Stellungnahme: Gesetzentwurf des Bundesministeriums des Innern zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Widerstandsfähigkeit kritischer Einrichtungen

Eine Chance, die Widerstandsfähigkeit kritischer nationaler Infrastrukturen durch qualifizierte Arbeitskräfte 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 Rezilienz und der nationalen Sicherheit Deutschlands.

Deutschland ist seit Jahren Ziel von hybrider Einflussnahme durch staatliche und nichtstaatliche Akteure. Hybride Bedrohungen umfassen den kombinierten Einsatz verschiedener Mittel wie Cyberangriffe, gezielte Propaganda und Desinformation, Sabotage, Spionage, Angriffe auf kritische Infrastrukturen, wirtschaftlicher Druck und Migration.[1] Gleichzeitig ist Deutschland aufgrund des allgemeinen Arbeitskräftemangels und des Mangels an Fachkräften weiterhin einem hohen Risiko für Cyberkriminalität ausgesetzt. Tatsächlich hat die ISC2-Studie „Cybersecurity Workforce Study 2024" einen Mangel an 120.000 Fachkräften im Bereich Cybersicherheit in Deutschland festgestellt.[2]

Das KRITIS-Dachgesetz ist ein wesentlicher Bestandteil der gesellschaftlichen Resilienz, der Modernisierung der Infrastruktur und der gezielten Fachkräfteentwicklung. ISC2 begrüßt die Initiative der deutschen Regierung und den aktuellen Regierungsentwurf. Wir möchten betonen, wie wichtig **eine größtmögliche Kohärenz mit der Umsetzung der NIS-2-Richtlinie ist.**

Daher empfehlen wir:

- **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.[3] ISC2 empfiehlt, **bestehende Strukturen für rollenbasierte Schulungen und Zertifizierungen wie das European Cyber Security Skills Framework (ECSF) der ENISA[4] 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.

[1] Siehe Bundesministerium der Verteidigung „Was sind hybride Bedrohungen?" (https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen/was-sind-hybride-bedrohungen--13692)
[2] Siehe ISC2-Studie zur Cybersicherheitsbelegschaft 2024 (https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study)
[3] Siehe ISC2-Studie zur Cybersicherheitsbelegschaft 2024 (https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study)
[4] 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)

Bewertung des Regierungsentwurfs durch ISC2:

Angesichts der zunehmenden Anzahl, Komplexität und des Ausmaßes hybrider Angriffe in Deutschland ist die zeitnahe Umsetzung des KRITIS-Dachgesetzes von entscheidender Bedeutung. ISC2 unterstützt den allgemeinen Ansatz im Entwurf der Bundesregierung, ist jedoch der Ansicht, dass wichtige Aspekte der Resilienz übersehen werden.

Um sicherzustellen, dass die Umsetzung des KRITIS-Dachgesetzes in Deutschland wirksam ist, empfehlen wir, die folgenden Aspekte zu berücksichtigen:

- Wir empfehlen, den Gesetzesentwurf zu verschärfen, indem **kritische Einrichtungen verpflichtet werden, nachzuweisen, dass sie über qualifizierte Fachkräfte verfügen und international anerkannte Standards für die Validierung und Entwicklung von Cybersicherheitskompetenz anwenden.**

    - Eine klare Bezugnahme auf diese Anforderungen, wie in Artikel 13 der Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (CER) gefordert, würde den Weg zu einem klareren Verständnis der für bestimmte Funktionen erforderlichen Fähigkeiten ebnen. Außerdem würde dies eine reibungslose Integration mit den Bestimmungen zu „Ausbildung und Fähigkeiten" der NIS-2-Richtlinie ermöglichen. Als Beispiel für einen rollenbasierten Ansatz möchten wir die politischen Entscheidungsträger, auf den von der ENISA definierte European Cybersecurity Skills Framework (ECSF) verweisen.

- **Wir empfehlen, die den Gesetzesentwurf in Verbindung mit der nationalen Cybersicherheitsstrategie vorzunehmen.**

    - Wir begrüßen zwar die Kooperationsklausel, doch reicht es nicht aus, die intrinsische Verbindung zwischen Cyber- und physischen Dimensionen nur auf operativer Ebene anzuerkennen. Erforderlich ist eine strategische Verankerung – einschließlich eines einheitlichen, national kohärenten Ansatzes für den Aufbau und die **Weiterentwicklung der Sicherheits- und Cybersicherheitsfachkräfte** sowie ihrer Kompetenzen **in Deutschland**.

Insgesamt muss die Umsetzung des KRITIS-Dachgesetzes in Deutschland über die Infrastruktur und die Reaktion auf Vorfälle hinausgehen und sich mit der grundlegenden Frage der Sicherheitskapazitäten befassen – den Menschen und Fähigkeiten hinter den Systemen und Prozessen. Mit einer kohärenten nationalen Strategie und nachhaltigen Investitionen kann Deutschland sicherstellen, dass seine Cybersicherheit und sein Sicherheitspersonal zu einem wichtigen Faktor für digitale Souveränität, Innovation und wirtschaftliche Widerstandsfähigkeit werden.

Unsere Empfehlungen im Detail

1. **Vollständige Umsetzung von Artikel 13 Absatz 1 Buchstabe f der EU-CER-Richtlinie, der kritische Einrichtungen verpflichtet, angemessene Ausbildungsanforderungen und Qualifikationen festzulegen.**

Paragraf 13 Absatz 3 Nummer 5 des aktuellen Entwurfs verlangt lediglich ein **„angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeitenden zu gewährleisten, einschließlich des Personals externer Dienstleister",** was die Gefahr einer uneinheitlichen Bewertung und Entwicklung von Cybersicherheitskompetenzen birgt. Um einheitliche Standards zu gewährleisten und den Cybersicherheitssektor

zu professionalisieren, empfehlen wir die Verwendung einer **klaren, kompetenzspezifischen Definition,** die einerseits einen **klaren Rahmen** bietet, aber auch **Flexibilität zum Lernen und Anpassen** lässt**.**

Punkt 5 sollte folgenden Wortlaut haben:

[...] ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeitenden zu gewährleisten, einschließlich des Personals externer Dienstleister, ***und die Festlegung angemessener Schulungsanforderungen und Qualifikationen.***

Begründung:

Der Entwurf hält hilfreich fest, dass für Betreiber, die sowohl das KRITIS-Dachgesetz als auch das NIS2UmsuCG einhalten, Systeme nach einem Allgefahrenansatz entwickelt werden sollten, der gleichzeitig die Widerstandsfähigkeit von IT-Systemen und physischen Komponenten berücksichtigt. Ein kompetenzbasierter Ansatz sollte für beide Gesetze gelten, da Betreiber wahrscheinlich Risikomanagementmaßnahmen als Teil eines einzigen Systems umsetzen werden, einschließlich Schulungen und Kompetenzentwicklung.

Wir empfehlen dringend einen Mentalitätswandel von anwendungsspezifischen Anforderungen hin zu kompetenzspezifischen Fähigkeiten. Ein solcher kompetenzbasierter Ansatz steht nicht im Widerspruch zu künftigen sektorspezifischen Resilienzstandards, da der Schwerpunkt auf relevanten Kenntnissen und Fähigkeiten liegt, die kalibriert werden können.

Aus der Perspektive der in der NIS-2-Richtlinie genannten Cybersicherheitsschulungen bieten internationale und europäische Frameworks bereits eine Referenz. Die ENISA bietet durch ihre Zuordnung des ECSF zu den Anforderungen der NIS-2-Richtlinie Klarheit, wie im Dokument „Cybersecurity Roles and Skills for NIS2 Essential and Important Entities" dargelegt. Darin werden die Cybersicherheitsrollen beschrieben, die zur Erfüllung der Anforderungen der NIS-2-Richtlinie erforderlich sind. 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.

ISC2 betont, dass Schulungen spezifische Kompetenzen behandeln und auf ihre Wirksamkeit überprüft, werden sollten, beispielsweise durch berufliche Qualifikationen. ISC2 fordert die politischen Entscheidungsträger dazu auf, Wirtschaft und Verwaltung 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.

2. Die Aktualisierung des KRITIS-Dachgesetz sollte in Verbindung mit der nationalen Cybersicherheitsstrategie erfolgen

Wir begrüßen die Verpflichtung der Regierung, die nationale Strategie zum Schutz kritischer Infrastrukturen von 2009 zu aktualisieren und zu erweitern.[5] Ohne eine kohärente und gemeinsame 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. Im Interesse der Kohärenz und Effizienz sollte die

[5] Siehe Bundesministerium des Innern „Nationale Strategie zum Schutz Kritischer Infrastrukturen" (https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI09324-kritis-strategie.html)

nationale KRITIS-Resilienzstrategie in Abstimmung und parallel zur nationalen Cybersicherheitsstrategie konzipiert werden, wie dies bereits in Artikel 7 der NIS-2-Richtlinie vorgeschrieben ist.[6]

Eine aktualisierte, übergreifende nationale Cybersicherheitsstrategie, die auf klaren Zielen basiert, mit europäischen Standards im Einklang steht und unter breiter Einbeziehung der Interessengruppen entwickelt wurde, würde den notwendigen Bezugspunkt für kohärentes Handeln bieten und sicherstellen, dass die Umsetzung der NIS-2-Richtlinie und des KRITIS-Dachgesetz zu einer dauerhaften Widerstandsfähigkeit führt.

Dies wird dazu beitragen, **strategische Ziele und politische Maßnahmen** zur Stärkung der IT- und physischen Sicherheit in kritischen Sektoren zu definieren, wobei ein besonderer Schwerpunkt auf **dem Aufbau von Kapazitäten und der nationalen Talentförderung** liegt**.**

Wie könnte dieser strategische Ansatz aussehen?

- Die Professionalisierung der Cybersicherheits- und Sicherheitsfachkräfte sollte als prioritäres Querschnittsthema in der Bildungs-, Arbeitsmarkt- und Sozialpolitik verankert werden – über die reine Digital- und Sicherheitspolitik hinaus.

- Ausbildungsanbieter (z. B. die Bundesagentur für Arbeit) sollten mit der Wirtschaft zusammenarbeiten, um relevante Programme und Qualifikationen anzubieten.

- Die Angleichung an die 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 wird international anerkannte und qualifizierte Fachkräfte im Bereich Cybersicherheit sichern.

- Öffentliche Mittel sollten zweckgebunden eingesetzt werden, um Organisationen, insbesondere kleinen und mittleren Unternehmen, den Aufbau von Cybersicherheitskompetenzen zu ermöglichen. Der Schwerpunkt sollte auf spezialisierten Funktionen sowie auf der Weiterqualifizierung und Ausbildung in Einstiegspositionen liegen, um eine solide Talentbasis aufzubauen.

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 die 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.

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