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:	2.1 Cybersecure tools, technologies and services relying on AI
Seiten:	18-21

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

2.1 KI-gestützte Werkzeuge, Technologien und Dienste für die Cybersicherheit

2.1.1 Ziele

Dieser Themenbereich befasst sich mit KI-gestützten Technologien (einschließlich GenAI) für nationale Behörden und zuständige Stellen, einschließlich nationaler und grenzübergreifender Cyber-Drehscheiben, CSIRTs, öffentlicher und privater Stellen in den Bereichen der NIS-2-Richtlinie, NCCs[1] usw. KI gestützte Technologien spielen eine wichtige Rolle bei der Bereitstellung zentraler operativer Fähigkeiten für europäische Cybersicherheits-Ökosysteme. Sie können auch primäre Eingabedaten für KI/ML-basierte Cybersicherheitswerkzeuge und -lösungen bereitstellen, die die Fähigkeit dieser Behörden zur Analyse, Erkennung und Abwehr von Cyberbedrohungen und -vorfällen verbessern sowie die Erstellung qualitativ hochwertiger Informationen über Cyberbedrohungen unterstützen. Insbesondere die Einführung der generativen KI[2] könnte eine Herausforderung und eine Chance für Cybersicherheitsverfahren und -anwendungen[3] darstellen.

---

1 Falls zutreffend und im Einklang mit den einzelnen nationalen Strategien.
2 “Cybersecurity in the age of generative AI”, September 2023, verfügbar unter: https://www.mckinsey.com/featured-insights/themes/cybersecurity-in-the-age-of-generative-ai
3 “The Need For AI-Powered Cybersecurity to Tackle AI-Driven Cyberattacks”, April 2024, verfügbar unter: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-need-for-ai-powered-cybersecurity-to-tackle-ai-driven-cyberat

Diese grundlegenden Technologien sollten eine effizientere Erstellung und Analyse von Informationen über Cyberbedrohungen [Eng.: Cyber Threat Intelligence (CTI)], die Automatisierung umfangreicher Prozesse, eine schnellere und skalierbarere Verarbeitung von Informationen über Cyberbedrohungen (CTI) und die Erkennung von Mustern für eine rasche Erkennung und Entscheidungsfindung ermöglichen.

Die Sicherheit der KI selbst, insbesondere von Systemen in der Lernphase, einschließlich des Missbrauchs von KI durch böswillige Akteure, muss ebenfalls angegangen werden. Dazu gehören die Durchführung von Risikobewertungen und die Minderung der mit KI-Technologien verbundenen Cybersicherheitsrisiken, die Umsetzung der Sicherheit von Lieferketten usw. sowie die Einhaltung der KI-Gesetzgebung [AI Act], der Anforderungen in Bezug auf geistiges Eigentum und der Datenschutz-Grundverordnung [DSGVO/ Eng.: GDPR].

Die zu entwickelnden KI-Technologien sollten nicht nur sicher, sondern auch leistungsfähig, robust und vertrauenswürdig sein. Vertrauenswürdige KI-Lösungen werden vor allem in der Einführungsphase hilfreich sein, in der die gesellschaftliche Akzeptanz von entscheidender Bedeutung ist.

2.1.2 Umfang (oder Anwendungsbereich)

Die Maßnahmen in diesem Bereich sollten die Entwicklung und den Einsatz von Cybersicherheitssystemen[4] und -werkzeugen auf Grundlage von KI-Technologien[5] - in Bereichen wie Bedrohungserkennung, Schwachstellenerkennung, Eindämmung von Bedrohungen, Wiederherstellung nach Zwischenfällen durch Selbstheilung, Datenanalyse und Datenaustausch - umfassen. Je nach Art der verarbeiteten Informationen müssen diese Aktivitäten auch mit den Rechten an geistigem Eigentum (IPR) und der Datenschutz-Grundverordnung [DSGVO/ Eng. GDPR] in Einklang stehen. Die vorgeschlagenen KI-Lösungen solltencybersicher sein.

Die Aktivitäten sollten mindestens eine der folgenden Maßnahmen umfassen:

- Kontinuierliche Mustererkennung und Identifizierung von Anomalien, die potenziell auf neue Bedrohungen hinweisen, Identifizierung neuer Angriffsvektoren und Ermöglichung einer fortschrittlichen Erkennung in einer sich entwickelnden Bedrohungslandschaft, dies umfasst ICT oder in operativer technischer Infrastruktur die Nutzung von offenen Technologien.
- Schaffung von CTI auf der Grundlage neuartiger Bedrohungserkennungsfähigkeiten.

---

4 “Multilayer Framework for Good Cybersecurity Practices for AI”, ENISA, Juni 2023, verfügbar unter:: https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai
5 “Cybersecurity of AI and Standardisation”, ENISA, March 2023, verfügbar unter: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standard

- Beschleunigung der Reaktion auf Vorfälle durch Echtzeit-Überwachung von Netzwerken zur Erkennung von Sicherheitsvorfällen und Generierung von Warnmeldungen oder Auslösung automatischer Reaktionen.
- Entschärfung von Malware-Bedrohungen durch Analyse des Code-Verhaltens, des Netzwerkverkehrs und der Dateieigenschaften, wodurch das Zeitfenster für Angreifer, Malware auszunutzen, verkleinert wird.
- Identifizierung von Schwachstellen und Unterstützung des Schwachstellenmanagements unter Berücksichtigung mehrerer Informationsquellen.
- Cybersicherheitsinstrumente und -lösungen zur Risikominderung an der Schnittstelle zwischen KI, IoT und intelligenten Netzen oder anderen Produktionsketten.
- Unterstützung der Wiederherstellung nach Vorfällen durch Selbstheilungsfähigkeiten.
- Verringerung der Wahrscheinlichkeit von Angriffen und präventive Identifizierung von Schwachstellen durch automatisierte Schwachstellenscans und Penetrationstests.
- Schutz sensibler Unternehmensdaten durch die Analyse von Zugriffsmustern und die Erkennung von anormalem Verhalten.
- Unternehmen durch Anonymisierung in die Lage versetzen, CTI und andere verwertbare Informationen für Analysen und Einblicke zu nutzen und weiterzugeben, ohne die Datensicherheit und den Datenschutz zu gefährden.
- Tools und Lösungen, die Produktsicherheit oder Cybersicherheit per Design/Default in Übereinstimmung mit den Anforderungen mit dem CRA bieten.
- Anbieter von Tools und Dienstleistungen können sich zu diesem Thema bewerben, auch wenn sie in einem Konsortium mit Cyber-Hubs arbeiten. Gegebenenfalls sollten Verbindungen zu Akteuren im Bereich des Hochleistungsrechnens hergestellt und Aktivitäten zur Förderung der Vernetzung mit diesen Akteuren durchgeführt werden. In gut begründeten Fällen können Anträge auf Zugang zur EuroHPC-Hochleistungsrecheninfrastruktur bewilligt werden.
- Die im Rahmen dieses Themas entwickelten Systeme, Instrumente und Dienste werden nationalen und/oder grenzübergreifenden Cyber-Drehscheiben, CSIRTs, zuständigen Behörden und anderen relevanten Behörden zur Lizenzierung zu günstigen Marktbedingungen zur Verfügung gestellt.
- Diese Maßnahmen zielen darauf ab, KI-gestützte Cybersicherheitskapazitäten für nationale und/oder grenzübergreifende Cyber-Drehscheiben und für nationale Behörden, einschließlich Cyber-

Drehscheiben und CSIRTs, bereitzustellen, die eine zentrale Rolle bei der Gewährleistung der Cybersicherheit nationaler Behörden, Anbieter kritischer Infrastrukturen und wesentlicher Dienste spielen. Diese Einrichtungen haben die Aufgabe, Bedrohungen der Cybersicherheit zu überwachen, zu verstehen und proaktiv zu bewältigen. Angesichts der entscheidenden operativen Rolle der Cyber-Drehscheiben bei der Gewährleistung der Cybersicherheit in der Union, der Art der beteiligten Technologien und der Sensibilität der verarbeiteten Informationen müssen sie vor möglichen Abhängigkeiten und Schwachstellen in der Cybersicherheit geschützt werden, um ausländische Einflussnahme und Kontrolle zu verhindern.

- Instrumente zum Schutz und zur Sicherung von KI-Lösungen im Einklang mit dem EU-Rechtsrahmen und unter Berücksichtigung der Anforderungen an Robustheit, Leistung, Vertrauen und ausgewogene Autonomie der KI.
- Beitrag zur Cybersicherheitszertifizierung von KI-gestützten Cybersicherheitslösungen und -systemen. Das Hauptziel der Cybersicherheitszertifizierung für KI-Systeme in der EU besteht darin, die mit KI-Technologien verbundenen Cybersicherheitsrisiken zu mindern und die Einhaltung des umfassenden EU-Rechtsrahmens, einschließlich des KI-Rechts, nachzuweisen. Durch die Einführung eines standardisierten, transparenten und strengen Zertifizierungsverfahrens will die EU das Vertrauen in KI-Technologien bei Nutzern, Entwicklern und Regulierungsbehörden gleichermaßen fördern.

2.1.3 Zu erbringende Leistungen

- Einsatz künstlicher Intelligenz und verschiedener KI-gestützter Technologien zur Unterstützung von Cyber-Hubs, CSIRTs, NCSCs, NIS SPOCs und anderen.
- Entwicklung, Erprobung und Validierung neuartiger KI-gestützter Cyber-Sicherheitswerkzeuge unter relevanten Bedingungen und Bereitstellung für Cyber-Hubs, CSIRTs, NCSCs, NIS SPOCs und andere.
- Verbesserung des Informationsaustauschs und der Zusammenarbeit zwischen nationalen und transnationalen Cyber-Hubs, CSIRTs, NCSCs, NIS SPOCs und anderen relevanten Akteuren, unterstützt durch KI/-gestützte Tools.
- Werkzeuge für die Automatisierung von Cybersicherheitsprozessen, wie z.B. die Erstellung, Analyse und Verarbeitung von CTI, um den Betrieb von Cyber-Hubs zu verbessern.
- Original europäische CTI Feeds oder Dienste.
- Sicherstellung, dass die fortschrittlichsten und innovativsten sicheren KI-Lösungen für den NIS-Sektor entwickelt und implementiert werden.

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

- Sichere KI-Lösungen und -Werkzeuge, die dem EU-Recht entsprechen. Förderung der Minderung der Risiken, die mit dem Missbrauch von KI durch böswillige Akteure verbunden sind, mit Schwerpunkt auf KI-Ethik und sicherer Nutzung.
- Beitrag zur Standardisierung und Zertifizierung vertrauenswürdiger und sicherer KI-Technologien.

Art der Maßnahme	Simple grant
Vorläufiges Budget	*45 Mio. EUR*
Vorläufige Ausschreibungsplanung	2025, 2026, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Technologieanbieter, Betreiber von Cyber-Hubs, Forschung und Hochschulen, Cybersicherheits-einrichtungen, öffentlicher Sektor, von der NIS-2-Richtlinie betroffene Einrichtungen, Privatsektor, andere einschlägige Akteure, die die Einführung sicherer KI-Lösungen im Internet unterstützen
Sicherheit	Die Einreichung von Anträgen und die Auftragsvergabe sind gemäß Artikel 12 Absatz 5 der Verordnung (EU) 2021/694 beschränkt.

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**