Regierungsentwurf zur Stärkung der Cybersicherheit

24.6.2026 - | Deutscher Bundestag

Liveübertragung: Donnerstag, 25. Juni, 9 Uhr.

In erster Lesung berät das Parlament am **Donnerstag, 25. Juni 2026,** den von der Bundesregierung angekündigten Gesetzentwurf „zur **Stärkung der Cybersicherheit**“ (21/6585(Dokument, öffnet ein neues Fenster)). Er soll nach 20-minütiger Debatte gemeinsam mit einem Antrag der Fraktion Die Linke „gegen die Einführung von Hackbacks“ (21/6653(Dokument, öffnet ein neues Fenster)) den Ausschüssen überwiesen werden. Federführend bei den weiteren Beratungen soll der Innenausschuss sein.

Gesetzentwurf der Bundesregierung

Die Regelung sieht mehr Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik, das Bundeskriminalamt sowie die Bundespolizei vor. Die Sicherheit und Handlungsfähigkeit von Staat, Wirtschaft und Gesellschaft in einem modernen, hoch technologisierten und digitalisierten Industrieland wie Deutschland beruhten in hohem Maße auf funktionierenden digitalen Prozessen und Infrastrukturen, schreibt die Regierung. Seit Jahren steige jedoch die Zahl von Cyberangriffen durch staatliche und nichtstaatliche Akteure.

Deutschland sei als führende Wirtschaftsnation in Europa verstärkt im Fokus hochprofessioneller Cyberangriffe mit großem Schadenspotenzial. Angesichts der geopolitischen Lage würden zudem auch hybride Bedrohungen zunehmend an Bedeutung gewinnen. „Dieser sicherheitspolitischen Herausforderung begegnet die Bundesregierung, indem sie die Erkennung und Abwehr von Cyberangriffen ausbaut und hierzu wirksame, angemessene und rechtssichere gesetzliche Grundlagen schafft“, heißt es.

Aufklärung und Erkennung konkreter Angriffe

Mit der Regelung soll die Aufklärung und die Erkennung konkreter Angriffe und langfristig laufender Angriffskampagnen verbessert werden. Zudem soll die Entdeckung konkreter Vorbereitungshandlungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgebaut werden.

Insbesondere gegen groß angelegte Cyberangriffe mit hohem Schadenspotenzial böten präventive Maßnahmen in den eigenen IT-Systemen allein keinen hinreichenden Schutz, schreibt die Bundesregierung. Es müssten daher für die Polizeien des Bundes und das BSI ergänzend Möglichkeiten zur Unterbindung solcher Cyberangriffe geschaffen werden, um gravierende Folgeschäden abwenden oder minimieren zu können.

Antrag der Linken

Gegen die Einführung von Hackbacks und offensiver Cyberabwehr„ wendet sich die Fraktion Die Linke in iihrem Antrag (21/6653(Dokument, öffnet ein neues Fenster)). Darin fordert die Fraktion die Bundesregierung auf, laufende Gesetzesvorhaben nicht weiter zu betreiben,
“die Hackbacks oder vergleichbare Maßnahmen der offensiven Cyberabwehr„ gesetzlich verankern

würden. Auch soll die Bundesregierung nach dem Willen der Fraktion keine Gesetzesvorhaben weiter betreiben, die dem Bundeskriminalamt (BKA) und der Bundespolizei ermöglichen, zur Abwehr von Cybergefahren ohne Wissen der Betroffenen in IT-Systeme einzudringen und diese auszulesen, zu verändern oder zu löschen.

Ebenso sollen dem Antrag zufolge von der Bundesregierung keine Gesetzesvorhaben weiter betrieben werden, "die DNS-Anbieter und Digitale Dienste zur Umleitung von Datenverkehr an das BKA und die Bundespolizei verpflichten könnten„. Dagegen soll die Bundesregierung laut Vorlage einen Gesetzentwurf vorlegen, der die defensive IT-Sicherheit mit den notwendigen Ressourcen insbesondere für das Bundesamt für Sicherheit in der Informationstechnik (BSI) stärkt.

"Verfassungsrechtliche Grenzen werden überschritten„

In dem Antrag schreibt die Fraktion, dass mit dem Koalitionsvertrag vom Mai 2025 ein Ausbau aktiver Cyberabwehr angekündigt worden sei. Mit dem Gesetzentwurf der Bundesregierung "zur Stärkung der Cybersicherheit„ (21/6585(Dokument, öffnet ein neues Fenster)) solle dieses Vorhaben umgesetzt werden, doch würden die Grenzen des "verfassungsrechtlich Möglichen„ dabei "klar überschritten„.

Mit dem Entwurf solle für BKA und Bundespolizei die Fähigkeit geschaffen werden, zur Abwehr von Cybergefahren Daten in IT-Systemen auszulesen, zu verändern und zu löschen, sowie Datenverkehr umzulenken und mitzulesen, führt die Fraktion weiter aus. Dies bedeute einen massiven Eingriff in informationstechnische Systeme, dem weder ein Richtervorbehalt noch ausreichende parlamentarische Kontrolle als grundrechtssichernde Mechanismen zur Seite gestellt würden. Auch ignoriere der Gesetzentwurf die Möglichkeit, dass Maßnahmen einer "aktiven Cyberabwehr„ auf Eingriffe in fremde staatliche IT-Infrastruktur hinauslaufen könnten. (hau/24.06.2026)

https://www.bundestag.de/dokumente/textarchiv/2026/kw26-de-cybersicherheit-1184344