475b Abs. 4 BGB.

dem Markt	und -Updates nach dem Inverkehrbringen der Produkte

5.2 Normen und Standards

Norm/Standard	Beschreibung
ETSI EN 303 645	• weltweit anwendbarer Mindestsicherheitsstandard für die sichere Entwicklung von IoT-Geräten • veröffentlicht durch die europäische Normungsorganisation ETSI (European Telecommunications Standards Institute) am 30. Juni 2020 • baut auf dem vorherigen Standard TS 103 645 auf • baut auf dem UK Code of Practice for Consumer IoT Security[39] auf • gemeinsam mit der Industrie entwickelt
IEC 62443	• internationale Normenreihe über „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme“ • beschreibt sowohl technische als auch prozessorale Aspekte der Industriellen Cyber-Sicherheit

5.3 Zertifizierungssysteme und Kennzeichen

Zertifizierungssystem/Kennzeichen	Beschreibung
Zertifizierung im Rahmen des EU Cybersecurity Act[40]	• europäischer Rechtsakt zur Cyber-Sicherheit („Cybersecurity Act“) ist am 27. Juni 2019 in Kraft getreten • der Rechtsakt bildet u.a. einen Rahmen für EU-weite Zertifizierungen für Produkte, Dienstleistungen und Prozesse der Informations- und Kommunikationstechnologien (IKT) • die Zertifikate gelten in allen Mitgliedsstaaten der EU und geben Auskunft über die erfüllten Anforderungen der Geräte an IT-Sicherheit → Berücksichtigung der Kritikalitätsstufe des zu zertifizierenden Produktes, Prozesses oder der Dienstleistung
Zertifizierungssysteme	• technische Prüforganisationen bieten weitere Zertifizierungssysteme von IoT-Geräten an

[39] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
[40] Rechtsakt zur EU-Cybersicherheit. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_DE.html

unabhängiger technischer Prüforganisationen	• basieren auf international anerkannten Normen und Standards (unter anderem ETSI EN 303645)
IT-Sicherheitskennzeichen des BSI	• freiwilliges IT-Sicherheitskennzeichen für Produkte, die für den Verbrauchermarkt bestimmt sind • Antragstellung durch Hersteller:innen seit Dezember 2021 möglich • wird auf Basis einer Eigenprüfung und Selbsterklärung der Hersteller:innen erteilt; Hersteller:innen verpflichten sich dabei, vom BSI erarbeitete oder existierende Standards einzuhalten; BSI führt im Rahmen der Antragstellung Plausibilitätsprüfung der Angaben und Selbsterklärung durch • produktspezifische Informationsseiten für Verbraucher:innen geben Auskunft über von den Hersteller:innen zugesicherte Sicherheitsmerkmale der gekennzeichneten Produkte, die zugrundeliegenden Standards und enthalten aktuelle Sicherheitsinformationen (bspw. zu Schwachstellen) • anlasslose (stichprobenartig) bzw. anlassbezogene (etwa bei Bekanntwerden einer Sicherheitslücke) Prüfung der gekennzeichneten Produkte im Rahmen der nachgelagerten Marktaufsicht des BSI • zunächst wird das Kennzeichen für Breitband-Router und E-Mail-Dienste vergeben • in Zukunft werden immer weitere Produktkategorien durch das BSI veröffentlicht, bspw. im Jahr 2022 im Bereich IoT (Basis ETSI EN 303 645)
Blauer Engel	• ein seit 1978 vergebenes Umweltzeichen für besonders umweltschonende Produkte und Dienstleistungen • Träger: Bundesumweltministerium • Zweck: Orientierung beim umweltbewussten Einkauf • ein von Dritten zertifiziertes Umweltzeichen • Beinhaltet Anforderungen zur „Kontinuität des Softwareproduktes“ (Punkt 3.1.3.3) ○ „Es muss möglich sein, das Softwareprodukt über einen längeren Zeitraum zu nutzen, ohne dass schwerwiegende Nachteile (insbesondere Probleme der IT-Sicherheit) auftreten. Dazu muss der Softwarehersteller eine Funktionalität anbieten, mit der das Softwareprodukt auf dem aktuellen Stand gehalten werden kann. Sicherheitsupdates müssen kostenlos erfolgen, Updates mit zusätzlicher Funktionalität sind davon ausgeschlossen. Der Antragsteller verpflichtet sich dazu, Sicherheitsupdates für das zu kennzeichnende Produkt

	für mindestens 5 Jahre ab Bereitstellungsende anzubieten.“[41]

[41] https://produktinfo.blauer-engel.de/uploads/criteriafile/de/DE-UZ%20215-202001-de%20Kriterien-2020-01-16.pdf

6 Lösungsansätze zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT

Im Folgenden sind die von den Teilnehmenden des Workstreams identifizierten Lösungsansätze zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT-Geräten aufgeführt. Die Übersicht erhebt keinen Anspruch auf Vollständigkeit, die dargestellten Lösungsansätze zeigen jedoch die Breite des Raums der Möglichkeiten. Die unterschiedlichen Spezifizierungsgrade der folgenden Lösungsansätze sind Ergebnis unterschiedlich tiefgehender Diskussionen der Workstream-Teilnehmer:innen zu den einzelnen Ansätzen und der in der Arbeitsgruppe vorhandenen Expertise. Die Detailtiefe der Ausarbeitung ist kein Indikator dafür, welche Ansätze zuerst oder mit höherer Priorität umgesetzt werden sollen. Die zwei priorisierten Handlungsempfehlungen des Workstreams werden in Kapitel 7 näher ausgeführt.

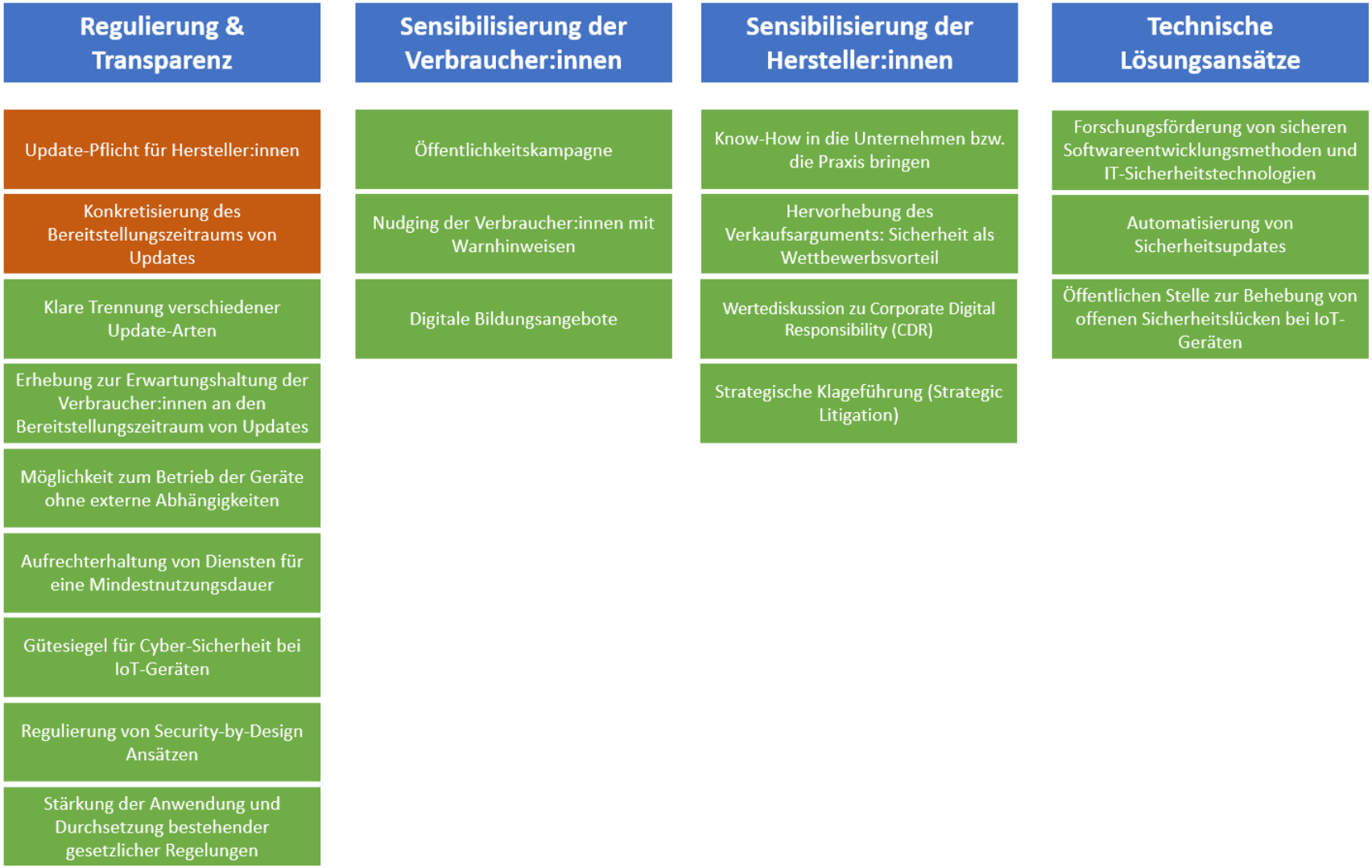

Abbildung 4: Übersicht über die im Workstream gesammelten und erarbeiteten Lösungsansätze (grün) und priorisierten Handlungsempfehlungen (orange) zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT-Geräten

6.1 Regulierung und Transparenz

Klare Trennung der verschiedenen Update-Arten

Unterschiedliche Update-Arten (funktionserhaltend, funktionsändernd, Sicherheit, Content) müssen, soweit technisch möglich und sinnvoll, voneinander getrennt und separat ausgeliefert werden. Jedem Update müssen die Informationen darüber beiliegen, was genau dadurch am Produkt verändert wird und insbesondere, ob es sich um ein Sicherheitsupdate handelt.

Durchführung einer Studie zur Erwartungshaltung der Verbraucher:innen an den Bereitstellungszeitraum von Updates bei IoT-Geräten

Bisher gibt es kein klares Bild und keine konkrete gesetzliche Festlegung, welche Erwartungshaltung die Verbraucher:innen an den Zeitraum haben, in dem IoT-Geräte mit Updates unterstützt werden sollen. Mithilfe einer repräsentativen Umfrage kann diese Fragestellung genauer untersucht werden, damit auf Basis der Ergebnisse faktenbasierte Entscheidungen für mögliche entsprechende Regulierungsansätze getroffen werden können.

Möglichkeit zum Betrieb der Geräte ohne externe Abhängigkeiten

Consumer-IoT-Geräte wie zum Beispiel Kühlschränke sollten in ihrer Kernfunktionalität auch offline und ohne externe Abhängigkeiten, zum Beispiel ohne Cloud-Dienste, funktionieren. Nach Ende des Support-Zeitraums sollte eine permanente Trennung von allen Netzwerkdiensten erfolgen können („Versiegeln“).

Aufrechterhaltung von Cloud-Diensten für eine Mindestnutzungsdauer

Consumer-IoT-Geräte sind meist Teil eines digitalen Ökosystems. Sichere Cloud-Dienste müssen vor diesem Hintergrund mitgedacht und für eine möglichst lange Mindestnutzungsdauer aufrechterhalten werden.

Gütesiegel für Cyber-Sicherheit bei IoT-Geräten

Für Verbraucher:innen ist es in vielen Fällen nicht erkennbar, welche Consumer-IoT-Geräte eine hohe Cyber-Sicherheit gewährleisten. Ein verpflichtendes Gütesiegel bzw. Kennzeichen für IoT-Geräte kann Verbraucher:innen in die Lage versetzen, zu überprüfen, welche Produkte grundlegende Sicherheitsstandards erfüllen.

Regulierung von Security-by-Design-Ansätzen

Verbraucherschutzorganisationen und IT-Sicherheitsexpert:innen weisen vielfach darauf hin, dass Security-by-Design-Prinzipien von Beginn an bei der Entwicklung von IoT-Geräten beachtet werden müssen. Die Anwendung dieser Ansätze sollte daher gesetzlich vorgeschrieben werden. Vorbild könnte die angestrebte Regulierung zu Cyber-Sicherheit bei IoT-Geräten in Großbritannien sein.[42]

Stärkung der Anwendung und Durchsetzung bestehender gesetzlicher Regelungen

Rechtliche Anforderungen, die Berührungspunkte zur IT-Sicherheit haben können, sind teilweise bereits gesetzlich normiert, etwa in Art. 32 DSGVO. Im Consumer-IoT-Bereich werden diese Vorgaben jedoch laut fachlicher Einschätzung einiger Workstream-Teilnehmer:innen

[42] https://www.gov.uk/government/news/new-cyber-laws-to-protect-peoples-personal-tech-from-hackers

noch nicht ausreichend aufgegriffen: weder von den Hersteller:innen bei der Gestaltung von Technik, noch von den Aufsichtsbehörden (beispielsweise, aber nicht allein, den Datenschutzbehörden) in der Gesetzesdurchsetzung und in der öffentlichen Debatte, wenn stattdessen neue Regelungen gefordert werden. Aus Sicht einiger Workstream-Teilnehmer:innen müssten jedoch keine neuen Regelungen, die leicht zu Inkonsistenzen führen können, eingeführt werden, wenn bestehende gesetzliche Normen zur Anwendung gebracht würden. In diesem Fall könnten bestehende aufsichtsbehördliche Strukturen und Prozesse für die Durchsetzung verwendet werden.

6.2 Sensibilisierung der Verbraucher:innen

Nudging der Verbraucher:innen mit Warnhinweisen

Laut den Interviewaussagen mehrerer Expert:innen für Verbraucherschutz und IT-Sicherheit haben Verbraucher:innen häufig ein geringes Verständnis und Bewusstsein beim Thema Cyber-Sicherheit. Warnhinweise, die auf dem Gerät oder über eine verbundene App angezeigt werden, können bei den Nutzer:innen ein Bewusstsein schaffen, entsprechende Sicherheitsmaßnahmen, beispielsweise das regelmäßige Updaten der Software, durchzuführen.

Öffentlichkeitskampagne, um das Bewusstsein der Verbraucher:innen für Sicherheitsrisiken bei IoT-Geräten zu erhöhen

Mithilfe einer Öffentlichkeits- bzw. Awarenesskampagne kann das Verständnis der Verbraucher:innen für die Sicherheitsrisiken bei der Nutzung von IoT-Geräten erhöht und ein Bewusstsein geschaffen werden, Sicherheitsaspekte bei der Kaufentscheidung miteinfließen zu lassen.

Digitale Bildung für Verbraucher:innen: Wie können Verbraucher:innen IoT-Geräte sicher nutzen

Analog zu Öffentlichkeitskampagnen können auch digitale Bildungsangebote das Verständnis und Bewusstsein der Verbraucher:innen für das Thema Cyber-Sicherheit von IoT-Geräten erhöhen.

6.3 Sensibilisierung der Hersteller:innen

Know-how in die Unternehmen bzw. die Praxis bringen

Nach Erfahrungen der Workstream-Teilnehmer:innen fehlt es vor allem KMU häufig an Know-how zu IT-Sicherheit im eigenen Unternehmen. Stattdessen werden diese Bereiche häufig ausgelagert, wobei unklar bleibt, wer die Qualitätssicherung der eingekauften Lösungen durchführen kann. Diese fehlenden Kompetenzen können zu Sicherheitsschwachstellen oder einer unzureichenden Implementierung von Sicherheitsmechanismen führen. Mithilfe eines allgemeinen Lastenhefts mit vorgegebenen Anforderungen an die IT-Sicherheit des zu entwickelnden Produkts oder Dienstes könnten die Unternehmen in die Lage versetzt werden, die eingekauften Lösungen zu prüfen. Dafür müssten die zentralen Informationen in einem niedrigschwelligen Format bereitgestellt werden.

Hervorhebung des Verkaufsarguments: Sicherheit als Wettbewerbsvorteil

Untersuchungen zeigen, dass IT-Sicherheit eine recht geringe Rolle beim Kauf von IoT-Geräten spielt.[43] Dies hängt jedoch in vielen Fällen mit fehlender Transparenz und Informationsasymmetrien zwischen den Verbraucher:innen und den Unternehmen zusammen.[44] Verbraucher:innen, die für das Thema Cyber-Sicherheit im IoT-Bereich sensibilisiert sind, können den Druck auf die Hersteller:innen erhöhen, sichere Geräte zu entwickeln.

Wertediskussion zu Corporate Digital Responsibility (CDR) in und mit Unternehmen

Die gesetzliche Regulierung spielt bei der Gewährleistung von Cyber-Sicherheit im IoT-Bereich eine zentrale Rolle. Gleichzeitig kann sie aber immer nur einen Teil zum Verbraucherschutz beitragen. So dauern Gesetzgebungsverfahren häufig sehr lange und die Regelungen bedürfen aufgrund allgemeiner und technikneutraler Formulierung auch häufig der Auslegung auf den konkreten Einzelfall, so dass die konkreten Anforderungen nicht immer von vornherein ersichtlich sind. Des Weiteren kann ein gesetzgeberischer „Zwang“ dazu führen, dass Unternehmen incentiviert werden, „nur“ die Gesetze einzuhalten bzw. Schlupflöcher zu suchen. Eine Wertediskussion in den Unternehmen sowie mit weiteren relevanten Akteuren zur IT-Sicherheit von IoT-Geräten und der Unternehmensverantwortung in der digitalen Gesellschaft könnte über die gesetzlichen Vorgaben hinaus positive Wirkungen in diesem Kontext erzielen. So könnten sich Unternehmen mit Maßnahmen wie zum Beispiel einer freiwilligen Selbstverpflichtung zur umfassenden Umsetzung von Security-by-Design-Ansätzen positiv in der Öffentlichkeit positionieren.

Strategische Klageführung (Strategic Litigation)

Nach Erfahrungen der Workstream-Teilnehmer:innen werden bereits bestehende gesetzliche Anforderungen an Cyber-Sicherheit teilweise von den Marktakteuren nicht eingehalten. Teilweise besteht auch Rechtsunsicherheit darüber, welche existierenden IT-Sicherheits-Frameworks aus rechtlicher Sicht eingesetzt werden sollen und aus Sicht der Dialogpartner:innen besitzen die zuständigen Aufsichtsbehörden oft nicht die notwendigen Kapazitäten, die Einhaltung durchzusetzen. In diesem Falle könnten klageberechtigte Akteure Klage gegen Hersteller:innen erheben, die vorgeschriebene Sicherheitsanforderungen nicht erfüllen. Gerichte könnten anschließend feststellen, welche Anforderungen auf welche Weise und nach welcher Auslegung bzw. welchem Framework umzusetzen sind.

6.4 Technische Lösungsansätze

Automatisierung von Sicherheitsupdates

Insbesondere bei displaylosen Consumer-IoT-Geräten ist häufig unklar, wie Sicherheitsupdates automatisch aufgespielt werden können. Es sollte gezielt Forschung betrieben werden, wie das Updateprozedere bei solchen Geräten effektiv umgesetzt werden kann.

---

[43] Ipsos MORI (2020): Consumer Attitudes Towards IoT Security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978685/Consumer_Attitudes_Towards_IoT_Security_-_Research_Report.pdf

[44] Morgner, P.; Mai, C.; Koschate-Fischer, N.; Freiling, F.; Benenson, Z. (2020, May): Security update labels: establishing economic incentives for security patching of IoT consumer products. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 429-446). IEEE.

Förderung der Forschung zur Umsetzung von sicheren Entwicklungsmethoden in der Softwareentwicklungspraxis und von praktisch nutzbaren IT-Sicherheitstechnologien

Laut den Interviewsausagen eines IT-Sicherheitsexperten ist die Implementierung von Security-by-Design-Ansätzen kostspielig und wird von Hersteller:innen nicht immer oder nur unzureichend umgesetzt. Generell fehlt häufig das entsprechende Know-how in den Unternehmen für die Umsetzung von IT-Sicherheitskonzepten. Es wäre wünschenswert, dass Security-Frameworks, Konzepte und Tools für die praktische Umsetzung von IT-Sicherheit, die einfach nutzbar sind, entwickelt und den Unternehmen bereitgestellt werden, sodass diese sich nicht mehr selbst um die Entwicklung entsprechender Ansätze kümmern müssen. Auch sollte die Forschung und Entwicklung von IT-Sicherheitstechnologien und deren Überführung in die Praxis gefördert werden. Beispiele dafür sind etwa homomorphe Verschlüsselungsverfahren oder Secure Multi-Party Computation.

Einrichtung einer öffentlichen Stelle zur Behebung von offenen Sicherheitslücken bei IoT-Geräten

Sobald IoT-Hersteller:innen vom Markt verschwinden, können sie keine Sicherheitsupdates für ihre Produkte mehr bereitstellen und mögliche Schwachstellen innerhalb ihrer Geräte identifizieren und beheben. In diesen Fällen könnte eine öffentliche Stelle die Verwaltung dieser Sicherheitslücken übernehmen und entsprechende Sicherheitsupdates für die Verbraucher:innen bereitstellen. Solch ein „After-Service-Dienstleister“ könnte zum Beispiel beim BSI angesiedelt sein.

7 Priorisierte Handlungsempfehlungen zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT

Aus den verschiedenen Lösungsansätzen kristallisierten sich in den gemeinsamen Diskussionen der Stakeholder:innen und in der Auseinandersetzung mit verschiedenen Expert:innenmeinungen zwei Ansätze heraus, die im Folgenden als priorisierte Handlungsempfehlungen tiefergehend ausformuliert werden. Aus Sicht der Arbeitsgruppe sind diese Empfehlungen sowohl erfolgversprechend als auch vergleichsweise einfach umzusetzen und sollten von den relevanten Entscheidungsträger:innen schnellstmöglich implementiert werden.

7.1 Handlungsempfehlung 1: Update-Pflicht für Hersteller:innen

Problemstellung

Im Rahmen der zum Januar 2022 in Kraft getretenen Umsetzungen der Warenkauf- und Digitale Inhalte-Richtlinie (WKRL und DIRL) werden Verkäufer:innen bzw. Unternehmer[45] verpflichtet, Aktualisierungen bzw. Software-Updates, die für den Erhalt der Vertragsmäßigkeit vernetzter Produkte erforderlich sind, bereitzustellen. Händler:innen müssen so die Funktionsfähigkeit und IT-Sicherheit der Geräte und digitalen Produkte auch nach ihrer Übergabe bzw. Bereitstellung gewährleisten. Darüber hinaus müssen Verbraucher:innen durch hinreichende Hinweise über diese Aktualisierungen informiert werden (§ 475b Abs. 4, § 327e Abs. 3, f Abs. 1 BGB).

Diese Update-Pflicht ist zweifelsohne zu begrüßen und stellt einen wichtigen und notwendigen Schritt zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT-Geräten dar. Gleichwohl gilt die Update-Pflicht nur für die Verkäufer:innen der vernetzten Produkte, aber nicht für die Hersteller:innen. In der Praxis wird dies zu Problemen führen, da die Verkäufer:innen im Gegensatz zu den Hersteller:innen meist keinen Einfluss auf die Entwicklung und Bereitstellung von Updates haben und dementsprechend nicht eigenständig in der Lage sind, der Aktualisierungspflicht nachzukommen. Stattdessen sind digitale Elemente typischerweise „stärker mit ihrem Hersteller verbunden als physische Produkte. Häufig ist ein Fernzugriff möglich; die Auslieferung von Updates erfolgt ohne nennenswerte logistische Kosten.“[46]

Umsetzung der Handlungsempfehlung

Damit die Update-Pflicht in der Praxis Wirkung entfaltet, sollten vor diesem Hintergrund analog zu den Verkäufer:innen auch die **Hersteller:innen von Consumer-IoT-Geräten zur Bereitstellung von Aktualisierungen verpflichtet werden**. Diese Pflicht sollte immer mindestens dann greifen, wenn Sicherheitslücken in Consumer-IoT-Geräten bekannt werden oder durch

[45] Das BGB, knüpft im Rahmen des Kaufrechts an den „Verkäufer“ einer Sache an, bei digitalen Produkten wird der Begriff „Unternehmer“ verwendet. Nachfolgend werden die Begriffe „Verkäufer:innen“, „Unternehmer“ und „Händler:innen“ als die direkten Vertragspartner:innen der Verbraucher:innen für den vorliegenden Bericht synonym verwendet.

[46] Vzbv (2021): Längere Gewährleistungsdauer fördert Nachhaltigkeit - Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zum Entwurf eines Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags. S.10. https://www.vzbv.de/sites/default/files/downloads/2021/01/07/stellngnahme_umsetzung_wkrl_07.01.2020.pdf

zuständige Behörden, zum Beispiel durch das BSI, gemeldet werden.[47] Aus Sicht des Workstreams wäre die Umsetzung solch einer Herstellerverpflichtung als Ergänzung der WKRL und DI-RL im BGB, welches in erster Linie die Rechtsbeziehungen zwischen Vertragspartner:innen und Privatpersonen regelt, jedoch eher ein Fremdkörper. Stattdessen sollte eine gewährleistungsähnliche Haftung zur Bereitstellung von Aktualisierungen für herstellende Unternehmen **in einer EU-Verordnung festgeschrieben** werden. Eine Festschreibung in einer vom Rat der Europäischen Union bereits angedachten horizontalen Gesetzgebung zu Cyber-Sicherheit bei IoT-Geräten[48] würde sich anbieten, sofern diese entwickelt wird. Eine öffentlich-rechtliche Verortung dieser Verpflichtung würde zudem den Vollzug durch Marktüberwachungsbehörden ermöglichen.

Komplementarität mit anderen EU-Gesetzen

Wichtig hervorzuheben ist, dass solch eine Gesetzesinitiative komplementär zu bestehenden EU-Gesetzen laufen müsste und so deren Wirksamkeit verstärken würde. Die Komplementarität zur DSGVO wäre insofern gegeben, da die hier geforderte Update-Pflicht in drei Punkten über die Verpflichtung zu Sicherheitsupdates hinausginge. Dabei ist zu beachten, dass Artikel 32 DSGVO, der die Sicherheit der Verarbeitung personenbezogener Daten betrifft, zwar keine ausdrückliche Verpflichtung des Verantwortlichen und Auftragsverarbeiters zu Sicherheitsupdates enthält. Aus der allgemein gehaltenen Formulierung, dass der Verantwortliche und Auftragsverarbeiter „geeignete technische und organisatorische Maßnahmen [treffen muss], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“, wird sich aber in den meisten Fällen eine Pflicht zu Sicherheitsupdates ableiten lassen. Dies gilt zumindest für die Zeit, in der personenbezogene Daten verarbeitet werden.[49]

Vor diesem Hintergrund würde die hier geforderte Update-Pflicht die DSGVO in Bezug auf die folgenden drei Punkte ergänzen: Erstens könnte eine eigenständige gesetzliche Verankerung einer Update-Pflicht ggf. auch Funktionsupdates betreffen, was die nachhaltige Nutzung von Geräten attraktiver machen würde. Zweitens richtet sich die DSGVO nur an die für die Datenverarbeitung Verantwortlichen und deren Auftragsverarbeiter, die nicht notwendigerweise mit den Hersteller:innen identisch sein müssen. Dies führt in der Praxis jedoch häufig zu Interessenskonflikten zwischen herstellenden und betreibenden Unternehmen von Technologien und nur zu einer zögerlichen Umsetzung der rechtlichen Verpflichtungen, da diese mit einem hohen Koordinationsaufwand und ungünstigen Anreizstrukturen einhergeht. Deswegen ist es ratsam, in einer eigenständigen Update-Pflicht gezielt die Hersteller:innen der IoT-Geräte in die Pflicht zu nehmen. Drittens ist die DSGVO nur anwendbar bei der Verarbeitung personenbezogener Daten. Trotz der Weite der datenschutzrechtlichen Definition des „Personenbezugs“ von Daten kann es Fälle geben, in denen die DSGVO nicht anwendbar ist (beispielweise wenn es mehrere Nutzer:innen eines IoT-Gerätes gibt oder wenn die Daten von Hersteller:innen anonymisiert werden und die Betroffenen daher nicht mehr „ausgesondert“, sprich iden-

[47] Vgl. auch Vzbv (2021): Längere Gewährleistungsdauer fördert Nachhaltigkeit - Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zum Entwurf eines Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags. S.11. https://www.vzbv.de/sites/default/files/downloads/2021/01/07/stellngnahme_umsetzung_wkrl_07.01.2020.pdf

[48] https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/

[49] Siehe auch Wagner, B.; Salzmann, M. (2019): IT-Sicherheit im Internet of Things: Überwachungspotential smarter Küchenhelfer, ZD-Aktuell 2019, 06731.

tifiziert werden können). Auch für solche Fälle, in denen nicht personenbezogene Daten verarbeitet werden, wäre eine solche Update-Pflicht, wie sie hier beschrieben wird, in einem eigenständigen Gesetz zu empfehlen.

Eine Komplementarität besteht daneben auch zum EU Cybersecurity Act. Mit dieser europäischen Verordnung wird zum einen das Mandat der EU-Cybersicherheitsagentur ENISA gestärkt, deren genuine Aufgabe es ist, die Informationssicherheit in der EU zu gewährleisten und stärken. Zum anderen wird damit ein EU-weit geltendes Rahmenwerk für die freiwillige IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen etabliert. Ein solches Zertifizierungssystem könnte auf den inhaltlichen und rechtlichen Vorgaben einer Update-Verpflichtung aufbauen. So könnte das Problem adressiert werden, dass Verbraucher:innen mangels entsprechender IT-Kenntnisse in den seltensten Fällen Sicherheitslücken selbst erkennen können, und zugleich die freiwillige Zertifizierung durch verpflichtende Updates aufgewertet werden.

7.2 Handlungsempfehlung 2: Konkretisierung des Bereitstellungszeitraums von Updates

Problemstellung

Im Rahmen der Aktualisierungspflicht ergibt sich ein zweites Problem: Der konkrete Zeitraum, in dem ein:e Verbraucher:in die Versorgung mit Updates erwarten kann, wurde vom Gesetzgeber nicht explizit festgeschrieben. So müssen gemäß §327f und §475b Absatz 4 BGB Updates für die Zeitspanne bereitgestellt werden, die ein:e Verbraucher:in „aufgrund der Art und des Zwecks“ des Produkts sowie „unter Berücksichtigung der Umstände und der Art des Vertrags erwarten kann“. Die Frist soll demnach von der Art und dem Zweck der Waren und der digitalen Funktionen abhängig sein. Es stehen jedoch keine konkreten Kriterien zu Verfügung, nach denen sich beim Kauf von vernetzten Geräten einschätzen ließe, wie lange Verkäufer:innen zur Bereitstellung notwendiger Aktualisierungen verpflichtet sein sollen. Zweifelsohne werden diese Formulierungen deshalb zu vielen Diskussionen und zu Rechtsunsicherheit führen.

Umsetzung der Handlungsempfehlung

Mehr Rechtssicherheit könnte indes erreicht werden, wenn alle **Hersteller:innen dazu verpflichtet würden, Angaben zur erwartbaren Nutzungsdauer der Geräte und zum Bereitstellungszeitraum von Updates zu machen**. Auf diese Weise hätten Verbraucher:innen einen Anhaltspunkt dafür, in welchem Zeitraum sie mit Aktualisierungen rechnen und diese einfordern können. Aus Sicht der Arbeitsgruppe sollte solch eine Verpflichtung der herstellenden Unternehmen ebenso wie die zuvor genannte Update-Pflicht **in einem EU-Gesetz festgeschrieben** werden. Auch in diesem Kontext würde sich die Aufnahme solch einer Regelung in die angedachte horizontale Gesetzgebung zu Cyber-Sicherheit bei IoT-Produkten anbieten. [50]

Wie der Bundesrat in einer Stellungnahme zum Entwurf des Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags anmerkte, besteht dabei das Risiko, „dass Hersteller bewusst eine kurze Nutzungsdauer angeben, die

[50] https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/

hinter der objektiven Erwartung und gegebenenfalls auch hinter dem regelmäßigen Gewährleistungszeitraum von zwei Jahren zurückbleibt". Auf der anderen Seite kann es sein, dass „der Wettbewerb ein wirkungsvolles Korrektiv bildet und ein flächendeckendes Absenken von Qualitätsversprechen der Hersteller verhindert."[51] Aus der Sicht der Arbeitsgruppe ist Letzteres zu erwarten, wenn alle Hersteller:innen verpflichtet werden, Informationen zur Mindestnutzungsdauer anzugeben, und die Verbraucher:innen die Möglichkeit haben, Kaufentscheidungen auf Basis dieser Angaben zu treffen.

Hier stellt sich aber die Frage nach wirksamen Anreizen für eine nachhaltige Nutzungsdauer. Um einerseits die Regelung offen für entsprechende positive Marktdynamiken zu halten, andererseits aber ein Unterlaufen der gesetzlich bereits vorgesehenen „erwartbaren Nutzungsdauer" zu verhindern, empfiehlt die Arbeitsgruppe daher, gesetzlich festzuschreiben, dass die von den Hersteller:innen angegebene Nutzungsdauer „zumindest" die erwartbare Nutzungsdauer im Sinne der Umsetzung der WKRL und DI-RL nicht unterschreiten darf. Damit würde die mit dem Begriff der „Erwartbarkeit" verbundene Rechtsunsicherheit von den Verkäufer:innen auf die Hersteller:innen übertragen. Dies ist aus rechtspolitischen Gesichtspunkten jedoch vertretbar, da die Verkäufer:innen die ihnen obliegende Update-Pflicht ohnehin vertraglich an die Hersteller:innen weitergeben werden, da sie gar nicht in der Lage sind, die Updates selbst bereitzustellen. Tatsächlich könnte eine entsprechende Update-Verpflichtung der Hersteller:innen vielmehr das in der Praxis befürchtete Problem entschärfen, bei dem Verkäufer:innen in Fällen marktmächtiger Hersteller:innen Gefahr laufen, dass diese ihrer Update-Pflicht angesichts der Verhandlungsmacht der Hersteller:innen gerade nicht in vollem Umfang an diese weitergeben können.

Zur Vermeidung der Rechtsunsicherheit seitens der Beteiligten wäre es schließlich zu empfehlen, die Dauer entsprechend bestimmter Warenklassen oder zumindest über eine Konkretisierung der Kriterien zur Auslegung der Erwartungshaltung festzulegen. Für solche Kriterien enthalten die Erwägungsgründe der WKRL bzw. die Begründung zum deutschen Umsetzungsgesetz bereits einige Beispiele wie etwa den Preis, Werbeaussagen oder Erkenntnisse über die übliche Nutzungsdauer für Sachen der jeweiligen Art („life-cycle"). Darüber hinaus sind weitere Kriterien zu empfehlen, wie insbesondere das Gesamtrisiko, das für die Nutzer:innen des Produkts, aber auch für Dritte ausgeht (insb. im Falle einer Übernahme der Kontrolle über die Sache durch Angreifer für einen Botnet-Angriff). Zumindest für die Ermittlung eines solchen Gesamtrisikos ist auch auf die Tatsache abzustellen, wie weit verbreitet die Nutzung des Produkts bzw. wie relevant das Produkt bei solchen Sicherheitsvorfällen (basierend auf Erfahrungswerten) ist. [52]

[51] Bundesrat (2021): Stellungnahme des Bundesrates zum Entwurf eines Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags. https://www.bundesrat.de/SharedDocs/drucksachen/2021/0101-0200/146-21(B).pdf;jsessionid=B32BB22E839E9392ABE230F69093A992.2_cid374?__blob=publicationFile&v=1

[52] Vgl. auch Vzbv (2021): Längere Gewährleistungsdauer fördert Nachhaltigkeit - Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zum Entwurf eines Gesetzes zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrags. S.15. https://www.vzbv.de/sites/default/files/downloads/2021/01/07/stellngnahme_umsetzung_wkrl_07.01.2020.pdf

8 Fazit

Cyber-Sicherheit und ökologische Nachhaltigkeit sind im Internet der Dinge untrennbar miteinander verbunden. Consumer-IoT-Geräte werden mit einem hohen Einsatz an Ressourcen und einem erheblichen Ausstoß von Emissionen hergestellt. Darüber hinaus entsteht bei der Entsorgung eine große Menge an Elektroschrott, dessen Gesamtvolumen seit Jahren kontinuierlich ansteigt. Grund hierfür ist unter anderem die Kurzlebigkeit von Elektro-Produkten wie IoT-Geräten, bei denen Softwarekomponenten über die Lebensdauer, Funktionalität und Zuverlässigkeit entscheiden. Bei diesen Geräten hat eine unzureichende Updatefähigkeit und mangelnde Cyber-Sicherheit direkte negative Auswirkungen auf die Umweltbilanz der Produkte. Je länger die Geräte genutzt werden können, desto eher rechtfertigen sich deren ökologische Kosten.

Vor diesem Hintergrund war es das Anliegen des Workstreams „Digitales Mindesthaltbarkeitsdatum“, die Zusammenhänge und Auswirkungen von unzureichender Cyber-Sicherheit im Internet der Dinge in Bezug auf ökologische Nachhaltigkeit aufzuzeigen und Lösungsansätze und Handlungsempfehlungen zur Verlängerung der sicheren Nutzungsdauer von Consumer-IoT-Geräten als Beitrag für mehr Nachhaltigkeit zu identifizieren.

Die Ergebnisse der Arbeitsgruppe verdeutlichen, dass es kein Allheilmittel, aber zumindest eine Vielzahl von ineinandergreifenden und einander verstärkenden Ansätzen in diesem Kontext gibt. Insgesamt wurden im Workstream 19 Lösungsansätze identifiziert, die sich in vier Bereiche unterteilen lassen: Regulierung & Transparenz, Sensibilisierung der Verbraucher:innen, Sensibilisierung der Hersteller:innen und technische Lösungsansätze. Aus den verschiedenen Lösungsansätzen kristallisierten sich in den gemeinsamen Diskussionen der Dialogpartner:innen sowie in der Auseinandersetzung mit verschiedenen Expert:innenmeinungen zwei Ansätze heraus, die als priorisierte Handlungsempfehlungen in Kapitel 7 tiefergehend ausformuliert wurden. Dabei handelt es sich um Empfehlungen, die sowohl erfolgversprechend als auch vergleichsweise einfach umzusetzen sind und bei denen keine oder nur geringe „unerwünschte Nebenwirkungen“ erwartet werden.

Im Konkreten empfiehlt die Arbeitsgruppe dabei, dass Hersteller:innen von Consumer-IoT-Geräten dazu verpflichtet werden,

1. Aktualisierungen für die Geräte bereitzustellen und
2. Angaben zur erwartbaren Nutzungsdauer der Geräte und zum Bereitstellungszeitraum von Updates zu machen.

Grundsätzlich sieht die Arbeitsgruppe jedoch Handlungsbedarf auf allen Ebenen, wie die Sammlung an Lösungsansätzen (Kapitel 6) verdeutlicht: Die Gewährleistung von Cyber-Sicherheit bei IoT-Geräten und die Verlängerung der sicheren Nutzungsdauer der Produkte ist eine gesamtgesellschaftliche Aufgabe, bei der insbesondere die Politik und Industrie, aber auch die Verbraucher:innen zusammenarbeiten und miteinbezogen werden müssen. Hoffnungen setzt die Arbeitsgruppe in diesem Kontext auch auf die im Koalitionsvertrag formulierten Ziele der Bundesregierung, ‚Nachhaltigkeit by design‘ zum Standard bei Produkten zu machen. Diese zielführenden Absichten der Bundesregierung müssen nun schnellstmöglich in die Praxis umgesetzt werden. Darüber hinaus hat die Recherche im Rahmen des Workstream verdeutlicht, wie wenig Forschungsergebnisse es zur Schnittstelle von Cyber-Sicherheit und Nachhaltigkeit im IoT-Bereich gibt. Weitere Forschung ist in diesem Themenfeld aus Sicht der Arbeitsgruppe dringend erforderlich.