Hickhack um Hackbacks?

Gesetzentwurf zur Stärkung der Cybersicherheit im Kabinett

28. Mai 2026

Am vergangenen Mittwoch, den 27. Mai 2026, hat die Bundesregierung den Entwurf für ein „Gesetz zur Stärkung der Cybersicherheit“ verabschiedet. Das Vorhaben enthält in erster Linie neue Befugnisse für die Sicherheitsbehörden des Bundes. Es umfasst aber auch Auswirkungen auf private Unternehmen, die im Zentrum dieses Briefings stehen sollen. Das Briefing bezieht sich auf den Stand des Referentenentwurfs aus dem Bundesministerium des Innern vom 24. Februar 2026.

Hintergrund

Vor dem Hintergrund wachsender Cyberangriffe auf private und öffentliche Einrichtungen soll mit dem Vorhaben die Zuständigkeitsverteilung bei der Cybersicherheit zwischen den Bundesbehörden weiterentwickelt werden. Die Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in den Bereichen der technischen Analyse, der Erstellung von Lagebildern sowie zur Unterstützung betroffener Einrichtungen sollen gestärkt werden.

Gleichzeitig sollen dem Bundeskriminalamt und der Bundespolizei erweiterte operative Befugnisse zur Abwehr schwerer Cyberangriffe eingeräumt werden. Dazu zählen vor allem Maßnahmen zur Steuerung oder Umleitung von Datenströmen sowie Eingriffe in informationstechnische Systeme.

Die Einführung von Befugnissen, mit denen Sicherheitsbehörden unter bestimmten Voraussetzungen in IT-Systeme eindringen können, um dort Daten zu löschen oder zu verändern („Hackback“), wäre ein neuer Ansatz in der bislang vor allem auf Abwehr- und Resilienz-Maßnahmen ausgerichteten deutschen Cybersicherheits-Architektur. Es ist davon auszugehen, dass dieser Teil des Vorhabens im weiteren Gesetzgebungsverfahren ausführlich beraten wird.

Auswirkungen auf private Unternehmen

Das von der Bundesregierung geplante Gesetz enthält verschiedene Auswirkungen auf private Unternehmen:

- Der Entwurf ermöglicht unter bestimmten Voraussetzungen Maßnahmen wie die Untersagung des Betriebs informationstechnischer Systeme, die Umleitung oder Unterbindung von Datenverkehr sowie Eingriffe in IT-Systeme zur Erhebung, Lö-

schung oder Veränderung von Daten. Je resilienter die Cybersicherheit eines Unternehmens ausgestaltet ist, umso weniger wahrscheinlich ist es, dass ein Unternehmen zum Adressaten dieser Maßnahmen wird. In diesem Zusammenhang ist die Einhaltung der Pflichten aus der deutschen Umsetzung der NIS-2-Richtlinie relevant.

- Die Anbieter digitaler Dienste sollen zur Bereitstellung sicherheitsrelevanter technischer Informationen gegenüber dem BSI verpflichtet werden.

- Der Entwurf sieht Maßnahmen zur Bekämpfung schädlicher Internet-Domains vor und erweitert die Befugnisse des BSI, insbesondere zur Änderung von Nameserver-Einträgen sowie zur Umleitung oder Unterbindung von Datenverkehr.

- Betreiber kritischer Anlagen sollen verpflichtet werden, Systeme zur Angriffserkennung einzusetzen und diese an das BSI anzubinden. Diese Systeme sollen fortlaufend relevante Betriebs- und Verfügbarkeitsdaten erfassen und automatisiert an das BSI übermitteln. In diesem Zusammenhang gewinnt die Umsetzung der Anforderungen des KRITIS-Dachgesetzes für betroffene Unternehmen an Bedeutung.

- Der Entwurf erweitert die Möglichkeiten des BSI zur technischen Unterstützung bei der Analyse von IT-Sicherheitsvorfällen. Auf Antrag betroffener Einrichtungen kann das BSI Maßnahmen durchführen, um Beeinträchtigungen aufzudecken, zu analysieren und die Sicherheit sowie Funktionsfähigkeit der Systeme wiederherzustellen.

- Der Entwurf sieht zudem Bußgeldvorschriften für Verstöße gegen Mitwirkungs- und Auskunftspflichten sowie gegen Offenbarungsverbote im Zusammenhang mit Cyberabwehrmaßnahmen vor.

Ausblick

Mit dem vorliegenden Gesetzentwurf soll die Regulierung der Cybersicherheit in Deutschland ergänzt werden. Melde- und Sorgfaltspflichten im Bereich der Cybersicherheit wurden erst kürzlich mit der deutschen Umsetzung der NIS-2-Richtlinie verschärft. Mit dem Inkrafttreten des KRITIS-Dachgesetzes werden die Betreiber kritischer Anlagen stärker reguliert. Unternehmen, die befürchten müssen, zum Ziel von Cyberangriffen zu werden, müssen künftig damit rechnen, dass die Behörde bei der Abwehr derartiger Angriffe eine größere Rolle spielen wollen – vorausgesetzt, das Gesetz zur Stärkung der Cyberabwehr wird durch den Gesetzgeber beschlossen.

***

BLOMSTEIN wird Sie über die weiteren Entwicklungen auf dem Laufenden halten. Bei Beratungsbedarf und anderen Fragen zum Thema Cybersicherheit stehen Ihnen Dr. Christopher Wolters, Konstantin Kuhle, Hanna Sophie Vetter sowie Dr. Moritz Schuchert und das gesamte Team jederzeit gerne zur Verfügung.

BLOMSTEIN | Wir beraten unsere internationalen Mandanten in den Gebieten Kartell-, Vergabe-, Außenwirtschafts- und Beihilferecht sowie ESG in Deutschland, Europa und – über unser globales Netzwerk – weltweit.