**Bundesrat** zu Drucksache **621/26**

**30.10.26**

In

# Beschluss
**des Deutschen Bundestages**

---

## Gesetz zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung)

Der Deutsche Bundestag hat in seiner 102. Sitzung am 15. Oktober 2026 zu dem von ihm verabschiedeten **Gesetz zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung) – Drucksachen 21/6134, 21/6512, 21/8622 –** die beigefügte Entschließung unter Buchstabe b auf Drucksache 21/8622 angenommen.

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.bundesanzeiger-verlag.de
ISSN 0720-2946

I. Der Deutsche Bundestag stellt fest:

Die aktuelle geopolitische Bedrohungslage durch Cyberangriffe, Sabotage und Spionage verdeutlicht den dringenden Bedarf, unsere kritische Infrastruktur resilienter und sicherer aufzustellen. Die Sicherheit unserer Mobilfunknetze im Großen genau wie die Sicherheit jedes einzelnen digitalen Produkts im Kleinen muss oberste Priorität in einer Zeit haben, in der sich Deutschland verstärkt hybriden Angriffen ausgesetzt sieht. Digitale und technologische Souveränität bedeuten dabei keine internationale Abschottung, sondern lediglich die Möglichkeit, tatsächliche Alternativen nutzen zu können und nicht in Abhängigkeiten zu verharren.

Mit dem NIS-2-Umsetzungsgesetz, dem KRITIS-Dachgesetz sowie dem europäischen Cyber Resilience Act und dem vorliegenden Durchführungsgesetz wurden bereits wichtige Schritte dieses Weges hin zu mehr Cybersicherheit und weniger Abhängigkeiten ermöglicht.

Dennoch sind die deutsche Wirtschaft, Verwaltung und Infrastrukturen weiterhin in hohem Maße von einzelnen Herstellern und Lieferketten abhängig. Geopolitische Eskalationen, Lieferkettenunterbrechungen, Sicherheitsvorfälle, fehlende Softwareupdates oder Ersatzteile können zu systemischen Risiken führen. Staaten wie China verpflichten in ihrem Land ansässige Hersteller zudem zur Zusammenarbeit mit ihren Geheimdiensten. Die Verwendung kritischer Komponenten nicht vertrauenswürdiger Anbieter birgt erhebliche Gefahren für die IT-Sicherheit, die nationale Sicherheit und die wirtschaftliche Stabilität. Wenn Systeme von Herstellern abhängen, die unmittelbar oder mittelbar unter dem Einfluss eines Drittstaates stehen, macht uns dies verwundbar. Durch das BSIG wird der Einsatz von kritischen Komponenten eines nicht vertrauenswürdigen Herstellers gegenüber Betreibern kritischer Anlagen (KRITIS) bereits reguliert und kann durch das Bundesministerium des Innern untersagt werden. Jedoch bestehen die genannten Gefahren nicht nur für KRITIS-Anlagen, sondern in jedem einzelnen Haushalt, in dem systemkritische Komponenten, beispielsweise Router im Telekommunikationsbereich und Wechselrichter im Bereich Energie, zum Einsatz kommen. In solchen Komponenten können versteckte Hintertüren eingebaut sein, die es ermöglichen können, den Datenverkehr unbemerkt zu überwachen oder abzufangen. Außerdem besteht die Gefahr, dass auf solche Komponenten aus der Ferne zugegriffen werden kann. Sind solche Komponenten erst einmal tief in einem System verbaut, wäre ihr Austausch nicht nur technisch herausfordernd, sondern vor allem teuer. Daher muss der Markt möglichst effektiv überwacht werden.

Digitale Souveränität und technologische Diversifizierung sind daher wesentliche Voraussetzungen für die Resilienz kritischer Infrastrukturen.

II. Der Deutsche Bundestag fordert die Bundesregierung der 21. Wahlperiode auf,

– im Rahmen der Marktüberwachung nach der Cyberresilienz-Verordnung durch das BSI als Marktüberwachungsbehörde, die Prüfung von Routern vorrangig durchzuführen und den bestehenden Rechtsrahmen auszuschöpfen;

– den bisherigen, erfolgreichen Weg weiter zu verfolgen und sich auf europäischer Ebene sowie im Rahmen anstehender Gesetzesvorhaben mit Nachdruck für die Reduzierung der Abhängigkeit kritischer Infrastrukturen von nicht vertrauenswürdigen Herstellern einzusetzen und die Diversifizierung kritischer Lieferketten zu stärken;

- sich auf europäischer Ebene im Rahmen der Verhandlungen zum Cybersecurity Act 2 für eine stärkere Regulierung von netz- beziehungsweise systemkritischen Komponenten nicht vertrauenswürdiger Anbieter auf dem EU-Binnenmarkt einzusetzen;
- sich auf europäischer Ebene für einen gemeinsamen risikobasierten Ansatz zur Sicherheit kritischer IKT-Lieferketten (IKT = Informations- und Kommunikationstechnologie) und zur Stärkung der digitalen Souveränität einzusetzen und diesen Weg gemeinsam mit den europäischen Partnern konsequent weiterzugehen;
- bei Beschaffungsaufträgen kritischer digitaler Komponenten neben technischen Sicherheitsanforderungen insbesondere Herstellerabhängigkeiten, Lieferketten, Update- und Wartungsmöglichkeiten sowie die Substituierbarkeit von Komponenten zu berücksichtigen;
- durch den Abbau von Abhängigkeiten in der kritischen Infrastruktur gleichzeitig auch deutsche und europäische Hersteller zu stärken, zum Beispiel in den Bereichen Heimrouter und Energieanlagen.