**Bundesrat** **Drucksache 680/17 (Beschluss)**

**15.12.17**

# Beschluss
**des Bundesrates**

---

## Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit")

**COM(2017) 477 final; Ratsdok. 12183/17**

Der Bundesrat hat in seiner 963. Sitzung am 15. Dezember 2017 gemäß §§ 3 und 5 EUZBLG die folgende Stellungnahme beschlossen:

1. Der Bundesrat begrüßt, dass die Kommission dem Thema "Cybersicherheit" große Aufmerksamkeit widmet. Ein sicherer Cyberraum hat sich zu einer Grundbedingung für das gesellschaftliche und wirtschaftliche Zusammenleben entwickelt und ist daher von übergeordnetem Interesse.

2. Er teilt die Einschätzung der Kommission, dass ein stärkeres gemeinsames Vorgehen der EU bei der Verbesserung der Abwehrfähigkeit im Bereich der Cybersicherheit durch engere Zusammenarbeit und Kooperation sinnvoll ist, um die rasant wachsenden Herausforderungen im Cyberraum zu bewältigen. Dabei ist auch die von der Kommission vorgeschlagene Initiative, die Cybersicherheit von IKT-Produkten und -Diensten zum Schutz und zum Nutzen der Verbraucherinnen und Verbraucher sowie zum Nutzen der Wirtschaft im EU-Binnenmarkt durch ein Zertifizierungssystem und die Verankerung von Sicherheitszielen zu erhöhen, vom Grundsatz her zu begrüßen und zu unterstützen.

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

3. Der Bundesrat geht dabei davon aus, dass unter den Begriff der IKT-Produkte und -Dienste auch Verbraucherprodukte für die elektronische Kommunikation sowie sonstige, vernetzte Verbraucherprodukte und verbrauchernahe Produkte wie beispielsweise Smart-Home-Produkte und intelligente Stromzähler fallen, die Informationen digital erfassen und übertragen.

4. Er begrüßt das Anliegen des Verordnungsvorschlages, einen einheitlichen Sicherheitsstandard für IT-Produkte und Dienstleistungen im Binnenmarkt der EU schaffen zu wollen. Angesichts des freien Verkehrs für Waren und Dienstleistungen und des vernetzten Charakters internetfähiger IT-Produkte ist augenfällig, dass eine Beschränkung auf rein nationale Regulierungen nicht sinnvoll ist.

5. Der Bundesrat wendet sich aber dagegen, dass der Verordnungsvorschlag die Europäische Agentur für Netz- und Informationssicherheit (ENISA) berechtigt, verbindliche Zertifizierungssysteme festzulegen, die nationale Systeme, selbst wenn sie einen höheren nationalen Standard etablieren, verdrängen.

   Der Verordnungsvorschlag berücksichtigt nicht, dass IT-Zertifizierungsverfahren auch ganz maßgeblich die nationale Sicherheit und Souveränität der Mitgliedstaaten betreffen. Dies gilt insbesondere für die Bewertung höherer Sicherheitsniveaus, insbesondere für die Sicherheit kryptografischer Verfahren.

   Durch die Regelung des Artikels 49 Absatz 1 des Verordnungsvorschlags würden nationale Zertifizierungssysteme für IKT-Produkte und -Dienste nach einer Übergangsfrist unwirksam, wenn diese inhaltlich unter ein entsprechendes europäisches System fallen. Die Einführung neuer nationaler Systeme in auf EU-Ebene geregelten Bereichen wäre durch Artikel 49 Absatz 2 des Verordnungsvorschlags untersagt. Hierdurch wird nicht in gebotenem Maße berücksichtigt, dass es sich bei Zertifizierungssystemen für IKT-Produkte und -Dienste keineswegs nur um Produkt- beziehungsweise Marktstandards handelt. Vielmehr sind IT-Sicherheitszertifikate eine Ausprägung der Systeme zur Gewährleistung der Informationssicherheit. Es handelt sich somit im Ergebnis auch um eine Frage der öffentlichen Sicherheit der Mitgliedstaaten. Diese Regelung ist nicht durch die gewählte allgemeine Binnenmarktkompetenz des Artikels 114 Absatz 1 AEUV gedeckt. Denn nach der Rechtsprechung des Europäischen Gerichtshofs verleiht Artikel 114

AEUV dem Unionsgesetzgeber keine allgemeine Kompetenz zur Regelung des Binnenmarktes. Ein auf der Grundlage von Artikel 114 AEUV erlassener Rechtsakt muss vielmehr tatsächlich zur Beseitigung bestehender Hemmnisse bei der Verwirklichung des Binnenmarktes beitragen oder spürbare Wettbewerbsverzerrungen beseitigen (vergleiche EuGH, Urteil vom 5. Oktober 2000, Rechtssache C-376/98, Bundesrepublik Deutschland gegen Europäisches Parlament und Rat der Europäischen Union).

Obwohl in Artikel 3 Absatz 3 des Verordnungsvorschlags vorgesehen ist, dass die Zuständigkeiten der Mitgliedstaaten im Bereich der Cybersicherheit sowie Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich von den Zielen und Aufgaben der ENISA unberührt bleiben - also nicht vom Mandat der ENISA umfasst sind -, berühren die Regelungen zum EU-Zertifizierungsrahmen in erheblichem Maße die öffentliche Sicherheit, sofern sie als umfassende Vorrangregelung ausgestaltet sind. Nicht berücksichtigt wurde zudem, dass auch der Bereich der öffentlichen Verwaltung von der Binnenmarktkompetenz nicht umfasst ist.

6. Der Bundesrat hat darüber hinaus Zweifel, ob der Verordnungsvorschlag im Hinblick auf die Ausgestaltung der europäischen Systeme für die Cybersicherheitszertifizierung den Grundsätzen der Subsidiarität nach Artikel 5 Absatz 3 EUV und der Verhältnismäßigkeit gemäß Artikel 5 Absatz 4 EUV entspricht. Nach Artikel 5 Absatz 4 EUV dürfen Maßnahmen der Union inhaltlich wie formal nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinausgehen. Sie müssen insbesondere erforderlich und angemessen sein.

7. Ziele des Verordnungsvorschlags sind insbesondere der Ausbau der Kapazitäten und der Abwehrbereitschaft der Mitgliedstaaten sowie die Verbesserung der Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit von IKT-Produkten und -Diensten, um das Vertrauen in den digitalen Binnenmarkt und die digitale Innovation zu stärken. Es bestehen jedoch bereits auf nationaler Ebene Strukturen und Zertifizierungsverfahren, die sich bewährt haben. Durch den Ausschluss ergänzender nationaler Systeme über ein europäisches System für die Cybersicherheit werden die Mitgliedstaaten in ihren effektiven Möglichkeiten zur Gestaltung ihrer nationalen Informationssicherheit erheblich beeinträchtigt. Für die Mitgliedstaaten bestünde somit die Gefahr, dass nationale Systeme zur

Gewährleistung der Informationssicherheit nicht effektiv umgesetzt werden könnten.

8. Ein derartiger Eingriff in die Angelegenheiten der nationalen Sicherheit der Mitgliedstaaten ist auch nicht erforderlich. Das Ziel der Stärkung der Cybersicherheit im Bereich des Binnenmarktes kann in gleich geeigneter Weise auch erreicht werden, wenn die europäischen Systeme für die Cybersicherheitszertifizierung durch nationale Zertifizierungssysteme für den öffentlichen Bereich ergänzt werden können. Die europäischen Systeme können hierfür eine gemeinsame Basis im Sinne eines Mindeststandards bilden.

9. Der Bundesrat betont, dass das vorgeschlagene Zertifizierungssystem nicht dazu dienen darf, gerechtfertigte nationale Anforderungen auszuhöhlen. Insbesondere wird kritisch gesehen, dass den Mitgliedstaaten lediglich ein Vorschlagsrecht beziehungsweise eine beratende Funktion bei der Ausarbeitung der jeweiligen Sicherheitszertifizierungssysteme nach Artikel 44 Absatz 1 des Verordnungsvorschlags eingeräumt wird und die Kommission darüber hinaus befugt ist, "auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems nach Artikel 55 Absatz 1 Durchführungsrechtsakte zu erlassen".

10. Im Hinblick auf die Ausweitung der Aufgaben der ENISA zu einer stärkeren operativen Zusammenarbeit auf Unionsebene ist zu berücksichtigen, dass die über eine Harmonisierung der Wettbewerbsbedingungen hinausgehenden Vorschläge zur Ausgestaltung der ENISA als eine Agentur mit operativen Befugnissen gegenüber den Mitgliedstaaten, insbesondere mit eigenen Analysekompetenzen, kritisch gesehen wird. Ein Mehrwert eigener Analysebefugnisse der ENISA erscheint fraglich.

11. Der Bundesrat bedauert zugleich, dass die Kommission lediglich einen Rahmen für eine Cybersicherheitszertifizierung schaffen will, der für die Unternehmen nicht obligatorisch ist.

    Die von der Kommission vorgesehene Freiwilligkeit der Zertifizierung erscheint im Hinblick auf internetfähige IT-Produkte nicht ausreichend. Das Botnetz "Mirai" hat vor Augen geführt, dass innerhalb kürzester Zeit eine halbe Million Geräte mit Schadsoftware infiziert und für die Ausführung von

digitalen Angriffen benutzt werden können. Um auszuschließen, dass internetfähige Geräte Schwachstellen für derartige Attacken aufweisen, regt der Bundesrat an, dass deren Zertifizierung zwingende Voraussetzung für die Marktzulassung wird.

12. Sollte bei den Verhandlungen auf EU-Ebene am freiwilligen Zertifizierungssystem festgehalten werden, bittet der Bundesrat die Bundesregierung darauf hinzuwirken, dass dieses System mitgliedstaatliche Verpflichtungen zur Zertifizierung von IKT-Produkten und -Diensten anhand von Anforderungen an die Datensicherheit und den Datenschutz wie beispielsweise nach § 24 des Messstellenbetriebsgesetzes für Smart-Meter-Gateways nicht ausschließt.

13. Aus Sicht des Bundesrates ist langfristig die Einführung EU-weiter verbindlicher Sicherheitsstandards sinnvoll. Würden solche Standards schrittweise eingeführt, beginnend mit den als besonders sensibel eingestuften Wirtschaftszweigen und Anwendungsfeldern, könnte dies eine Etablierung von IT-Sicherheitszertifizierungen auch in anderen Bereichen deutlich fördern.

14. Der Bundesrat weist darauf hin, dass die EU mit verbindlichen Sicherheitsanforderungen nicht allein stünde. Die Kommission selbst hat in ihrer Mitteilung "Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen" (BR-Drucksache 654/17) darauf hingewiesen, dass in einer Reihe von Drittstaaten bereits verbindliche Cybersicherheitsanforderungen in wichtigen Wirtschaftszweigen darüber entscheiden, ob Waren und Dienstleistungen aus der EU dort einen Marktzugang erhalten.

15. Im vorliegenden Verordnungsvorschlag sind die Sicherheitsziele der Zertifizierung auf das gefahrlose Erreichen des von den Nutzerinnen und Nutzer eines IKT-Produkts oder einer Dienstleistung verfolgten Nutzungszwecks ausgerichtet. Mit der Einführung von Vertrauenswürdigkeitsstufen richtet die Kommission das Niveau der IT-Sicherheit an deren Sicherheitsbedürfnis aus. Verarbeitet ein IKT-Produkt keine personenbezogenen Daten oder hat es keinen Einfluss auf Prozesse, deren Störung nach Einschätzung von Käuferinnen und Käufern oder Dienstleistungsnehmerinnen und -nehmern zu einem Schaden führen kann, werden viele Kundinnen und Kunden kein großes Sicherheitsbedürfnis entwickeln.

16. Dabei verkennt der von der Kommission gewählte Regelungsansatz aus Sicht des Bundesrates einerseits, dass IKT-Produkte und Dienstleistungen in unterschiedlich sensiblen Bereichen eingesetzt werden können. Beispielsweise kann eine durch einen Cybervorfall herbeigeführte Fehlfunktion eines internetfähigen Gerätes durchaus physische Gefahren im bestimmungsgemäßen Gebrauch herbeiführen, mitunter nicht nur für Verbraucherinnen und Verbraucher, die die Kaufentscheidung getroffen haben, sondern auch für Dritte.

17. Der Bundesrat gibt andererseits zu bedenken, dass auch eine Stör- und Angriffsanfälligkeit von IKT-Produkten in aus Sicht der Käuferin oder des Käufers wenig sensiblen Bereichen durchaus zu breiten und bedrohlichen Auswirkungen führen kann, wenn diese für Angriffe auf Systeme in ganz anderen Bereichen genutzt wird.

18. Er ist überzeugt, dass es daher nicht überall der Auswahlentscheidung der Endverbraucherinnen und -verbraucher überlassen bleiben kann, ob Geräte oder Dienstleistungen eine "niedrige" oder "hohe" Vertrauenswürdigkeitsstufe aufweisen oder jedweder Zertifizierung entbehren. Der Bundesrat fordert die Bundesregierung auf, hier in den weiteren Beratungen auf eine Komplexität der Regulierung zu drängen, die dem Gegenstand angemessen ist.

19. Er stellt fest, dass entgegen der Behauptung des Verordnungsvorschlags keine ausreichende Abstimmung mit anderen Politikfeldern der EU stattfindet. Im Bereich der Datensicherheit gibt es in Artikel 42 der Datenschutz-Grundverordnung bereits eine Zertifizierung für Produkte, die den rechtlich verbindlichen Anforderungen des "privacy by design" beziehungsweise "privacy by default" nach Artikel 25 der Datenschutz-Grundverordnung entsprechen.

20. Der Bundesrat weist darauf hin, dass damit zugleich für einen Teilbereich von IKT-Produkten und -Dienstleistungen (beispielsweise cloud-Services) rechtlich verbindliche Vorgaben bestehen, die unmittelbar die "Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von gespeicherten, übermittelten und verarbeiteten Daten, Funktionen und Diensten" (Artikel 43 des Verordnungsvorschlags) betreffen.

21. Aus seiner Sicht ist es für die Nutzerinnen und Nutzer nur schwer nachvollziehbar, wenn zukünftig dasselbe Produkt oder dieselbe Dienstleistung zwei Zertifikate mit unterschiedlichen Rechtsfolgen tragen sollte.

22. Aus Sicht des Bundesrates sollte geprüft werden, ob in die Zertifizierung auch Anforderungen an den Datenschutz aufgenommen werden können, die wie die Verpflichtung zu datenschutzfreundlichen Voreinstellungen (privacy by default) oder zur datenschutzfreundlichen Gestaltung (privacy by design) nach Artikel 25 der Datenschutz-Grundverordnung sinnvollerweise am Produkt selbst ansetzen. Mit der inhaltlichen Erweiterung der produktbezogenen Zertifizierung auf Datenschutzaspekte würde eine Lücke bei der Verwirklichung der Datenschutzziele der Datenschutz-Grundverordnung geschlossen. Zudem könnte eine mögliche, für die Verbraucherinnen und Verbraucher unübersichtliche Häufung von Zertifizierungen der Cybersicherheit einerseits und des Datenschutzes andererseits vermieden werden.

23. Der Bundesrat bemängelt ferner, dass sich an die im Verordnungsvorschlag vorgesehenen Zertifizierungssysteme weder hier noch in anderen Rechtsgrundlagen der EU begleitende Gewährleistungsverpflichtungen für die Hersteller anschließen. Dies betrifft sowohl eine fehlende Verpflichtung zu regelmäßigen Sicherheitsupdates als auch die Haftung für Schäden, die durch fehlende Behebung von Sicherheitsmängeln entstanden sind. Im Übrigen verweist der Bundesrat auf seine Stellungnahme vom 24. November 2017 (BR-Drucksache 654/17 (Beschluss)).

24. Er nimmt den Verordnungsvorschlag zum Anlass darauf hinzuweisen, dass neben den technischen Voraussetzungen für sichere Software-Updates nach Artikel 45 Buchstabe g des Verordnungsvorschlags auch ein vertraglicher Anspruch der Verbraucherinnen und Verbraucher auf Bereitstellung von Software-Updates während der üblichen Lebensdauer des Produkts erwogen werden sollte, wenn das Produkt ohne die Updates auf Grund rechtlicher Vorschriften nicht mehr bestimmungsgemäß verwendet werden dürfte. Dies könnte beispielsweise bei der in Kraftfahrzeugen für die assistierte oder automatisierte Fahrzeugsteuerung verwendeten Software der Fall sein, wenn diese aus Gründen der Verkehrssicherheit und zum Schutz vor Cyberangriffen aktualisiert werden muss.

25. Der Bundesrat weist darauf hin, dass mit Verabschiedung der Richtlinie (EU) 2016/1148 vom 6. Juli 2016 über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-Richtlinie) bereits ein wichtiger Schritt zu einer Mindestharmonisierung und Gewährleistung einer hohen Netz- und Informationssicherheit erreicht wurde, um der wachsenden Bedeutung der Netz- und Informationssicherheit Rechnung zu tragen.

26. Er fordert, dass eine Ausweitung der Aufgaben der ENISA beziehungsweise der NIS-Richtlinie erst dann auf den Weg gebracht wird, wenn die NIS-Richtlinie in allen Mitgliedstaaten umgesetzt und die vorgesehene Überprüfung der Kohärenz der mitgliedstaatlichen Ansätze durchgeführt wurde.

27. Der Bundesrat übermittelt diese Stellungnahme direkt an die Kommission.