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
Förderthema:	2.10 Coordinated preparedness testing and other preparedness actions
Seiten:	47-50

2.10 Koordinierte Cybersicherheitstests und andere Vorsorgemaßnahmen

Diese Maßnahme umfasst zwei Maßnahmen aus dem Cyber-Solidaritätsgesetz, die sich auf das Cybersicherheitsnotfallverfahren beziehen: (1) koordinierte Cybersicherheitstests für Einrichtungen, die in hochkritischen Sektoren in der gesamten Union tätig sind, und (2) andere Vorsorgemaßnahmen für Entitäten, die in hochkritischen Sektoren und anderen kritischen Sektoren tätig sind.

2.10.1 Ziele

Diese Maßnahmen sollen die Bemühungen der Mitgliedstaaten und der Union zur Verbesserung des Schutzes vor und der Widerstandsfähigkeit gegen Cyberbedrohungen ergänzen (nicht kopieren), insbesondere in Bezug auf kritische Infrastrukturen und Industrieanlagen. Hierzu sollen die Mitgliedsstaaten in ihren Bemühungen, sich auf Cyberbedrohungen und -vorfälle vorzubereiten mit Fachwissen und Erfahrungen unterstützt werden.

Die Anträge sollten einen Beitrag zu mindestens einem der folgenden Ziele leisten:

- (Teil 1) Koordinierte Cybersicherheitstests von Entitäten, die in hochkritischen Sektoren in der gesamten Union tätig sind (einschließlich Penetrationstests und Gefährdungseinschätzung), unter Berücksichtigung von Informations- und Kommunikationstechnik sowie Betriebstechnologien/industriellen Kontrollsystemen.
- (Teil 2) Sonstige Vorsorgemaßnahmen für Entitäten, die in hochkritischen Sektoren und anderen kritischen Sektoren tätig sind (z. B. Schwachstellenüberwachung, Übungen und Schulungen).

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

2.10.2 Umfang (oder Anwendungsbereich)

[Teil 1 Koordinierte Cybersicherheitstests]

Die Bereitstellung von Dienstleistungen (für Entitäten, die ganz oder teilweise unter das Cyber-Solidaritätsgesetz der EU-Kommission fallen, aus den hochkritischen Sektoren aus Annex 1 der EU-Richtlinie (EU) 2022/2555 und näher benannt im „call for proposal"-Dokument für jeden der Calls unter diesem Topic) zur Absicherung gegen Cybersicherheitsbedrohungen soll Maßnahmen aus der folgenden Liste beinhalten:

Unterstützung bei der Suche nach potentiellen Schwachstellen:

- Entwicklung von Szenarien für **Penetrationstests**. Die vorgeschlagenen Szenarien können Netzwerke, Anwendungen, Virtualisierungslösungen, Cloud-Lösungen, industrielle Kontrollsysteme und IoT umfassen.
- Unterstützung bei der Durchführung von Tests zur Ermittlung potenzieller Schwachstellen bei wichtigen Einrichtungen, die kritische Infrastrukturen betreiben.
- Unterstützung der Einführung digitaler Werkzeuge und Infrastrukturen zur Ausführung von Testszenarien und zur Durchführung von Übungsaufgaben wie z. B. die Entwicklung standardisierter Cyberbereiche ("Cyber-Ranges") oder anderer Testeinrichtungen, die in der Lage sind, die Merkmale kritischer Sektoren (z. B. Energie, Verkehr usw.) oder anderer von NIS-2 betroffener Sektoren zu imitieren, um die Durchführung von Cyberübungen zu erleichtern, insbesondere (falls anwendbar) für grenzübergreifende Szenarien.
- Bewertung und/oder Erprobung der Cybersicherheitsfähigkeiten von Einrichtungen und Sektoren der Mitgiedsstaaten (einschließlich Präventions-, Detektions- und Reaktionsfähigkeiten auf Vorfälle sowie **sektorenübergeifender Stresstests**), Bewertungs- und Konformitätsaktivitäten zur Erhöhung des Reifegrads, z. B. auf der Grundlage etablierter Reifegradmodelle und/oder einschlägiger Bewertungs- und Konformitätsregelungen.
- Bewertung und/oder Prüfung der Cybersicherheitsfähigkeiten der betroffenen Einrichtungen (einschließlich der Bewertung und des Managements von Risiken in der Lieferkette).
- Beratungsdienste, die Empfehlungen zur Verbesserung zur Verbesserung von Sicherheit und Leistungsfähigkeit der Infrastrukturgeben.

Unterstützung bei **Bedrohungseinstufungen und Risikobewertungen**, z.B.:

- beim Bedrohungseinstufungsprozess über dessen gesamten Lebenszyklus ab Implementierung
- in Form von kundenspezifischen Risikoszenarioanalysen

Die Unterstützung richtet sich an die zuständigen Behörden der Mitgliedstaaten, die eine zentrale Rolle bei der Umsetzung der NIS-2-Richtlinie spielen, wie z. B. die Computer Security Incident Response Teams (CSIRTs) und die nationalen Cybersicherheitsbehörden.

[Teil 2 - Sonstige Maßnahmen zur Abwehrbereitschaft]

Im zweiten Teil, ergänzend zu den bereits in Teil 1 gelisteten Dienstleistungen(Unterstützung bei der Prüfung auf potenzielle Schwachstellen und Unterstützung bei der Bedrohungseinstufung und dem

Risikomanagement), die nachstehend benannten Dienstleistungen zur Unterstützung der Cyber-Abwehrbereitschaft von Entitäten in hochkritischen oder anderen kritischen Sektoren gemäß Anhang I und II der NIS-2-Richtlinie.

Unterstützung von **Bedrohungseinstufungen und Risikobewertungen**:

- Risikomanagement der Lieferkette im Rahmen von Risikobewertungsdiensten.

Risikoüberwachungsdienste:

- Spezifische kontinuierliche Risikoüberwachung wie attack surface monitoring (Angriffsflächenüberwachung), Risikoüberwachung von Vermögenswerten und Schwachstellen.

Unterstützung des koordinierten Schwachstellenoffenlegens und -managements:

- Förderung der Übernahme nationaler CVD-Richtlinien[1] und der EU-Datenbank für Sicherheitslücken.
- Koordinierte Offenlegung von Schwachstellen und rechtzeitige Verbreitung von Sicherheits-Patches. Standardisierung der Art und Weise, wie Informationen zwischen den verschiedenen Akteuren im Umgang mit Sicherheitslücken ausgetauscht werden.
- CVD-Anwendungen, die mehrere Quellen von Schwachstelleninformationen unter Verwendung offener Standards oder Technologien verwalten. (z. B. Forschende, Anbietende, CSIRTs)
- Sensibilisierung für die Übernahme bewährter Verfahren für das Schwachstellenmanagement.

Gezielte Übungen und Schulungen:

- Die Entwicklung von umfassenden, auch internationalen, Schulungsprogrammen und Workshops für Cybersicherheits-Fachkräfte, die die neuesten Trends der Cyberbedrohungen, Angriffsmethoden und bewährten Praktiken für vorgreifendes Bedrohungsmanagement und die Prävention abdecken. Feststellung des Absicherungsgrades, Bewertung der Cybersicherheitsfähigkeiten.
- Kontinuierliche Lernaktivitäten im Bereich der Cybersicherheit[2] fördern und entwickeln, um mit allen Cybersicherheitsanforderungen Schritt zu halten, die sich aus den EU-Verordnungen und -Richtlinien zur Cybersicherheit ergeben, darunter die NIS-2-Richtlinie, CSA, CSoA, DORA, EECC, GDPR und CRA.

Die Unterstützung richtet sich an die zuständigen Behörden der Mitgliedstaaten, die eine zentrale Rolle bei der Umsetzung der NIS-2-Richtlinie spielen, an die Computer Security Incident Response Teams (CSIRTs), einschließlich der sektorspezifischen CSIRTs, an die Security Operation Centres (SOCs)/Cyber Hubs, an die hochkritischen und anderen kritischen Sektoren, an die Akteure aus der Industrie (einschließlich der Information Sharing and Analysis Centres - ISACs) und an alle anderen Akteure, die in den Anwendungsbereich der NIS-2-Richtlinie fallen, wie DORA, CSA etc.

---

1 Coordinated Vulnerability Disclosure Policies in the EU, ENISA, 2022, verfügbar unter: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-euassessment

2 Based on ECSF

Ferner kann Unterstützung gewährt werden bei der CEF-Anbindung von öffentlichen oder privaten Organisationen, die an der Umsetzung der NIS-2-Richtlinie arbeiten und somit potentielle Nutzer der CEF Cybersecurity Core Service Platforms sind.Die Maßnahme kann auch der Industrie - mit besonderem Schwerpunkt auf Start-ups und KMU – dabei helfen, die durch das Cyber Resilience Act geschaffenen Industrie- und Marktchancen zu nutzen sowie die Umsetzung der NIS-2-Richtlinie zu unterstützen.

2.10.2 Leistungsumfang

Die zu erbringenden Leistungen werden ebenfalls in zwei Teilen gegliedert.

Der erste Teil umfasst:

- die verstärkte Zusammenarbeit, Abwehrbereitschaft und Widerstandsfähigkeit im Bereich der Cybersicherheit in der EU; Dienste zur Unterstützung der Abwehrbereitschaft
- sowie Bedrohungs- und Risikobewertungsdienste.

Darüber hinaus für den zweiten Teil:

- Risikoüberwachungsdienste.
- die bessere Einhaltung der Vorschriften, koordinierte Offenlegung von Schwachstellen und Monitoring.
- verbesserte Fähigkeiten, durch Übungen und Schulungen, der Organisation von Veranstaltungen, Workshops, Konsultationen von Interessengruppen und White Papers.

Für "Koordinierte Cybersicherheitstests":

Art der Maßnahme	Simple Grant
Vorläufiges Budget	*25 Mill. EUR (5 Mill. EUR in 2025, 10 Mill. EUR in 2026 and 10 Mill. EUR in 2027)*
Vorläufige Ausschreibungsplanung	2025, 2026, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Staatliche Stellen, wie Cybersicherheitsbehörden oder CSIRTs. Öffentliche Einrichtungen, die der NIS-2-Richtlinie unterliegen, CRA, CSA, CSoA, DORA etc.
Sicherheit	Die Einreichung von Anträgen und die Auftragsvergabe sind gemäß Artikel 12 Absatz 5 der Verordnung (EU) 2021/694 beschränkt.

Für „ **Sonstige Maßnahmen zur Abwehrbereitschaft":**

Art der Maßnahme	Simple Grants
Vorläufiges Budget	*15 Mill. EUR (5 Mill. EUR in 2026 and 10 Mill. EUR in 2027)*

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

Vorläufige Ausschreibungsplanung	2026, 2027
Vorläufige Projektdauer	3 years
Implementierung	ECCC
Zielgruppe	Staatliche Stellen, die als für zuständige Cybersicherheitsbehörden oder CSIRTs fungieren, Nationale Cyber-Hubs, die von den Mitgliedstaaten identifiziert wurden. Öffentliche Einrichtungen und andere Stellen, die der NIS-2-Richtlinie unterliegen (hochkritische und andere kritische Sektoren), CRA, CSA, CSoA, DORA usw. Oder[3]: Interessenvertreter der Industrie, andere öffentliche und private Stellen, die die Umsetzung der NIS-2-Richtlinie unterstützen können (zusammen mit oder für hochkritische und andere kritische Sektoren), CRA, CSA, CSoA, DORA, GDPR usw.; vertrauenswürdige Anbieter von Cybersicherheitsdiensten.
Sicherheit	Die Einreichung von Anträgen und die Auftragsvergabe sind gemäß Artikel 12 Absatz 5 der Verordnung (EU) 2021/694 beschränkt.

3 Hier sollte es separate Ausschreibungen für die unterschiedlichen Zielgruppen geben.