BDI

INNONATION

STELLUNGNAHME | DIGITALPOLITIK | CYBERSICHERHEIT

Gesetz zur Stärkung der Cybersicherheit

Stellungnahme der deutschen Industrie zum Entwurf des Bundesministeriums des Innern

17. März 2026

Executive Summary

Deutschland befindet sich täglich im Fadenkreuz international operierender, teils staatlich gelenkter Cyberkrimineller. Der BDI unterstützt daher das Ziel des Gesetzgebers, die Cybersicherheit in Deutschland weiter zu stärken und die staatliche Handlungsfähigkeit gegenüber zunehmend komplexen Bedrohungslagen auszubauen. Eine effiziente staatliche Cyberabwehr ist ein elementarer Bestandteil zur Wahrung von Cybersicherheit und damit der öffentlichen Sicherheit in der modernen Informations- und Kommunikationsgesellschaft. Ein verbesserter Informationsaustausch zu Cyberrisiken sowie erweiterte und effektive Reaktionsmechanismen sind hierfür essenziell. Entscheidend ist jedoch, dass neue Befugnisse und Pflichten klar eingeordnet, verhältnismäßig ausgestaltet und eng mit bestehenden Strukturen verzahnt werden. Es ist ein mehr als überfälliger Schritt, dass die Polizeien des Bundes und das BSI ergänzende Möglichkeiten zur Unterbindung von Cyberangriffen erhalten, um gravierende Folgeschäden abwenden oder minimieren zu können. Gleichsam ist eine Eskalationsspirale zwischen Staat und nationalen wie international agierenden Cyberkriminellen zu vermeiden.

Der BDI würde es begrüßen, wenn das Bundesministerium vor Verabschiedung des Gesetzentwurfs zur Stärkung der Cybersicherheit folgende Anpassungen am folgenden Entwurf vornehmen würde:

- **Weitreichende staatliche Kompetenzen und kooperativer Ansatz:** Die deutsche Industrie sieht die pro-aktiven, weitreichenden Befugnisse der Bundespolizei, des Bundeskriminalamts und des Bundesamts für Sicherheit in der Informationstechnik teils sehr kritisch. Cybersicherheit lässt sich nur im engen Schulterschluss zwischen Staat und Wirtschaft nachhaltig stärken. Der Gesetzentwurf sollte daher stärker auf kooperative Modelle setzen und bestehende erfolgreiche Ansätze explizit berücksichtigen. Wichtig ist, den bürokratischen Aufwand so gering als möglich zu halten und Doppelstrukturen zu vermeiden. Ein Kooperationsmodell kann zudem flexibler und schneller auf geänderte Bedrohungsszenarien reagieren. Zudem können bei einem kooperativen Ansatz einvernehmlich auf den konkreten Fall zugeschnittene Lösungen getroffen werden.
- **Zugriff auf Daten:** Da teils hochsensible Daten an staatliche Stellen übermittelt werden sollen, müssen zwingend die Einhaltung des Need-to-know-Prinzips und sichere Schnittstellen sowohl bei der Weitergabe an als auch innerhalb von Behörden gewährleistet werden.
- **Bußgeldrahmen und Fristen:** Während der BDI grundsätzlich Unterstützungspflichten für Wirtschaftsakteure bei staatliche Eingriffsrechten unterstützt und die in § 104 Absatz 1 genannten Ordnungswidrigkeitstatbestände als angemessen erachtet, sehen wir erheblichen Korrekturbedarf bei der Höhe des Bußgeldes bei Ordnungswidrigkeiten. Ferner muss der Gesetzgeber zwingend realistische Fristen einführen, denn eine technisch und rechtlich saubere Reaktion auf Sicherheitsvorfälle erfordert Zeit, Abstimmung und Validierung. Zudem erhöhen pauschale Pflichten das Risiko unbeabsichtigter Fehler oder ineffizienter Maßnahmen.

Steven Heckler | Senior Referent Cybersicherheit und Digitale Unternehmensidentitäten | s.heckler@bdi.eu | www.bdi.eu

Inhaltsverzeichnis

Die steigende Bedrohungslage aus dem Cyberraum: Betroffenheit der Industrie

Cybersicherheit ist entscheidend für den Erfolg digitaler Geschäftsmodelle, dem Vertrauen in die digitale Transformation zahlreicher Lebensbereiche und damit der digitalen Gesellschaft als Ganzes. Gleichzeitig ist ein stetiger Anstieg an kriminellen Handlungen im Cyberraum festzustellen, der von immer wirkungsmächtigeren DDoS-Angriffen, Botnetzen und weiteren Angriffsvektoren gekennzeichnet ist. Cyberkriminelle greifen heutzutage keineswegs ausschließlich staatliche Einrichtungen, Betreiber kritischer Infrastrukturen oder Einzelpersonen an. Vielmehr ist die deutsche Industrie tagtäglich sowohl direkt (in Werken, entlang der gesamten Lieferkette sowie über Angriffe auf ihre Mitarbeiterinnen und Mitarbeiter) als auch indirekt (über Angriffe auf die von ihr gefertigten Produkte) zigtausenden Angriffen durch Cyberkriminelle sowie staatliche Stellen aus aller Welt konfrontiert.

Drei Viertel der Unternehmen der deutschen Wirtschaft sind in den letzten zwei Jahren Opfer von Datendiebstahl, Spionage oder Sabotage geworden. Der Schaden für die deutsche Wirtschaft beläuft sich laut einer Bitkom-Studie für diesen Zeitraum auf fast 290 Milliarden Euro.[1] Digitale Angriffe verursachten bei sieben von zehn Unternehmen einen Schaden. Zudem registrierte allein die Deutsche Telekom AG im März 2026 mehr als 212 Millionen Cyberangriffe auf ihre Honeypots pro Tag.[2] Zum Vergleich: Im April 2017 verzeichnete die Telekom lediglich vier Millionen Angriffe pro Tag.

Die steigende Bedrohungslage aus dem Cyberraum spiegelt sich in der Beurteilung der bedeutendsten Geschäftsrisiken durch Unternehmen wider: Laut dem ALLIANZ RISK BAROMETER 2026 stufen Expertinnen und Experten in Unternehmen Cyberangriffe als bedeutendste Bedrohung für unternehmerisches Handeln in Deutschland ein.[3]

Angesichts der Quantität an bereits heute existierenden Schadprogrammen, der zunehmenden Kommerzialisierung von Cyberkriminalität sowie dem zu erwartenden Anstieg an vernetzbaren Produkten stellt sich die Frage, welche Kompetenzen ein wehrhafter Staat zukünftig im Cyberraum – im zivilen wie militärischen – bedarf, um die Sicherheit von Leib und Leben (engl. *safety*) sowie die Wahrung der öffentlichen Sicherheit (engl. *security*) gewährleisten zu können.

Während Cyberkriminelle global agieren, ist Deutschlands innenpolitische Antwort fragmentiert. Sechzehn Ordnungsrechte der Länder sowie zahlreiche Bundesgesetze bilden die rechtliche Grundlage für rechtsstaatliches Agieren im Cyberraum. Angesichts der stetig steigenden Bedrohungslage für Unternehmen, Bürger und den Staat als Ganzes, spricht sich der Bundesverband der Deutschen Industrie e.V. für die Einführung eines einheitlichen nationalen Ordnungsrahmens sowie für eine eng umgrenzte Stärkung von Bundeskompetenzen im Bereich der „aktiven Cyberabwehr“ aus.

[1] Bitkom. 2025. Wirtschaftsschutz 2025. URL: https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf
[2] Telekom AG. 2026. Sicherheitstacho. URL: https://www.sicherheitstacho.eu/#/de/tacho
[3] Allianz. 2026. Allianz Risk Barometer 2026: Cyber bleibt weltweit Top-Risiko, während KI-Risiken auf Platz 2 springen. URL: https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026/de.html#

Bewertung im Detail

Artikel 1: Änderung des Bundespolizeigesetzes

§ 41a Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik

Der Bundespolizei werden in § 41a Abs. 2 Nr. 1 – 3 sehr weitreichende Befugnisse zur Abwehr von Cyberattacken eingeräumt. Die deutsche Industrie sieht diese pro-aktiven, weitreichenden Befugnisse der Bundespolizei sehr kritisch. Es ist aus unserer Sicht nicht notwendig oder sinnvoll, dass die Bundespolizei selbstständig in die Netze der Telekommunikationsanbieter oder Anbieter von digitalen Diensten eingreift. Es würde eine Befugnis für die Bundespolizei ausreichen, bestimmte Maßnahmen, wie das Abschalten von Bot-Netzen oder die Umleitung von maliziösem Verkehr anzuordnen. Sollte das Bundesinnenministerium der Bundespolizei die vorgesehenen weitreichenden Befugnisse übertragen wollen, so ist zwingend sicherzustellen, dass Nutzende von Telekommunikationsinfrastrukturen keine Regressansprüche gegen die Anbieter von IKT-Diensten stellen können, wenn aufgrund einer Maßnahme der Bundespolizei Daten verloren gehen oder IKT-Dienste nicht verfügbar sind.

Im Hinblick auf die Maßnahmen unter § 41 a Abs. 2 Nr. 3 (Hackback) sehen wir keinen Fall, in dem ein Hackback auf Systeme des Angreifers oder Systeme Dritter, die vom Angreifer genutzt werden, ein angemessenes Abwehrmittel wäre. In der Regel ist die für den Angriff verwendete IP-Adresse bekannt, sodass der Zugriff auf die eigenen Systeme immer auch durch reines Blocken der IP-Adresse in den angegriffenen Systemen abgewehrt werden kann. Zudem ist nicht sichergestellt, dass bei Maßnahmen gegen die angreifenden Systeme auch die Systeme des Angreifers oder der Angreifer selbst erreicht werden.

Die Mitwirkungsverpflichtungen in Abs. 9 sind unkonkret. Die „unverzügliche Mitwirkungspflicht“ ist nicht hinreichend präzise beschrieben und schafft dadurch unnötige Unsicherheiten hinsichtlich Umfang und technischer Umsetzung der Verpflichtungen. Es ist zu klären, inwieweit es über die Erteilung von erforderlichen Auskünften hinaus geht. Eine Beteiligung privater Telekommunikationsanbieter und Anbieter digitaler Dienste erachten wir grundsätzlich als problematisch – insbesondere ein sogenannter Hackback darf ganz grundsätzlich kein Instrument der Privatwirtschaft oder von privaten Personen und Einrichtungen sein. Es kann sich vielmehr nur um eine Verteidigungsmaßnahme eines Staates im Rahmen seines Gewaltmonopols handeln. Allein aus diesem Grund lehnen wir Mitwirkungspflichten von Providern beim Hackback ab.

Ebenso sollten second-order-Effekte für Menschen sowie für die deutsche Industrie vorab bewertet und so weit als möglich vermieden werden. Aktive Gegenangriffe bergen grundsätzlich ein hohes Risiko, unbeteiligte Dritte zu treffen. Dies muss so weit als möglich reduziert werden. Mit Blick auf Industrieprozesse ist festzustellen, dass durch die zunehmende Vernetzung und die Verwendung von Cloud-Diensten in der Informationstechnik (IT) und der Betriebstechnik (Operational Technology = OT) starke Abhängigkeiten entstehen. Diese werden häufig nicht vollständig in der Nutzerkette verstanden. Werden diese Abhängigkeiten bei Hackbacks nicht vorab analysiert, drohen erhebliche Kollateralschäden. Jeglichem Hackback sollte eine detaillierte Bewertung dieser second-order-Effekte vorausgehen. Daher bedarf es des Aufbaus von Fähigkeiten zur Evaluierung und Vermeidung etwaiger Sekundäreffekte bei den mit staatlichen Gegenmaßnahmen im Cyberraum betrauten Stellen.

Da Cyberkriminelle auf Gegenmaßnahmen aus Deutschland mit erneuten Gegenmaßnahmen reagieren können, gilt es zu prüfen, ob potenziell von etwaigen neuerlichen Gegenmaßnahmen Dritter betroffene Unternehmen frühzeitig gewarnt werden könnten. Die deutsche Industrie sollte befähigt werden, notwendige Schutzmaßnahmen treffen zu können. Es gilt, eine Eskalationsspierale im Cyberraum unbedingt zu vermeiden.

§ 104

Während der BDI grundsätzlich Unterstützungspflichten für Wirtschaftsakteure bei staatlichen Eingriffsrechten unterstützt und die in § 104 Absatz 1 genannten Ordnungswidrigkeitstatbestände als angemessen erachtet, sehen wir erheblichen Korrekturbedarf bei der Höhe des Bußgeldes bei Ordnungswidrigkeiten.

Artikel 2: Änderung des BSI-Gesetzes

§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

Die deutsche Industrie unterstützt ausdrücklich, dass das BSI bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines IT- Systems einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung oder bei Vorliegen von Anhaltspunkten für eine solche Beeinträchtigung in herausgehobenen Fällen auf Ersuchen der betroffenen Einrichtung oder des betroffenen Betreibers Maßnahmen treffen darf, die zur Suche und Identifikation der Beeinträchtigung der Sicherheit und Funktionsfähigkeit ihrer IT-Systeme oder zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen IT-Systems erforderlich sind. Wir begrüßen ausdrücklich, dass das BSI für erste Maßnahmen, die zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergriffen werden, keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhebt.

§ 15 Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit

Die deutsche Industrie erachtet die Verpflichtungen an Telekommunikationsanbieter und Digitale-Dienste-Anbieter zur Herausgabe sehr umfassender Datensätze nach Aufforderung des BSI als zu weitgehend und einseitig. Die deutsche Industrie würde ein Kooperationsmodell zum Austausch von relevanten Daten zum gegenseitigen Nutzen zielführender und erfolgversprechender als eine einseitige Pflicht zur Herausgabe von hochsensiblen Daten ansehen. Da hochsensible Daten abgefragt werden, muss sichergestellt sein, dass nur jene Stellen, die die Informationen unbedingt im Rahmen der Cyberabwehr benötigen, darauf zugreifen können und zudem der Datenaustausch über sichere technische Schnittstellen erfolgt. Eine Datenherausgabe an das BSI darf nur unter Beachtung der Vorgaben der DSGVO erfolgen, insbesondere nur für festgelegte, eindeutige und legitime Zwecke. Eine einfache Lagebeurteilung ist hierfür nicht ausreichend. Auch eine Weitergabe der gewonnenen Erkenntnisse innerhalb der Behörde oder weitere Behörden darf nur über gesicherte Kanäle erfolgen und unter Wahrung der Vertraulichkeit. Der Grundsatz der Datenminimierung (Notwendigkeit der übermittelnden Daten für den verfolgten Zweck) ist zu beachten. Die betreffenden Daten werden unter Einsatz von großem zeitlichem und wirtschaftlichem Aufwand gewonnen. Um das Geschäftsmodell von Cybersicherheitsunternehmen nicht zu konterkarieren ist es unerlässlich, eine angemessene Vergütung für die Zurverfügungstellung der Daten zu vorzusehen.

§ 16 Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten

Die deutsche Industrie unterstützt den Vorstoß, dass DNS-Diensteanbieter nach § 2 Nr. 8a DNS-basierten Schutz anbieten sollen. Entgegen dem Entwurf sollte der DNS-basierte Schutz zugleich auf vom BSI veröffentlichten Informationen sowie denen eigenen Erkenntnissen der Unternehmen beruhen. Ferner sollte statt „Sicherheitsrisiken für Informationstechnik“ der Gesetzgeber besser allgemein von „Sicherheitsrisiken“ sprechen, da beispielsweise Phishing-Websites nicht primär ein Sicherheitsrisiko für IT darstellen, sondern vielmehr für Identitätsdaten und mittelbar für Vermögen von Betroffenen. Der DNS-basierte Schutz sollte deshalb eine Standardeinstellung sein, die die Kunden auf Wunsch verlassen können. Die Formulierung sollte nicht als „Opt-In“, sondern „Opt-Out“ ausgestaltet werden. Alles andere führt zu unnötigem bürokratischem Mehraufwand.

§ 16a Anordnungen des Bundesamtes gegenüber Top Level Domain Name Registries und Registraren

Die in § 16a vorgesehene bloße Unterrichtung der BfDI reicht nicht aus. Besonders kritisch ist zudem, dass Widerspruch und Anfechtungsklage gegen entsprechende Anordnungen keine aufschiebende Wirkung entfalten sollen. Vergleichbare Eingriffe in die Domain-Infrastruktur wurden von der Rechtsprechung bereits kritisch bewertet.

§ 17 Absatz 2

Die deutsche Industrie sieht die Änderungen in § 17, die es dem BSI erlaubt, Datenverkehr umzuleiten oder zu blockieren, kritisch. Diese werfen aus unserer Sicht grundlegende Governance- und Aufsichtsfragen auf. Solche Eingriffe können erhebliche Auswirkungen auf die Integrität von Diensten, auf Kundenvertrauen sowie auf internationale Datenflüsse haben. Daher ist es zwingend nötig, Eingriffsbefugnisse klar zu begrenzen, transparent ausgestalten und an hohe rechtliche und fachliche Hürden zu knüpfen. Ferner müssen robuste Kontroll- und Aufsichtsmechanismen vorgesehen und der Grundsatz der staatlichen Zurückhaltung gewahrt werden.

§ 31 Absatz 2

Der derzeitige Wortlaut des vorgeschlagenen § 31 Abs. 2 sieht vor, dass Angriffserkennungssysteme die Betriebsparameter und Verfügbarkeitsindikatoren der kritischen Anlage kontinuierlich und automatisch erfassen und auswerten sowie an das BSI übermitteln müssen, sofern das Bundesamt nicht auf diese Anforderung verzichtet. Dies würde bedeuten, dass jede kritische Anlage, wie beispielsweise Kraftwerke und deren Leitsysteme, technisch in der Lage sein muss, eine permanente Verbindung zum BSI herzustellen. Dies ist problematisch, da die Herstellung einer permanenten Verbindung naturgemäß die Angriffsfläche vergrößert und einen zusätzlichen Ausfallpunkt schafft. Außerdem würde das BSI dadurch zu einem zentralen Sammelpunkt für hochsensible Betriebsdaten, darunter beispielsweise kerntechnische Informationen, werden. Ein Angriff auf die zentrale Behörde würde daher das Risiko bergen, dass sensible Informationen aus allen angeschlossenen Anlagen offengelegt werden. Die entsprechende Vorgabe sollte gestrichen werden.

Artikel 3: Änderung des Bundeskriminalamtgesetzes

Da die dem Bundeskriminalamt (BKA) eingeräumten Eingriffsbefugnisse im Wesentlichen denen der Bundespolizei entsprechen – nur dass sich die Zuständigkeitsbereiche unterscheiden – gelten mit Blick auf §§ 62 b bis e im Allgemeinen unsere Kommentierungen zu Artikel 1.

§ 62c Untersagung des Betriebs informationstechnischer Systeme

Der BDI unterstützt grundsätzlich die Möglichkeit, dass das Bundeskriminalamt (BKA) zur Abwehr einer Gefahr nach § 62b Absatz 1 den Betrieb eines IT-Systems untersagen darf. Dabei ist zwingend der Grundsatz der Verhältnismäßigkeit zu wahren. Ferner müssen die Betreiber des entsprechenden IT-Systems informiert werden, insbesondere wenn es sich dabei um Betreiber öffentlicher Telekommunikationsnetze handelt.

§ 62e Erheben, Löschen und Verändern von Daten in informationstechnischen Systemen

Es ist zwingend sicherzustellen, dass die Auswirkungen auf Dritte, die durch das Erheben, Löschen und Verändern von Daten in informationstechnischen Systemen entstehen, auf ein Mindestmaß begrenzt werden.

Um Gefahren für die Allgemeinheit sowie kritische Infrastrukturen zu minimieren, kann das Erheben, Löschen und Verändern von Daten in informationstechnischen Systemen notwendig sein. Die Bundesregierung muss jedoch zwingend sicherstellen, dass durch eine vom BKA durchgeführte

Maßnahme keine Haftungsansprüche gegenüber Herstellern von Produkten oder Betreibern von Dienstleistungen entstehen.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29
10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU-Transparenzregister: 1771817758-48

Lobbyregister: R000534

Autor
Steven Heckler
Senior Referent Cybersicherheit und Digitale Unternehmensidentitäten
T: +49 30 2028-1523
s.heckler@bdi.eu

BDI-Dokumentennummer: D 2249