Bundesrat zu Drucksache **654/26**

13.11.26

In

Beschluss
des Deutschen Bundestages

Gesetz zur Stärkung der Cybersicherheit

Der Deutsche Bundestag hat in seiner 108. Sitzung am 12. November 2026 zu dem von ihm verabschiedeten **Gesetz zur Stärkung der Cybersicherheit – Drucksachen 21/6585, 21/7406, 21/9159 –** die beigefügte Entschließung unter Buchstabe b auf Drucksache 21/9159 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:

Cyberangriffe in Deutschland nehmen in Qualität und Quantität zu. Deutschland als führende Wirtschaftsnation in Europa ist verstärkt im Fokus auch hochprofessioneller Cyberangriffe mit großem Wirkpotenzial. Angesichts der geopolitischen Lage gewinnen auch hybride Bedrohungen zunehmend an Bedeutung. Der Krieg in der Ukraine verdeutlicht, wie essenziell Cybersicherheit für einen modernen Staat wie Deutschland ist. Die Gewährleistung einer verlässlichen und sicheren Nutzung der Informationstechnologie und der zugrundeliegenden Kommunikationsinfrastruktur ist elementare Voraussetzung für das Funktionieren des Gemeinwesens.

Mit dem Gesetz zur Stärkung der Cybersicherheit werden wirksame, angemessene und rechtsklare gesetzliche Grundlagen geschaffen, um derartige Cyberangriffe erkennen und abwehren zu können. So werden die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Aufklärung und Detektion konkreter Angriffe und langfristig laufender Angriffskampagnen sowie zur Detektion konkreter Vorbereitungshandlungen ausgebaut. Insbesondere gegen groß angelegte Cyberangriffe mit großem Schadenspotenzial bieten präventive Maßnahmen in den eigenen IT-Systemen allein allerdings keinen hinreichenden Schutz. Für die Polizeien des Bundes werden daher auch Möglichkeiten zur Unterbindung solcher Cyberangriffe geschaffen, um gravierende Folgeschäden abwenden oder minimieren zu können. Dazu zählen neben der Detektion von Angriffsmustern und -strukturen auch Maßnahmen im Netz, die den Schaden begrenzen, und – als letztes Mittel – der Eingriff in Systeme der Angreifer. Damit werden die Fähigkeiten zur aktiven Cyberabwehr gezielt ausgebaut.

Mit der Ausweitung staatlicher Cyberfähigkeiten und -befugnisse übernehmen dann neben der Bundeswehr mehrere Bundesbehörden eigenständige Aufgaben im Bereich der aktiven Cyberabwehr. Cyberabwehrmaßnahmen sind an strenge Voraussetzungen geknüpft und bergen auch Risiken. Ein Datenstrom kann nur einmal umgeleitet oder eine Domain nur einmal beschlagnahmt werden. Dazu zählt auch das operative Risiko, dass eine Maßnahme einer Behörde unwissentlich laufende Maßnahmen einer anderen Behörde oder von Dienststellen im Geschäftsbereich des Bundesministeriums der Verteidigung gefährden oder dem Gegner offenbaren kann, besonders bei langfristig angelegten Maßnahmen. Daher sind bei der operativen Fallbearbeitung ein behördenübergreifendes enges Zusammenwirken von BSI, Polizeien, Nachrichtendiensten und der Bundeswehr und ein gemeinsames unverstelltes Lagebild unverzichtbar und es braucht einen abgestimmten Rahmen zum Umgang mit potenziellen Konflikten zwischen den Sicherheitsbehörden.

Entscheidend für ein Mehr an Cybersicherheit sind daher neben den notwendigen neuen Befugnissen ein einheitliches und ganzheitliches Lagebild und ein Gesamtüberblick über alle Cyberabwehrmaßnahmen sowie ein enges Zusammenwirken aller an der Cyberabwehr beteiligten Akteure. Ein wesentlicher Ort dafür ist die zentrale Cybersicherheitsbehörde des Bundes, das BSI, und das dort verortete Nationale Cyber-Abwehrzentrum (Cyber-AZ). Das Cyber-AZ wurde im Zuge der Umsetzung der Cybersicherheitsstrategie für Deutschland 2011 als gemeinsame, behörden- und institutionenübergreifende Plattform für einen verbesserten und beschleunigten Informationsaustausch zwischen den beteiligten Behörden und Einrichtungen und zur stärkeren Koordinierung von Schutz- und Abwehrmaßnahmen gegen IT-Sicherheitsvorfälle in Deutschland eingerichtet. Es bietet eine verlässliche und praxiserprobte Plattform zur Koordinierung

herausgehobener Cybervorfälle, auf die für die Koordinierung der Cyberabwehr aufgesetzt werden kann.

Die aktuelle Cybersicherheitsstrategie für Deutschland der Bundesregierung aus dem Jahr 2021 bildet den Rahmen bis 2026. Notwendig ist daher eine Weiterentwicklung der Cybersicherheitsstrategie der Bundesregierung mit dem Ziel einer klaren Rollen- und Aufgabenverteilung und einem intensiveren Informationsaustausch. Zudem ist das BSI weiter zu stärken und zu einer zentralen Stelle für Fragen der Informations- und Cybersicherheit auszubauen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. die anstehende Weiterentwicklung der Cybersicherheitsstrategie 2026 vorzulegen und dabei angesichts der aktuellen geopolitische Bedrohungslage durch Cyberangriffe insbesondere auch den Rahmen für das Cyber-Abwehrzentrum (AZ) als zentrale und behördenübergreifende Plattform für die Cyberabwehr weiterzuentwickeln;

2. das mit der Cybersicherheitsstrategie 2011 eingerichtete Nationale Cyber-AZ weiter als maßgeblichen Akteur bei Cyberangriffen auszubauen und den Informationsaustausch aller an der IT-Sicherheit beteiligter Akteure, insbesondere auch mit Blick auf aktive Cyberabwehrmaßnahmen, auf dieser Plattform zu intensivieren;

3. das Cyber-AZ als zentrale Koordinationsplattform auszugestalten, auf der die behördenübergreifende Erst-Abstimmung von Cybervorfällen stattfindet; hier wird zuerst festgestellt, ob ein Vorfall einen staatlichen Hintergrund haben könnte oder nicht; bei der operativen Fallbearbeitung ist ein behördenübergreifendes Zusammenwirken von BSI, Polizeien, Nachrichtendiensten und der Bundeswehr unverzichtbar; die Behörden sollen sich, unter Wahrung der notwendigen Geheimhaltung, über das Ergreifen von Maßnahmen gegenseitig informieren; das Cyber-AZ ist der zentrale Ort für die Abklärung etwaiger operativer Betroffenheiten anderer Sicherheitsbehörden;

4. eine stärkere und schnellere Einbindung der Wirtschaft und der Länder für die Erstellung ganzheitlicher und sektoraler Lagebilder sicherzustellen; die Innenministerkonferenz hat 2024 das Konzept und die Voraussetzungen (u. a. zur sicheren technischen Anbindung) für die Einbindung der Länder in das Cyber-AZ beschlossen; die Umsetzung soll priorisiert werden;

5. das BSI im Rahmen der Weiterentwicklung der Cybersicherheitsstrategie als die zentrale Cybersicherheitsbehörde des Bundes weiter zu stärken; das Cyber-AZ soll auch zukünftig im BSI verortet sein; entscheidend für die Cybersicherheit ist – unter der Wahrung der notwendigen Geheimhaltung – ein einheitliches, ganzheitliches und unverstelltes IT-Lagebild – inklusive der aktuellen aktiven Cyberabwehrmaßnahmen; die Weiterentwicklung des Cyber-AZ in der anstehenden Cybersicherheitsstrategie soll ein solches gemeinsames ganzheitliches Lagebild sicherstellen; im Bereich der aktiven Cyberabwehr soll eine klare Rollen- und Aufgabenverteilung sichergestellt werden;

6. mit Blick auf den ressourceneffizienten Einsatz und insbesondere mit Blick auf die digitale Souveränität und den Abbau bestehender problematischer Abhängigkeiten die notwendigen technischen Mittel für eine wirksame Abwehr von Cyberangriffen zu entwickeln;