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:

“Digital Europe Cybersecurity Work Programme 2025-2027“
Version 1, März 2025 herausgegeben vom ECCC

https://cybersecurity-centre.europa.eu/document/8af166e1-69c5-4ccd-b38f-5a3ffe43ad73_en

Förderbereich:	Cyber Solidarity Act implementation – European Cybersecurity Alert System
Förderthema:	2.7 National Cyber Hubs
Seiten:	37-41

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

2.7 National Cyber Hubs

Ein Mitgliedsstaat, der sich entscheidet, am European Cybersecurity Alert System teilzunehmen, soll ein National Cyber Hub benennen bzw. errichten. Dieses soll als eigenständige Entität unter der Hoheit des jeweiligen Mitgliedsstaates operieren.

National Cyber Hubs agieren als Referenzpunkt und Zugangspunkt zu anderen öffentlichen und privaten Organisationen auf nationaler Ebene. Sie sammeln und analysieren Informationen über Cyberbedrohungen und -vorfälle und tragen diese auch einem Cross-Border Cyber Hub zu. Sie können Daten und Informationen zu relevanten Cyberbedrohungen und -vorfällen (wie CTI) erkennen, zusammenfassen und analysieren und nutzen hierzu topmoderne Technologien mit dem Ziel, Vorfälle zu verhindern.

Wie bereits erwähnt, wird für den folgenden Programmzyklus der Fokus auf der Fortsetzung von Maßnahmen liegen, die bereits in den vergangenen Jahren initiiert wurden.

2.7.1 Ziele

Ziel ist die Errichtung oder Stärkung von National Cyber Hubs mit topmodernen Tools für das Monitoring, Verständnis und proaktive Management von Cybereereignissen, in enger Zusammenarbeit mit betroffenen Entitäten wie CSIRTs, ISACs, etc. Sofern möglich werden sie auch Informationen und Feeds anderer Ländern nutzen können, um die dort gesammelten Daten und Analysen in Form von Frühwarnungen auf need-to-know-Basis an betroffene kritische Infrastrukturen herauszugeben.

National Cyber Hubs könnten zudem die mögliche Überwachung unterseeischer Infrastruktur (wie Unterseekabel) hierbei vorausschauend mitbedenken.

2.7.2 Umfang (oder Anwendungsbereich)

Das Ziel ist es, in neuen oder bestehenden National Cyber Hubs Kapazitäten auszubauen, z.B. durch Ausrüstung, Tools und Datenfeeds sowie Kosten für die Datenanalyse, Kommunikation mit Cross-Border Cyber Hubs etc. Beispielsweise kann dies Automatisierungs-, Analyse- und Korrelationstools beinhalten oder CTI-Datenfeeds verschiedener Ebenen von Felddaten über SIEM-Daten bis hin zu höherstufig klassifizierter CTI.

Automatisierung ist ein Schlüsselaspekt bei der effizienten Datenverarbeitung und -handhabung. Wo möglich sollen etablierte Standards wie das Common Security Advisory Framework (CSAF) genutzt werden, um Sicherheitsratschläge oder um Nachrichten zum Thema Cybersicherheit zu sammeln und zu verarbeiten (vgl. z.B. das IntelMQ Projekt). Anwendungen die von Cyber Hubs 7 SOCs entwickelt wurden, sollten kompatibel zu europäischen Standardisierungsprojekten wie der europäischen Schwachstellendatenbank EU vulnerability database (EUVD) sein. Nationale Cyber Hubs sollten sich zudem topaktuelle Technologien wie künstliche Intelligenz und dynamisches Lernen zur Bedrohungslandschaft und deren Kontext zunutze machen. Dies schließt auch die Nutzung geteilter Cybersicherheitsinformationen mit ein, welche soweit wie möglich auf existierenden Taxonomien und / oder Strukturen basiert werden sollen, um einen sicheren Austausch und eine sichere Speicherung von Informationen zu gewährleisten. Die Maßnahmen sollten auf Live-Netzdaten und anderen Schulungsdaten aufbauen, die in der Anfangsphase benötigt werden. Sofern möglich sollten KMU als letztendliche Empfänger der operativen Cybersicherheitsinformationen in Betracht gezogen werden.

Ein Schlüsselelement ist die Umwandlung fortgeschrittener KI, Datenanalysen und anderen einschlägigen Cybersicherheitsinstrumenten von Forschungsergebnissen in funktionsfähige Instrumente sowie deren weitere Erprobung und Validierung unter realen Bedingungen in Verbindung mit dem Zugang zu Hochleistungsrechenanlagen (z. B. zur Verbesserung der Korrelations- und Erkennungsfunktionen von Cross-Border Plattformen). Solche Aktivitäten werden in Abschnitt 2.3, der sich mit KI für Cybersicherheit befasst, und in Punkt 2.3.1 genannt und zur Finanzierung vorgeschlagen.

Darüber hinaus könnten die nationalen Cyber Hubs auch den Einsatz von Lösungen für die Überwachung und den Schutz kritischer unterseeischer Infrastrukturen wie Unterseekabel und die Erkennung bösartiger Aktivitäten in deren Umfeld in Betracht ziehen, um die Widerstandsfähigkeit und Sicherheit dieser für die globale Kommunikation wichtigen Infrastruktur zu verbessern. Die Reaktion auf eine solche hybride Bedrohung könnte auch ein Situationsbewusstsein umfassen, das durch die Sammlung und Analyse von Sensordaten vor Ort auf See sowie von relevanten Satellitenbildern erfolgt. Für eine solche Tätigkeit sind operative Synergien mit dem Copernicus-

Weltraumprogramm der EU und insbesondere mit dessen Sicherheitsdienst erforderlich.

Eine weitere wichtige Aufgabe der nationalen Cyber Hubs ist die Erleichterung des Wissenstransfers und -austauschs sowie die Unterstützung von Schulungsinitiativen für alle erforderlichen Aufgaben im Bereich der Cybersicherheit, beispielsweise auf der Grundlage des Europäischen Qualifikationsrahmens für Cybersicherheit (ECSF). Beispielsweise haben die Cyber Hubs/SOCs, die sich mit kritischen Infrastrukturen befassen, eine Schlüsselrolle und sollten von dem Wissen und der Erfahrung, welche in den nationalen Cyber Hubs gesammelt wird, profitieren.

Nationale Cyber Hubs sind verpflichtet, Informationen mit anderen Akteuren in einem für alle Seiten vorteilhaften Informationsaustausch teilen und zudem innerhalb der nächsten zwei Jahre die Teilnahme an einem grenzüberschreitenden Cross-Border Cyber Hub zu beantragen, um Informationen mit anderen nationalen Cyber Hubs auszutauschen.

Um dieses Ziel zu erreichen, wird ein Aufruf zur Interessensbekundung veröffentlicht, um jeweils innerhab der Mitgliedstaaten Organisationen zu benennen, die die notwendige Befähigung für die Aufnahme und den Betrieb nationaler Cyber Hubs haben.

Bewerber, die sich an der Aufforderung zur Interessenbekundung beteiligen, sollten die Ziele und Zielvorgaben des nationalen Cyber Hubs darlegen, dessen Rolle und Verhältnis zu anderen Cybersecurity-Akteuren beschreiben sowie ggf. auf eventuelle Zusammenarbeit mit anderen öffentlichen oder privaten Cybersecurity Stakeholdern eingehen.

Zudem sollten Antragstellende folgendes darlegen:

- Detaillierter Plan zu den angedachten Maßnahmen und Aufgaben des nationalen Cyber Hubs
- Informationen zur Vorgehensweise und Operationalisierung, inklusive der Beschreibung der angedachten Dauer der jeweiligen Aktivitäten
- Hauptmeilensteine und -projektleistungen
- Informationen zu den geplanten angebotenen Dienstleistungen
- Informationen zu Ausrüstung, Werkzeugen und Dienstleistungen, die noch beschafft und integriert werden müssen, um das nationale Cyber Hub, dessen Dienstleistungen und Infrastruktur aufzubauen

Um die o.g. Aktivitäten eines Cross-Border Cyber Hubs zu fördern, sind die beiden folgenden Workstreams vorgesehen:

1. **[Procurement] Eine gemeinsame Beschaffungsmaßnahme**

   Eine gemeinsame Beschaffungsmaßnahme mit dem Mitgliedsstaat, welcher am Cross-Border Cyber Hub beteiligt ist: gefördert wird die Beschaffung von Infrastruktur, Tools und Dienstleistungen, welche für den Aufbau des Cross-Border Cyber Hubs notwendig sind.

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

2. **[Building up and running the Cross-Border Cyber Hub] Aufbau und Betrieb des Cross-Border Cyber Hubs**

   Zudem wird es folgende Förderungen geben:

   a) für die Vorbereitungen zur Einrichtung des nationalen Cyber Hubs, u.a.
      - für dessen Interaktion und Kooperation mit anderen Stakeholdern
      - sowie hierbei anfallende laufende (Betriebs-)Kosten
   b) um den effektiven Betrieb des nationalen Cyber Hubs zu ermöglichen, z.B.
      - die Nutzung von über Workstream 1 (gemeinsame Beschaffungsmaßnahme) erworbenen Infrastruktur-Tools und Dienstleistungen
      - Hierbei würden ebenfalls Meilensteine und Projektleistungen zur Fortschrittsanzeige benannt werden.

Bewerbungsanträge sollten für beide Workstreams gestellt werden. Bewerbungsanträge werden im Rahmen von Evaluierungsprozessen geprüft. Die Förderung wird ausschließlich für jene Anträge gewährt, für die zuvor die Evaluierung für die gemeinsame Beschaffungsmaßnahme erfolgreich verlaufen ist.

Diese Maßnahmen zielen auf die Errichtung oder Stärkung von nationalen Cyber Hubs, welche eine zentrale Rolle in der Gewährleistung der Cybersicherheit der nationalen Behörden, Anbieter kritischer Infrastrukturen und essentiellen Dienstleister einnehmen. Cyber Hubs sind (in Zusammenarbeit mit den anderen nationalen und regionalen Organisationen) damit beauftragt, Cybersicherheitsbedrohungen zu überwachen, verstehen und proaktiv zu managen. Cyber Hubs werden eine entscheidende Rolle in der Gewährleistung der Cybersicherheit in der EU spielen und werden sensible Informationen verarbeiten.

Gemäß Artikel 22 Absatz (3) (a) der EU-Verordnung Reg (EU) 2025/38, welcher Artikel 12 der EU-Verordnung (EU) 2021/694 ergänzt, gilt:

Art 12 (5) der EU-Verordnung 2021/694 soll keine Anwendung finden, wenn alle Bedingungen des Art 12(5a) erfüllt sind. Diese lauten:

a) unter Berücksichtigung der Ergebnisse der gemäß Artikel 9 Absatz 4 der Verordnung (EU) 2025/38 erstellten Aufstellung besteht ein reales Risiko, dass die Instrumente, Infrastruktur oder Dienste, die erforderlich und ausreichend dafür sind, dass die betreffende Maßnahme angemessen zu den Zielen des europäischen Warnsystems für Cybersicherheit beitragen kann, von Rechtsträgern, die in einem Mitgliedstaat niedergelassen sind oder als dort niedergelassen gelten und die von einem Mitgliedstaat oder von einem Staatsangehörigen eines Mitgliedstaats kontrolliert werden, nicht zur Verfügung gestellt werden können;
b) das mit einer Beschaffung über solche Rechtsträger im Rahmen des europäischen Warnsystems für Cybersicherheit einhergehende Sicherheitsrisiko steht in einem angemessenen Verhältnis zu den damit

verbundenen Vorteilen und steht den grundlegenden Sicherheitsinteressen der Union und ihrer Mitgliedstaaten nicht entgegen.

Derzeit laufen erste Kartierungsversuche. Bis zum Abschluss der Kartierung und im Einklang mit den Regelungen des Cyber Solidarity Act, wird die Teilnahme an den unter diesem Topic gewährten Ausschreibungen den Beschränkungen des Artikel 12(5) unterliegen, wie im Anhang 3 dieses Work Programmes dargelegt. Diese Sicherheitsvorkehrungen könnten später angepasst werden, wenn die Ergebnisse der Kartierung der Dienstleistungen nach Artikel 9(4) des Cyber Solidarity Act durch das ECCC vorliegen.

2.7.3 Zu erbringende Leistungen

Nationale Cyber Hubs von Weltrang quer durch die Union ausgestattet mit hochsicherer Infrastruktur, welche - unter Berücksichtigung gut etablierter Standards für Verbreitungs- und Automatisierungsprozesse - als Clearingstelle für die Detektion, Sammlung und Speicherung von Daten zu Cybersicherheitsbedrohungen, zur Analyse dieser Daten und zum Verbreiten und Berichten von CTI, Prüfberichten und Analysen dienen.

Fähigkeiten zur Aufklärung von Bedrohungen und zum Lagebewusstsein sowie Aufbau von Kapazitäten zur Unterstützung einer verstärkten Zusammenarbeit zwischen Akteuren im Bereich der Cybersicherheit, einschließlich privater und öffentlicher Akteure.

- Gezielte Schulungen auf der Grundlage des ECSF zur Verbesserung der Kapazitäten von Cybersicherheitsfunktionen.
- Anwendungen zur automatisierten Benachrichtigung privater und öffentlicher Akteure über gefährdete oder unsichere Systeme.

Art der Maßnahme	Aufruf zur Interessensbekundung – Call for Expression of Interest – workstream on Joint procurement with Member States
Vorläufiges Budget	*35 Mio. EUR – Die per Delegation authorisierte Behörde soll die Kontingente für die Maßnahmen nach Abschnitt 2.7 an die in den erhaltenen Einsendungen angefragten Kontingente anpassen.*
Vorläufige Ausschreibungsplanung	2025, 2026
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Körperschaften des öffentlichen Rechts, die als nationale Cyber Hubs dienen und als solche von den Mitgliedstaaten anerkannt wurden.
Sicherheit	Die Maßnahme unterliegt den Beschränkungen des Artikel 12(5) der Regulation (EU) 2021/694. Weitere Ausführungen zu den sicherheitsrelevanten Be-dingungen für

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

	Fördermittel und Auftragsvergabe befinden sich in den Absätzen „third country participation“ und „procurement from non-EU entities“ dieses Dokumentes. Further explanation on Grants and Procurement conditions relevant for security is provided in the ‘third country par-ticipation’ and ‘procurement from non-EU entities’ para-graphs of this document.

Art der Maßnahme	Aufruf zur Interessensbekundung – Call for Expression of Interest – workstream on Simple Grants
Vorläufiges Budget	*Wird noch definiert --. Die per Delegation authorisierte Behörde soll die Kontingente für die Maßnahmen nach Abschnitt 2.7 an die in den erhaltenen Einsendungen ange-fragten Kontingente anpassen.*
Vorläufige Ausschreibungsplanung	2025, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Erfolgreiche Antragstellende auf den Workstream “Joint procurement with Member States”
Sicherheit	Die Maßnahme unterliegt den Beschränkungen des Artikel 12(5) der Regulation (EU) 2021/694. Weitere Ausführungen zu den sicherheitsrelevanten Bedingungen für Fördermittel und Auftragsvergabe befinden sich in den Absätzen „third country participation“ und „procurement from non-EU entities“ dieses Dokumentes.

NKCS

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**