21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)064
vom 10. Oktober 2025

Schriftliche Stellungnahme

von ISC2 vom 8. Oktober 2025

Öffentliche Anhörung

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

BT-Drucksache 21/1501

Stellungnahme: Gesetz zur Umsetzung der NIS-2-Richtlinie in Deutschland (NIS2UmsuCG) – Eine Chance, die nationale Cyber-Resilienz durch qualifizierte Fachkräfte im Bereich Cybersicherheit in Deutschland zu verbessern

Zusammenfassung

Mit der Einrichtung des 500 Milliarden Euro Sondervermögens der Bundesregierung für Infrastruktur und Klimaneutralität hat Deutschland seine Absicht signalisiert, die nationale Widerstandsfähigkeit zu stärken. Dies ist ein entscheidender Schritt zur Verbesserung der Resilienz und der nationalen Sicherheit Deutschlands.

Dennoch war Deutschland in den vergangenen Jahren mehrfach Ziel von Cyberangriffen, die erhebliche finanzielle Schäden für die deutsche Wirtschaft verursacht haben. Hinzu kommt, dass eine veraltete digitale Infrastruktur sowie ein genereller Fachkräfte- und Kompetenzmangel das Risiko von Cyberkriminalität in Deutschland weiterhin deutlich erhöhen. Tatsächlich hat die ISC2-Studie „Cybersecurity Workforce Study 2024" einen Mangel an 120.000 Fachkräften im Bereich Cybersicherheit in Deutschland festgestellt.[1]

Die NIS2-Richtlinie bietet eine wichtige Möglichkeit durch eine robuste Cyberabwehr, die Modernisierung der Infrastruktur und eine gezielte Personalentwicklung zu beheben. ISC2 begrüßt die Initiative der deutschen Regierung und den aktuellen Regierungsentwurf.

Wir empfehlen:

- **Behebung des wachsenden Fachkräftemangels**
  Die Zahl der Fachkräfte im Bereich Cybersicherheit in Deutschland ist auf 439.000 gesunken, was einem Mangel von 120.000 Fachkräften entspricht.[2] ISC2 empfiehlt, **bestehende Strukturen für rollenbasierte Schulungen und Zertifizierungen wie das European Cyber Security Skills Framework (ECSF) der ENISA[3] zur Definition „ausreichender und notwendiger Fähigkeiten" zu nutzen.**

- **Cybersicherheit als strategisches und nationales Thema angehen**
  ISC2 empfiehlt, dass die deutsche Bundesregierung **bis 2027 eine aktualisierte nationale Cybersicherheitsstrategie** vorlegt, die auch Fachkräfteentwicklung und Kompetenzen mit einbezieht.

- **Mobilität von internationalen Fachkräften ermöglichen**
  ISC2 empfiehlt **Deutschland, der International Cybersecurity Workforce Coalition beizutreten** und die gegenseitige Anerkennung von Zertifizierungen in internationalen Abkommen anzustreben.

Bewertung des Regierungsentwurfs durch ISC2:

Angesichts der zunehmenden Anzahl, Komplexität und des Ausmaßes von Cyberangriffen in Deutschland ist die zeitnahe Umsetzung der NIS-2-Richtlinie von entscheidender Bedeutung. ISC2 unterstützt den

[1] Siehe ISC2-Studie zur Cybersicherheitsbelegschaft 2024 (https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study)
[2] Siehe ISC2-Studie zur Cybersicherheitsbelegschaft 2024 (https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study)
[3] Siehe von der ENISA entwickelte Rollen und Kompetenzen im Bereich Cybersicherheit (https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities)

allgemeinen Ansatz im Entwurf der deutschen Bundesregierung, ist jedoch der Ansicht, dass wichtige Aspekte der Cybersicherheit übersehen werden.

Um eine wirksame Umsetzung der NIS-2-Richtlinie in Deutschland zu gewährleisten, empfehlen wir insbesondere, die folgenden Aspekte im Entwurf zu berücksichtigen:

- Wir empfehlen, den Gesetzesentwurf durch **klarere Beschreibungen des Bedarfs an Cybersicherheitskompetenz und Leitlinien zu den Ausbildungs- und Zertifizierungsanforderungen** zu verstärken.

    - **Die Anforderungen an die Schulungen im Cybersicherheitsbereich, die beispielsweise in den §38 und §43 des Entwurfs der Bundesregierung genannt werden, sollten präzisiert werden, um ein gemeinsames Verständnis von „ausreichenden Kenntnissen und Fähigkeiten" zu schaffen.** Zur Klärung dieser Begriffe empfehlen wir, auf die von der ENISA definierten Rollen des European Cyber Security Skills Framework (ECSF) Bezug zu nehmen.[4]

- **Aufnahme eines Artikels, der eine spezielle nationale Cybersicherheitsstrategie gemäß Artikel 7 der NIS-2-Richtlinie fordert**.[5]

    - Dies ist notwendig, da die letzte Cybersicherheitsstrategie zuletzt im Jahr 2021 aktualisiert wurde. Angesichts der bedeutenden technologischen und geopolitischen Entwicklungen der letzten Jahre **empfehlen** wir **eine Aktualisierung bis 2027**, **einschließlich eines eigenen Abschnitts über die Entwicklung von Fachkräften und Kompetenzen in Deutschland.**

Insgesamt muss die Umsetzung der NIS-2-Richtlinie in Deutschland über die Reaktion auf Vorfälle hinausgehen und sich mit der grundlegenden Frage der Cybersicherheitskapazitäten befassen. ISC2 ermutigt die politischen Entscheidungsträger, international anerkannte Standards zu integrieren, rollenbasierte Zertifizierungen einzuführen und eine nationale Zentralstelle für Cybersicherheitskompetenzen zu benennen. Mit einer kohärenten nationalen Strategie und nachhaltigen Investitionen kann Deutschland sicherstellen, dass seine Cybersicherheitsfachkräfte zu einem wichtigen Faktor für digitale Souveränität, Innovation und wirtschaftliche Widerstandsfähigkeit werden.

Unsere Empfehlungen im Detail

1. **Anforderungen an Schulungen zur Cybersicherheit und rollenbezogene Kompetenzstandards präzisieren und mit Verweisen auf einschlägige Standards hinterlegen, um den Begriff „ausreichende Kenntnisse und Fähigkeiten" eindeutig zu definieren.**

Die §38 und §43 des aktuellen Regierungsentwurfs beziehen sich auf „ausreichende Kenntnisse und Fähigkeiten", die Akteure der Verwaltung und des privaten Sektors gewährleisten müssen.

Wir sind der Ansicht, dass dieser Verweis angesichts der aktuellen Bedrohungen für die Cybersicherheit unklar und unzureichend ist.

Die Paragraphen sollten folgenden Wortlaut enthalten:

> *Schulungs- und Zertifizierungsprogramme für Cybersicherheit sollten rollenspezifisch sein, sich am Europäischen Qualifikationsrahmen für Cybersicherheit (ECSF) orientieren und auf weltweit anerkannten Bewertungssystemen basieren.*

Der deutsche NIS2-Entwurf muss die von der ENISA entwickelten Kriterien berücksichtigen, um eine ausreichende Anzahl an Fachkräften aufzubauen, die die nationale Sicherheit stärken und zu einem florierenden Cybersicherheitssektor in Deutschland beitragen können.

[5] Siehe Artikel 7 der Richtlinie (EU) 2022/2555 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1754901247047)

Wir empfehlen außerdem, einen entsprechenden Verweis in §30 des Regierungsentwurfs aufzunehmen. Bislang fehlt ein solcher Verweis in diesem Artikel.

Begründung:

Europäische Frameworks liefern bereits belastbare Referenzen. Die ENISA präzisiert durch die Abbildung des ECSF die Anforderungen der NIS-2-Richtlinie, welche Cybersicherheitsrollen zur Erfüllung der Vorgaben erforderlich sind; dies wird im Dokument „Cybersecurity Roles and Skills for NIS2 Essential and Important Entities"[6] dargelegt.

ISC2 fordert die politischen Entscheidungsträger dazu auf, Institutionen zu verpflichten, dass sie berufliche Qualifikationen verwenden, die mit weltweit anerkannten Standards wie ISO/IEC 17024 übereinstimmen, um sicherzustellen, dass Personen, die diese Rollen ausüben, über die erforderlichen Kompetenzen verfügen.

Eine unzureichende Klarstellung in den oben genannten Absätzen birgt das Risiko, dass unterschiedliche Definitionen von Kompetenzen zur Anwendung kommen. Cyberkriminelle wissen, wie sie systemische Lücken ausnutzen können.

ISC2 betont, dass Schulungen gezielt auf ihre spezifische Cybersicherheitskompetenzen ausgerichtet und auf ihre Wirksamkeit überprüft werden sollten, beispielsweise durch berufliche Qualifikationen. Wir sprechen uns für einen klaren Paradigmenwechsel im Entwurf aus: weg von anwendungsspezifischen Vorgaben, hin zu eindeutig definierten, kompetenzbasierten Anforderungen.

Eine solche Verankerung in kompetenzspezifischen Prinzipien und Fähigkeiten bietet weitreichende Vorteile, da sie auf viele Situationen anwendbar sind und nicht nur auf bestimmte Szenarien und Anwendungsbereiche beschränkt sind. Cybersicherheitsexperten mit beruflichen Qualifikationen weisen nicht nur nach, dass sie über die erforderlichen Kompetenzen verfügen, sondern sind auch verpflichtet, ihre Kompetenzen kontinuierlich zu aktualisieren, um in einem sich schnell entwickelnden Sektor relevant zu bleiben.

Auf diese Weise können Institutionen und Regulierungsbehörden die Angemessenheit von Schulungen anhand klar definierter Wissens- und Kompetenzkriterien bewerten. Die Verwendung von Qualifikationen, die den ECSF-Rollen entsprechen, ermöglicht vergleichbare Standards über Sektoren und Mitgliedstaaten hinweg – was für eine harmonisierte Anwendung der NIS-2-Richtlinie und die EU-weite Cyberresilienz und Mobilität qualifizierter Cybersicherheitsfachkräfte von entscheidender Bedeutung ist.

2. Aufnahme eines Artikels, der eine spezielle nationale Cybersicherheitsstrategie gemäß Artikel 7 der EU-NIS-2-Richtlinie fordert

Dem derzeitigen Cybersicherheitsansatz Deutschlands fehlt ein einheitlicher Rahmen zur Koordinierung von Politik, Investitionen und Personalentwicklung über alle Sektoren hinweg. Ohne eine kohärente und kollektive Strategie bleiben die Bemühungen fragmentiert, reaktiv und sind nicht in der Lage, mit der Geschwindigkeit und dem Ausmaß der sich entwickelnden Bedrohungen Schritt zu halten. Eine aktualisierte nationale Cybersicherheitsstrategie[7] – mit klaren Zielen, abgestimmt auf europäische Standards und entwickelt unter breiter Einbeziehung der Interessengruppen – würde den notwendigen Bezugspunkt für konsequentes Handeln bieten und sicherstellen, dass die Umsetzung der NIS-2-Richtlinie zu einer dauerhaften Widerstandsfähigkeit führt.

Laut einem vertraulichen Bericht des Bundesrechnungshofs, der im Juli durchgesickert ist, wurde die Cybersicherheitsstrategie 2021 nie als geeigneter Rahmen für Maßnahmen genutzt. Eine Aktualisierung war

[6] Siehe von der ENISA entwickelte Rollen und Kompetenzen im Bereich Cybersicherheit (https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities)
[7] Siehe „Cybersicherheitsstrategie für Deutschland" (https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=3)

während der vergangenen Legislaturperiode geplant, wurde jedoch aufgrund des Regierungswechsels auf Eis gelegt.

Die Umsetzung der NIS-2-Richtlinie ist die richtige Gelegenheit, um den Prozess des Umdenkens in der Cybersicherheitsstrategie in Deutschland grundlegend in Gang zu setzen.

Wir empfehlen, einen Artikel über die Aktualisierung einer nationalen Cybersicherheitsstrategie aufzunehmen:

Die Bundesregierung entwickelt bis 2027 eine aktualisierte nationale Cybersicherheitsstrategie, die strategische Ziele und politische Maßnahmen zur Stärkung der Cybersicherheit in allen Sektoren definiert, mit besonderem Schwerpunkt auf dem Aufbau von Cybersicherheitskapazitäten und der nationalen Fachkräfteentwicklung.

Begründung

Was sollten die wichtigsten Prioritäten der neuen nationalen Cybersicherheitsstrategie Deutschlands sein?

- **Stärkung und Ausbau der Cybersicherheitsfachkräfte:**

    - Die Professionalisierung der Fachkräfte im Bereich Cybersicherheit sollte ein vorrangiges Thema in der Bildungs-, Arbeits- und Sozialpolitik sein, das über den Bereich der Digitalisierung und Sicherheit hinausgeht. Nur so können die Kompetenzen den gesellschaftlichen Herausforderungen in dem erforderlichen Umfang gerecht werden.

    - Ausbildungs- und Schulungseinrichtungen (z. B. die Bundesagentur für Arbeit) sollten mit der Wirtschaft zusammenarbeiten, um relevante Cybersicherheitsprogramme und -qualifikationen anzubieten.

    - Die Angleichung an rollenbasierten Qualifikationen des ECSF in den Einstellungsrahmen des öffentlichen Dienstes (TVöD), in den Lehrplänen von Hochschulen und Berufsschulen sowie in der Personalpolitik des privaten Sektors international anerkannte an qualifizierte Fachkräften für die Cybersicherheit sicher.

    - Die Angleichung an die ECSF-rollenbasierten Qualifikationen in Einstellungsrahmen des öffentlichen Dienstes (TVöD), in universitären und beruflichen Lehrplänen sowie in Personalstrategien der Privatwirtschaft wird eine international anerkannte und qualifizierte Cybersicherheitsarbeitskraft sicherstellen.

    - Öffentliche Mittel sollten zweckgebunden eingesetzt werden, um Unternehmen - insbesondere dem Mittelstand - den Aufbau von Cybersicherheitskompetenzen zu ermöglichen. Der Schwerpunkt sollte auf spezialisierten Funktionen sowie auf der Weiterqualifizierung und Ausbildung in Einstiegspositionen liegen, um eine solide Grundlage an Fachkräften aufzubauen.

- **Deutschland zur führenden Nation in der globalen Cyberdiplomatie und der internationalen Mobilität von Arbeitskräften machen**

    - **Deutschland sollte die Aktualisierung der Nationalen Cybersicherheitsstrategie nutzen, um seine internationale Rolle in der Cybersicherheit grundlegend neu auszurichten.** Wir empfehlen, dass Deutschland eine führende Rolle übernimmt: Aufbauend auf seiner Innovationskraft sollte es sein internationales Engagement ausweiten, um zum

Vorreiter in der Cybersicherheit zu werden. Deutschlands weltweit führende Unternehmen in der Fertigungsindustrie, der Verteidigungsindustrie, der Automobilwirtschaft und im Finanzsektor sind in globale Lieferketten eingebettet. Ein aktives internationales Engagement ermöglicht es, die Resilienz dieser Lieferketten auf ein höheres Mindestniveau zu heben und damit heimische Unternehmen, Kritische Infrastrukturen sowie globale Partner zu schützen. Zugleich kann Deutschland seine Rolle als standardsetzende Gestaltungsmacht in der Cybersicherheit ausbauen, die Nachfrage nach deutschen Cybersecurityprodukten und -dienstleistungen steigern und deren Positionierung als vertrauenswürdige globale Anbieter stärken.

- **Deutschland sollte den Beitritt zur „International Coalition on Cyber Security Workforce" der britischen Regierung[8] in Betracht ziehen**, die bereits vom Canadian Centre for Cyber Security (Kanada), dem Dubai Electronic Security Centre (Regierung von Dubai), der Cyber Security Authority (Ghana), dem National Centre of Incident Readiness and Strategy for Cybersecurity (Japan), der Cyber Security Agency of Singapore (Singapur) und dem Department for Science, Innovation and Technology (Vereinigtes Königreich) unterstützt wird. Da die Koalition die Entwicklung von Arbeitskräften und die Professionalisierung des Sektors diskutieren will, könnte Deutschland die Bedürfnisse deutscher Unternehmen vermitteln und so im Ausland ausgebildeten Cybersicherheitsspezialisten eine schnelle Integration in den deutschen Markt ermöglichen. Dies würde wiederum die Wettbewerbsfähigkeit steigern, die Widerstandsfähigkeit der Lieferkette stärken und Deutschlands Bereitschaft signalisieren, ein globaler Knotenpunkt für Exzellenz im Bereich Cybersicherheit zu sein. Engagierte internationale Maßnahmen zur Entwicklung von Arbeitskräften könnten Deutschlands Ansehen unter seinen Verteidigungs- und Sicherheitsverbündeten stärken.

- **Deutschland sollte bilaterale und multilaterale Handelsverhandlungen nutzen, um die gegenseitige Anerkennung von Qualifikationsrahmen für deutsche Cybersicherheitsexperten zu fördern** und so seine Cybersicherheitsprodukte und -dienstleistungen regional und global zu vermarkten. Dies stärkt den Ruf Deutschlands als proaktive Cybermacht, die Wirtschaftswachstum mit digitaler Sicherheit verbindet.

Über ISC2

ISC2 ist die weltweit größte Non-Profit-Organisation für zertifizierte Cybersicherheitsfachkräfte mit über 265.000 Mitgliedern – darunter 60.000 in Europa und 4.600 in Deutschland. Unsere international anerkannten Zertifizierungen sind ISO/IEC 17024-akkreditiert und eng mit dem EU Cybersecurity Skills Framework (ECSF) verknüpft. Mit Programmen wie der Beteiligung an der EU Cyber Skills Academy, die 20.000 Menschen in Europa den kostenfreien Einstieg in die Cybersicherheit ermöglicht, setzen wir uns gezielt für die Förderung von Kompetenzen ein. Unsere Mitglieder sind zertifizierte Cybersicherheitsexperten, die für den Schutz unserer Regierungen, Volkswirtschaften, kritischen Infrastrukturen und persönlichen Daten verantwortlich sind.

[8] Siehe „Gemeinsame Erklärung: Internationale Koalition für Cybersicherheitskräfte" (https://www.gov.uk/government/publications/international-coalition-on-cyber-security-workforces/joint-statement-international-coalition-on-cyber-security-workforces)