NETZ- UND INFORMATIONSSICHERHEIT AUCH FÜR VERBRAUCHER STÄRKEN

Stellungnahme des Verbraucherzentrale Bundesverbandes zu dem Entwurf für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS 2) vom 16.12.2020

25.01.2021

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 Entwurf für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS 2-E) der Europäischen Kommission (EU-Kommission) ist eine evidenzbasierte Weiterentwicklung der Richtlinie zur Gewährleistung einer hohen Netz- und Informationssicherheit (NIS-RL). Er ist dazu geeignet, das allgemeine IT-Sicherheitsniveau in der Europäischen Union zu erhöhen. Davon werden auch Verbraucher mittelbar profitieren. Der Entwurf der NIS 2 stellt eine wichtige Komponente in der europäischen Cybersicherheitsgesetzgebung dar. Aber die Entscheidung, weiterhin hauptsächlich Schlüsselakteure mit Netzwerkrelevanz und deren technische Infrastrukturen in den Blick zu nehmen, lässt Regelungslücken in Bezug auf digitale Produkte für Verbraucher weiterhin bestehen und löst grundlegende Probleme nicht. Die Richtlinie stellt keine Verbraucherschutzgesetzgebung dar, Verbraucher werden in ihrem Anwendungsbereich lediglich an einigen Stellen „mitgemeint“. Daher muss auch in anderen Gesetzesinitiativen[1] dafür gesorgt werden, dass die Entwicklungsprinzipien Security by Design und Security by Default für alle relevanten digitalen Verbraucherprodukte gesetzlich verpflichtend gemacht werden.

II. ABSTRACT

On 16 December 2020, the European Commission published a legislative proposal (NIS 2) to replace the Directive on security of network and information systems (NIS Directive). The European Commission aims to achieve a high common level of cybersecurity in the European Union. The Federation of German Consumer Organisations (vzbv) supports the effort of the Commission, as it benefits consumers indirectly in their use of digital products. Various provisions have been added to NIS 2 that are likely to improve the cooperation and information sharing between national cybersecurity authorities as well as to improve their capabilities to effectively supervise the providers of digital services. vzbv welcomes the extension of scope, most notably to social media. Also, the new obligation to inform recipients of services, hence consumers, of security problems is a significant improvement.

However, NIS 2 mainly remains a legislation to prevent, and to react to, large-scale security incidents with far-reaching repercussions. To this end, it regulates the technologies and processes that are used to produce and to provide products, not the products themselves. This limitation in scope, albeit consistent and clear-cut, leaves critical regulatory gaps with respect to many types of digital services offered to consumers. Therefore, further improvements have to be made to the European cybersecurity legislation in order to make sure that reasonable baseline security measures are implemented in all types of digital consumer products. These obligatory security measures should include at least the following:

- Encrypted transmission and storage of sensitive data
- Secure authentication mechanisms
- Provision of security updates over a reasonable time period

[1] Zum Beispiel ein möglicher neuer horizontaler Rechtsakt zur Cybersicherheit vernetzter Geräte. S. Rat der Europäischen Union (2020): Council Conclusions on the cybersecurity of connected devices, https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf, 21.01.2021.

III. EINLEITUNG

Die EU-Kommission hat am 16.12.2020 einen Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS 2-E) veröffentlicht[2]. Der neue Entwurf ist das Ergebnis des Review-Verfahrens für die geltende NIS-Richtlinie[3]. Im Rahmen dieses Verfahrens wurde unter anderem eine öffentliche Konsultation durchgeführt, an der sich der Verbraucherzentrale Bundesverband (vzbv) beteiligt hat[4].

Der Entwurf wurde zusammen mit einer neuen Cybersicherheitsstrategie und einem neuen Richtlinienentwurf zur Sicherheit kritischer Einrichtungen veröffentlicht[5]. Der vzbv begrüßt, dass die EU-Kommission ihre Cybersicherheitspolitik angesichts der Gefahrenlage fortentwickelt. Denn eine Erhöhung des allgemeinen Sicherheitsniveaus wichtiger Netz- und Informationssysteme kommt direkt oder indirekt auch Verbraucherinnen und Verbrauchern[6] zu Gute. Die folgende Analyse aus Verbrauchersicht zeigt jedoch, dass die bestehenden und die geplanten Regelungen einen großen Teil der digitalen Angebote für Verbraucher gar nicht oder nur unzureichend in Bezug auf Informationssicherheit regulieren.

IV. POSITIONEN IM EINZELNEN

1. ERWEITUNG DES ANWENDUNGSBEREICHS (ART. 2 NIS 2-E)

Die geltende NIS-RL[7] erhebt über Sicherheitsanforderungen und Berichtspflichten für Anbieter kritischer „wesentlicher Dienste“ (Art. 14 NIS-RL) hinaus auch Anforderungen für einige wichtige digitale Dienste (Art. 16 NIS-RL), wobei diese Anforderungen weniger streng sind und beispielsweise lediglich eine anlassbezogene Ex-post-Überprüfung durch staatliche Stellen vorsehen (Art. 17 NIS-RL).

---

[2] Europäische Kommission (2020): Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0823, 21.01.2021.

[3] Europäische Kommission (2020): Cybersecurity – review of EU rules on the security of network and information systems, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive, 21.01.2021.

[4] Verbraucherzentrale Bundesverband e.V. (2020): Consultation on the revision of the NIS Directive (Beantwortung des Fragebogens), https://www.vzbv.de/sites/default/files/downloads/2020/10/13/nis-konsultation-fragebogen-submitted.pdf , 19.01.2021.

[5] Europäische Kommission (2020): Neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen, https://ec.europa.eu/commission/presscorner/detail/de/IP_20_2391, 21.01.2021.

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

[7] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016L1148, 21.02.2021.

Im neuen Entwurf der NIS 2 hat die EU-Kommission den Katalog der in den Anwendungsbereich fallenden Dienste erweitert und neu strukturiert[8]. Die Unterteilung in zwei Dienstearten mit unterschiedlichen Anforderungen wird aber grundsätzlich beibehalten[9]. Zu den in NIS 2-E als „wichtig“ eingestuften Diensten gehören auch Angebote im Bereich Soziale Medien, dadurch wird eine aus Verbrauchersicht besonders problematische Regulierungslücke geschlossen[10]. Cloud-Computing-Dienste hingegen fallen nun in den Bereich der wesentlichen Dienste[11]. Ebenfalls in diese Gruppe sind Telekommunikationsanbieter gekommen[12], für die aktuell die Bestimmungen des europäischen Kodex für die elektronische Kommunikation[13] gelten.

> Die Hereinnahme von Social-Media-Diensten in NIS 2-E ist ein bedeutender Fortschritt, da diese Diensteart für Verbraucher von hoher Relevanz ist. Neben diesen sinnvollen Erweiterungen ist auch von Vorteil, dass andere Branchen des produzierenden Gewerbes in den Anwendungsbereich aufgenommen worden sind[14]. Allerdings zeigt eine nähere Analyse der Regelungsinhalte, dass nicht alle Gefahren, denen Nutzer der genannten Dienste und Produkte ausgesetzt sind, adäquat adressiert werden (s. u. Abs. 3).

2. VERZICHT AUF VOLLHARMONISIERUNG (ART. 3 NIS 2-E)

Die Folgenabschätzung der EU-Kommission hat ergeben, dass die Bemühungen der einzelnen Mitgliedstaaten um ein höheres Cybersicherheitsniveau auf nationaler Ebene und die Ergebnisse dieser Bemühungen höchst uneinheitlich sind[15]. Eine vollharmonisierende Richtlinie hätte Länder mit einer stark entwickelten Cybersicherheitslandschaft wie Deutschland möglicherweise in der Umsetzung eigener, weitergehender Maßnahmen behindert. Unter anderem wäre der Spielraum für mögliche Verbesserungen durch das beschlossene Zweite IT-Sicherheitsgesetz[16] möglicherweise begrenzt worden.

> Die Anwendung des Mindestharmonisierungsprinzips ist aus Verbrauchersicht zu begrüßen.

---

[8] Europäische Kommission (2020): Annexes to the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72172. 21.01.2021, Anhang I, Anhang II.

[9] Zu den unterschiedlichen Aufsichtssystemen für die beiden Dienstekategorien s. Erwägungsgrund 70 NIS 2-E.

[10] Annexes, Anhang II, S. 10, Nr. 6.

[11] Ebd. Anhang I, S. 7, Nr. 8.

[12] Ebd.

[13] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32018L1972, 21.01.2021.

[14] Annexes, Anhang II S. 9 f. Nr. 3-5.

[15] Europäische Kommission (2020), Commission Staff Working Document / Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Part 1/3, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72176, 21.01.2021, S 13 ff.

[16] S. Verbraucherzentrale Bundesverband e.V. (2020): IT-Sicherheit im Verbraucheralltag stärken, https://www.vzbv.de/dokument/it-sicherheit-im-verbraucheralltag-staerken, 21.01.2021.

3. RISIKOMANAGEMENT (ART. 18 NIS 2-E)

In Artikel 18 NIS 2-E werden Anforderungen an Dienste zum Schutz von IT-Systemen, die Anbieter „bei der Erbringung ihrer Dienste nutzen“, aufgestellt. Es werden also nicht Produkte selbst, sondern die für ihre Bereitstellung oder Produktion genutzten Systeme reguliert. In Branchen außerhalb des eigentlichen digitalen Marktes kann so die Qualität und Verfügbarkeit der angebotenen Waren und Dienstleistungen erhöht werden. Die eigentlichen Produkte werden weiterhin durch andere Regelwerke wie etwa die Produktsicherheitslinie erfasst. In Bezug auf digitale Dienste ist es jedoch nachteilig, dass der Regelungsbereich der NIS 2 nicht explizit auch digitale Produkte umfasst. So ist fraglich, ob hinreichende Sicherheitsanforderungen für Social-Media-Apps aus den genannten Regelungen abgeleitet werden können. Hier sollten zum Beispiel Vorschriften für sichere Authentisierungsmechanismen wie die 2-Faktor-Authentisierung explizit genannt und verpflichtend gemacht werden. Diese in den Produkten implementierten Sicherheitsmaßnahmen (Security by Design) müssen auch bereits bei Auslieferung der Produkte aktiviert sein, um ihre volle Wirkung zu entfalten (Security by Default).

Weil aber auch der neue Entwurf der NIS 2 auf wichtige und wesentliche Dienste ausgerichtet und sein Anwendungsbereich entsprechend reduziert ist, erscheint die NIS 2 nicht als der richtige gesetzgeberische Ort, um diese produktspezifischen Anforderungen für digitale Verbraucherprodukte allgemein verbindlich zu machen. Eine zuverlässige Implementierung dieser Sicherheitsmechanismen könnte durch eine Verbesserung der Vorschriften in mehreren Rechtsakten auf europäischer Ebene folgen. Zu nennen sind in diesem Zusammenhang die Produktsicherheitsrichtlinien in Bezug auf die IT-Sicherheit von Software und vernetzten Geräten[17] sowie ein möglicher künftiger horizontaler Rechtsakt zur Cybersicherheit vernetzter Geräte und assoziierter Dienste[18].

> Hersteller und Anbieter sollten zu einem hinreichenden IT-Sicherheitsniveau ihrer digitalen Produkte gesetzlich verpflichtet werden. Zu diesen Maßnahmen sollten gehören:
>
> - Verschlüsselte Speicherung und Übertragung sensibler Daten
> - Starke Authentisierungsmechanismen
> - Bereitstellung von Sicherheitsupdates über einen hinreichend langen Zeitraum

4. MELDEPFLICHTEN (ART. 20 NIS 2-E)

Nach der geltenden Richtlinie sind Anbieter digitaler Dienste nicht verpflichtet, im Falle von IT-Sicherheitsvorfällen ihre potentiell geschädigten Kunden zu benachrichtigen (Art. 16 NIS-RL[19]). Schnelle und zielgerichtete Information ist in diesen Fällen aber notwendig, um Verbrauchern die Möglichkeit zu geben, eigene Sicherheitsvorkehrungen zu treffen, und ihre Daten zu schützen. Der neue Entwurf der NIS 2 enthält die Verpflichtung für Anbieter, auch den Nutzern ihrer Dienste zeitnah Informationen zum Vorfall und zu möglichen Schutzmaßnahmen zu übermitteln (Art. 20 Nr. 2 NIS 2-E). Informationsinhalte, das Format und der Prozess der Benachrichtigung können in Durchführungsrechtsakten näher geregelt werden (Art. 20 Nr. 11 S. 1 NIS 2-E).

---

[17] Verbraucherzentrale Bundesverband e.V. (2020): Sichere Produkte schaffen mehr Verbrauchervertrauen https://www.vzbv.de/dokument/sichere-produkte-schaffen-mehr-verbrauchervertrauen, 21.01.2021.

[18] S. o. Fußnote 1.

[19] Art. 16 Nr. 7 NIS-RL enthält lediglich eine Kann-Bestimmung zur Information der Öffentlichkeit.

Die Informationsbedürfnisse unterscheiden sich naturgemäß stark danach, ob staatliche Behörden, geschädigte Unternehmen oder Privatpersonen adressiert werden. Daher sollten in den Durchführungsrechtsakten je eigene Regeln für diese Adressatengruppen erlassen werden. Informationen für Verbraucher müssen allgemein verständlich und lösungsorientiert sein. Außerdem müssen geeignete Informationskanäle genutzt werden. Bei Online-Marktplätzen etwa, die über lokal installierte Apps angeboten werden, bieten sich In-App-Benachrichtigungen an. Es sollte hingegen vermieden werden, dass wichtige Sicherheitsinformationen über die gleichen Kanäle wie Werbenachrichten versendet und daher leicht übersehen werden.

> Diensteanbieter müssen Informationen zu Sicherheitsvorfällen nach NIS 2-E zielgruppenspezifisch, lösungsorientiert und über geeignete Informationskanäle kommunizieren. Die Kommission sollte entsprechende Durchführungsrechtakte nach Art. 20 Abs. 11 NIS 2-E erlassen.

5. WEITERE REGELUNGEN

NIS 2-E führt neue Institutionen und Prozesse ein, die das allgemeine IT-Sicherheitsniveau in der Europäischen Union verbessern sollen. Dazu gehört beispielsweise ein zentrales Register für wichtige und wesentliche Diensteanbieter bei der europäischen Behörde ENISA (Art. 25 NIS 2-E).

> Art. 25 NIS 2-E und weitere Bestimmungen zur europäischen IT-Sicherheitsarchitektur können das allgemeine IT-Sicherheitsniveau in der Europäischen Union erhöhen. Diese Bestimmungen sind aus Verbrauchersicht positiv zu bewerten.