

Stellungnahme

März 2026

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

Zusammenfassung

Das Bundeskabinett hat am 27. August 2025 drei Eckpunkte zur Erhöhung der Cybersicherheit beschlossen. Der Referentenentwurf eines Gesetzes zur Stärkung der Cybersicherheit adressiert eine erste Säule der vorgesehenen Maßnahmen. Bitkom erkennt die Notwendigkeit an, die Cybersicherheit zu erhöhen und die Fähigkeiten des Staates im Cyberraum weiterzuentwickeln. Seit Jahren nehmen Cyberangriffen zu; allein im vergangenen Jahr entstand der deutschen Wirtschaft ein Schaden von 202,4 Milliarden Euro

Der Gesetzentwurf wird seinem eigenen Anspruch nur dann gerecht, wenn neue Befugnisse mit klaren Zuständigkeiten, ausreichenden Ressourcen und einer widerspruchsfreien Aufgabenverteilung einhergehen. Der im Entwurf vorgesehene Personalaufwuchs bei Bundespolizei, BSI und BKA adressiert zwar bestehende Ressourcendefizite, lässt aber offen, ob er für die neuen Aufgaben und Befugnisse ausreicht. Zugleich wirft der Entwurf Fragen der Aufgabenverteilung auf, insbesondere mit Blick auf die vorgesehene Bündelung neuer Fähigkeiten bei der Bundespolizei und beim BKA. Der Gesetzgeber sollte daher zusätzliche Zuständigkeiten kritisch prüfen und vorhandene Ressourcen im Sinne eindeutiger behördlicher Zuständigkeiten effizienter ordnen. Auch Synergien mit anderen Ressorts im Nationalen Sicherheitsrat, insbesondere dem Bundesministerium der Verteidigung (BMVg), sollten geprüft werden. Auch hier wird das Ziel des vorliegenden Gesetzesentwurfs verfolgt, sodass die Zuständigkeiten und Aufgabenteilung zwischen diesen beiden geklärt werden sollten, um Bürokratie und Ausgaben zu reduzieren.

Wirksame Cybersicherheit sollte vor allem über Kooperation, Prävention und resiliente Strukturen erreicht werden. Bewährte Ansätze wie koordinierte Schwachstellenmeldungen, strukturierte Threat-Intelligence-Programme und etablierte Formate des vertrauensvollen Austauschs zwischen Unternehmen und Sicherheitsbehörden sollten systematisch eingebunden und weiterentwickelt werden. Kooperative Modelle haben gegenüber starren gesetzlichen Verpflichtungen den Vorteil, dass sie schneller und zielgenauer auf wechselnde Angriffsszenarien reagieren können. Die Erfahrungen der vergangenen Jahre zeigen, dass hoheitliche Anordnungen

häufig bürokratische Prozesse auf beiden Seiten auslösen, ohne inhaltlich stets die wirksamste Antwort auf konkrete Gefährdungslagen zu sein. Zugleich sollte der Fokus stärker auf präventiven Sicherheitsmaßnahmen liegen, insbesondere entlang der digitalen Lieferkette. Eine solche Ausrichtung stärkt die Resilienz und kann dazu beitragen, tiefgreifende staatliche Eingriffe auf unvermeidbare Ausnahmesituationen zu begrenzen. Soweit der Entwurf dennoch weitreichende Eingriffsbefugnisse vorsieht, müssen diese verhältnismäßig, sicher ausgestaltet und praktisch umsetzbar sein. Für die Digitalwirtschaft gehen damit erhebliche Mitwirkungs- und Auskunftspflichten einher, die Fragen der digitalen Souveränität, der Datenhoheit und der technischen Sicherheit staatlicher Zugriffe aufwerfen. Andernfalls besteht das Risiko, das Versprechen digitaler Souveränität und den Schutz vor unverhältnismäßigen staatlichen Zugriffen zu beeinträchtigen, die einen Grundpfeiler der Demokratie in Deutschland und Europa bilden.

Der Entwurf unterschätzt die praktischen und finanziellen Folgen für die betroffenen Unternehmen erheblich. Insbesondere sichere Schnittstellen und zusätzlicher Personalaufwand können erhebliche Kosten verursachen, sodass angemessene Aufwandsentschädigungen vorgesehen werden müssen. Darüber hinaus bleibt unberücksichtigt, dass Unternehmen erhebliche Investitionen in die Cyberabwehr tätigen und die aus der Datenanalyse gewonnenen Erkenntnisse auch Kunden zur Verfügung stellen. Neben einer Entschädigung müssen deshalb auch diese Leistungen vergütet werden.

Viele der vorgesehenen Verpflichtungen, gehen über bestehende europäische Mindestanforderungen hinaus und führen zu weiterem Gold-Plating. Nach dem Entwurf trifft dies insbesondere auf die neuen Anforderungen an TLD Name Registries und Registrare zu, die im kürzlich beschlossenen NIS2-Umsetzungsgesetz geregelt wurden. Die Digitalwirtschaft unterstützt die Handlungsfähigkeit des Staates im Cyberraum; dies darf jedoch nicht zu zusätzlicher Bürokratie und Nachteilen für Wettbewerb, Resilienz und den Innovationsstandort Deutschland insgesamt führen. Unternehmen sind bereits mit einer Vielzahl von Umsetzungsanforderungen konfrontiert, sodass sich zusätzliche nationale Sonderwege nachteilig auswirken würden, insbesondere wenn man im europäischen Ausland aktiv ist. In diesem Zusammenhang ist auch die vorgesehene Sanktionshöhe besonders kritisch zu bewerten: Verstöße gegen Anordnungen nach dem BKA-Gesetz oder gegen Mitwirkungspflichten nach dem Bundespolizeigesetz sollen künftig mit Geldbußen bis zu 20 Millionen Euro geahndet werden können. Doch hohe Strafen allein führen nicht zu mehr Cybersicherheit. Der Bußgeldrahmen sollte im Vergleich zu bestehenden deutschen und europäischen Sanktionssystemen sorgfältig eingeordnet werden, um eine verhältnismäßige Ausgestaltung sicherzustellen. Die vorgesehenen Bußgelder sind daher auf 10 Millionen Euro zu deckeln.

Die im Entwurf vorgesehenen „unverzüglichen“ Fristen stehen in einem Spannungsverhältnis zu den tatsächlichen Anforderungen einer sicheren technischen Umsetzung. Angesichts des teilweise erheblichen Einschätzungsdefizits hinsichtlich der Folgen hoheitlichen Handelns in hochkomplexen informationstechnischen Systemen besteht die erhebliche Gefahr, dass das Kriterium der Unverzüglichkeit zu Umsetzungsfehlern sowie zu Beeinträchtigungen der Verfügbarkeit und Integrität von Systemen führt und hierdurch wirtschaftliche Schäden auf Seiten der Unternehmen

verursacht. Dies gilt in besonderem Maße für Netzinfrastrukturen: Zugriffe auf aktive Netzkomponenten oder zentrale Steuerungssysteme können weitreichende Auswirkungen auf Verfügbarkeit, Stabilität und Sicherheit ganzer Netzsegmente entfalten. Eine technisch und rechtlich belastbare Reaktion auf Sicherheitsvorfälle erfordert daher Zeit für sorgfältige Prüfung, Abstimmung und Validierung. Realistische, risikobasierte Zeitvorgaben dienen dem Ziel der Sicherheit besser als formale Geschwindigkeit.

Wo der Staat tief in technische Systeme und betriebliche Abläufe eingreift, muss die Wirkung dieser Eingriffe systematisch überprüft werden. Daher sollte der Entwurf auch eine Evaluierung vorsehen. Angesichts der weitreichenden Befugnisse und Pflichten müssen Auswirkungen und Vollzugserfahrungen systematisch überprüft werden. Dabei sollten neben rechtlichen auch praktischen Effekten auf Sicherheitsvorfälle, Wiederherstellungszeiten, Kooperationsprozesse und betriebliche Resilienz erfasst werden.

Artikel 1: Bundespolizeigesetz (BPolG)

§ 41a BPolG-E

Der vorgeschlagene § 41a BPolG-E wirft in seiner konkreten Ausgestaltung erhebliche rechtliche und praktische Fragen auf. Dies betrifft insbesondere die Systematik der Eingriffsbefugnisse, die technische Umsetzbarkeit einzelner Maßnahmen, die Einbindung von Telekommunikations- und Digitaldiensteanbietern sowie Transparenz der Eingriffe gegenüber Betroffenen.

Zunächst überzeugt die im Entwurf vorgesehene Unterscheidung zwischen privaten und nicht-privaten informationstechnischen Systemen (§ 41a Abs. 5 BPolG-E) nicht. Moderne IT-Infrastrukturen sind in der Praxis häufig durch Mischnutzung geprägt, etwa wenn berufliche und private Anwendungen auf denselben Geräten oder Plattformen stattfinden. Die gesetzliche Differenzierung wird diesen Realitäten nicht ausreichend gerecht und lässt insbesondere offen, wie mit Daten umzugehen ist, die einen Unternehmensbezug haben, ohne dass das betroffene System eindeutig als „nicht privat“ einzuordnen ist. Dadurch entstehen potenzielle Schutzlücken und erhebliche Rechtsunsicherheiten für Unternehmen und Nutzer.

Darüber hinaus räumt § 41a Abs. 2 BPolG-E der Bundespolizei sehr weitreichende operative Befugnisse ein. Diese reichen von der Untersagung des Betriebs informationstechnischer Systeme über die Umleitung oder Unterbindung von Datenverkehr bis hin zu aktiven Eingriffen in informationstechnische Systeme durch das Löschen oder Verändern von Daten. Aus Sicht der digitalen Wirtschaft erscheint es nicht erforderlich, der Bundespolizei eigenständige Eingriffe in Netzinfrastrukturen von Telekommunikations- oder digitalen Diensteanbietern zu ermöglichen. Zweckmäßiger wäre es, der Bundespolizei lediglich die Befugnis einzuräumen, erforderliche Maßnahmen, etwa die Abschaltung von Botnetzen oder die Umleitung schädlichen Datenverkehrs, gegenüber den jeweiligen Betreibern anzuordnen, allerdings nur auf Grundlage eines Gerichtsbeschlusses.

Problematisch sind die in § 41a Abs. 2 Nr. 3 BPolG-E vorgesehenen Maßnahmen, die faktisch sogenannte Hackbacks ermöglichen. Aktive Gegenmaßnahmen im Cyberraum sind mit erheblichen Risiken verbunden. Aufgrund der häufig unsicheren Attribution besteht die Gefahr, dass Maßnahmen nicht die tatsächlichen Angreifer, sondern kompromittierte Systeme unbeteiligter Dritter treffen. Vor diesem Hintergrund ist es aus Datenschutz- und Grundrechtsperspektive nicht mit deutschen und europäischen Grundrechten vereinbar, wenn eine Information der Betroffenen dauerhaft unterbleibt. Vielmehr sollten jedenfalls Höchstfristen vorgesehen werden, nach deren Ablauf die Betroffenen von den Maßnahmen Kenntnis erlangen müssen, um ihre Rechte geltend zu machen oder auf die Maßnahme zu reagieren. Insbesondere dann, wenn auch Unbeteiligte von den Eingriffen betroffen waren. Hinzu kommt, dass zweifelhaft ist, ob solche Eingriffe überhaupt geeignet sind, laufende Angriffe effektiv zu unterbinden, da diese regelmäßig über verteilte und kurzfristig wechselnde Infrastrukturen erfolgen und sich in vielen Fällen bereits durch defensive Maßnahmen, etwa das Blockieren schädlicher Verbindungen, wirksam begrenzen lassen. Besonders problematisch ist schließlich auch, dass ein Rollback informationstechnischer Datenveränderungen nur verpflichtend sein soll, „soweit dies technisch möglich“ ist.

Schließlich wirft auch die in § 41a Abs. 9 BPolG-E vorgesehene Mitwirkungspflicht für Telekommunikationsanbieter und Anbieter digitaler Dienste Fragen auf. Der Begriff der „unverzöglichen Mitwirkung“ bleibt unklar und schafft erhebliche Unsicherheiten hinsichtlich Umfangs und technischer Umsetzung der Verpflichtungen. Insbesondere eine Beteiligung privater Anbieter an aktiven Gegenmaßnahmen im Cyberraum erscheint problematisch. Solche Maßnahmen können nur im Rahmen staatlicher Verantwortung und unter klar definierten rechtlichen Grenzen erfolgen. Daher sollten Mitwirkungspflichten präzise gefasst und auf klar begrenzte, technisch umsetzbare Unterstützungsleistungen beschränkt werden.

Im Rahmen der Änderungen des BPolG-E sind außerdem Regelungen problematisch, die das Verhältnis zwischen staatlichen Eingriffsbefugnissen und Transparenz gegenüber Betroffenen zulasten der Nachvollziehbarkeit verschieben. So soll die Bundespolizei nach § 41a Absatz 10 BPolG-E gegenüber Betreibern informationstechnischer Systeme oder verpflichteten Anbieter digitaler Dienste anordnen können, Kundinnen und Kunden nicht zu informieren, etwa wenn ein IT-System abgeschaltet oder Datenverkehr gesperrt wird. Zur Begründung wird angeführt, dass andernfalls Maßnahmen der Gefahrenabwehr oder Strafverfolgung behindert werden könnten. Aus Sicht des Bitkom ist bei derartigen Informationsverboten jedoch besondere Zurückhaltung geboten, da sie die Möglichkeit der Betroffenen einschränken, Auswirkungen auf die eigene IT-Sicherheit rechtzeitig zu erkennen und angemessen darauf zu reagieren, und zugleich die Transparenz staatlichen Handelns weiter reduziert. Maßnahmen wie Systemabschaltungen, Datenverkehrsumleitungen oder technische Eingriffe ohne Kenntnis der Betroffenen können unbeabsichtigte Folgewirkungen haben, etwa den Verlust forensischer Informationen, die Unterbrechung kritischer Geschäftsprozesse oder die Erschwerung von Wiederherstellungsmaßnahmen. Darüber hinaus bergen verdeckte oder kurzfristige Eingriffe in laufende informationstechnische Systeme erhebliche Risiken für die Betriebssicherheit und die wirksame Bewältigung von IT Sicherheitsvorfällen.

Artikel 2: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Das BSIG-E sieht eine Ausweitung der Durchsetzungsbefugnisse des BSI vor, unter anderem zur Überprüfung der Nutzung von Angriffserkennungssystemen und die Ausleitung der gesammelten Daten an das BSI durch Betreiber kritischer Anlagen. Derartige Vorgaben stellen faktisch eine Form des „Gold-Plating“ dar und weichen vom harmonisierten Regulierungsansatz der Europäischen Union ab. Aus Sicht der digitalen Wirtschaft sollte stattdessen die Anerkennung international etablierter Sicherheitsstandards (z.B. ISO/IEC 27001) stärker in den Mittelpunkt gestellt werden. Mit Blick auf den Netzbetrieb muss außerdem eindeutig sein, dass die Verantwortung für die Netzsicherheit bei den Betreibern und nicht beim BSI liegt. Maßnahmen des BSI sollten daher kooperativ, verhältnismäßig und klar abgegrenzt ausgestaltet sein, ohne sensible Informationen offenzulegen oder faktisch neue technische Standards zu setzen. Bestehende Ressourcen könnten so wirksamer für konkrete Maßnahmen zur Stärkung der IT-Sicherheit eingesetzt werden.

§11 BSIG-E

Die in § 11 BSIG-E vorgesehene Stärkung der operativen Unterstützungsfähigkeit des BSI ist zu begrüßen. Der Entwurf ermöglicht den Einsatz von Mobile Incident Response Teams (MIRTs) bereits bei einem Verdacht und schafft damit die Voraussetzung, dass das BSI auf Ersuchen der betroffenen Einrichtung frühzeitig tätig werden kann. Bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems sollen Maßnahmen zur Suche und Identifikation der Beeinträchtigung sowie zur Wiederherstellung der Sicherheit beziehungsweise Funktionsfähigkeit ergriffen werden können. Ebenfalls positiv ist, dass der Entwurf vorsieht, für erste Maßnahmen zur Schadensbegrenzung und zur Sicherstellung des Notbetriebes vor Ort keine Gebühren oder Auslagen zu erheben. Dadurch werden finanzielle Hürden für eine schnelle Einbindung des BSI reduziert und die Wahrscheinlichkeit erhöht, dass Unterstützung im Krisenfall ohne Verzögerung abgerufen wird.

§15 BSIG-E

Mit § 15 Abs. 6 BSIG-E werden Anbieter öffentlich zugänglicher Telekommunikationsdienste sowie Anbieter digitaler Dienste verpflichtet, auf Anforderung sicherheitsrelevante technische Informationen an das BSI zu übermitteln. Ausweislich der Gesetzesbegründung können darunter auch Verkehrs- und Steuerungsdaten sowie technische Informationen fallen, die Unternehmen im Rahmen eigener Verkehrsanalyse- und Sicherheitsmaßnahmen auswerten, etwa auf Grundlage von § 12 Abs. 1 und § 19 Abs. 4 TDDDG sowie § 165 Abs. 2 TKG. Eine solche Datenübermittlung kann grundsätzlich zur Erstellung eines umfassenderen Lagebilds beitragen.

Das Ziel, relevante technische Erkenntnisse über Bedrohungen und Angriffsaktivitäten für die Erstellung des nationalen Cyberlagebilds stärker zu bündeln, wird unterstützt.

Gleichzeitig sprechen wir uns gegen eine breite Verpflichtung zur Bereitstellung „sicherheitsrelevanter technischer Informationen“ aus, die im Konflikt mit bestehenden Geschäftsmodellen, insbesondere im Bereich der Bedrohungserkennung und Cybersicherheitsanalyse, stehen könnte.

Sollte der verpflichtende Ansatz beibehalten werden, ist zu berücksichtigen, dass die Erhebung und Aufbereitung der betreffenden Daten teilweise mit erheblichem technischem und personellem Aufwand verbunden ist. Daher sollten für die Bereitstellung von Informationen angemessene Vergütungsregelungen vorgesehen werden kann.

Zudem wäre bei Einführung einer solchen Verpflichtung eine klare gesetzliche Eingrenzung sowohl der Datenkategorien als auch der Auslösungstatbestände erforderlich. Eine bloße Lagebeurteilung reicht hierfür nicht aus; vielmehr braucht es transparente, gegebenenfalls nach Schwere des erwarteten Angriffs abgestufte Schwellenwerte. Zugleich muss gesetzlich klargestellt werden, dass die Datenverarbeitung strikt zweckgebunden erfolgt und unter Beachtung des Grundsatzes der Datenminimierung auf die für die gesetzlichen Aufgaben des BSI tatsächlich erforderlichen Informationen beschränkt bleibt. Dies gilt besonders für personenbezogene und sonstige hochsensible technische Daten. Soweit personenbezogene Daten betroffen sind, müssen die bestehenden spezialgesetzlichen Verfahren Anwendung finden; eine Herausgabe darf nur im Wege der Bestandsdatenauskunft nach § 12 BStG nach Maßgabe des § 174 TKG und der hierzu entwickelten verfassungsrechtlichen Anforderungen erfolgen. Zudem ist gesetzlich eindeutig festzulegen, welche Personen und Behörden Zugriff auf diese Daten erhalten dürfen, damit personenbezogene und hochsensible Informationen nicht an Unberechtigte gelangen. Eine derart präzise Ausgestaltung schafft Rechtssicherheit für Unternehmen und verbessert zugleich die Belastbarkeit des nationalen Cyberlagebilds.

Des Weiteren besteht aus Sicht der Praxis Präzisierungsbedarf hinsichtlich der parallel verwendeten Begriffe „Schwachstellen“, „Verwundbarkeiten“ und „Sicherheitslücken“, um Auslegungsunsicherheiten zu vermeiden. Zudem sollte sichergestellt werden, dass neue Pflichten kohärent mit bestehenden Regelungen zur Informationsweitergabe und Incident Response ausgestaltet sind und Doppelmeldungen vermieden werden.

Neben der vorgesehenen Bereitstellungspflicht sollte der Informationsaustausch zudem systematisch als bidirektionaler Austausch ausgestaltet werden. Unternehmen investieren bereits erhebliche Ressourcen in die Analyse von Angriffsmustern und technischen Indikatoren. Für eine wirksame Cyberabwehr ist es daher zentral, dass sicherheitsrelevante Erkenntnisse nicht nur an staatliche Stellen übermittelt werden, sondern dass auch vom BSI gewonnene Erkenntnisse und Lageinformationen strukturiert an betroffene Unternehmen zurückgespielt werden. Ein solcher Ansatz würde sowohl die Qualität des Lagebilds als auch die operative Cyberresilienz der beteiligten Akteure stärken.

§16 & 16a BSIG-E

Die vorgesehenen Änderungen in § 16 BSIG-E sowie die Einführung von § 16a BSIG-E erweitern die Eingriffsbefugnisse des Bundesamtes im Bereich der Domain-Infrastruktur erheblich. Insbesondere die Möglichkeit, gegenüber Top Level Domain Name Registries und Domain-Name-Registry-Dienstleistern Änderungen an Nameservereinträgen anzuordnen, stellt einen tiefgreifenden Eingriff in die technische Funktionsweise der Domain-Infrastruktur dar. Solche Maßnahmen können erhebliche Auswirkungen auf Dienste, Kundenvertrauen und internationale Datenflüsse haben und sollten daher nur unter klar definierten rechtlichen Voraussetzungen erfolgen.

Zudem gehen die vorgesehenen Befugnisse über die Anforderungen des europäischen Rechtsrahmens, insbesondere im Kontext der NIS-2-Umsetzung, hinaus. Für international tätige Anbieter entstünden zusätzliche nationale Compliance-Pflichten, die eigene Prozesse und Ressourcen erfordern würden.

Auch aus rechtsstaatlicher Perspektive wirft die Regelung Fragen auf. Staatliche Eingriffe in die Domain-Infrastruktur müssen wirksamer gerichtlicher und unabhängiger aufsichtsrechtlicher Kontrolle unterliegen, um exekutive Überdehnungen zu verhindern. Vor diesem Hintergrund reicht die in § 16a BSIG-E vorgesehene bloße Unterrichtung der BfDI nicht aus. Gerade bei grundrechtsrelevanten Maßnahmen muss die datenschutzrechtliche Kontrolle institutionell wirksam abgesichert sein. 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. So hat das Verwaltungsgericht Frankfurt am Main eine von der BaFin angeordnete DNS-Sperre wegen fehlender gesetzlicher Grundlage als rechtswidrig aufgehoben (VG Frankfurt am Main, Urteil der 7. Kammer vom 17. Januar 2024, Az. 7 K 407/22.F). Dies verdeutlicht die hohen rechtlichen Anforderungen an derartige Eingriffsbefugnisse.

Mit Blick auf § 16 Absatz 6 BSIG-E ist zudem sicherzustellen, dass DNS-Diensteanbieter bei der Umsetzung eines DNS-basierten Schutzes nicht ausschließlich auf vom Bundesamt veröffentlichte Informationen angewiesen sind, sondern auch eigene Erkenntnisse und bestehende Sicherheitsmechanismen einbeziehen können. Darüber hinaus erscheint der Begriff „Sicherheitsrisiken für die Informationstechnik“ zu eng gefasst. Viele missbräuchliche Domains, etwa im Zusammenhang mit Phishing oder betrügerischen Online-Angeboten, zielen nicht unmittelbar auf informationstechnische Systeme, sondern auf Identitätsdiebstahl oder Vermögensschäden. Eine klarere und breitere Definition, etwa durch den Begriff „malizöse Domains“, könnte hier zu einer praxisgerechteren Ausgestaltung beitragen. Das BSI sollte zudem ausreichende Ressourcen einplanen, da für die korrekte Klassifizierung als Phishing häufig eine manuelle Überprüfung erforderlich ist.

§17 BSIG-E

Die in § 17 BSIG-E vorgesehenen Befugnisse des BSI, den Datenverkehr zu bestimmten Domains oder Anschlusskennungen umzuleiten oder zu blockieren, stellen einen besonders weitreichenden Eingriff in die technische Funktionsweise des Internets dar.

Positiv hervorzuheben ist, dass der Entwurf mit DNS-Blocklisten erstmals eine klare gesetzliche Grundlage schafft, auf die sich Betreiber von DNS-Resolvern bei entsprechenden Maßnahmen berufen können. Dies kann zur Rechtssicherheit beitragen, wenn Anbieter freiwillig Maßnahmen zur Eindämmung von Schadverkehr umsetzen.

Maßnahmen dieser Art können jedoch erhebliche Auswirkungen auf die Integrität von Diensten, auf Kundenvertrauen sowie auf internationale Datenflüsse haben und sollten daher nur unter engen rechtlichen Voraussetzungen eingesetzt werden. DNS-basierte Sperr- oder Umleitungsmaßnahmen sind aus technischer und regulatorischer Sicht ein problematisches Instrument. Sie können zu unbeabsichtigten Nebenwirkungen führen, etwa wenn legitime Dienste oder Inhalte betroffen sind, und stehen grundsätzlich im Spannungsverhältnis zu einer offenen und verteilten Internetarchitektur. Gleichzeitig ist die Wirkung begrenzt, weil die IP-Adressen der maliziösen Domains auch nach einer Änderung der Nameserver-Einträge weiterhin im Internet erreichbar bleiben. Eine verstärkte Konzentration von Diensten auf wenige Anbieter infolge regulatorischer Risiken kann zudem zu einem „Flaschenhalseffekt“ führen, der die Resilienz digitaler Infrastrukturen insgesamt schwächt.

Darüber hinaus besteht das Risiko, dass weitreichende Eingriffsbefugnisse im Bereich von DNS- und Datenverkehrsmaßnahmen internationale Anbieter davon abhalten könnten, ihre Dienste im deutschen Markt anzubieten. Eine regulatorische Umgebung, die hohe Eingriffs- und Haftungsrisiken schafft, kann dazu führen, dass Anbieter ihre Aktivitäten in andere Märkte verlagern. Dies würde langfristig Wettbewerb, Innovationsfähigkeit und die Resilienz der digitalen Infrastruktur schwächen.

Befugnisse sollten klar begrenzt, transparent ausgestaltet und an hohe rechtliche sowie technische Anforderungen geknüpft werden, die Eingriffe nur als Ultima Ratio zulassen. Hierzu gehört auch die Notwendigkeit eines Gerichtsbeschlusses, um die Rechtmäßigkeit und Verhältnismäßigkeit der Anordnungen zu gewährleisten. Anordnungen dürfen unter keinen Umständen die vertraglich zugesicherte Verfügbarkeit und Integrität von unbeteiligten Kunden-Umgebungen gefährden. Ziel muss es sein, Sicherheitsmaßnahmen so auszugestalten, dass sie die Stabilität und Offenheit der Internetinfrastruktur stärken, ohne unbeabsichtigte negative Auswirkungen auf Wettbewerb, Innovation und die internationale Einbindung des deutschen Digitalstandorts zu erzeugen.

§31 BSIG-E

Die Verpflichtung für Betreiber kritischer Anlagen, Systeme zur Angriffserkennung einzusetzen, entspricht grundsätzlich dem Stand der Technik und wird von vielen Betreibern bereits heute umgesetzt. Maßnahmen wie Intrusion-Detection- und Intrusion-Prevention-Systeme sowie kontinuierliche Sicherheitsüberwachung sind etablierte Bestandteile moderner IT-Sicherheitsarchitekturen. Wichtig ist aus Sicht der Praxis, dass vorhandene marktübliche Sicherheitslösungen und Prozesse anerkannt werden und bestehende Sicherheitsarchitekturen nicht durch zusätzliche regulatorische Vorgaben unnötig überformt werden.

Die in § 31 Absatz 2 BSI-G-E vorgesehene dauerhafte und automatisierte Ausleitung von Parametern, Betriebsmerkmalen und Verfügbarkeitsindikatoren aus Systemen zur Angriffserkennung an das Bundesamt ist in ihrer derzeitigen Fassung abzulehnen. Dabei ist insbesondere klarzustellen, dass Systeme zur Angriffserkennung der Erkennung und Bewertung sicherheitsrelevanter Ereignisse sowie der Sicherstellung der Verfügbarkeit kritischer Dienstleistungen dienen, nicht jedoch dem eigentlichen Verfügbarkeitsmonitoring, das regelmäßig durch spezialisierte Systeme erfolgt. Die im Gesetzentwurf verwendeten Begriffe „Parameter“, „Merkmale aus dem laufenden Betrieb“ und „regelmäßige Verfügbarkeitsindikatoren“ bleiben zudem weitgehend unbestimmt und eröffnen dem Bundesamt einen erheblichen Spielraum bei der inhaltlichen und technischen Ausgestaltung der Anbindung. Dies birgt die Gefahr, dass Systeme zur Angriffserkennung über ihren eigentlichen Zweck hinaus für zusätzliche Aufgaben herangezogen werden, die sie in dieser Form weder leisten sollen noch praxisgerecht abbilden können. Erforderlich ist daher eine präzise gesetzliche Festlegung, welche konkreten Datenkategorien in welchem Umfang und in welcher Form übermittelt werden dürfen, damit die Verpflichtung nicht faktisch zu einer strukturell permanenten und inhaltlich offenen Ausleitung von Betriebsdaten aus kritischen Infrastrukturen führt.

Auch aus sicherheitstechnischer Perspektive wirft die vorgesehene Architektur der kontinuierlichen Anbindung Fragen auf. Eine zentralisierte Netzwerktopologie, bei der zahlreiche Betreiber kritischer Infrastrukturen dauerhaft mit einer Bundesbehörde verbunden sind, kann neue Angriffsflächen schaffen. Insbesondere könnte eine solche „Hub-and-Spoke“-Struktur ein Ziel für Angreifer darstellen. Im Falle einer Kompromittierung der Schnittstellen oder Verbindungspunkte bestünde die Gefahr, dass eine eigentlich defensiv konzipierte Maßnahme selbst zu einem potenziellen Angriffsvektor wird. Vor diesem Hintergrund erscheint ein stärker dezentraler oder ereignisbasierter („Push-basierter“) Ansatz vorzuzugewürdigt, bei dem sicherheitsrelevante Daten nur unter klar definierten Voraussetzungen übermittelt werden.

Schließlich geht die vorgesehene Verpflichtung zur kontinuierlichen Datenübermittlung über die Anforderungen der NIS-2-Richtlinie und anderer europäischer Cyberregulierungen hinaus und würde damit eine nationale Sonderpflicht begründen. Aus Sicht der Praxis sollte daher eine präzise gesetzliche Eingrenzung erfolgen, sodass sich die Datenübermittlung auf klar definierte sicherheitsrelevante Indikatoren beschränkt und verhältnismäßig ausgestaltet ist. Gleichzeitig sollte sichergestellt werden, dass der zusätzliche technische und organisatorische Aufwand für Betreiber kritischer Anlagen angemessen berücksichtigt wird. Dies gilt insbesondere vor dem Hintergrund, dass Umfang und Ausgestaltung der Datenübertragung bislang weitgehend offenbleiben und derzeit weder einheitliche Schnittstellen noch standardisierte Austauschformate für Systeme zur Angriffserkennung bestehen. Die Umsetzung würde daher in erheblichem Maße von den jeweiligen Herstellern abhängen und könnte im Einzelfall aufwändige, spezifische Integrationen erforderlich machen. Vor diesem Hintergrund sollte eine angemessene und hinreichend lange Umsetzungsfrist vorgesehen werden.

§50 BSIG-E

Die vorgeschlagene Schärfung von § 50 Absatz 1 BSIG-E erscheint nicht angemessen. Sie ändert eine Regelung, die erst vor wenigen Monaten in Kraft getreten ist, ohne dass hierfür bislang ein praktischer Bedarf nachvollziehbar dargelegt wurde. Die vorgesehene Vereinfachung des Zugangs zu Domain-Namen-Registrierungsdaten für deutsche Sicherheitsbehörden durch die Streichung der Erfordernis, hierfür im Einzelfall ein legitimes Interesse zu begründen, wirft erhebliche datenschutzrechtliche Fragen auf.

Artikel 3: Bundeskriminalamtgesetz (BKAG)

Die dem BKA eingeräumten Eingriffsbefugnisse entsprechen im Wesentlichen denen der Bundespolizei, nur dass sich die Zuständigkeitsbereiche unterscheiden. Auch hier sind die vorgesehenen Änderungen und insbesondere die geplante Befugnis als kritisch zu bewerten.

Zudem bestehen Zweifel an den Plänen, dass der Entwurf weitreichende Fähigkeiten in erheblichem Umfang beim BKA konzentrieren will, obwohl vergleichbare Befugnisse auch von anderen Behörden wie dem BND oder dem BfV angestrebt werden. Eine solche Bündelung sollte nicht allein damit begründet werden, dass beim BKA bereits entsprechende Kapazitäten vorhanden sind. Vielmehr sollte der Gesetzgeber prüfen, ob eine Aufgabenverteilung erforderlich ist, die sich primär an Zweckmäßigkeit, klaren Zuständigkeiten und einer nachvollziehbaren Verantwortungsarchitektur orientiert.

§62e BKAG-E

Der in § 62e BKAG-E vorgesehene Ansatz wird, auch mit Blick auf die bereits zu § 41a Abs. 2 Nr. 3 BPolG-E dargestellten Bedenken, kritisch gesehen. Der Entwurf knüpft den Eingriff in ein informationstechnisches System nur dann an einen Richtervorbehalt, wenn ein privates informationstechnisches System betroffen sein soll. Die Abgrenzungskriterien hierfür sind jedoch so unbestimmt, dass sie in der Praxis häufig erst nach einem Zugriff belastbar verifiziert werden können. Gerade in hochgradig virtualisierten Mehrnutzer-Netzen lässt sich oftmals erst nach einem Zugriff feststellen, ob private Systeme betroffen sind. Damit wird faktisch dem BKA selbst die maßgebliche Beurteilung beziehungsweise Prognose darüber übertragen, ob ein Richtervorbehalt erforderlich ist. Dieses Regelungsmuster ist aus Bitkom-Sicht nicht auf § 62e BKAG-E beschränkt, sondern prägt auch weitere Eingriffsrechte im Entwurf und verstärkt insgesamt das Risiko einer unzureichenden rechtsstaatlichen Absicherung.

Der Richtervorbehalt sollte angesichts der Intensität des Grundrechtseingriffs grundsätzlich für alle informationstechnischen Systeme gelten. Die Differenzierung zwischen privaten und nicht-privaten Systemen führt in modernen IT- und Cloud-Umgebungen zu erheblichen Abgrenzungsunsicherheiten. Zudem sollten Ausnahmen wegen „Gefahr im Verzug“ bei Eingriffen in gewerblich betriebene Cloud-Infrastrukturen gestrichen oder auf engste Ausnahmefälle, insbesondere dringende

Gefahren für Leib und Leben, beschränkt werden, um Rechtssicherheit und den Schutz von Kundeninfrastrukturen vor übereilten Eingriffen zu stärken.

Artikel 4: Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten

Der Entwurf sieht neue Pflichten für Anbieter digitaler Dienste vor, Nutzer über bekannte Störungen und Bedrohungen zu informieren. Diese Regelung erscheint nicht erforderlich, da Diensteanbieter bereits im Rahmen der NIS-2-Richtlinie umfassenden Meldepflichten bei Sicherheitsvorfällen unterliegen. Die Einführung einer zusätzlichen nationalen Informationspflicht schafft eine parallele Meldestruktur und erhöht die regulatorische Komplexität für betroffene Unternehmen. Gleichzeitig besteht die Gefahr, dass häufige oder redundante Benachrichtigungen zu einer geringeren Aufmerksamkeit der Nutzer („Meldemüdigkeit“) führen.

Weitere nationale Gesetzgebung eng an den Vorgaben der NIS-2-Richtlinie ausgerichtet werden, um doppelte Compliance-Anforderungen zu vermeiden. Ziel sollte ein möglichst kohärentes „One-Stop-Shop“-Modell für Cybersicherheitsmeldungen sein, anstatt paralleler nationaler Meldepflichten, die den europäischen Bestrebungen zur Vereinfachung und Harmonisierung der Cyberregulierung entgegenlaufen.

Anstatt neue Strukturen und Anforderungen zu schaffen, sollten bestehende Möglichkeiten der Cyberabwehr und zum Schutz von Kunden vor betrügerischen Aktivitäten besser genutzt werden können. Die datenschutzrechtlichen Vorschriften sind zum Teil zu eng gefasst, bzw. es keine ausreichend klaren Rechtsgrundlagen für bestimmte Abwehrmaßnahmen. Die praktischen Schutzmechanismen bleiben somit hinter den technischen Möglichkeiten und das Vertrauen in die Telekommunikation wird geschwächt. Ein Beispiel ist die fehlende Rechtsgrundlage für das Filtern von Phishing SMS. § 3 und § 12 TDDDG könnten angepasst werden, um die Möglichkeit der technischen Auswertung von Daten zum Schutz der Kunden vor Vermögensschäden durch Phishing SMS erweitert werden.

Wir schlagen außerdem vor, die folgenden Teile des TDDDG und TKG so zu schärfen, dass den Telekommunikationsunternehmen mehr Möglichkeiten zur Cyberabwehr und Betrugsprävention eingeräumt werden:

§ 12 TDDDG

§ 12 Abs. 1 TDDDG sollte eine eindeutige gesetzliche Grundlage für die Speicherung und Analyse von Verkehrs- und Steuerdaten für Systeme zur Angriffserkennung darstellen. Zurzeit dürfen Verkehrsdaten nur zur Störungserkennung verarbeitet werden. Der Störungsbegriff ist derzeit zu sehr auf technische Störungen eingegrenzt, er sollte auch bereits zeitlich vorgelagerte Planungsphasen von Cyberangriffen erfassen. Diese Daten werden auch für die Erstellung eines umfassenden Lagebildes, wie hier im Gesetzesentwurf angelegt, benötigt.

Hierzu korrespondierend muss auch eine längere Speicherdauer möglich sein. Die Speicherdauer ist bisher nicht gesetzlich geregelt, wird aber bei der Störungserkennung von der Rechtsprechung und BfDI auf 7 Tage begrenzt. Wenn Daten für die zeitlich vorgelagerte Angriffserkennung benötigt werden, ist hierfür eine längere Speicherdauer notwendig. Der § 12 Abs. 1 TDDDG muss also über die Störung hinaus die Datenverarbeitung zum Betreiben von Systemen zur Angriffserkennung (solange hierfür erforderlich) ermöglichen.

§ 12 Abs. 4 TDDDG sollte um ein weiteres Beispiel für eine rechtswidrige Inanspruchnahme ergänzt werden, nämlich das täuschungsbedingte Erlangen von Zugangsdaten, bspw. Benutzerkonto-Daten oder Account-Daten. Damit kann klargestellt werden, dass Maßnahmen zum Schutz vor Smishing/Phishing getroffen werden können. Zusätzlich sollte das Ziel der Regelung um den Schutz der Endnutzer vor Vermögensschäden ergänzt.

§ 169 TKG

Es braucht eine eindeutige Rechtsgrundlage für Umleitung und Blockieren von maliziösem Datenverkehr. § 169 Abs. 7 TKG sollte so erweitert werden, sodass der Datenverkehr nicht nur von und zu Störungsquellen blockiert werden, sondern auch zu maliziösen Inhalten, soweit dies zum Schutz der Nutzer vor Vermögensschäden erforderlich ist.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Leiter Sicherheit

T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik

Copyright

Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.