08.05.2026

**BUNDESVERBAND IT-MITTELSTAND E.V. (BITMI)**

# Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Cybersicherheit des Bundeministeriums des Innern und für Heimat

## Zusammenfassung

Der IT-Mittelstand unterstützt die Zielsetzung des Referentenentwurfs, die Cybersicherheit in Deutschland zu stärken. In der vorliegenden Form bestehen jedoch erhebliche Bedenken hinsichtlich der praktischen Umsetzbarkeit, der Verhältnismäßigkeit einzelner Maßnahmen sowie der Auswirkungen auf die Wettbewerbsfähigkeit mittelständischer Unternehmen.

Kritisch sind aus Sicht des IT-Mittelstands besonders

- die weitreichenden Eingriffsbefugnisse staatlicher Stellen in zentrale Infrastrukturen von Unternehmen,
- die fehlende Differenzierung bei Bußgeldern,
- unklare und potenziell überfordernde Mitwirkungs- und Informationspflichten sowie zusätzliche bürokratische Belastungen im Zusammenspiel mit bestehenden europäischen Regulierungen wie der NIS-2-Richtlinie und dem Cyber Resilience Act.

Darüber hinaus bestehen wesentliche Unklarheiten hinsichtlich der konkreten Ausgestaltung der Zusammenarbeit zwischen staatlichen Stellen und mittelständischer IT-Wirtschaft. Insbesondere fehlt es an klar definierten, praktikablen Mechanismen für einen strukturierten Informationsaustausch und eine verlässliche Kommunikation, die für eine wirksame Cybersicherheitsarchitektur essenziell sind.

**Bundesverband IT-Mittelstand e.V.**
Haus der Bundespressekonferenz
Schiffbauerdamm 40 | 10117 Berlin
www.bitmi.de

**Ansprechpartner**
Konstantin Elsässer
Telefon +49 30 22 60 50 05
politik@bitmi.de

## Aus Sicht des Bundesverbands IT-Mittelstand e.V. (BITMi) sind folgende Punkte hervorzuheben:

**1. Erweiterte Befugnisse staatlicher Behörden (§ 41a BPolG-E, §§ 62b–g BKAG-E)**

Der Referentenentwurf sieht in § 41a BPolG-E sowie in den §§ 62b–g BKAG-E eine erhebliche Ausweitung der Befugnisse von Sicherheitsbehörden wie der Bundespolizei und des Bundeskriminalamtes vor. Diese Entwicklung wird vom IT-Mittelstand kritisch bewertet, da weder die technische Umsetzung noch Transparenzmechanismen gegenüber Unternehmen und deren Kunden klar sind. Insbesondere ist festzustellen, dass neue Zuständigkeiten für die Bundespolizei im Cybersicherheitsbereich geschaffen werden, ohne die bestehende Rolle des Bundesamtes für Sicherheit in der Informationstechnik als etablierten Partner der Wirtschaft angemessen einzubeziehen. Die parallele Ausweitung von Kompetenzen birgt das Risiko ineffizienter Doppelstrukturen und erschwert eine klare Aufgabenteilung zwischen den beteiligten Behörden. Dadurch besteht das Risiko unklarer Ansprechpartner für Unternehmen des IT-Mittelstand und zusätzlicher bürokratischer Aufwand.

**2. Eingriffe in IT-Systeme und Offenbarungsverbote (§ 41a BPolG-E, §§ 62b–g BKAG-E)**

Die in § 41a BPolG-E sowie den §§ 62b–g BKAG-E geregelten Eingriffsbefugnisse ermöglichen es staatlichen Stellen, Daten auf IT-Systemen zu erheben, zu verändern oder zu löschen, ohne die betroffenen Unternehmen darüber zu informieren. Diese Maßnahmen werfen erhebliche rechtliche und praktische Fragen auf. Darüber hinaus geraten IT-Dienstleister in Konflikt mit ihren vertraglichen Informationspflichten gegenüber ihren Kunden. In komplexen IT-Umgebungen, etwa bei Cloud- oder Multi-Tenant-Infrastrukturen, können solche Eingriffe zudem unbeabsichtigte Auswirkungen auf unbeteiligte Dritte haben.

**3. Bürokratiezuwachs und unklarer Erfüllungsaufwand (Vorblatt S. 6, Abschnitt E.2)**

Im Vorblatt des Referentenentwurfs (S. 6, Abschnitt E.2) wird der Erfüllungsaufwand für die Wirtschaft lediglich als „moderat“ und teilweise nicht quantifizierbar beschrieben. Diese Einschätzung steht im Widerspruch zur tatsächlichen Belastung, die sich aus den vorgesehenen Regelungen für den IT-

**Bundesverband IT-Mittelstand e.V.**
Haus der Bundespressekonferenz
Schiffbauerdamm 40 | 10117 Berlin
www.bitmi.de

**Ansprechpartner**
Konstantin Elsässer
Telefon +49 30 22 60 50 05
politik@bitmi.de

Mittelstand ergibt. Während staatlicherseits umfangreiche personelle und finanzielle Ressourcen eingeplant sind, bleibt der zusätzliche Aufwand für Unternehmen, insbesondere für KMU, unzureichend berücksichtigt. Die kumulative Wirkung neuer Pflichten im Zusammenspiel mit bestehenden europäischen Vorgaben wie der NIS-2-Richtlinie und dem Cyber Resilience Act führt zu einer erheblichen zusätzlichen bürokratischen Belastung.

**4. Fehlende Staffelung der Bußgelder (§ 104 BPolG-E, § 87a BKAG-E)**

Die in § 104 BPolG-E sowie § 87a BKAG-E vorgesehenen Bußgelder von bis zu 20 Millionen Euro für Verstöße gegen Offenbarungsverbote sowie bis zu 10 Millionen Euro für Verstöße gegen Mitwirkungspflichten sind aus Sicht des IT-Mittelstands nicht verhältnismäßig ausgestaltet. Da keine Differenzierung nach Unternehmensgröße oder wirtschaftlicher Leistungsfähigkeit vorgesehen ist, können diese Sanktionen für kleine und mittlere Unternehmen existenzbedrohende Auswirkungen haben. Eine an Umsatz oder Unternehmensgröße orientierte Staffelung erscheint daher empfehlenswert.

**5. Pflichten für Anbieter digitaler Dienste (Art. 4, § 19 Abs. 5 und 6 TDDDG-E)**

Die in Art. 4 in Verbindung mit § 19 Abs. 5 und 6 TDDDG-E vorgesehenen Verpflichtungen zur unverzüglichen Information von Nutzern über Sicherheitsrisiken sind in ihrer konkreten Ausgestaltung nicht hinreichend präzisiert. Insbesondere bleibt unklar, was unter „angemessenen technischen Mitteln“ im jeweiligen Einzelfall zu verstehen ist. Diese Unbestimmtheit führt zu Rechtsunsicherheit bei den betroffenen Unternehmen. Zudem fehlen klar definierte, sichere und authentifizierbare Kommunikationswege zwischen Behörden und Unternehmen. Gerade für KMU besteht die Gefahr, dass sie ihre Pflichten mangels klarer Vorgaben nicht vollständig erkennen oder erfüllen können.

**6. Unklare Mitwirkungspflichten (§ 41a Abs. 9 BPolG-E, § 62d Abs. 2 BKAG-E)**

Die Verpflichtung zur „unverzüglichen Mitwirkung“ gemäß § 41a Abs. 9 BPolG-E sowie § 62d Abs. 2 BKAG-E stellt insbesondere kleinere Anbieter vor erhebliche operative Herausforderungen. Da weder konkrete Fristen noch abgestufte Anforderungen definiert sind, wird implizit vorausgesetzt, dass alle betroffenen Unternehmen jederzeit kurzfristig komplexe technische Maßnahmen umsetzen können. Dies entspricht nicht den betrieblichen Realitäten vieler KMU, die häufig nicht über durchgehende Betriebs- oder Bereitschaftsstrukturen verfügen.

**Bundesverband IT-Mittelstand e.V.**
Haus der Bundespressekonferenz
Schiffbauerdamm 40 | 10117 Berlin
www.bitmi.de

**Ansprechpartner**
Konstantin Elsässer
Telefon +49 30 22 60 50 05
politik@bitmi.de

**7. Datenübermittlung an das BSI (§ 15 Abs. 6 BSIG-E)**

Die in § 15 Abs. 6 BSIG-E vorgesehenen umfassenden Datenübermittlungspflichten an das Bundesamt für Sicherheit in der Informationstechnik stellen hohe technische sowie organisatorische Anforderungen an die betroffenen Unternehmen. Für viele mittelständische Anbieter sind diese Anforderungen nur mit erheblichem zusätzlichem Aufwand umsetzbar. Gleichzeitig ist nicht vorgesehen, dass die Unternehmen im Gegenzug systematisch von den gewonnenen Erkenntnissen über Verbesserungspotenziale ihrer eigenen Cybersicherheit profitieren, wodurch ein unausgewogenes Verhältnis zwischen Pflichten und Nutzen entsteht.

**8. Rolle des BSI im Bereich Threat Intelligence (§ 16 Abs. 6 BSIG-E)**

Die Regelung in § 16 Abs. 6 BSIG-E sieht vor, dass das BSI verstärkt als Anbieter von Threat-Intelligence-Leistungen auftritt, unter anderem durch die Veröffentlichung von Listen maliziöser Domains und die Einführung entsprechender Schutzpflichten. Die vorgesehenen Schwellenwerte betreffen insbesondere mittelständische Unternehmen. Dadurch entsteht eine direkte Überschneidung mit bestehenden privatwirtschaftlichen Sicherheitsangeboten, die bereits funktionierende Sicherheitsnetze gewährleisten. Etablierte Formate des vertrauensvollen Austauschs auf Augenhöhe zwischen Unternehmen und Sicherheitsbehörden sollten systematisch weiterentwickelt werden und nicht durch staatliche Anbieter ersetzt werden. Aus ordnungspolitischer Sicht ist eine klare Abgrenzung staatlicher und privatwirtschaftlicher Aufgaben erforderlich.

**09. Domain-Dekonnektierung (§ 16a BSIG-E)**

Die in § 16a BSIG-E vorgesehene Möglichkeit zur Domain-Dekonnektierung ohne aufschiebende Wirkung stellt einen besonders weitreichenden Eingriff dar. Da Domains zentrale Bestandteile unternehmerischer IT-Infrastrukturen sind, kann eine kurzfristige Abschaltung erhebliche Auswirkungen auf Kommunikationssysteme, Schnittstellen und gesamte Wertschöpfungsketten haben. Darüber hinaus besteht das Risiko, dass Maßnahmen auch unbeteiligte Systeme betreffen, etwa bei komplexen Hosting-Strukturen oder bei missbräuchlicher Nutzung über Dritte. Die fehlende aufschiebende Wirkung von Rechtsbehelfen verstärkt diese Problematik zusätzlich.

**10. Auskunftspflichten zu Domain-Registrierungsdaten (§ 50 Abs. 1 BSIG-E)**

**Bundesverband IT-Mittelstand e.V.**
Haus der Bundespressekonferenz
Schiffbauerdamm 40 | 10117 Berlin
www.bitmi.de

**Ansprechpartner**
Konstantin Elsässer
Telefon +49 30 22 60 50 05
politik@bitmi.de

Die in § 50 Abs. 1 BSIG-E geregelten Auskunftspflichten zu Domain-Registrierungsdaten, einschließlich der vorgesehenen Frist von 72 Stunden, sind aus praktischer Sicht mit erheblichen Herausforderungen verbunden. Insbesondere bleibt unklar, wie die Authentizität und Berechtigung von Anfragen verlässlich geprüft werden sollen. Die Öffnung für „sonstige Zugangsnachfrager“ erhöht zudem das Risiko missbräuchlicher Anfragen. Ohne standardisierte, sichere Kommunikationskanäle und klare Validierungsmechanismen ist eine rechtssichere Umsetzung kaum gewährleistet.

**Ansprechpartner bei Rückfragen:**

Konstantin Elsässer, Referent Digitalpolitik, politik@bitmi.de