Positionspapier zur Umsetzung der NIS-2 Richtlinie

Sehr geehrte Damen und Herren,

Vielen Dank für die Möglichkeit einer Teilnahme an der Verbändeanhörung zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. ISC2 begrüßt den **jüngsten Referentenentwurfs des Bundesministeriums für Inneres und Heimat zur Umsetzung der NIS-2-Richtlinie ein** und ist der Ansicht, dass dieser durch klarere Beschreibungen des Bedarfs an Cybersicherheits-Know-how und Fachkräften verstärkt werden könnte. **ISC2** würde die Gelegenheit begrüßen, mit deutschen Behörden zusammenzuarbeiten, um deutsche Fachkräfte im Bereich der Cybersicherheit zu stärken.

Der aktuelle Gesetzentwurf erkennt den steigenden Bedarf an Cybersecurity-Fachkräften an und enthält bereits mehrere Passagen, in denen die Abhängigkeit von der Qualifikation deutlich wird. **Die Lücke zwischen der Nachfrage nach Cybersicherheitsspezialisten und den verfügbaren Arbeitskräften zu schließen, ist zwingend notwendig.** Es ist von entscheidender Bedeutung, Cyberfachkräfte in Deutschland zu ermutigen, die für die Einhaltung der NIS-2-Richtlinie erforderlichen spezifischen Fähigkeiten zu erwerben, was konzertierte politische Bemühungen erfordert.

ISC2 schlägt daher folgende Änderungen am Gesetzentwurf vor:

- Wir empfehlen einen **nationalen Cybersecurity-Aktionsplan** für Fachkräfte in Deutschland. Ein solcher Aktionsplan sollte sich an bestehenden Programmen in Frankreich[1] oder den Niederlanden[2] orientieren. Wir sind der Meinung, dass diese Initiativen als Beispiel für einen deutschen Cybersecurity Workforce Action Plan dienen könnten, der in einer konzertierten Aktion unter Federführung des Bundesministeriums für Arbeit, des Bundesministeriums für Inneres und Heimat und des Bundesministeriums für Digitales und Verkehr entwickelt werden sollte. Darüber hinaus sollten Strategien entwickelt werden, um die Mobilität der Arbeitskräfte zu verbessern und Cybersecurity-Kompetenzen zu fördern, in engem Dialog mit anderen europäischen Ländern.

- Um die Arbeitskräfte- und Qualifikationslücken zu verkleinern, fordern wir die Bundesregierung auf, **öffentlich-private Partnerschaften auszubauen**, die dazu beitragen, die Finanzierung zu sichern und die Entwicklung von Arbeitskräften voranzutreiben, und gleichzeitig solche Initiativen so zu koordinieren, dass sie in Synergie mit den Finanzierungsmöglichkeiten von EU-Programmen wie „Digital Europe“ arbeiten. Während die Cyberagentur ein gutes Beispiel für eine öffentlich koordinierte Anstrengung ist, würden wir empfehlen, dass eine solche Organisation als „One-Stop-Shop“ für die Koordinierung der Ausbildung, Weiterbildung und Koordination von Arbeitskräften innerhalb Deutschlands dienen könnte.

- Darüber hinaus würden wir die **Zusammenarbeit mit internationalen Zertifizierungsstellen fördern.** Dies könnte den bürokratischen Aufwand verringern, das Angebot erweitern, die Interoperabilität zwischen den EU-Mitgliedstaaten erleichtern und den Zugang zu den internationalen Märkten für Cybersicherheit verbessern.

- **Wir empfehlen, dass die Anerkennung von Personenzertifizierungen zwischen den nationalen Rechtsordnungen harmonisiert wird.** Da es sich bei Cybersicherheitsexperten oft um hochqualifizierte Arbeitskräfte handelt, sind wir der Meinung, dass ein rein nationaler Ansatz nicht ausreichen würde, um die Fachkräftelücke zu schließen. Deutschland sollte seine

[1] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

[2] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028#:~:text=People%20and%20businesses%20should%20be,of%20digital%20products%20and%20connections.

Cyber-Fachkräfte mit europäischen Partnern abstimmen und Tools wie das European Cybersecurity Framework (ECSF) stärker nutzen.

- Im Rahmen seiner Verpflichtungen gemäß Abschnitt 3 besteht für das BSI bzw. Deutschland die Möglichkeit, innerhalb der in Artikel 14 der NIS-2-Richtlinie eingerichteten Kooperationsgruppe eine Führungsrolle zu übernehmen, von der erwartet wird, dass sie *„bewährte Praktiken im Zusammenhang mit der Umsetzung dieser Richtlinie, auch in Bezug auf Fähigkeiten und Kapazitätsaufbau, austauscht"*, indem es **die Rolle des Informationssicherheitskoordinators wirksam stärkt**. In Deutschland könnte dies durch eine Stärkung der Rolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Bundesministerium des Innern und Heimat erreicht werden.

- In Deutschland gibt es einen Mangel an Reaktion auf Cybersicherheitsvorfälle. Während der bestehende Gesetzesentwurf den Schwerpunkt auf die Prävention legt, ist die Fähigkeit und Kapazität zur Reaktion auf Vorfälle eine Grundlage für die nationale Cyber-Resilienz und reduziert die Auswirkungen von Cyber-Vorfällen. **Wir sind der Meinung, dass verbesserte Meldeverfahren mit einem Schwerpunkt auf dem Aufbau von Fähigkeiten zur Reaktion auf Vorfälle einhergehen sollten.** Dies sollte nicht nur für Einrichtungen der kritischen Infrastruktur gelten, sondern auch für Unternehmen. Das „Assured Cyber Incident Response"-Programm[3] des britischen National Cyber Security Centre ist ein Beispiel dafür, wie die Regierung diese Branche fördern und stärken kann.

- Eine weitere Option könnte darin bestehen, den **Umfang der vom BSI angebotenen Personenzertifizierungen zu erweitern oder zu replizieren**, um die zur Erfüllung der NIS-2 erforderlichen Aufgaben (Abschnitt 54), insbesondere das Risikomanagement, zu berücksichtigen und die wachsende Nachfrage nach qualifizierten Fachkräften im öffentlichen Dienst und in kritischen Infrastrukturen zu decken.

ISC2 ist der Ansicht, dass diese Änderungen an der Gesetzgebung notwendig und ein wichtiger Schritt in die richtige Richtung sind, um sicherzustellen, dass die Umsetzung der NIS-2-Richtlinie ihr Ziel erreicht, Deutschland zukunftssicher und widerstandsfähig gegen die heutigen Herausforderungen im Bereich Cybersicherheit zu machen. ISC2 freut sich auf die Gelegenheit, mit den deutschen Behörden zusammenzuarbeiten, um die deutschen Cybersicherheitsfachkräfte zu stärken, was letztendlich zu mehr cybersicheren Produkten und besser geschützten Verbrauchern führen wird.

Über ISC2

ISC2 ist die weltweit größte gemeinnützige Organisation von zertifizierten Cybersicherheitsexperten. Wir haben fast 650.000 Mitglieder, Partner und Kandidaten weltweit und über 60.000 in der EU. Unsere Mitglieder sind zertifizierte Cybersicherheitsexperten, die für den Schutz unserer Regierungen, Volkswirtschaften, kritischen Infrastrukturen und persönlichen Daten verantwortlich sind.

Kontakt

Edward Parsons

Vice President Global Markets and Member Relations

eparsons@isc2.org

+44 2030531575

[3] https://www.ncsc.gov.uk/schemes/cyber-incident-response#:~:text=is%20it%20for%3F-,What%20is%20the%20NCSC%20assured%20Cyber%20Incident%20Response%20scheme%3F,victim%20of%20a%20cyber%20attack.