VERNETZTE GERÄTE UND DIGITALE DIENSTE SICHER GESTALTEN

Herausforderungen und Lösungsansätze zur europäischen Cybersicherheitsgesetzgebung aus verbraucherpolitischer Sicht

9. Oktober 2020

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

- Alle digitalen Dienste und vernetzten Geräte sollten *by Design* und *by Default* grundlegende Sicherheitsanforderungen verpflichtend erfüllen müssen.
- Die aktuell geltende europäische Cybersicherheitsgesetzgebung ist in Bezug auf Verbraucherinteressen lückenhaft und technisch zu unspezifisch. In der in Überarbeitung befindlichen NIS-Richtlinie[1] sollten daher Sicherheitsstandards sektorübergreifend und für weitere verbraucherrelevante Dienstarten wie beispielsweise Social-Media-Plattformen festgeschrieben werden. Vernetzte Geräte im „Internet der Dinge“ stellen aufgrund ihres hybriden Charakters zwischen konventionellem physischem Produkt und IT-System ein legislatives Handlungsfeld sui generis dar. Für diese sollte daher ein eigener europäischer Rechtsrahmen geschaffen werden, der verpflichtende Sicherheitsanforderungen regelt.

II. ABSTRACT

The level of cyber threats to consumer data and personal IT-infrastructures remains alarmingly high. Legislation for digital services and devices with respect to safety and security issues is still incomplete and too unspecific when it comes to concrete technical measures. To remedy this lack of regulation, the Federation of German Consumer Organisations (vzbv) proposes the following suggestions:

- An extention of the scope of the Directive on security of network and information systems (NISD) to more types of digital services and to smaller service providers.
- A new horizontal law to tackle security issues of connected devices in the so-called Internet of Things for consumers.

Both regulations need to include references to reasonable baseline security measures as well as to international technical standards. Extending the scope of NISD is expected to close the gaps left by the current directive and sector-specific legislation. The unique characteristics of connected devices as „cyberphysical systems“ lead to new challenges and call for a new horizontal legislative approach handling the novel risk induced by the Internet of Things. The two proposed approaches are likely to increase trust in connected devices and digital services and thereby stimulate the digital market in the EU.

[1] Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, RL 2016/1148/EU.

III. NEUE UND ALTE HERAUSFORDERUNGEN

Die gerade beendete öffentliche Konsultation zur Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) bietet einen guten Anlass, die Cybersicherheitslage mit Blick auf digitale Dienste und vernetzte Geräte aus der Perspektive der Verbraucherinnen und Verbraucher[2] in der Europäischen Union (EU) insgesamt zu beleuchten. Denn die Bedeutung digitaler Dienste und vernetzter Produkte im Privatbereich ist unvermindert hoch. Nach dem Durchbruch des Personal Computers in den Neunziger Jahren und des Internets in den 2000er Jahren gewann in der darauffolgenden Zeit das Phänomen des „Ubiquitous Computing“[3] an Bedeutung: Demnach werden immer mehr Lebensbereiche digital begleitet. Neben den etablierten und weiter wachsenden Diensten wie Personal Cloud, Online-Marktplatz und Social-Media-Anwendungen kommen vermehrt vernetzte Geräte im „Internet der Dinge“ (Internet of Things, IoT) auf den Markt. Mittlerweile lebt fast ein Drittel der Menschen in Deutschland in Haushalten mit solchen Produkten[4]. Denn insbesondere die Digitalisierung der häuslichen Umgebung bietet große Potentiale zur Erhöhung von Energieeffizienz, persönlicher Sicherheit und Komfort: Mit so genannten „Smart Home“-Systemen[5] kann beispielsweise die heimische Heizungsanlage über das Mobiltelefon gesteuert und energetisch optimiert werden[6], diverse Assistenzsysteme können älteren Menschen und solchen mit Handicaps alltägliche Routineaufgaben erleichtern[7]. Digital gesteuerte und vernetzte Alarm- und Schließanlagen[8] überwachen umfassender als analoge Systeme das eigene Haus und lassen sich dennoch komfortabel über digitale Endgeräte fernsteuern[9].

Bei diesen digitalen Angeboten spielen die Anbindung an das Internet und eine große Zahl von im Haus verteilten Sensoren und Aktoren[10] eine entscheidende Rolle. Dadurch entstehen aber viele neue Sicherheitsrisiken. Wenn Schließsysteme aufgrund von Softwarefehlern oder durch gezielte Angriffe falsch gesteuert werden, ist nicht nur die Vertraulichkeit von personenbezogenen Daten in Gefahr, sondern mitunter auch die

---

[2] Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Mehrfachbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[3] Pipek, Volkmar: „Ubiquitous Computing“, Enzyklopädie der Wirtschaftsinformatik, 2020, https://enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Rechnernetz/Ubiquitous-Computing/index.html, 23.09.2020.

[4] Bitkom e.V.: 3 von 10 Deutschen haben ein smartes Zuhause, 2019, https://www.bitkom.org/Presse/Presseinformation/3-von-10-Deutschen-haben-ein-smartes-Zuhause, 23.09.2020.

[5] Wikipedia: „Smart Home“, 2020, https://de.wikipedia.org/wiki/Smart_Home, 23.09.2020.

[6] Emmer, Wolfgang: Smarte Thermostate: Die besten Lösungen für smarte Heizungssteuerung, 2020, https://www.pcwelt.de/a/smarte-thermostate-die-besten-loesungen-fuer-smarte-heizungssteuerung,3443628, 23.9.2020.

[7] Verivox: Selbstbestimmt im Alter durch Smart Home, https://www.verivox.de/smarthome/themen/senioren/, 23.09.2020.

[8] DasHaus: Smarte Alarmanlagen: Mehr Sicherheit im Haus dank digitaler Technik, https://www.haus.de/smart-home/smarte-alarmanlagen-mehr-sicherheit-im-haus, 23.09.2020.

[9] Schreiber, Manuel: Elektronisches Türschloss nachrüsten und per Smartphone steuern (Smart Home), 2018, https://www.chip.de/artikel/Elektronisches-Tuerschloss-nachruesten-und-per-Smartphone-steuern-Smart-Home_139974455.html, 23.09.2020.

[10] S. Wikipedia: „Aktor“, 2020, https://de.wikipedia.org/wiki/Aktor, 23.09.2020.

persönliche Sicherheit: Durch die Ausnutzung von IT-Sicherheitslücken in Schließsystemen können sich Einbrecher ganz ohne physische Gewalt den Zugang zum geschützten Wohnraum verschaffen[11]. Und in „smarten“ Spielzeugen werden seit Jahren immer wieder Schwächen entdeckt, mit deren Hilfe Angreifer beispielsweise eingebaute Mikrofone zum Ausspionieren des heimischen Kinderzimmers nutzen können[12]. Bei vernetzten Geräten bestehen also neben Problemen der digitalen *Cybersicherheit*[13] auch Gefahren hinsichtlich der physischen *Produktsicherheit* – beide Sicherheitsbegriffe bedingen sich bei vernetzten Geräten gegenseitig, denn ein gehacktes vernetztes Gerät kann auch keine Produktsicherheit gewährleisten. Neue Gefahren für Verbraucher gesellen sich also zu mittlerweile altbekannten, denn nach wie vor reißen die Meldungen über Hackingangriffe auf Webserver und auf klassische Endnutzer-Hardware wie Router nicht ab[14]. Entsprechend besorgt zeigen sich die Verbraucher: In einer aktuellen Umfrage des Verbraucherzentrale Bundesverbandes (vzbv) geben 76 Prozent der Befragten an, sich wegen einer möglichen ungewollten Weiterverbreitung ihrer persönlichen Daten zu sorgen[15]. 75 Prozent geben an, in den letzten zwölf Monaten im privaten Umfeld einen IT-Sicherheitsvorfall erlebt zu haben[16].

Während größere Unternehmen meist über komplexe IT-Sicherheitsinfrastrukturen und kompetente Ansprechpartner verfügen, sind Daten und Systeme von Privatpersonen vergleichsweise schlecht geschützt: Beispielsweise ist für digitale Dienste die unsichere Authentisierung mit einem Passwort nach wie vor der Normalfall[17]. Viele vernetzte Geräte sind gar nicht oder lediglich mit leicht herauszufindenden Passwörtern gesichert, und eine sichere Authentisierung erfolgt häufig auch nicht[18].

---

[11] Whittaker, Zack: Security flaws in a popular smart home hub let hackers unlock front doors, 2019, https://techcrunch.com/2019/07/02/smart-home-hub-flaws-unlock-doors/, 23.09.2020.

[12] Stiftung Warentest: Wie vernetzte Spielkameraden Kinder aushorchen, 2017, https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/, 23.09.2020.

[13] Der Begriff Cybersicherheit wird hier als Oberbegriff von Daten- und IT-Sicherheit verwendet, d.h. er bezieht sich auf die Vertraulichkeit, Verfügbarkeit und Integrität von digitalen Daten als auch auf die Verfügbarkeit von IT-Systemen und deren Funktionalitäten. Vgl. Wikipedia, „Informationssicherheit“ , 2020, https://de.wikipedia.org/wiki/Informationssicherheit, 23.09.2020.

[14] S. der jüngste Angriff auf Twitter-Konten: tagesschau.de: 17jähriger nach Twitter-Hack festgenommen, 01.08.2020, https://www.tagesschau.de/ausland/twitter-festnahme-hack-101.html, 23.09.2020.

[15] Verbraucherzentrale Bundesverband: Erwartungen und Erfahrungen der Verbraucherinnen und Verbraucher. Erkenntnisse der Marktbeobachtung des vzbv, 2020, https://www.vzbv.de/sites/default/files/downloads/2020/06/16/ergebnisbericht_it-sicherheit_0.pdf, Folie 6, 06.10.2020.

[16] Ebd., Folie 7, 06.10.2020.

[17] Bei den vielen Anbietern, beispielsweise Google, muss diese Funktion nachträglich aktiviert werden: Google: Mehr Sicherheit für ihr Google-Konto, 2020, https://www.google.com/landing/2step/, 22.09.2020.

[18] T. Alladi, V. Chamola, B. Sikdar and K. R. Choo (2020): „Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, Vol. 9, Nr. 2, S. 17-25, doi: 10.1109/MCE.2019.2953740. S. 20 ff.

IV. SICHERHEITSANFORDERUNGEN AUS VERBRAUCHERSICHT

Die oben geschilderten Sicherheitsprobleme entstehen häufig dadurch, dass Daten unverschlüsselt gespeichert und gesendet werden und Nutzerzugänge unzureichend gesichert sind. Es ist also offensichtlich, dass die Risiken, denen Verbraucher im digitalen Raum und bei der Nutzung vernetzter Geräte ausgesetzt sind, mit vergleichsweise einfachen technischen Sicherheitsvorkehrungen drastisch reduziert werden könnten. Daher sollten alle digitalen Dienste und vernetzten Geräte verpflichtend mit grundlegenden Sicherheitsmaßnahmen konstruiert (*Security by Design*) und den Verbrauchern übergeben werden müssen, so dass diese sie nicht erst durch umständliches Konfigurieren sicher machen müssen (*Security by Default*). Da die Sicherheit von digitalen Diensten und vernetzen Geräten dynamisch ist und sich stetig verändert, ist es erforderlich, dass sie durch Sicherheitsupdates auch kontinuierlich auf dem jeweiligen Stand der Technik seitens der Anbieter aufrechterhalten wird.

DER VZBV FORDERT

Digitale Dienste und vernetzte Geräte, sollten *by Design und by Default* mit folgenden Sicherheitsanforderungen angeboten werden müssen:

- Verschlüsselte Übertragung und Speicherung von Daten
- Sichere Authentisierungsverfahren (z.B. 2-Faktor-Authentisierung)
- Schutz von Anwendungen und Daten mit Passwörtern auf einem angemessenen Sicherheitsniveau
- Regelmäßige und ausreichend lange Bereitstellung von Sicherheitsupdates

Diese Sicherheitsanforderungen sind von großer Wichtigkeit für digitale Dienste sowie vernetzte Geräte und die in ihnen verbaute Software und sollten seitens der Anbieter verpflichtend gewährleistet werden müssen. Denn nur wenn Daten verschlüsselt übertragen werden, können sie von Dritten nicht oder nur mit großem Aufwand unautorisiert ausgelesen werden. Werden mobile vernetzte Endgeräte wie Smartphones gestohlen, sind die darauf befindlichen Daten nur dann sicher, wenn sie verschlüsselt gespeichert wurden. Und nur die sichere Authentisierung kann verhindern, dass Geräte, die über eine Netzverbindung gesteuert werden, über einfach herauszufindende Passwörter „gekapert“ und missbräuchlich verwendet werden können. Dies gilt sowohl für den Zugriff auf vernetzte Geräte als auch für die Nutzung von webbasierten Diensten, die mit vernetzten Geräten verbunden sind und Daten zur Nutzung der Geräte und zu ihren Besitzern auf Servern des Anbieters speichern. Aber auch viele andere digitale Dienste in Form von Webanwendungen für Verbraucher werden nicht auf einem hinreichenden Sicherheitsniveau angeboten. Webmail-Dienste, Social-Media-Anwendungen, Online-Marktplätze und andere Dienste, die sensible Daten verarbeiten, sollten die Authentisierung sowie Datentransport und -speicherung gemäß den oben genannten Punkten sicher gestalten.

V. BESTEHENDE GESETZLICHE REGELUNGEN

In den bestehenden europäischen Rechtsakten, die Regelungen zur IT- und Datensicherheit enthalten[19], liegt bislang der Fokus auf dem „Funktionieren des Binnenmarkts“[20] und der Absicherung kritischer Infrastrukturen. Die datenschutzrechtlichen Verordnungen, vor allem die Datenschutzgrundverordnung (DSGVO), stellen hier eine Ausnahme dar, denn im Datenschutz steht der „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“[21] im Vordergrund. Gesetze zur IT- und Datensicherheit wie der Cybersicherheitsakt und die NIS-Richtlinie sind primär auf den Schutz von Gemeingütern ausgerichtet. Den individuellen Schutzinteressen von Verbrauchern hinsichtlich der Sicherheit ihrer persönlichen IT-Systeme, vernetzen Geräte, digitalen Identitäten und Datenbestände wird dabei nicht immer in hinreichendem Maße Rechnung getragen, wie die folgende Übersicht zeigt.

1. NIS-RICHTLINIE

Die NIS-Richtlinie verpflichtet Anbieter von Cloud-Computing-Plattformen, digitalen Marktplätzen und Suchmaschinen dazu, „geeignete und verhältnismäßige technische und organisatorische“ Sicherheitsmaßnahmen zum Schutz ihrer Systeme zu treffen[22]. Im Falle eines Sicherheitsvorfalls von besonderer Schwere müssen die zuständigen öffentlichen Stellen informiert werden[23]. Zwar handelt es sich bei der Richtlinie um die erste horizontale Regulierung von IT-Systemen in Bezug auf Cybersicherheit und damit aus verbraucherpolitischer Sicht um einen Fortschritt. Dennoch gibt es aus Sicht des vzbv beispielsweise folgende Schutzlücken:

- Die Definition der „digitalen Dienste“ im Anwendungsbereich der NIS-Richtlinie umfasst nur die oben genannten drei Angebotstypen. Social-Media-Plattformen sind hingegen ausgeschlossen[24]. Dies ist höchst problematisch, da auch solche Dienste große Mengen an nutzergenerierten und personenbezogenen Daten verarbeiten und für die private und teilweise auch die geschäftliche Kommunikation eine sehr große Rolle spielen. Cyberangriffe wie Identitäts- oder Datendiebstahl können daher enorme finanzielle Schäden und Konsequenzen für die soziale Existenz der Betroffenen nach sich ziehen.
- Vernetzte Geräte und -Systeme sowie sonstige Hardware (Router) werden in der NIS-Richtlinie nicht behandelt.

---

[19] Aus unserer Sicht sind einschlägig und werden hier diskutiert: NIS-Richtlinie, Cybersicherheitsakt (881/2019/EU), Datenschutzgrundverordnung (2016/679/EU), Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie, 2002/58/EG), Europäischer Kodex für elektronische Kommunikation (2018/1972/EU), Funkgeräterichtlinie (2014/53/EU), Produktsicherheitsrichtlinie (2001/95/EG).

[20] NIS-Richtlinie, Art. 1 (1).

[21] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, Art. 1 (1).

[22] NIS-Richtlinie, Art. 16 (1).

[23] Ebd. Art. 16 (3).

[24] Ebd. Anh. III, Art. 4 (17), (18), (19).

- Es sind nur „erhebliche“ Schäden ab einer bestimmten Zahl betroffener Nutzer meldepflichtig[25]. Außerdem muss der Anbieter lediglich öffentliche Stellen, nicht aber seine betroffenen Kunden informieren. Die öffentlichen Stellen müssen ihrerseits Informationen nicht an betroffene Privatpersonen weiterleiten. Das heißt, dass es anders als in der DSGVO[26] kein grundsätzliches Recht auf Information für Betroffene gibt.
- Von den genannten Bestimmungen des Artikels 16 der NIS-Richtlinie sind kleine und mittlere Unternehmen (KMU) ausdrücklich ausgenommen[27].

Im Hinblick auf den Verbraucherschutz und die oben genannten Sicherheitsanforderungen (vgl. Abschnitt IV) für digitale Dienste und vernetzte Geräte erweisen sich die Regelungen der NIS-Richtlinie also als lückenhaft. Dies ist damit zu erklären, dass das Ziel der Richtlinie in Bezug auf digitale Dienste der Schutz der Volkswirtschaften insgesamt ist, die Sicherheitsinteressen von privaten Endnutzern stehen hingegen nicht im Vordergrund.

2. WEITERE GESETZE

Mehrere weitere Rechtsakte erlegen Anbietern digitaler Dienste und Produkte Pflichten hinsichtlich der Absicherung ihrer Infrastrukturen auf. So fordert die Funkgeräterichtlinie, die prinzipiell auch auf vernetzte Geräte angewendet werden kann, allgemein Sicherheitsvorrichtungen zum Schutz personenbezogener Daten[28]. Bei der Allgemeinen Produktsicherheitsrichtlinie[29] ist hingegen weder der Geltungsbereich so festgelegt, dass darunter auch vernetzte Geräte fallen, noch lässt sich der verwendete Sicherheitsbegriff über die physische und chemische Produktsicherheit hinaus auf Probleme der Cybersicherheit ausweiten[30].

Für den Bereich der Kommunikationsdienste und -netze fordert die Datenschutzrichtlinie für elektronische Kommunikation Maßnahmen zur technischen Sicherheit[31]. Der Anwendungsbereich dieser Richtlinie umfasst aber lediglich Kommunikationsdienste wie Internet-Service-Provider, nicht hingegen so genannten Over-the-Top-Telekommunikationsdienste wie Instant-Messaging. Für diese Dienste werden im Europäischen Kodex für elektronische Kommunikation Sicherheitsanforderungen erhoben. Diese sind in Bezug auf technische Vorgaben etwas konkreter als die NIS-Richtlinie, insofern sie beispielsweise die Verschlüsselung von Daten nahelegen, aber eben nicht verpflichtend

---

[25] Ebd. Art. 16 (4).

[26] DSGVO, Art. 34. Diese Regelung greift nur, wenn davon auszugehen ist, dass sich ein Vorfall auf personenbezogene Daten bezieht. Der Verlust anderer Daten mit materiellem oder immateriellem Wert für den Nutzer und Fehlfunktionen an digitalen Diensten oder Produkten bleiben davon unberührt.

[27] NIS-Richtlinie, Art. 16 (11).

[28] Richtlinie 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG. Ebd. Art. 3 (3) e.

[29] Richtlinie 2001/95/EG über die allgemeine Produktsicherheit.

[30] Vgl. Verbraucherzentrale Bundesverband e. V.: Sichere Produkte stärken das Verbrauchervertrauen, 2020, https://www.vzbv.de/sites/default/files/downloads/2020/10/05/20-10-01_vzbv_positionspapier_produktsicherheit.pdf, 06.10.2020. S. 14.

[31] Konsolidierter Text: Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). Ebd. Art. 4.

vorgeben[32]. Auch die DSGVO erlegt den für die Verarbeitung personenbezogener Daten verantwortlichen Stellen, beispielsweise Betreibern von Webmail-Diensten, grundsätzlich Maßnahmen zur Absicherung der bei ihnen verarbeiteten Daten auf[33]. Diese Regelung schreibt aber ebenfalls keine der in Abschnitt IV genannten Sicherheitsmaßnahmen zwingend vor.

Es gibt also auf EU-Ebene keinen Rechtsrahmen, der das Konstruktionsprinzip *Security by Design* und *Security by Default* sektorübergreifend für alle digitalen Dienste und vernetzten Geräte verpflichtend vorgibt sowie technisch in hinreichendem Maße konkretisiert.

FAZIT

Security by Design und *Security by Default* für von Verbrauchern genutzte vernetzte Geräte und Dienste sind durch bislang bestehende EU-Rechtsakte nicht verpflichtend vorgegeben. Sicherheitsanforderungen an digitale Dienste und vernetzte Geräte sind auf EU-Ebene gesetzlich nur unzureichend geregelt.

VI. LEGISLATIVE LÖSUNGSANSÄTZE

1. NIS-RICHTLINIE

Es existiert keine horizontale EU-Gesetzgebung zur Cybersicherheit, welche die von Verbrauchern genutzten digitalen Dienste hinreichend regelt. Die dadurch bedingten Regulierungslücken, zum Beispiel in Bezug auf Social-Media-Anwendungen, können in der bestehenden Gesetzeslage kurzfristig am ehesten durch eine Anpassung der NIS-Richtlinie behoben werden. Daher sollte der Geltungsbereich dieses Gesetzes auf kleinere Unternehmen und auf weitere Arten digitaler Dienste, mindestens aber auf die ansonsten kaum regulierten Social-Media-Anwendungen ausgeweitet werden. Außerdem sind eine größere Regelungstiefe und eine technische Konkretisierung nötig.

DER VZBV FORDERT

- Die Erweiterung des Geltungsbereichs der NIS-Richtlinie auf weitere digitale Dienste, u.a. Social-Media-Plattformen und kleinere Unternehmen
- Die Erweiterung der Meldepflicht, so dass Betroffene direkt informiert werden müssen im Falles eines Sicherheitsvorfalls. Dies muss auch bei Vorfällen mit wenigen betroffenen Personen geschehen.
- Die Konkretisierung der aus Verbrauchersicht erforderlichen Sicherheitsanforderungen im Sinne von *Security by Design* und *Security by Default* für digitale Dienste

2. REGULIERUNG VON VERNETZTEN GERÄTEN

Vernetzte Geräte bedürfen als „cyberphysische Systeme“ eines eigenen Rechtsrahmens, denn die Verbindung von physischen Produkten mit vernetzten IT-Systemen führt zu gänzlich neuen Herausforderungen mit Blick auf die Cybersicherheit. Im Sinne einer „kontinuierlichen Konformität“ muss der Sicherheitsstandard zum Zeitpunkt der

[32] Richtlinie 2018/1972/EU über den europäischen Kodex für die elektronische Kommunikation. Ebd. Art. 40.

[33] DSGVO, Art. 32.

Inverkehrbringung durch einen Mechanismus zur Einspielung von Sicherheitsupdates des Herstellers erhalten bleiben. Einige Fragen in diesem Zusammenhang sind durch eine Modernisierung und Erweiterung der Allgemeinen Produktsicherheitsrichtlinie zu klären[34].

DER VZBV FORDERT

Es sollte ein neuer horizontaler Rechtsrahmen für vernetzte Geräte geschaffen werden, der folgende Anforderungen an die Cybersicherheit enthält:

- Verpflichtung zur Gewährleistung von *Security by De*sign und *Security by Default*
- Verschlüsselte Speicherung und Übertragung sensibler Daten
- Sichere Authentisierungsmechanismen
- Bereitstellung von Sicherheitsupdates über die erwartbare Lebensdauer des Produkts, um eine Sicherheit nach dem Stand der Technik zu gewährleisten
- Spezifische technische Normen und Standards zur Konkretisierung von Sicherheitsmaßnahmen (Die EU-Kommission sollte die Entwicklung solcher Normen für vernetzte Geräte weiter vorantreiben.)

Wie die eingangs vorgetragenen Schilderungen der technischen Risiken und der Bedrohungslage für Verbraucher zeigen, sind Änderungen der aktuellen Rechtslage dringend nötig. Neben der Wahrung der informationellen Selbstbestimmung, die ein hohes individuelles Rechtsgut darstellt, sprechen auch makroökonomische Faktoren dafür: Einerseits ist die Vermeidung von IT-Sicherheitsvorfällen wirtschaftlich lohnend, weil Prophylaxe langfristig günstiger ist als die Bewältigung der durch Cyberattacken verursachten materiellen Schäden. Andererseits belebt ein gestärktes Vertrauen der potentiellen Kunden gegenüber vernetzen Geräten und digitalen Diensten die digitale Wirtschaft und ist eine Voraussetzung für ihr weiteres Wachstum. Denn IT-Systeme für den Einsatz in sensiblen privaten Lebensbereichen haben langfristig nur eine Chance, wenn sie vertrauenswürdig und zuverlässig sind. Dies kann nur erreicht werden, wenn es einen Rechtsrahmen gibt, der verpflichtende Sicherheitsanforderungen für digitale Dienste und vernetzte Geräte für Verbraucher festlegt.

[34] Sichere Produkte stärken das Verbrauchervertrauen, S. 14 f.