HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Originaltext auf Englisch finden Sie in folgendem Dokument:

“Horizon Europe Work Programme 2025: Civil Security for Society“
14. Mai 2025 herausgegeben vom ECCC / EU-Kommission

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en?prefLang=de

Förderbereich: Increased Cybersecurity

Förderthema: HORIZON-CL3-2025-02-ECCC-02: New advanced tools and processes for Operational Cybersecurity

Seiten: 95-98

Deutsche Übersetzung des Förderthemas durch das NKCS/ NCC-DE als unterstützendes Informationsangebot erstellt:

HORIZON-CL3-2025-02-ECCC-02: Neue Werkzeuge und Prozesse für die operative Cybersicherheit

Erwartete Auswirkungen

Vom ECCC eingeleitete Aktion zur Aufnahme der im Abschnitt "Ziel - Erhöhte Cybersicherheit" dieses Teils des Arbeitsprogramms dargelegten Formulierung "erwartete Auswirkungen".

Erwartete Ergebnisse

Die Nutzung von und die Abhängigkeit von Informations- und Kommunikationstechnologien sind zu grundlegenden Aspekten in allen Bereichen der Wirtschaft geworden. Öffentliche Verwaltungen, Unternehmen und Bürger sind über Sektoren und Grenzen hinweg stärker vernetzt und voneinander abhängig als je zuvor. Diese stärkere Nutzung digitaler Technologien erhöht die Anfälligkeit für Cybersicherheitsvorfälle, Schwachstellen und deren mögliche Auswirkungen. Gleichzeitig sehen sich die Mitgliedstaaten mit wachsenden Cybersicherheitsrisiken und einer insgesamt komplexen Bedrohungslandschaft konfrontiert, wobei das Risiko eines schnellen Übergreifens von Cybervorfällen von einem Mitgliedstaat auf andere besteht.

Darüber hinaus werden Cyber-Operationen zunehmend in hybride und kriegerische Strategien integriert, mit erheblichen Auswirkungen auf das Ziel. Insbesondere der aktuelle geopolitische Kontext wird von einer Strategie feindlicher Cyberoperationen begleitet, was die Wahrnehmung und Bewertung der kollektiven Cybersecurity-Krisenmanagement-Bereitschaft der EU grundlegend verändert und dringenden Handlungsbedarf erfordert. Die Bedrohung durch einen möglichen groß

angelegten Vorfall, der erhebliche Störungen und Schäden an kritischen Infrastrukturen und Datenräumen verursacht, erfordert eine erhöhte Bereitschaft auf allen Ebenen des Cybersicherheitsökosystems der EU. In den letzten Jahren hat die Zahl der Cyberangriffe dramatisch zugenommen, darunter auch Angriffe auf die Lieferkette, die auf Cyberspionage, Ransomware oder Unterbrechung abzielen. Auch die Schwachstellenlandschaft ist bedrohlich. Der ENISA Threat Landscape Report 2024 zählt insgesamt 19.754 Schwachstellen. Diese Menge an Schwachstellen kann nicht manuell von Menschen verwaltet werden. Es besteht ein Bedarf an einer automatisierten Verwaltung von Schwachstellen auf der Grundlage etablierter Standards wie dem Common Security Advisory Framework (CSAF) .

Was die Erkennung von Cyber-Bedrohungen und -Vorfällen angeht, so ist es dringend notwendig, den Informationsaustausch zu verstärken und unsere kollektiven Fähigkeiten zu verbessern, um die Zeit, die für die Erkennung von Cyber-Bedrohungen und die Schadensbegrenzung benötigt wird, drastisch zu verkürzen, bevor sie große Schäden und Kosten verursachen können. Obwohl viele Bedrohungen und Vorfälle im Bereich der Cybersicherheit eine potenziell grenzüberschreitende Dimension haben, ist der Austausch relevanter Informationen zwischen den Mitgliedstaaten aufgrund der Verflechtung digitaler Infrastrukturen nach wie vor begrenzt. Es wird erwartet, dass die Vorschläge diese neue Bedrohungslandschaft mit der Entwicklung von fortschrittlichen Rahmenwerken, Servicetools und Prozessen im Einklang mit der einschlägigen EU-Gesetzgebung (NIS2, Cyber Resilience Act, Cyber Solidarity Act) angehen.

Schließlich sollte der Schwerpunkt auf der Entwicklung innovativer Rahmen, Technologien, Werkzeuge, Prozesse und Dienste liegen, die die Cybersicherheitskapazitäten für die operative und technische Zusammenarbeit im Bereich der Cybersicherheit im Einklang mit der einschlägigen EU-Politik stärken, mit besonderem Schwerpunkt auf NIS2, dem Gesetz über die Cybersolidarität und der EU-Cybersicherheitsstrategie sowie den rechtlichen und ethischen Anforderungen.

Die Vorschläge sollten mindestens zwei der folgenden erwarteten Ergebnisse ansprechen:

- Verbessertes Situationsbewusstsein durch fortschrittliche Cyber Threat Intelligence Frameworks, Tools und Dienstleistungen sowie Cybersecurity-Risikobewertungen von kritischen Lieferketten in der EU,

- Rahmenwerke, Werkzeuge und Dienste für die Abwehr von Cyber- und hybriden Bedrohungen in der Informations- und Kommunikationstechnologie (IKT) und der Betriebstechnologie (OT), einschließlich Übungen zur Cybersicherheit,

- Erweiterte Funktionalität des Security Operations Centre/Computer Security Incident Response Teams (SOC/CSIRT) durch fortschrittliche Tools und Dienste für die Erkennung, Analyse, Bearbeitung von Vorfällen, einschließlich Reaktion und Berichterstattung, sowie die Behebung von Problemen,

- Entwicklung von Test- und Versuchsanlagen für fortschrittliche Tools und Prozesse für die operative Cybersicherheit, einschließlich der Erstellung digitaler Zwillinge für kritische Infrastrukturen und wesentliche und wichtige Einrichtungen gemäß der Definition in NIS2,

- Entwicklung und Pilotimplementierung von sektor- und/oder grenzübergreifenden Rahmenwerken, Diensten und Instrumenten für das Cyber-Krisenmanagement,

- Rahmenwerke, Dienste und Instrumente, die auf Mechanismen und Prozesse für eine verstärkte operative Zusammenarbeit zwischen öffentlichen Stellen abzielen (CSIRT-Netzwerk, EU-

CyCLONe). Eine Ausweitung der oben genannten Maßnahmen auf wesentliche und wichtige Stellen, wie in der NIS2 definiert, wäre von Vorteil.

Umfang

Von den Vorschlägen wird erwartet, dass sie die entwickelten Rahmenwerke, Werkzeuge, Dienste und Prozesse durch Pilotimplementierungen demonstrieren, an denen die relevanten nationalen Cybersicherheitsbehörden und/oder wesentliche und wichtige Einrichtungen, wie in NIS2 definiert, beteiligt sind und die unter Beteiligung der führenden europäischen Cybersicherheitsbranche durchgeführt werden. Die Vorschläge sollten die Auswirkungen der bevorstehenden Gesetzgebung, insbesondere des Cyber Resilience Act, berücksichtigen.

Reale Anwendungen und die Benutzerfreundlichkeit der entwickelten Lösungen sollten bei den Vorschlägen im Vordergrund stehen.

Die Teilnahme der folgenden Arten von Unternehmen ist sehr erwünscht: innovative europäische Start-ups und KMUs mit einer nachgewiesenen Erfolgsbilanz im Bereich der Cybersicherheitsinnovation auf EU-Ebene (z.B. aktive Teilnahme an erfolgreichen EU-finanzierten Projekten, einschließlich Cybersicherheitsprojekten im Rahmen von Horizont Europa, Cybersicherheitsprojekten im Rahmen des Programms Digitales Europa oder EIC Pathfinder- oder Accelerator-Projekten), europäische Start-ups und KMU, die eine etablierte operative Zusammenarbeit mit den zuständigen nationalen Cybersicherheitsbehörden nachweisen können, europäische Start-ups und KMU, die Kapitalbeteiligungen von nationalen, europäischen oder privaten Risikokapitalfonds für Cybersicherheitsaktivitäten erhalten haben usw. Die Teilnahme dieser Start-ups und KMU mit einer aktiven Rolle bei der Umsetzung der vorgeschlagenen Maßnahme (Projektkoordinierung, technische Koordinierung, Leitung der Pilotimplementierung usw.) würde als Vorteil betrachtet werden.

Art der Maßnahme	Innovation Actions
Vorläufiges Budget	*23,55 Mio. EUR*
Vorläufiges Budget pro Projekt	*4,5-6 Mio. EUR*
Zuwendungsberechtigt	Rechtsträger mit Sitz in EU-Mitgliedstaaten und assoziierten Länder, die nicht direkt oder indirekt von Drittländern kontrolliert werden
Technologiereifegrad	Projektstart mindestens TRL 4, Projektende mindestens TRL 7
Abrechnung	Förderfähige Kosten werden als Lump Sums (Pauschalbeträge) gewährt
Sicherheit	Einige Aktivitäten, die sich aus diesem Thema ergeben, können die Verwendung von als Verschlusssache eingestuften Hintergrundinformationen und/oder die Erstellung von sicherheitsempfindlichen Ergebnissen (EU-Verschlusssachen und SEN) beinhalten. Bitte beachten Sie die entsprechenden Bestimmungen in Abschnitt B Sicherheit - EU-Verschlusssachen und sensible Informationen der Allgemeinen Anhänge.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Das **Nationale Koordinierungszentrum für Cybersicherheit (NKCS/ NCC-DE)**

berät zu **EU-Fördermöglichkeiten in der Cybersicherheit**

und hilft bei der **Vernetzung mit EU-Partnern**.

Sie erreichen uns unter **nkcs@bsi.bund.de**