Bundesrat **Drucksache** **654/1/17**

13.11.17

Empfehlungen
der Ausschüsse

EU - In - R - V - Wi

zu **Punkt …** der 962. Sitzung des Bundesrates am 24. November 2017

Gemeinsame Mitteilung an das Europäische Parlament und den Rat - Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen

JOIN(2017) 450 final

A

Der **federführende Ausschuss für Fragen der Europäischen Union**

empfiehlt dem Bundesrat, zu der Vorlage gemäß §§ 3 und 5 EUZBLG wie folgt Stellung zu nehmen:

1. Der Bundesrat begrüßt, dass die Kommission dem Thema der Sicherheit informationstechnischer Systeme große Aufmerksamkeit widmet. Digitale Technologien prägen den Alltag der Menschen und die Produktions- und Dienstleistungsketten der Wirtschaft. Deren sichere Ausgestaltung und Anwendung ist nicht nur Zukunftsaufgabe, sondern aktuelle Herausforderung.

2. Der Bundesrat teilt die Auffassung der Kommission, dass eine wesentliche Bedingung für die Verbesserung der Cybersicherheit darin besteht, dieses Thema in der Ausbildung der öffentlichen Verwaltung sowie in Lehrplänen sonstiger Berufsausbildungseinrichtungen und Hochschulen zu verankern. Der Bundesrat begrüßt, dass dabei neben den im engeren Sinne im Bereich der Cybersicherheit tätigen Arbeitnehmerinnen und Arbeitnehmern und den

...

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

übrigen IKT-Fachkräften auch weitere Beschäftigtengruppen sowie Bürgerinnen und Bürger mit Sensibilisierungsmaßnahmen und Informationskampagnen in den Blick genommen werden. Der Bundesrat bekräftigt, dass die Sicherheit informationstechnischer Systeme nicht nur eine Frage der Technik ist, sondern eine Frage der Arbeitsprozesse und der Qualifizierung der Nutzerinnen und Nutzer.

3. Der Bundesrat nimmt zustimmend zur Kenntnis, dass die Kommission die Bedeutung der Verschlüsselung für die Wahrung von Grundrechten wie der Meinungsfreiheit und des Schutzes personenbezogener Daten sowie für die Sicherheit des elektronischen Geschäftsverkehrs hervorhebt. Dass Verschlüsselungstechnologien sich weiter verbreiten, stärker genutzt werden und damit die Sicherheit in der digitalen Kommunikation steigern, hängt maßgeblich davon ab, dass die Nutzerinnen und Nutzer entsprechenden Anwendungen vertrauen können.

4. Zugleich darf nicht außer Acht gelassen werden, dass Verschlüsselung durch Terroristen und andere Kriminelle zur Vorbereitung und Durchführung schwerer Straftaten missbraucht wird. Der Bundesrat unterstützt daher die Überlegungen der Kommission, die Rolle der Verschlüsselung beim Schutz der inneren Sicherheit und bei strafrechtlichen Ermittlungen näher zu untersuchen.

5. Der Bundesrat spricht sich dafür aus, bei Fragen der Haftung über Schäden hinaus, die den Unternehmen und Lieferketten entstehen, auch die besonderen Schadensbilder bei privaten Nutzerinnen und Nutzern von IT-Produkten und -Dienstleistungen sowie dem öffentlichen Sektor in den Blick zu nehmen.

6. Die Gewährleistungsrechte von Verbraucherinnen und Verbrauchern bedürfen im Zusammenhang mit Sicherheitslücken von IT-Produkten und -Dienstleistungen einer klaren Justierung. Der Bundesrat bittet die Kommission, hier Vorschläge für eine zeitgemäße Konkretisierung von Mängelbeseitigungsrechten zu entwickeln. Es sollte eine Pflicht zur Bereitstellung von Sicherheitsupdates in Erwägung gezogen werden, die transparente Vorgaben dazu enthält, wie schnell, regelmäßig und für welchen Zeitraum Hersteller den Verbraucherinnen und Verbrauchern entsprechende Angebote unterbreiten müssen.

7. Der Bundesrat regt die Entwicklung eines Kriterienkataloges an, in welchen sensiblen Bereichen der von der Kommission angestrebte Aufbau von IT-Sicherheitskompetenzen der öffentlichen Hand sich auf die Fähigkeit zur eigenständigen Durchführung von IT-Sicherheitszertifizierungen erstrecken sollte.

8. Aus Sicht des Bundesrates wird die Mitteilung den Potenzialen quelltextoffener Software ("Open Source") für die Steigerung der IT-Sicherheit nicht gerecht. Der Bundesrat bittet die Kommission um eine konzeptionelle Klärung, inwieweit die öffentliche Hand zur Steigerung der IT-Sicherheit beitragen kann, indem sie selbst "Open Source"-Technologie einsetzt und deren Weiterentwicklung fördert. In diesem Zusammenhang sollten zudem die wirtschaftlichen Chancen - auch für kleine und mittelständische IT-Unternehmen in Europa - betrachtet werden.

9. Der Bundesrat mahnt eine klarere Definition der Begriffe "Cybersicherheit" und "Cyberabwehr" an.

Begründung zu Ziffern 1 bis 3 und 5 bis 9 (nur gegenüber dem Plenum):

Die Mitteilung ist Teil einer Reihe von Anstrengungen der EU zur Verbesserung der Sicherheit informationstechnischer Systeme. Bei der Qualifizierung werden bereits mannigfaltige Anstrengungen unternommen. Die konzeptionellen Herausforderungen stellen sich dabei über die Grenzen von Nationalstaaten hinweg in vergleichbarer Weise dar.

Dabei gilt es, auch die jenseits des wirtschaftlichen Wachstums bestehende Bedeutung von IT-Sicherheitskompetenzen für das Leben der Bürgerinnen und Bürger hinreichend in die Überlegungen einzubeziehen. Dies gilt auch hinsichtlich des Einsatzes von Verschlüsselungstechnologien, denen eine ganz grundlegende Funktion für die Wahrung von Grundrechten zukommen.

Eine Meldepflicht ist nicht erst bei schweren Vorfällen zu erwägen. Die Meldung von Vorfällen kann und sollte zum normalen und integralen Bestandteil des betrieblichen Sicherheitsmanagements werden.

Die Kommission lässt eine Auseinandersetzung mit der IT-sicherheitspolitischen Bedeutung von Software vermissen, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann ("open source"). Diese ist oftmals durchaus Basis kommerzieller Nutzungen und bietet den Vorteil, dass der offene Quelltext eine Fehlersuche und -diskussion auch über die Kompetenzen des ihn einsetzenden Akteurs hinaus ermöglicht und beschleunigt.

Eine klar zivile Ausrichtung auf eine Härtung gegen Angriffe bietet den Vorteil, dass entsprechende Konzepte sich nicht auf die Beschaffenheit der Angreifer beziehen müssen - seien es Kriminelle, Nachrichtendienste oder von fremden Mächten beauftragte oder geduldete Angreifer ("hybride Bedrohung"). Insofern kann eine Bündelung über Sektorengrenzen hinweg praktikabel sein.

Demgegenüber muss eine Bündelung ziviler, polizeilicher und militärischer Maßnahmen gegen Angreifer in Deutschland der Verfassungsrechtslage zum "digitalen Bundeswehreinsatz im Innern" gerecht werden. Die Mitteilung zielt darauf ab, zivile und militärische Cybersicherheitsmaßnahmen sowohl im Bereich der Forschung als auch der laufenden Lagebeobachtung (Zusammenarbeit von Europol. INTCEN, EAD, GSVP-Missionen) und mittels einer verstärkten Kooperation von EU und NATO zu verschränken.

Zu hinterfragen ist in diesem Zusammenhang auch, dass das europäische Netz von Cybersicherheitskompetenzzentren sowie das Europäische Kompetenzzentrum für Cybersicherheitsforschung um eine "Cyberabwehrdimension ergänzt werden könnten". Der Kommission geht es hierbei nicht lediglich um Forschung und Entwicklung von Cybersicherheitslösungen. Mit "Informationsaustausch" und "koordinierten Reaktionen" wird auch die Vollzugsebene der Cyberabwehr angesprochen.

Es erschließt sich letzthin nicht, warum die Kommission sich nicht auf die Schaffung effektiver IT-sicherheitsrelevanter Marktzugangsregelungen konzentriert und stattdessen eine EU-Cybersicherheitsindustrie fördern möchte.

B

10. Der **Ausschuss für Innere Angelegenheiten**,

der **Rechtsausschuss**,

der **Ausschuss für Verteidigung** und

der **Wirtschaftsausschuss**

empfehlen dem Bundesrat, von der Vorlage gemäß §§ 3 und 5 EUZBLG Kenntnis zu nehmen.