VERNETZTE GERÄTE VON VERBRAUCHER:INNEN CYBERSICHER MACHEN

Zusammenfassung der Stellungnahme des Verbraucherzentrale Bundesverbands (vzbv) zum Vorschlag der Europäischen Kommission für den Cyber Resilience Act (CRA)

20. Dezember 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. EINLEITUNG

Die Europäische Kommission hat am 15. September 2022 im Rahmen Europas Digitaler Dekade einen Vorschlag für horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen vorgelegt.[1] Mit der Entwicklung des Internets der Dinge (engl. *Internet of Things* (IoT)) und der Digitalisierung haben vernetzte Geräte und digitale Dienste immer mehr Anwender:innen gewonnen. Auch vor dem Hintergrund der Covid-Pandemie hat die Nutzung von Lösungen zur digitalen Kommunikation sowie die Arbeit im Home-Office die Nutzung von drahtlosen Geräten oder Software noch einmal bedeutend verstärkt. Wurden 2018 weltweit noch etwa 9 Milliarden vernetzte Geräte verwendet, gehen Schätzungen davon aus, dass diese Zahl bis 2025 auf 25 Milliarden ansteigen wird.[2]

Gleichzeitig steigt die Zahl der Schwachstellen, wie immer neue Sicherheitsvorfälle und Datenleaks verdeutlichen.[3] Bereits drei von vier Deutschen waren Opfer von Cyberkriminalität.[4] Die Sorge von Verbraucher:innen ist dementsprechend groß: Mehr als ein Drittel der deutschen Verbraucher:innen nehmen IT-Sicherheitsaspekte wie unverschlüsselte Datenaustausche (79 Prozent), unsichere Voreinstellungen auf Geräten (76 Prozent) oder die frühzeitige Einstellung von Sicherheitsupdates (75 Prozent) seitens eines Herstellers als risikoreich wahr.[5] Der Wunsch nach Cybersicherheit, die geräteseitig von Anfang an gegeben ist und auch während der Nutzung eines Produktes bestehen bleibt, ist dementsprechend groß.[6]

Verbraucher:innen können sich bisher jedoch lediglich auf den guten Willen von Herstellern verlassen. Informationen zur IT-Sicherheit finden sich selten auf Produkten und Angaben sind mitunter nicht zuverlässig. Gleichzeitig werden technische Systeme immer komplexer, die mit ihnen verbundenen Datenverarbeitungen immer schwieriger zu überblicken. Nutzer:innen ist es kaum möglich, digitale Produkte und Dienstleistungen zu nutzen und die Sicherheitsanforderungen sowie Risiken oder Lücken selbstständig zu erkennen. In der Folge erwerben sie unsichere Produkte und sind dadurch verschiedensten Sicherheitsrisiken ausgesetzt. Das zeigen Tests von europäischen Verbraucherschutzorganisationen an zahlreichen Produkten wie zum Beispiel Smart Toys und Smart Watches, die zu Spionagezwecken gehackt werden können oder Sicherheitskameras und Staubsaugerroboter, die einfach per Fernzugriff manipulierbar sind.[7]

---

[1] Europäische Kommission: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454, 02.11.2022

[2] Schätzung des Telekommunikationsverbands GSMA (2018); 21.02.20220: https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf, 24.10.2022

[3] Information is beautiful: World's Biggest Data Breaches & Hacks, 2022, https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/; 24.10.2022

[4] NordVPN: Studie Cybervorfälle, https://nordvpn.com/de/blog/nordvpn-studie-cybervorfaelle/, 31.10.2022

[5] Verbraucherzentrale Bundesverband: Cybersicherheit bei vernetzten Geräten stärken, 2022, https://www.vzbv.de/pressemitteilungen/cybersicherheit-bei-vernetzten-geraeten-staerken, 31.10.2022

[6] Verbraucherzentrale Bundesverband: IT-Sicherheit bei Anschaffung, 2020, https://www.vzbv.de/multimedia/infografik-it-sicherheit-bei-anschaffung, 31.10.2022

[7] BEUC: Factsheet – How the EU can make smart products consumer-proof, 2018, https://www.beuc.eu/publications/beuc-x-2018-103_safety_of_connected_products.pdf, 02.11.2022

Der Cyber Resilience Act (CRA) kann diesen Missstand beheben und Verbraucher:innen einerseits digital absichern und andererseits ihre Rechte bei Cybersicherheitsvorfällen stärken.

II. ZUSAMMENFASSUNG

Der Verbraucherzentrale Bundesverband (vzbv) begrüßt den Vorschlag der Europäischen Kommission über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen.[8] Verpflichtende Anforderungen sind unabdinglich für ein sicheres digitales Umfeld von Nutzer:innen.

Ein starker Rechtsrahmen muss sich auf drei Säulen stützen:

- ein umfassender Anwendungsbereich mit ausreichenden Grundanforderungen für alle vernetzten Produkte
- ein starkes Zertifizierungssystem mit externen Kontrollen für besonders risikoreiche Produkte und
- eine wirksame Marktüberwachung und Durchsetzung.

1. GRUNDLEGENDE CYBERSICHERHEITSANFORDERUNGEN UND PFLICHTEN VON HERSTELLERN

Der vzbv begrüßt den breiten Anwendungsrahmen der Verordnung. Die Vernetzung von IoT-Produkten macht es notwendig, alle Geräte zu sichern, um ein System ausreichend schützen zu können. Daher sind ausreichende Mindestanforderungen unumgänglich. Dazu gehören im Wesentlichen die Konzepte *security by design* und *security by default,* die während des Produktlebenszyklus angewandt werden müssen.

Ausweitung des Anwendungsbereichs auf Cloud-Dienste (Artikel 2)

Um ein sicheres digitales Umfeld für die Verbraucher:innen zu schaffen, darf der Anwendungsbereich des CRA nicht eingeschränkt werden. Auch Cloud-Dienste wie Software-as-a-Service (SaaS) müssen daher eingeschlossen werden.

Vorkehrungen für eine sichere Entsorgung und das Recycling (Anhang I, Abschnitt 1. Nummer 3)

Die Sicherung des kompletten Produktlebenszyklus muss Vorkehrungen für die sichere Vernichtung oder das Recycling eines vernetzten Produkts oder die Einstellung eines digitalen Dienstes berücksichtigen. Die CRA muss belastbare Anforderungen für eine mögliche Entsorgung hinzufügen.

Ausnahmslose Pflicht zur sicheren Verschlüsselung (Anhang I, Abschnitt 1. Nummer 3(c))

Sichere Verfahren dürfen nicht durch Lücken in der Verschlüsselung unterminiert werden. Nur eine starke Ende-zu-Ende-Verschlüsselung kann die Vertraulichkeit

[8] Europäische Kommission: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454, 02.11.2022

von Daten und Kommunikation gewährleisten. Der CRA muss sich ausnahmslos zur Verschlüsselung bekennen.

- **Trennung von Sicherheits- und funktionalen Updates (Anhang I, Abschnitt 1. Nummer 3(k))**

  Der CRA muss Hersteller verpflichten, Updates einfach und leicht zugänglich bereitzustellen und über den Zweck und die Auswirkungen eines Updates informieren. Sicherheitsupdates sollten nach Möglichkeit getrennt von funktionsändernden Updates ausgeliefert werden.

- **Sicherung von wesentlichen und manuellen Funktionen (Anhang I, Abschnitt 1. Nummer 3(f))**

  Die Ausführung von wesentlichen Grundfunktionen eines vernetzten Produktes muss stets sichergestellt werden. Vor allem Haushaltsgeräte oder Geräte, die zu Sicherheitszwecken eingesetzt werden, dürfen in ihrer Grundfunktion nicht durch Störungen wie unterbrochene Internetverbindungen oder Systemabstürze eingeschränkt werden. Die Funktionsfähigkeit des ursprünglichen Zwecks eines intelligenten Produkts muss unabhängig von der Vernetzung gewährleistet werden.

- **Gewährleistung ausreichend langer Versorgung mit Updates (Art. 10, Abs. 6)**

  Sicherheitsupdates müssen für mindestens die durchschnittliche Nutzungsdauer eines Produktes ausgeliefert werden. Die Begrenzung der Update-Pflicht auf fünf Jahre im Vorschlag des CRA ist unzureichend. Vor allem Smart Home Geräte wie Waschmaschinen und Kühlschränke aber auch Laptops und andere Geräte sind deutlich länger im Einsatz. Eine Einschränkung widerspricht dem Nachhaltigkeitsgebot und zwingt Verbraucher:innen Produkte austauschen zu müssen.

- **Zentrale Kontaktstelle für Cybersicherheit (Anhang II, Nummer 2)**

  Verbraucher:innen muss eine Anlaufstelle zur Verfügung gestellt werden, die für das Thema Cybersicherheit zuständig ist. Der CRA muss sicherstellen, dass diese Kontaktstelle dazu beiträgt, Anliegen im persönlichen Kontakt zu klären, Fälle und Sicherheitslücken aufzunehmen und zu verarbeiten und bei Problemen oder Vorfällen Hilfestellungen zu leisten.

2. RISIKOKLASSIFIZIERUNG VON PRODUKTEN MIT DIGITALEN ELEMENTEN

Intelligente Geräte sind besonders schützenswert, wenn sie persönliche und sensible Daten sammeln und für den Einsatz im Bereich Gesundheit, Sicherheit oder aber für Grundversorgungsleistungen vorgesehen sind. Dies muss in einer Risikoeinteilung berücksichtigt werden (Artikel 6).

- **Erwägung von Gefahren für Verbraucher:innen (Art. 6)**

  Eine Risikobewertung muss stets die Gefährdung für die Unversehrtheit von Verbraucher:innen berücksichtigen. Ein Vorfall, der das körperliche und seelische Wohlbefinden bedroht oder schädigt, die Privatsphäre verletzt oder finanzielle Schäden verursacht, muss als besonders kritisch und schwerwiegend für einen einzelnen Nutzer angesehen werden.

- **Schutz des privaten Raums und sensiblen Bereichen wie Gesundheit und Sicherheit (Art. 6, Abs. 2 (b))**

Produkte, die besonders schützenswerte Daten erheben und verarbeiten und in privaten Haushalten zum Einsatz kommen, müssen im CRA als risikoreicher eingestuft werden. Insbesondere Geräte, die auch zu Gesundheitszwecken eingesetzt werden, wie verschiedene Wearables, und Smart Home Geräte, die unterschiedlichste Daten aus der Intimsphäre von Nutzer:innen sammeln, sind besonders sensibel. Auch Produkte, die Sicherheitsfunktionen erfüllen, wie Türschlösser oder Alarmsysteme sind als kritisch einzustufen.

Berücksichtigung von Produkten kleinerer Hersteller (Art. 6, Abs. 2 (d))

Es ist wichtig, einzuschätzen, wie viele Menschen von einem möglichen Vorfall betroffen sein könnten, um die Kritikalität eines Produktes zu bewerten. Dennoch dürfen Produkte kleinerer Hersteller wie kleine und mittlere Unternehmen (KMU) oder Start-ups dadurch nicht durchs Raster fallen, weil sie nicht zu den meistverkauften Produkten gehören. Die Betrachtung der Anzahl von Betroffenen muss die Marktbedingungen berücksichtigen und Produkte von relevanten Herstellern einschließen.

Berücksichtigung der Folgenschwere für den Einzelnen (Art. 6)

Die Risikobewertung muss die Auswirkungen eines möglichen Vorfalls auf einzelne Verbraucher:innen einbeziehen. Dabei müssen finanzielle Schäden sowie Beeinträchtigungen der physischen und psychischen Unversehrtheit berücksichtigt werden.

Ergänzung von kritischen Verbraucherprodukten (Anhang III, Klasse I)

Die im Anhang III aufgelisteten, kritischen Produkte in Klasse I müssen um weitere Produkte aus dem Verbrauchersegment ergänzt werden. Aufgenommen werden müssen Sicherheitsprodukte wie Schlösser, Alarmsysteme, Kameras und Feuermelder. Auch Smart Home Produkte vor allem im Bereich Heizung, Strom und Lüftung und der Bereich Wearables sind als kritisch einzustufen. Zuletzt müssen alle Produkte für Kinder, wie Spielzeuge, Babyphones und Bildungstools einbezogen werden.

3. ZERTIFIZIERUNG UND KONFORMITÄTSBEWERTUNG

Zertifikate geben Verbraucher:innen verlässliche Informationen zu bestimmten Produkteigenschaften. Gerade im Bereich der Cybersicherheit bietet sich die Chance durch klare und sichtbare Angaben Orientierung zu schaffen und informierte Entscheidungen zu Produkten zu treffen. Folgende Punkte müssen bei den Bestimmungen zur Zertifizierung und Konformitätsbewertung in Artikel 24 des CRA vorgesehen werden:

Unabhängige Zertifizierung bei KI-Produkten (Art. 8)

Vernetzte Produkte und Dienste, die Künstliche Intelligenz anwenden, sind doppelt risikoreich. Hier muss eine unabhängige Zertifizierung aus Modul C und Modul H verpflichtend vorgegeben werden (Annex VI, CRA). Nur so können Cybersicherheitsrisiken und Risiken im Umgang mit KI zuverlässig und nachhaltig minimiert und Missbrauch oder Manipulation sicher ausgeschlossen werden.[9]

[9] KI-Produkte werden laut Artificial Intelligence Act (AIA) als risikoreich eingestuft, wenn in harmonisierten Rechtsakten eine Konformitätsbewertung durch notifizierte Stellen vorgeschrieben ist. Produkte mit digitalen Elementen und KI Anwendungen, die im CRA demnach nicht in Klasse I oder Klasse II Annex III fallen, werden demnach im AIA nicht als Hochrisiko Systeme eingestuft.

- **Eine Zertifizierung durch Dritte muss für alle Hersteller möglich sein (Art. 24, Abs. 1)**

  Hürden wie finanzielle Mittel und die personelle Ausstattung dürfen vor allem kleinere und mittlere Unternehmen nicht von einer Zertifizierung durch notifizierte Stellen abhalten. Der CRA muss hier Möglichkeiten für KMU bieten, um Wettbewerbsverzerrungen zum Vorteil von Tech-Riesen zu entgehen.

- **Verpflichtende Unabhängige Zertifizierung für alle kritischen Produkte (Art. 24, Abs. 2)**

  Kritische Produkte der Klasse I und Klasse II (Anhang III) müssen zwingend eine externe Zertifizierung durch notifizierte Stellen durchlaufen. Produkte der Klasse I müssen dabei mindestens eine Plausibilitätsprüfung von Dritten zur Erfüllung der Cybersicherheitsvorgaben wie sie in Modul B und C vorgesehen ist, durchführen (EU Baumusterprüfverfahren und interne Fertigungskontrolle).

4. MARKTÜBERWACHUNG UND RECHTSDURCHSETZUNG

Der vzbv begrüßt die Offenlegungspflichten zu Sicherheitsvorfällen sowie die Kooperationen zwischen unterschiedlichen Marktaufsichtsbehörden, die der CRA vorgibt.

Folgende Punkte müssen bei Meldungen und Kontrollen in Artikel 11 & 43 sowie in Anhang I Abschnitt 2 aufgenommen werden:

- **24 Stunden Meldungsvorgabe zur Information von Verbraucher:innen (Art. 11)**

  Bei Bekanntwerden einer ausgenutzten Schwachstelle müssen Verbraucher:innen umgehend von Herstellern und Anbietern informiert werden. Auch wenn noch kein Update bereitsteht oder das Problem noch nicht behoben werden konnte, garantiert eine schnelle Meldung, dass Folgeschäden minimiert werden und Betroffene Schutzvorkehrungen wie das Abkoppeln eines Gerätes vom Netz vornehmen können. Eine Warnung muss daher innerhalb von 24 Stunden herausgegeben werden.

- **Starke Auskunftsrechte für Verbraucher:innen (Art. 11, Abs. 4)**

  Hersteller müssen betroffene Nutzer:innen über Cybersicherheitsvorfälle informieren. Mögliche Schäden müssen für Betroffene schnell abschätzbar sein. Fehler und Schwachstellen müssen so weit offengelegt werden, dass Haftungsansprüche mit den Informationen geltend gemacht werden können.

- **Gezielte Meldungen an betroffene Verbraucher:innen (Anh. I Ab. 2 Punkt 4)**

  Informationen zu Sicherheitslücken müssen gezielt für Betroffene bereitgestellt werden. Für betroffene Produkte müssen leicht zugängliche und einfach verständliche Informationen zur Verfügung gestellt werden, zum Beispiel im Rahmen von Updates.

- **Kontrollmechanismen für Zivilgesellschaft und Verbraucher:innen (Art. 43)**

  Cybersicherheit hängt maßgeblich von der Aufdeckung von Schwachstellen durch verschiedene Akteure ab. Der CRA fokussiert sich jedoch lediglich auf Meldungen

---

Vgl: Europäische Kommission: Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, Art. 6 (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, 02.11.2022

von Herstellern selber und riskiert so einen Flaschenhals und potenzielle Interessenskonflikte. Verbraucher:innen und Verbraucherorganisationen sowie Forschung und Wissenschaft müssen bei Verdacht eine Untersuchung der Marktaufsichtsbehörden von betroffenen Produkten initiieren können.

Private Rechtsdurchsetzung ermöglichen

Soft- und Hardwarefehler betreffen meist eine Vielzahl von Verbraucher:innen. Gleichzeitig können einzelne Betroffene Haftungsansprüche meist nicht alleine geltend machen. Daher braucht es die Möglichkeiten der privaten Rechtsdurchsetzung. Der CRA muss Sammelklagen ermöglichen und in die EU-Verbandsklagerichtlinie aufgenommen werden.[10]

5. BUßGELDER UND STRAFEN

Nur empfindliche Konsequenzen können die flächendeckende Einhaltung der Cybersicherheitsvorgaben bewirken. Dabei müssen Sanktionen eine abschreckende Wirkung besitzen. Insbesondere bei Vorgaben für Maximalstrafen müssen verschiedene Auslegungen, Schweregrade und Urteile berücksichtigt werden, um sicherzustellen, dass Strafen angemessen bleiben.

Eine Orientierung bilden kürzlich erlassene oder derzeit verhandelte Digitalrechtsakte. So sehen der Artificial Intelligence Act (AIA)[11] oder der Digital Services Act (DSA)[12] Bußgelder von bis zu sechs Prozent des weltweiten Jahresumsatz vor und sind damit mehr als doppelt so hoch, wie der im CRA vorgesehene Höchstsatz von zweieinhalb Prozent.

Empfindliche Strafen zur Vermeidung von Verstößen (Art. 53)

Der CRA muss die Höchstbeträge der Bußgelder deutlich erhöhen und dabei mindestens das bestehende Niveau aus aktuellen Rechtsakten von sechs Prozent des weltweiten Jahresumsatzes eines Unternehmens festsetzen.

[10] Europäisches Parlament: Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, 2020, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32020L1828&from=EN, 02.11.2022

[11] Europäische Kommission: Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, Art. 71 (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, 02.11.2022

[12] Europäische Kommission: Verordnung des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), Art. 52, 2022, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065&from=EN, 01.11.2022