IT-SICHERHEIT FÜR VERNETZTE GERÄTE UND DIGITALE DIENSTE

Vorschläge des Verbraucherzentrale Bundesverbandes zur Konsultation zu einem europäischen Gesetz über Cyberresilienz

25. Mai 2022

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. ZUSAMMENFASSUNG

Der Verbraucherzentrale Bundesverband e.V. (vzbv) begrüßt die Initiative der Europäischen Kommission (EU-Kommission) für ein Gesetz über Cyberresilienz (CRA). Vernetzte Geräte ziehen zunehmend in Haushalte von Verbraucher:innen ein und erleichtern den Alltag in immer mehr Bereichen. Der Entwicklung steht jedoch ein Sicherheitsdefizit gegenüber, denn da immer mehr vernetzte Produkte in Gebrauch sind, nehmen auch die Sicherheitsmängel zu, die Manipulationen ermöglichen. Bislang fehlt es an gesetzlichen Mindestanforderungen für IT-Sicherheit, die Hersteller verpflichten, Produkte des *Internets of Things* (IoT) über alle Branchen hinweg sicher zu gestalten.

Um Verbraucher:innen zu schützen, braucht es europäische Regeln, die Hersteller zur Einhaltung von klar definierten IT-Sicherheitsanforderungen verpflichten. Dabei müssen die Prinzipien des *Security by Design* und *Security by Default* befolgt werden. Vernetzte Geräte und digitale Dienste müssen auf die Einhaltung der Vorgaben kontrolliert werden.

Das angekündigte Gesetz über Cyberresilienz muss daher folgendes leisten:

- Verpflichtende Mindestanforderungen an IT-Sicherheit von IoT Geräten und Anwendungen stellen. Diese müssen verbindlich und europaweit für alle Sektoren gültig sein.
- IT-Sicherheitsanforderungen über den gesamten Lebenszyklus abdecken (Design, Herstellung, Vertrieb, Nutzung und Entsorgung oder Recycling).
- Flächendeckende, unabhängige Konformitätsbewertungen vorschreiben und Marktüberwachung über den Lebenszyklus eines vernetzten Produktes hinaus regeln.
- Verbraucher:innen ins Zentrum von Sicherheitsanforderungen stellen. IT-Sicherheit kann nur gelingen, wenn die Fähigkeiten, Einschränkungen und Gewohnheiten von Nutzer:innen mit einbezogen werden.

II. ABSTRACT

During the last years, the use of connected devices and digital services by consumers has steadily increased. The Internet of Things (IoT) can make everyday life easier and the popularity of connected products is growing fast. Nevertheless, the level of security regarding consumers' IoT products remains alarmingly low. While the EU has developed rules and standards regarding the cybersecurity of critical infrastructure and some specific sectors, a horizontal act covering the cybersecurity of consumer products is still lacking. The Federation of German Consumer Organisations (vzbv) therefore welcomes the EU Commission's initiative for a Cyber Resilience Act (CRA).

In order to protect consumers, a comprehensive European regulation is needed. Producers and providers of connected products and digital services must be responsible for complying with basic cybersecurity requirements. This should involve the principles of security by design and security by default, which must be respected in all stages of the product life cycle.

The Cyber Resilience Act should include the following requirements:

- Introducing clear obligations for producers and providers of connected devices and digital services to adhere to specific minimum-requirements for cybersecurity, which must be applied to all sectors.
- Ensuring the compliance with the cybersecurity requirements through the whole life cycle of an IoT product including the design, production, sales, use, disposal and/or recycling.
- Establishing comprehensive, independent conformity assessments and regulate a continuous market surveillance that is executed during the whole life cycle.
- Applying a consumer-centric approach of cybersecurity taking the capabilities, limitations and habits of users taken into account.

III. EINLEITUNG

Vernetzte Geräte sind im Alltag vieler Verbraucher:innen immer weiter verbreitet. Von der Rückfahrkamera zum Einparken im Auto, dem Smart TV zum Streaming oder smarten Insulinpumpen für Diabetes-Patient:innen und intelligentem Spielzeug kann fast jeder Bereich des Alltags heute vernetzt werden. Das *Internet of Things* (IoT) vernetzt Technologien, verbindet Sensoren mit Software, sodass Geräte selbstständig miteinander kommunizieren und autonome Entscheidungen treffen können. Aber vor allem Smart Home Systeme und IoT-Produkte weisen immer wieder Sicherheitsmängel auf. Daher begrüßt der Verbraucherzentrale Bundesverband e.V. (vzbv) die Initiative der Europäischen Kommission (EU-Kommission) für gesetzliche Mindestanforderungen an die IT-Sicherheit von vernetzten Geräten.

IT-Sicherheit wird in der Entwicklung von allen digitalen Produkten und Dienstleistungen, Software und Hardware, bislang nur ungenügend mitgedacht. Das öffnet Tür und Tor für Manipulationen und Schadsoftware. Die Folgen reichen von Datenschutzverletzungen, Datendiebstahl oder Betrug bis zu physischen Schäden und Gefahren. Berichte zu Datenlecks und Hacks häufen sich, Passwörter und E-Mail-Adressen tauchen öffentlich zugänglich im Netz auf, und immer mehr Nutzer:innen sind persönlich betroffen.[1] Neben finanziellen Schäden können Angriffe jedoch auch die physische Unversehrtheit bedrohen. Smart Home Systeme werden etwa vermehrt für Stalking-Zwecke ausgenutzt.[2] Auch im medizinischen Bereich ergeben sich Risiken für Verbraucher:innen. So wurden etwa Sicherheitslücken bei vernetzten Insulinpumpen öffentlich, die aufgrund von unverschlüsselt übertragenen Daten angreifbar waren.[3] Aus Sicht der Verbraucher:innen ist die IT-Sicherheit in Deutschland ungenügend. Nur 2,4 Prozent der Bevölkerung zeigte sich 2022 in einer Befragung mit dem Stand der Cybersicherheit zufrieden, 42,6 Prozent sahen bei der IT-Sicherheit im gesamten Digitalbereich den dringendsten Handlungsbedarf.[4]

Der Wunsch nach verpflichtenden Regeln für die IT-Sicherheit von vernetzten Geräten ist hoch und Verbraucher:innen fühlen sich unter den vorherrschenden Bedingungen nicht hinreichend geschützt: 70 Prozent der Verbraucher:innen wünschen sich gesetzlich festgeschriebene, einheitliche Mindestanforderungen.[5]

---

[1] Brühl, Jannis; Muth, Max: Datenleck:"Collection #1" - Riesen-Leak von E-Mail-Adressen und Passwörtern aufgetaucht, 2019, https://www.sueddeutsche.de/digital/datenleck-passwoerter-collection1-1.4291534, 09.05.2022; Information is beautiful: World's Biggest Data Breaches & Hacks, 2021, https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, 09.05.2022.

[2] Lu, Donna: How Abusers Are Exploiting Smart Home Devices, 2019, https://www.vice.com/en/article/d3akpk/smart-home-technology-stalking-harassment, 26.04.2022.

[3] Jansen, Jonas: Wenn IT-Einbrecher lebenswichtige Medizingeräte entern, 2016, https://www.faz.net/aktuell/wirtschaft/insulin-wenn-it-einbrecher-lebenswichtige-medizingeraete-entern-14467704.html, 26.04.2022.

[4] Eco: Digitalpolitisches Barometer; 2022, https://www.eco.de/presse/eco-digitalbarometer-ueber-zwei-drittel-aller-buergerinnen-unzufrieden-mit-digitaler-transformation-in-ihrem-bundesland/, 26.04.2022.

[5] vzbv: Verbraucher:innen wünschen sich gesetzliche Regelungen, 2022, https://www.vzbv.de/pressemitteilungen/cybersicherheit-verbraucherinnen-wuenschen-sich-gesetzliche-regelungen, aufrufbar ab: 13.06.2022.

IV. IT-SICHERHEITSRISIKEN FÜR VERBRAUCHER:INNEN

Die vielfachen Risiken und die Unsicherheit im Umgang mit IoT Geräten verdeutlichen, dass die IT-Sicherheit von vernetzten Produkten und digitalen Diensten in der Europäischen Union (EU) ohne flächendeckende und gesetzliche Verpflichtungen nicht ausreichend von den Herstellern berücksichtigt und umgesetzt wird. Für Verbraucher:innen ergeben sich daraus Gefahren im Alltag, da Basisanforderungen wie Verschlüsselung, sichere Authentisierungsverfahren oder die Bereitstellung von Sicherheitsupdates bei vielen Apps oder Geräten nicht zur Verfügung stehen.

In einer Studie zu Sicherungsmaßnahmen von Online-Accounts untersuchte der vzbv über 200 digitale Dienste aus 16 Branchen. Dabei zeigte sich, dass Sektoren ohne bereits existierende branchenspezifische Regulierungen eine sichere 2-Faktor-Authentisierung (2FA) nicht flächendeckend zur Account-Sicherung anboten. Auch in den Fällen, in denen 2FA verfügbar war, blieb das Sicherungssystem in vielen Fällen optional und gehörte nicht zur Standardeinstellung. Im Online-Handel standen bei 77 Prozent der untersuchten Anbieter zur Account-Sicherung gar keine Option zur 2FA zur Verfügung.[6] Hier können sich Verbraucher:innen vor Daten- oder Identitätsdiebstahl und finanziellen Schäden ohne gesetzliche Pflichten nicht ausreichend schützen.

Bei Untersuchungen von vernetzten Produkten werden immer wieder Schwachstellen und Sicherheitslücken aufgedeckt, die auch auf eine unzureichende Priorisierung von Sicherheit seitens der Hersteller zurückzuführen ist. Im Jahr 2021 testete die belgische Verbraucherschutzorganisation Test-Achats/Test-Aankoop (TA) die Sicherheit von 16 Smart Home Geräten, darunter smarte Türschlösser, Babyphones, Alarmanlagen oder Saugrobotter sowie die dazugehörigen Apps. Insgesamt ergaben sich dabei 54 Schwachstellen, wobei eine von vier Schwachstellen kritisch war oder sogar einen hohen Schweregrad mit Blick auf mögliche Sicherheitsvorfälle aufwies.[7] Unter anderem konnten Schwachstellen über eine WLAN-Verbindung ausgenutzt werden, sodass Geräte durch einen Wi-Fi-Deauthentifikation-Angriff von der WLAN-Verbindung getrennt wurden und nicht mehr ordnungsgemäß funktionierten. Dadurch ließen sich etwa Alarmanlagen ausschalten oder Türschlösser öffnen. Des Weiteren verschlüsselten viele Geräte die Kommunikation zwischen Gerät und App nicht, verfügten über unzureichende Standardeinstellungen, oder ließen sich leicht über eine ungeschützte physische Schnittstelle manipulieren. Für die Hersteller der Produkte wäre es möglich, die Mängel zu beheben, während Verbraucher:innen im Großteil der Fälle keine Einflussmöglichkeit haben.

Auch wenn Mängel bestehen und Herstellern bekannt sind, ist es für Verbraucher:innen in den meisten Fällen kaum ersichtlich, welche IT-Sicherheitsanforderungen ein vernetztes Produkt erfüllt, denn Informationen über die Sicherheitseigenschaften eines Produktes sind kaum verfügbar. Gleichzeitig lassen sich Herstellerangaben nicht ein-

[6] Vzbv: Anbieter und Hersteller zu IT-Sicherheit verpflichten, 2022, https://www.vzbv.de/pressemitteilungen/anbieter-und-hersteller-zu-it-sicherheit-verpflichten, 07.04.22.

[7] Euroconsumers: Hackable home project: Euroconsumers unveils worrying results for smart device owners, 2021, http://assets.ctfassets.net/iapmw8ie3ije/1YOk8JU1LogUJFn898wLH1/7302188d91713d1b007811c4e8343c84/Hackable_home_press_release.pdf, 12.04.22.

fach überprüfen und auch Sicherheitsvorfälle müssen nur in bestimmten Fällen offengelegt werden. Laut einer Studie der niederländischen Verbrauchervereinigung (Consumentenbond) stellt nur einer von fünf Herstellern Informationen dazu bereit, wie lange für ein vernetztes Produkt Updates zur Verfügung gestellt werden.[8] Das führt zu Unsicherheiten und Vertrauensverlusten aufseiten der Verbraucher:innen. Im Verbraucherreport 2021 des vzbv gaben 56 Prozent der Befragten an, dass sie sich im Internet und Bereich Digitales nicht ausreichend geschützt fühlten.[9] Die Sorge spiegelt sich auch in IT-Sicherheitsvorfällen: Im Jahr 2021 haben die Delikte im Bereich der Cyberkriminalität in Deutschland um zwölf Prozent zugenommen.[10] Die Zahlen bestätigen die Beobachtungen der Verbraucherzentralen: Drei Viertel der Verbraucher:innen gaben 2019 an, innerhalb der letzten 12 Monate von einem IT-Sicherheitsvorfall betroffen gewesen zu sein.[11] Ein Drittel aller eingegangenen Beschwerden sind Produkten und Dienstleistungen im digitalen Bereich zuzuschreiben.[12] Gleichzeitig bleibt ein Großteil der Vorfälle unerkannt, weshalb im Bereich der Cyberkriminalität von einer großen Dunkelziffer ausgegangen wird.[13]

Insgesamt wünschten sich 2020 77 Prozent der Verbraucher:innen strengere Vorgaben für Hersteller, 71 Prozent befürworteten mehr staatliche Produktsicherheitskontrollen.[14] IT-Sicherheit spielt dabei eine zentrale Rolle: 94 Prozent aller Verbraucher:innen wünschten sich mehr Schutz von Anwendungen und Daten vor unberechtigten Zugriffen. Eine Lösung wäre die Versorgung von Geräten und Software mit Sicherheitsupdates. Diese hielten 93 Prozent bei Bekanntwerden von Sicherheitslücken für wichtig; 91 Prozent wünschten sich Sicherheitsupdates für eine angemessene Dauer.[15]

VERPFLICHTENDE IT-SICHERHEITSANFORDERUNGEN FÜR IOT GERÄTE

- Die Risiken von IoT-Geräten sind vielfältig und die Zahlen von Delikten im Bereich der Cyberkriminalität steigen seit Jahren kontinuierlich an. Vor Datenmanipulation, Spam und Phishing oder Identitätsdiebstahl mit finanziellen Schaden sind Verbraucher:innen unzureichend geschützt.
- Um Verbraucher:innen zu schützen, braucht es flächendeckende, europäische Regeln, die Hersteller zur Einhaltung von IT-Sicherheitsanforderungen verpflichten. Vernetzte Geräte und digitale Dienste müssen auf die Einhaltung der Vorgaben kontrolliert werden.

[8] Consumentenbond: Fabrikanten informeren onvoldoende over updates, 2022, https://www.consumentenbond.nl/nieuws/2022/fabrikanten-informeren-onvoldoende-over-updates, 11.04.2022.

[9] vzbv: Verbraucherreport 2021, 2021, S. 5, https://www.vzbv.de/sites/default/files/2021-10/21_10_12_Verbraucherreport-Ergebnisse_Summary_FINAL_0.pdf, 29.03.2022.

[10] BKA: Bundeslagebild Cybercrime 202, 2021, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110, 10.05.2022.

[11] vzbv: IT-Sicherheit: Erwartungen und Erfahrungen der Verbraucherinnen und Verbraucher - Erkenntnisse der Marktbeobachtung des vzbv, 2020, S. 7, https://www.vzbv.de/pressemitteilungen/verbraucher-setzen-it-sicherheit-voraus, 29.03.2022.

[12] vzbv: Verbraucherspiegel, 2021, https://www.vzbv.de/marktbeobachtung/verbraucherspiegel, 29.03.2022.

[13] BKA: Bundeslagebild Cybercrime 202, 2021, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110, 10.05.2022.

[14] vzbv: Verbraucherreport 2021, 2021, S. 6, https://www.vzbv.de/sites/default/files/2021-10/21_10_12_Verbraucherreport-Ergebnisse_Summary_FINAL_0.pdf, 29.03.2022.

[15] vzbv: IT-Sicherheit: Erwartungen und Erfahrungen der Verbraucherinnen und Verbraucher - Erkenntnisse der Marktbeobachtung des vzbv, 2020, https://www.vzbv.de/pressemitteilungen/verbraucher-setzen-it-sicherheit-voraus, 29.03.2022.

V. IT-SICHERHEIT IN DER EU

1. BESTEHENDER RECHTSRAHMEN IN DER EU UND HORIZONTALE REGELUNGEN

Der europäische Rechtsrahmen für Produktsicherheit wurde für physische Produkte entwickelt. Wenn es um Cybersicherheit geht, ist jedoch mehr nötig, als zu prüfen, ob das Material eines Smartphones ungefährlich ist, oder das Display nicht splittert. Die spezifischen Sicherheitsanforderungen wie der Schutz vor Manipulation oder Störungen bei IoT-Geräten und digitalen Diensten nimmt der bestehende Rechtsrahmen der EU bislang nicht in den Blick. Das hat zu unterschiedlichen Regelwerken in den Mitgliedsstaaten geführt. Hier braucht es eine klare europäische Regulierung, die verschiedene Regelwerke harmonisiert und hohe Mindestanforderungen europaweit durchsetzen kann.

Mit Blick auf Produkte für Verbraucher:innen wurden vor allem einzelne und als besonders kritische Produktgruppen vertikal reguliert (Fahrzeuge, Medizinprodukte, Funkanlagen oder Messgeräte). Die Begriffe "Sicherheit" und "Cybersicherheit" werden allerdings nicht grundlegend definiert, um Verbraucher:innen im Umgang mit IoT-Geräten vor Sicherheitsvorfällen zu schützen. Dabei legt der Rechtsakt zur Cybersicherheit umfassende IT-Schutzziele dar. Daraus gehen jedoch keine Pflichten hervor, die Hersteller für einen Zugang zum europäischen Binnenmarkt befolgen müssen. So führt der Rechtsakt zur Cybersicherheit, der 2019 in Kraft trat, zwar ein Schema für eine Cybersicherheitszertifizierung ein, dieses bleibt jedoch freiwillig, sodass die Anforderungen in der Praxis nicht aufgegriffen wurden. Auch der 2022 verabschiedete delegierte Rechtsakt zur Funkanlagenrichtlinie legt Cybersicherheitsanforderungen fest. Die Anforderungen treten jedoch erst im August 2024 in Kraft und müssen noch von den europäischen Normungsorganisationen (ETSI, CEN, CENELEC) in Standards umgesetzt werden. Die Anforderungen haben zudem einen eingeschränkten Anwendungsbereich und gelten nur zum Zeitpunkt des Inverkehrbringens eines Produktes.[16]

Um Cybersicherheit ganzheitlich zu betrachten, müssen der Produkt- sowie der Sicherheitsbegriff an die Entwicklungen im Bereich des IoT angepasst werden. Als Produkt müssen auch nicht-physische Produkte wie eigenständige Software gelten, die immer komplexer werden. Hier braucht es eindeutige Anforderungen an die Softwarequalität unter Einbezug von Sicherheitskriterien. IT-Sicherheit muss für Hard- und Software mindestens die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit umfassen und sowohl gegen Angriffe als auch unbeabsichtigte Fehler und Ereignisse schützen. Bislang werden die Ziele jedoch nur in Bruchstücken im europäischen Rechtsrahmen gesichert. Der delegierte Rechtsakt zur Funkanlagenrichtlinie regelt etwa, dass drahtlose Geräte Kommunikationsnetze beeinträchtigen, enthält aber keine Anforderungen mit Blick auf die Geräte selbst. Die anstehende Reform der Produktsicherheitsverordnung greift Aspekte der Cybersicherheit auf, bleibt jedoch unvollständig, indem etwa der Schutz vor unautorisierten Zugriffen nicht gewährleistet wird und die Verordnung ebenfalls nur zum Zeitpunkt des Markteintritts anwendbar ist.

---

[16] Delegierte Verordnung (EU) 2022/30 der Kommission vom 29. Oktober 2021 zur Ergänzung der Richtlinie 2014/53/EU, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0030&from=EN, 11.05.2022.

Eine horizontale Regulierung (Politikoption 5[17]) ist am geeignetsten, um den IT-Sicherheitsstandard von IoT-Produkten in der gesamten EU zu erhöhen und das Vertrauen von Verbraucher:innen nachhaltig zu stärken. Flächendeckende Anforderungen vermeiden überschneidende Regulierungen oder Gesetzeslücken und etablieren einen klaren und einheitlichen Rechtsrahmen. Die freiwilligen Vorgaben und unterschiedliche nationale Umsetzungen der Sicherheitszertifizierung des CSA haben zu einer Fragmentierung des Cybersicherheitslevels in der EU geführt. Ein breiter Anwendungsbereich in einem horizontalen Gesetz kann sicherstellen, dass der Binnenmarkt harmonisiert wird und für alle Hersteller gleiche Wettbewerbsbedingungen gelten.

HERSTELLER ZUR CYBERSICHERHEIT VERFPLICHTEN

- Die bestehenden Regelungen nehmen IoT-Produkte nicht ausreichend in den Blick und müssen ergänzt werden. Für einen umfassenden Schutz bedarf es einer grundlegenden Definition von Cybersicherheit in einem horizontalen Rechtsakt, der eine Harmonisierung von vernetzten Geräten auf dem Binnenmarkt sicherstellen kann.
- IT- Sicherheitsanforderungen müssen verbindlich und EU-weit über alle Sektoren hinweg vorgeschrieben werden. Aus den Mindeststandards müssen klare Pflichten für die Hersteller sowie Vorschriften für die Überwachung der Anforderungen nach dem Inverkehrbringen eines Produktes oder Dienstes hervorgehen.
- Hersteller müssen verpflichtet werden, IT-Sicherheitsanforderungen bei vernetzten Produkten über den Lebenszyklus hinaus (Design, Herstellung, Vertrieb, Nutzung und Entsorgung oder Recycling) zu erfüllen.

2. IT-SICHERHEITSZIELE DER EU (ART. 51 RECHTSAKT ZUR CYBERSICHERHEIT)

Der Rechtsakt zur Cybersicherheit (CSA) enthält eine umfassende Auflistung der Sicherheitsziele für eine freiwillige Cybersicherheitszertifizierung.[18] Hierauf sollte die EU-Kommission einen verpflichtenden Rahmen für die IT-Sicherheit von Produkten und Diensten aufbauen.

Die Ziele beinhalten den Schutz gegen unbefugte Zugriffe und Speicherung für den gesamten Lebenszyklus eines vernetzten Produktes oder Dienstes (Art. 51 (a,b) CSA). Außerdem sollen Sicherheitslücken ermittelt und Zugriffe und Datenverarbeitungen dokumentiert werden (Art. 51 (c,d,e,f) CSA). Bekannte Sicherheitslücken werden überprüft und bei einem Sicherheitsvorfall muss gewährleistet werden, dass der Zugang zu Diensten, Funktionen und Daten zeitnah wieder zur Verfügung steht. Die Sicherheitsziele folgen damit dem Prinzip des *Security by Design*, die auch für verwendete Software und Hardware in Produkten gilt (Art. 51 (j) CSA), die ebenfalls frei von bekannten Sicherheitslücken sein sollen und sichere Updates gewährleisten müssen. Auch das

[17] EU Kommission: Sondierung zu einer Folgenabschätzung - Ares(2022)1955751, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Gesetz-uber-Cyberresilienz-neue-Cybersicherheitsvorschriften-fur-digitale-Produkte-und-Nebendienstleistungen_de, 18.05.22.

[18] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881, 11.05.2022.

Prinzip *des Security by Default* wird in Art. 51 (i) des CSA geregelt, der die Voreinstellungen und Technikgestaltung auf Sicherheit prüft.[19]

Die Ziele sind umfassend angelegt und können bei Anwendung einen Mindestschutz gegen Fehler oder Angriffe bereitstellen. Dennoch zeigen sich rechtliche Unklarheiten, die im CRA weiter ausdifferenziert werden müssen, um einen vollständigen Schutz zu gewährleisten.[20] So sollten Vertraulichkeit, Integrität und Verfügbarkeit von vernetzten Geräten und Diensten je als eigenes Schutzziel definiert werden.

Neben der Ausdifferenzierung und Konkretisierung der Sicherheitsziele werden im Rechtsakt für Cybersicherheit keine verpflichtenden Vorgaben für Hersteller und Anbieter definiert. Der CRA muss diese Lücke schließen und Mindestanforderungen gesetzlich verankern, um die Ziele auf dem europäischen Binnenmarkt durchzusetzen. Dazu sollten die Sicherheitsziele des Rechtsakts zur Cybersicherheit als Grundlage dienen und über alle Sektoren hinweg gültig sein.

RECHTSSICHERE DEFINITION DER IT-SCHUTZZIELE

Die IT-Schutzziele müssen rechtssicher gestaltet sein und die Vertraulichkeit, Verfügbarkeit und Integrität von IT-Systemen und Produkten als übergeordnetes Sicherheitsziel definiert werden.

3. RISIKOBASIERTE KATEGORIEN VON VERNETZTEN GERÄTEN UND DIGITALEN DIENSTEN

Auf Basis des Rechtsaktes zur Cybersicherheit könnte eine risikobasierte Einteilung von vernetzten Geräten und webbasierten Anwendungen vorgenommen werden. In Art. 52 CSA werden digitale Dienste und vernetzte Geräte grundsätzlich in die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ und/oder „hoch““ eingeteilt.[21]

Diese Einteilung birgt jedoch Gefahren. Insgesamt bewerten Verbraucher:innen die IT-Sicherheit von vernetzten Geräten kritisch. Jede:r vierte Verbraucher:in hielt in einer Studie von Deutschland sicher im Netz e.V. (DsiN) aus dem Jahr 2021 vernetzte Haustechnik für gefährlich.[22] Daher muss gewährleitstet werden, dass alle Produkte unabhängig von einer Risikoeinteilung die grundlegenden IT-Schutzziele erfüllen. Die Grundanforderungen müssen sicherstellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit von digitalen Diensten und vernetzten Produkten auch bei Produkten einer niedrigen Vertrauenswürdigkeitsstufe gewahrt werden. Gleichzeitig ist bei einer Einteilung entscheidend, nach welchen Kriterien das Risikopotenzial für verschiedene Produktgruppen beurteilt wird. Die Eigenschaften sowie die Nutzung der Produkte müssen

[19] Ebd.

[20] Stewart Ferguson, Donald David: European Cybersecurity Certification Schemes and cybersecurity in the EU internal market, 2022, *Int. Cybersecur. Law Rev.* https://link.springer.com/article/10.1365/s43439-021-00044-5#citeas; 05.05.2022.

[21] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881, 11.05.2022.

[22] Deutschland Sicher im Netz: DsiN Sicherheitsindex 2021, 2021, https://www.sicher-im-netz.de/file/13161/download?token=se3us1Mq, 05.04.2022.

mit Blick auf mögliche Manipulationen und Schäden analysiert werden. So kann etwa von einem smarten Wasserkocher ein hohes Risiko ausgehen, wenn dieser mit einem Heimnetzwerk verbunden ist und für Sprachbefehle ein Mikrophon integriert hat. Bei einem IT-Sicherheitsvorfall könnte damit über das Gerät Zugriff auf ein Smart-Home-System erlangt werden oder das Mikrophon zum Abhören genutzt werden. 78 Prozent der Verbraucher:innen bewerten 2022 daher den Zugriff auf Kamera, Mikrophon oder Standortdaten als Sicherheitsrisiko. Die Anbindung an eine Cloud empfinden 63 Prozent als sicherheitsrelevant.[23]

Ein anderes Risiko ergibt sich aus der Nutzungsdauer von Geräten. Diese weichen teilweise stark voneinander ab. Insbesondere Haushaltsgeräte wie Kühlschränke oder Waschmaschinen, aber auch Türschlösser sind oftmals über einen Zeitraum von bis zu zehn Jahren im Einsatz. Auch Handys sind heute länger im Einsatz, werden allerdings durchschnittlich nach dreieinhalb Jahren ausgetauscht.[24] Der technische Support für ein Smartphone liegt meist bei vier bis fünf Jahren. Für langlebigere Produkte braucht es jedoch andere Vorgaben, sonst laufen Verbraucher:innen Gefahr, dass einer smarten Waschmaschine über Jahre hinweg keine Sicherheitsupdates mehr zur Verfügung gestellt werden und das Produkt durch veraltete Software anfällig für Angriffe wird. Auch unter Nachhaltigkeitsgesichtspunkten muss die Versorgung mit Updates und Support sichergestellt bleiben. Dies muss bereits im Design der Produkte mit vorgesehen werden, so dass etwa ältere Hardware ausgetauscht werden kann, oder die Reparatur und Wartung durch spezialisierte Dienstleister vom Hersteller ermöglicht wird.

IT-SICHERHEIT FÜR ALLE RISIKOKLASSEN VERPFLICHTEN

- Die grundlegenden IT-Schutzziele müssen auf alle Produkte unabhängig der Risikoklassen angewandt werden.
- Sicherheitsrelevante Produkteigenschaften wie Kameras und Mikrophone, Anbindung an Heimnetzwerke und Clouds oder die Nutzungsdauer sollen als Kriterien für die Einteilung von Risikoklassen einbezogen werden.

VI. KERNFORDERUNGEN FÜR DEN CRA

Durch IoT-Geräte und Dienste hat sich die Vulnerabilität von Verbraucher:innen im digitalen Bereich stark erhöht. Sie sind im Umgang mit vernetzten Geräten Risiken ausgesetzt, die sie nicht einschätzen und überblicken können. Dabei sind sie gezwungen sich auf die Herstellerangaben zur technischen und organisatorischen Sicherung von Produkten zu verlassen. Die derzeitige Situation muss dringend auf europäischer Ebene angepasst werden, um Verbraucher:innen im Umgang mit vernetzten Geräten ausreichend zu schützen. Analog zur klassischen Produktsicherheit muss der CRA die Cybersicherheit von Produkten vorschreiben, um zu gewährleisten, dass vernetzte Produkte und digitale Dienste sicher sind.

[23] vzbv: Verbraucher:innen wünschen sich gesetzliche Regelungen, 2022, https://www.vzbv.de/pressemitteilungen/cybersicherheit-verbraucherinnen-wuenschen-sich-gesetzliche-regelungen, aufrufbar ab: 13.06.2022.

[24] Euler Hermes: Can 5G reignite the Smartphone industry?, 2022, https://www.allianz-trade.com/content/dam/onemarketing/aztrade/allianz-trade_com/en_gl/erd/publications/the-watch/2022_02_035G.pdf, 16.05.2022.

1. IT-SICHERHEIT ÜBER DEN GESAMTEN LEBENSZYKLUS

Um vernetzte Produkte sicher zu gestalten, muss IT-Sicherheit über den gesamten Lebenszyklus eines vernetzten Gerätes oder digitalen Dienstes mitbedacht und sichergestellt werden. Das umfasst alle Phasen und setzt bereits bei der Idee, dem Design und der Herstellung an. 75 Prozent der Verbraucher:innen besorgt es, wenn Sicherheitsupdates für Produkte eingestellt werden.[25] Während der zu erwartenden Nutzungsdauer müssen Hersteller verpflichtet werden, IT-Sicherheitslücken für ihre digitalen Produkte und Dienste zu schließen und Verbraucher:innen Sicherheitsupdates und Informationen zu Sicherheitsvorfällen zügig und niederschwellig zur Verfügung stellen. Des Weiteren muss die Entsorgung oder das Recycling sicher möglich sein. Auch hier müssen Daten weiter geschützt oder Anwendungen sicher und nachhaltig gelöscht werden können.

Verbraucher:innen müssen darauf vertrauen können, dass Produkte und Dienste von vorneherein sicher angelegt sind und bei Vorfällen und Veränderungen auch während ihrer Lebensdauer mit Sicherheitsupdates versorgt werden. Daher müssen neue Lücken überwacht, gemeldet und geschlossen werden und Produkte auf neue technische Voraussetzungen hin angepasst werden.

UPDATE-PFLICHT FÜR HERSTELLER

- Hersteller müssen verpflichtet werden, Sicherheitslücken bei Bekanntwerden umgehend zu schließen.
- Sicherheitsupdates müssen für den gesamten Zeitraum der erwartbaren Nutzungs- und Lebensdauer eines digitalen Dienstes oder vernetzten Produktes bereitgestellt werden.
- Sicherheitsupdates müssen als solche gekennzeichnet werden und einfach und deutlich erläutern, wozu sie dienen und was sich mit der Installation genau ändert. Sicherheitsupdates dürfen zudem nicht für andere Aktualisierungszwecke genutzt werden. Dazu müssen sie, soweit technisch möglich, von anderen Update-Arten (funktionserhaltende, funktionsverändernde Updates, Content-Updates) getrennt werden.

2. SECURITY BY DESIGN UND SECURITY BY DEFAULT

Verbraucher:innen sehen sich im Umgang mit IoT zahlreichen Risiken ausgesetzt. Das unverschlüsselte Senden und Empfangen von Informationen nehmen 79 Prozent der Verbraucher:innen als Sicherheitsrisiko wahr, 76 Prozent sind besorgt über unzureichende Standardsicherheitseinstellungen auf Geräten und 73 Prozent würden sich sicherer fühlen, wenn sie ihre Nutzerkonten mit einem zweiten Faktor schützen können.[26]

Sicherheitsanforderungen müssen deshalb schon bei der Entwicklung von Soft- und Hardware in allen Schritten umgesetzt werden. Schwachstellen müssen minimiert werden und eine verschlüsselte Übertragung und Speicherung von Daten sowie sichere Authentisierungsverfahren (etwa 2-Faktor-Authentisierung) müssen in allen Produkten

[25] vzbv: Verbraucher:innen wünschen sich gesetzliche Regelungen, 2022, https://www.vzbv.de/pressemitteilungen/cybersicherheit-verbraucherinnen-wuenschen-sich-gesetzliche-regelungen, aufrufbar ab: 13.06.2022.

[26] Ebd.

verpflichtend sichergestellt werden. Außerdem müssen Anwendungen und Daten mit Passwörtern auf einem angemessenen Sicherheitsniveau geschützt werden, sodass unsichere und Standard-Passwörter bereits in den Einstellungen ausgeschlossen werden. Zuletzt müssen Produkte und Dienste auch mit entsprechend sicheren Voreinstellungen versehen und bei der Entwicklung mit Blick auf eine sichere Anwendung abgesichert sein.

IT-SICHERHEIT VON ANFANG AN MITDENKEN

IT-Sicherheit muss kontinuierlich mitgedacht werden. Dafür muss Produktdesign neu gedacht werden und Sicherheitsaspekte in jeden Schritt einbezogen werden. Sicherheitsprozesse müssen so gestaltet sein, dass bekannte Risiken standardmäßig ausgeschlossen sind und neue Sicherheitslücken schnell und nachhaltig geschlossen werden.

3. ANWENDERFREUNDLICHE SICHERHEITSLÖSUNGEN

Verbraucher:innen dürfen nicht länger als das schwächste Glied der „IT-Sicherheitskette“ betrachtet werden. Digitale Produkte und Dienste werden nur dann sicher, wenn Sicherheitsansätze Verbraucher:innen in den Mittelpunkt stellen. Sicherheitsrelevante, menschliche Fehler im Umgang mit IoT-Geräten ergeben sich aus Systemen, die technikzentriert sind und im täglichen Umgang überfordern oder behindern.

Benutzeroberflächen müssen intuitiv und leicht zu bedienen sein, es muss abgewogen werden, welche Sicherungssysteme automatisch laufen können und wo es der Entscheidung von Nutzer:innen bedarf. Auch Sicherheitshinweise und Meldungen müssen so gestaltet sein, dass sie einfach und verständlich informieren und Verbraucher:innen situativ befähigen, sich sicherheitskonform zu verhalten. Sicherheitsfunktionen und Anforderungen müssen für Verbraucher:innen erkennbar und sichtbar sein, um effektiv zu schützen.

Dafür ist eine sichere und datenschutzfreundliche Technikgestaltung entscheidend. IT-Sicherheit muss die Lebensrealität von Verbraucher:innen in den Fokus nehmen, denn sichere Lösungen, können nur unter Einbezug ihrer Gewohnheiten, Möglichkeiten und Einschränkungen erfolgreich sein. „*Usable Security*“ muss im gesamten Lebenszyklus mitbedacht werden, sodass Systeme immer mit Blick auf die menschliche Anwendung designt werden.

USABLE SECURITY

Ein Produkt oder eine Dienstleistung muss Sicherheitslösungen bereitstellen, die einfach zu verstehen und zu erlernen sind sowie von Verbraucher:innen schnell umgesetzt werden können. Dafür müssen sie einfach zu merken sein und müssen auch von Verbraucher:innen akzeptiert werden.

4. UNABHÄNGIGE KONFORMITÄTSBEWERTUNGEN

Der New Legislative Framework (NLF) ist das europäische Konzept für die technische Harmonisierung des EU-Binnenmarktes. Es legt die Regeln zur Konformitätsbewertung von Produkten fest, die Sicherheitsanforderungen entsprechen müssen. Der Rahmen

basiert auf einem Vertrauensprinzip und sieht vor, dass Hersteller mit einer CE-Erklärung auf einem Produkt selbst erklären können, geltenden Sicherheitsanforderungen zu entsprechen. Handelt es sich um risikoträchtige Produkte, braucht es anstelle einer Herstellerselbsterklärung eine Prüfung durch unabhängige und notifizierte Stellen.

Der Rechtsakt zur Cybersicherheit teilt Produkte, Dienste und Prozesse in die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ und „hoch“ ein, macht jedoch keine Angaben dazu, welche Produkte in die jeweiligen Schemata der Cybersicherheitszertifikate fallen (Artikel 52 (1) CSA). Eine Kategorisierung soll daher mit Blick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalles erfolgen.

Insbesondere IoT-Geräte bergen vielfältige Risiken und können beispielsweise durch ihre Vernetzung oder den massenhaften Einsatz von baugleichen Teilen hohen Schaden verursachen. Diese Risiken müssen sich in den Kontrollen wiederspiegeln. Um eine unabhängige Zertifizierung durch notifizierte Stellen im Rahmen des NLF zu ermöglichen, müssen IoT-Geräte und digitale Dienste als risikoträchtige Produkte definiert werden.

KONTROLLEN MÜSSEN RISIKO MITEINBEZIEHEN

IoT-Produkte müssen unabhängig geprüft werden, um feststellen zu können, dass IT-Sicherheitsanforderungen erfüllt werden. Hierfür müssen die Möglichkeiten des NLF für IT-Sicherheitsanforderungen ausgeschöpft werden. Dazu sollten verpflichtende Konformitätsbewertungen durch akkreditierte Dritte (Third-Party) auf Basis von verbindlichen Normen eingeführt werden und eine konstante Marktüberwachung stattfinden. Marktkontrollen müssen nach der Zulassung regelmäßig, unangekündigt und unabhängig stattfinden. Nur so können sich Verbraucher:innen auf die Angaben der Hersteller verlassen und Vertrauen in die Sicherheit von Produkten und Diensten aufbauen.