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:	New technologies, AI & post-quantum transition
Förderthema:	2.6 Uptake of innovative cybersecurity solutions for SME
Seiten:	33-35

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

2.6 Innovative Cybersicherheitslösungen für KMU

Die Maßnahme zielt darauf ab, die Industrie- und Marktbereitschaft von KMU zu verbessern, um die Anforderungen an die Cybersicherheit von KMU zu erfüllen, wie sie in den einschlägigen EU-Rechtsvorschriften zur Cybersicherheit festgelegt sind, z.B. im Cyber Resilience Act, der sicherere Hardware- und Softwareprodukte gewährleistet.

2.6.1 Ziele

Die Vorschläge sollten zur Erreichung mindestens eines dieser Ziele beitragen:

- Verfügbarkeit von innovativen Werkzeugen und Dienstleistungen, die KMU bei der Einhaltung der EU-Rechtsvorschriften zur Cybersicherheit unterstützen.
- Verfügbarkeit innovativer Werkzeuge und Dienste, die KMU dabei unterstützen, einen Vorfall zu melden und nach Möglichkeit bei der Wiederherstellung zu helfen und sich mit den zuständigen Behörden auszutauschen (d.h. Zusammenarbeit mit Cyber-Hubs, CSIRTs (auch im Zusammenhang mit dem CSIRT-Netz) und / oder ISACs, z.B. für hochkritische und andere kritische Sektoren)
- Verbesserte Sicherheits- und Meldeverfahren und -mittel in der EU.
- Verbesserung der Sicherheit der Netz- und Informationssysteme in der EU.
- Industrie- und Marktbereitschaft für den vorgeschlagenen Cyber Resilience Act.

- Unterstützung der Cybersicherheitszertifizierung im Einklang mit dem Cybersicherheitsgesetz.
- Unterstützung der Lieferkettenpartner bei standardisierten Selbstbewertungen und Zertifizierungen. Unterstützung der nachgelagerten Partner in der Lieferkette bei der schrittweisen Verbesserung der Cyber Resilienz.
- Bewältigung der Herausforderung, die erforderlichen technischen Fähigkeiten für den Umgang mit einer komplexen Technologielandschaft zu finden, die stark auf umfangreichen Konfigurationen und Funktionen basiert.
- Cyber-Toolkit als Service zur Unterstützung von KMU bei der Verwaltung von Cyber-Risiken, der Definition und Umsetzung ihrer Cyber-Sicherheitsstrategie, einschließlich mehrerer Funktionen zur Risikobewertung, Erkennung von Schwachstellen und Bedrohungen usw.
- Support- und Incident-Response-Funktionen für KMU.

2.6.2 Umfang (oder Anwendungsbereich)

Die Maßnahme konzentriert sich auf die Unterstützung von mindestens einer der im nächsten Abschnitt aufgeführten Prioritäten.

2.1.2 Zu erbringende Leistungen

Entwicklung eines Cyber-Toolkits als Dienstleistung zur Unterstützung von KMU beim Management von Cyber-Risiken bei der Festlegung und Umsetzung ihrer Cybersicherheitsstrategie. Das Toolkit könnte mindestens eines der folgenden Elemente enthalten:

- Schnittstellen zur Anbindung an bestehende SaaS-Anwendungen wie Personal-, Rechnungs- und Finanzmanagement-, CRM- und Buchhaltungssysteme usw., die von KMU häufig zur Erhöhung ihrer Cybersicherheit genutzt werden.
- Eine Funktion, die die Bewertung und das Management der Cybersicherheitsrisiken eines KMU und das Risikomanagement der Lieferkette unterstützt. Diese Funktion sollte eine Risikobewertung durchführen, Empfehlungen zur Risikominderung geben und Optionen aufzeigen.
- Eine Schnittstelle zu bestehenden Werkzeugen, die die Analyse und Bewertung des Ausmaßes des Cyberrisikos eines KMU auf der Grundlage von Informationen, die beim Scannen der digitalen Infrastruktur gesammelt wurden, und von Daten, die von autorisierten Benutzern bereitgestellt wurden, unterstützen.
- Eine Funktion, die auf der Grundlage der von der Risikomanagementfunktion gesammelten Informationen, Warnungen über Schwachstellen und Bedrohungen ausgibt.

- Eine Funktion, die KMU mit einem CSIRT oder einem Cyber Hub verbindet, um einen Vorfall zu melden und bei der Wiederherstellung zu helfen, falls möglich.
- Eine Zuordnung und ein zentrales Fenster/Portal zu bestehenden Tools und Lösungen, die auf die Unterstützung von KMU im Bereich der Cybersicherheit abzielen.
- Werkzeuge zur Unterstützung von Erkennung, Vorbeugung und Reaktion in betrieblichen Technologieinfrastrukturen unter Verwendung offener Standards oder Technologien.

Unterstützungs- und Reaktionsbefähigung bei Vorfällen für KMU:

- Nichtkommerzielle Cybersecurity-Hotline mit einem standardisierten Rahmen und Richtlinien für Reaktionszeiten, Eskalationsverfahren und den Umfang der geleisteten Unterstützung.
- Eine voll funktionsfähige, mehrsprachige Hotline, die KMUs zeitnahe und genaue Unterstützung im Bereich der Cybersicherheit bietet, was zu weniger erfolgreichen Cyberbetrügereien und besserer digitaler Hygiene führt.
- Eine nationale Cyber-Response-Plattform für Cyber-Ersthelfer, um Erfahrungen auszutauschen, relevante Nachrichten zu teilen und Diskussionen über Herausforderungen und neu auftretende Cyber-Bedrohungen zu führen, ergänzend zu den bestehenden Cyber-Krisenmanagement-Strukturen.
- Spezialisierte Schulungsmodule für (öffentliche und private) Ersthelfer in verschiedenen Sektoren wie Gesundheitswesen, Finanzen, Energie und Verkehr.

Hilfsmittel und Plattformen:

- Kontrollzentrum und Gremium für die Meldung von Vorfällen und die Entsendung von Einsatzkräften.
- KMU-Benutzeroberfläche für die Meldung von Vorfällen in Verbindung mit dem Cyber-Toolkit. Benutzer können einen Vorfall melden, Anweisungen zur Reaktion erhalten und Informationen darüber bekommen, wie sie Unterstützung bei der Reaktion erhalten können. Ein KI-Assistent, der mit einem Kontrollzentrum verbunden ist, könnte ebenfalls enthalten sein.
- Schnittstellen zu den nationalen Behörden und grenzüberschreitenden Plattformen (CBP) für die Meldung von Vorfällen und den Informationsaustausch.

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

Art der Maßnahme	SME Support Action
Vorläufiges Budget	*30 Mio. EUR*
Vorläufige Ausschreibungsplanung	2025, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	KMU, private und öffentliche Einrichtungen, die die NIS-2-Richtlinie und das Gesetz über die Widerstandsfähigkeit gegen Cyberangriffe umsetzen, Forschung und Hochschulen usw.
Sicherheit	Die Einreichung von Anträgen und die Auftragsvergabe sind gemäß Artikel 12 Absatz 5 der Verordnung (EU) 2021/694 beschränkt.

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**