



Ausschussdrucksache 21(4)224
vom 30. September 2026

Schriftliche Stellungnahme
von ISC2 vom 30. September 2026

zu dem

Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung der Cybersicherheit
BT-Drucksache 21/6585

Stellungnahme: Gesetz zur Stärkung der Cybersicherheit

Zusammenfassung

Die Bedrohungslage im Cyberraum ist weiterhin hoch und komplex. Die Dringlichkeit wird durch aktuelle Zahlen unterstrichen. So weist das Bundeslagebild Cybercrime 2025 des Bundeskriminalamts insgesamt mehr als 330.000 Cybercrime-Straftaten aus.¹ Laut einer Bitkom-Umfrage aus dem Jahr 2026 verursachen Cyberangriffe auf Unternehmen in Deutschland jährlich Schäden zwischen 160,4 und 205,8 Milliarden Euro.²

Mit der Umsetzung der NIS2-Richtlinie und des KRITIS-Dachgesetzes wurden wichtige erste Schritte zur Stärkung der Resilienz kritischer und wichtiger Einrichtungen unternommen. Wirksame Cybersicherheit hängt jedoch von Menschen ab. Die ISC2 Workforce Study zeigt einen erheblichen Bedarf an Cybersicherheitsfachkräften in Deutschland: 40% der Befragten gaben an, dass in ihren Organisationen ein kritischer oder erheblicher Kompetenzbedarf besteht, während es im Jahr 2024 noch 29% waren. Dies stellt ein unmittelbares Hindernis für die Umsetzung der Cybersicherheitsgesetzgebung und den Schutz des deutschen Cyberraums dar. 60% der Befragten in Deutschland sehen den Fachkräftemangel als größtes Hindernis bei der Einhaltung von Cybervorschriften. Gesetzgeberischer Anspruch und personelle Kapazitäten sind eng miteinander verknüpft und sollten gemeinsam angegangen werden – beginnend mit diesem Gesetzentwurf.

Der Gesetzentwurf schafft zwar erhebliche neue Befugnisse und sieht 377 neue spezialisierte Stellen bei BKA, Bundespolizei und BSI vor.³ Dabei handelt es sich um qualifizierte Analystenstellen im Bereich der Bedrohungserkennung. Der Gesetzentwurf enthält jedoch keinen Verweis auf den Europäischen Kompetenzrahmen für Cybersicherheit, keinen beruflichen Kompetenzstandard für die Personen, die diese Befugnisse ausüben, und keine Anforderungen an deren Qualifikation.

Neue Befugnisse, neue Datenströme und neue Systeme werden nur dann wirksam sein, wenn sie von qualifizierten, kontinuierlich geschulten und rollenbezogen ausgebildeten Cybersicherheitsfachkräften umgesetzt werden.

Empfehlungen von ISC2

Angesichts der zunehmenden Zahl, Komplexität und Größenordnung von Cyberangriffen in Deutschland erfordert eine wirksame Cyberabwehr nicht nur Befugnisse und technische Systeme, sondern auch qualifizierte Fachkräfte.

Wir empfehlen, die im Gesetzentwurf vorgesehenen Befugnisse, Datenströme und technischen Verpflichtungen um einen verbindlichen Kompetenzrahmen zu ergänzen. Dabei sollten Rollen, Aufgaben und Schulungsanforderungen am Europäischen Kompetenzrahmen für Cybersicherheit (European Cybersecurity Skills Framework, ECSF) der ENISA ausgerichtet werden. Die Kompetenzen sollten durch eine einschlägige Ausbildung, bewertete praktische Erfahrung oder eine unabhängige Zertifizierung nachgewiesen werden. Durch kontinuierliche berufliche Weiterbildung ist sicherzustellen, dass die Kompetenzen auf dem aktuellen Stand bleiben.

¹ Vgl. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2026/Presse2026/260512_PM_BLB_Cybercrime.html

² Vgl. <https://www.bitkom.org/sites/main/files/2026-09/bitkom-studienbericht-wirtschaftsschutz-2026.pdf>

³ Vgl. https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwurfe/CI1/cyberabwehr-RefE.pdf?__blob=publication-File&v=4

Eine unabhängige Zertifizierung bietet eine externe Überprüfung der Kompetenz durch eine nach ISO/IEC 17024 akkreditierte Stelle und muss regelmäßig erneuert werden. Die mit diesem Gesetzentwurf eingeführten Befugnisse erfordern ein ausgeprägtes technisches Verständnis des jeweiligen Kontexts und der betroffenen Systeme, damit sie verantwortungsvoll ausgeübt werden können. Durch die Ausrichtung der Kompetenzanforderungen am ECSF haben Bürgerinnen und Bürger sowie staatliche Stellen die Gewissheit, dass diese Befugnisse von kompetenten Fachkräften ausgeübt werden.

Der Regierungsentwurf bietet hier folgende Anknüpfungspunkte:

1. **Der Regierungsentwurf sieht in §31 BSI-Gesetz vor, dass Betreiber kritischer Anlagen verpflichtet sind, Systeme zur Angriffserkennung für relevante informationstechnische Systeme, Komponenten und Prozesse einzusetzen, die für das Funktionieren der von ihnen betriebenen kritischen Anlagen von wesentlicher Bedeutung sind.**

Künftig sollen Betreiber außerdem verpflichtet werden, Verfügbarkeitsindikatoren, Angriffsindikatoren und Informationen über Schwachstellen automatisiert an das BSI zu übermitteln. Das BSI wird nach Anhörung der Betreiber und Wirtschaftsverbände die Anforderungen an die Anbindung und Datenübermittlung festlegen.

Wir sind der Ansicht, dass hier ein ausdrücklicher Verweis auf rollenbezogene Kompetenz-, Schulungs- und Qualifikationsanforderungen ergänzt werden sollte.

Der Paragraph sollte wie folgt ergänzt werden:

Bei der Festlegung der Anforderungen an Systeme zur Angriffserkennung, deren Anbindung und die Datenübermittlung soll das Bundesamt neben den technischen Anforderungen auch Mindestanforderungen an Rollen, Kompetenzen und Schulungen festlegen. Diese sind für einen wirksamen Betrieb sowie für Analyse, Bewertung, Eskalation und Reaktion erforderlich.

Die Kompetenzanforderungen sollen dabei auf dem Europäischen Kompetenzrahmen für Cybersicherheit basieren. Die Betreiber müssen sicherstellen, dass die in diesen Rollen eingesetzten Mitarbeitenden diese Anforderungen erfüllen. Die Kompetenz kann durch eine einschlägige Ausbildung, bewertete praktische Erfahrung oder eine unabhängige Zertifizierung nachgewiesen werden und muss durch kontinuierliche berufliche Weiterbildung aktuell gehalten werden.

Begründung:

Die geplante Anbindung der von den betroffenen Betreibern eingesetzten Systeme zur Angriffserkennung an das Bundesamt ist ein wichtiger Schritt, um das Lagebild zu verbessern. Der Regierungsentwurf ist jedoch stark technisch ausgerichtet. Eine automatisierte Datenübermittlung allein führt weder zu wirksamer Cyberabwehr noch zu einem besseren Verständnis der Bedrohungslage. Entscheidend ist, dass die erhobenen Daten fachgerecht bewertet, priorisiert und in geeignete Reaktionsmaßnahmen übersetzt werden. Dafür werden qualifizierte Cybersicherheitsanalytistinnen und -analysten benötigt. Diese müssen nicht nur beim BSI, sondern auch bei den Betreibern selbst tätig sein.

2. **Der Regierungsentwurf im §68d BKA-G sieht vor, dass das Bundeskriminalamt gefahrenbezogene Daten in einem informationstechnischen System, von dem die Gefahr ausgeht, auslesen, löschen oder verändern darf – auch mit technischen Mitteln und ohne das Wissen der betroffenen Person.**

Zu diesem Zweck müssen nach Möglichkeit technische Vorkehrungen getroffen werden, um sicherzustellen, dass das Auslesen, Löschen oder Verändern von Daten auf gefahrenbezogene Daten beschränkt bleibt.

Wir sind der Ansicht, dass ein rechtsstaatlicher Qualitätsmaßstab ergänzt werden muss. Je eingriffsintensiver eine Maßnahme ist, desto höher müssen die Anforderungen an die Qualifikation, die Dokumentation, die fachliche Aufsicht und die kontinuierliche Fortbildung der handelnden Personen sein.

Der Paragraph sollte im Absatz 3 wie folgt ergänzt werden:

Bei Maßnahmen zur Umleitung, Sperrung oder Veränderung des Datenverkehrs sowie beim Auslesen, Löschen oder Verändern gefahrenbezogener Daten müssen hohe fachliche Mindeststandards eingehalten werden.

Dazu gehören rollenbezogene Qualifikationen, regelmäßige Schulungen, dokumentierte praktische Erfahrung, technische und rechtliche Fortbildung sowie die lückenlose Nachvollziehbarkeit der ergriffenen Maßnahmen.

Diese Standards soll das Bundesministerium des Innern nach Anhörung des Bundesamts für Sicherheit in der Informationstechnik auf Grundlage des Europäischen Kompetenzrahmens für Cybersicherheit festlegen. Die Erfüllung dieser Anforderungen kann durch eine einschlägige Ausbildung, bewertete praktische Erfahrung oder eine unabhängige Zertifizierung nachgewiesen werden.

Begründung:

Der Regierungsentwurf beschreibt die neuen Aufgaben des Bundeskriminalamts selbst als komplex und technisch besonders anspruchsvoll. Die neuen Befugnisse betreffen Eingriffe in sensible technische Systeme und können auch Dritte betreffen.

Aus unserer Sicht sollte der Gesetzgeber daher klarstellen, dass eine professionelle Cyberabwehr nicht allein durch neue Befugnisse gewährleistet ist, sondern durch qualifizierte Fachkräfte, klar definierte Rollen, kontinuierliche Fortbildung und überprüfbare Standards.

Umsetzung

Diese Anforderungen sollten praxisgerecht und verhältnismäßig ausgestaltet werden. Bereits beschäftigte Mitarbeitende sollten ihre Kompetenz über einen der anerkannten Nachweiswege, einschließlich bewerteter praktischer Erfahrung, belegen können.

Nach Veröffentlichung der Anforderungen durch das BSI sollten Betreiber 24 Monate Zeit erhalten, um diese zu erfüllen. Für die neuen polizeilichen Befugnisse sollten die Standards von Beginn an gelten. Die Kosten für die Schulung der eigenen Mitarbeitenden sollten von den Arbeitgebern getragen werden. Die Schulung für die neuen Stellen auf Bundesebene sollte gemeinsam mit diesen Stellen budgetiert werden. Kleinere Betreiber sollten die Anforderungen im Einklang mit dem Verhältnismäßigkeitsgrundsatz auch durch den Einsatz qualifizierter Dienstleister erfüllen können.

Über ISC2

ISC2 ist die weltweit größte gemeinnützige Organisation für zertifizierte Cybersicherheitsfachkräfte und zählt mehr als 270.000 Mitglieder – darunter 40.000 in Europa und 5.300 in Deutschland. Unsere international anerkannten Zertifizierungen sind nach ISO/IEC 17024 akkreditiert und eng am EU-Kompetenzrahmen für Cybersicherheit (ECSF) ausgerichtet. Durch Programme wie unsere Beteiligung an der EU Cyber Skills Academy, die mehr als 50.000 Menschen in Europa einen kostenlosen Einstieg in den Bereich Cybersicherheit ermöglicht, setzen wir uns gezielt für die Förderung von Kompetenzen ein. Unsere Mitglieder sind zertifizierte Cybersicherheitsexpertinnen und -experten, die für den Schutz unserer staatlichen Institutionen, Volkswirtschaften, kritischen Infrastrukturen und personenbezogenen Daten verantwortlich sind.