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-01: Generative AI for Cybersecurity applications

Seiten: 93-95

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

HORIZON-CL3-2025-02-ECCC-01: Generative KI für Cybersecurity-Anwendungen

Erwartete Auswirkungen

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

Erwartete Ergebnisse

Um die erwarteten Ergebnisse zu erzielen und die strategischen Vermögenswerte, Interessen, Autonomie und Sicherheit der Union zu schützen, ist die Teilnahme an diesem Thema auf Rechtspersonen mit Sitz in den Mitgliedstaaten und assoziierten Ländern beschränkt.

Um den Schutz der strategischen Interessen der Union und ihrer Mitgliedstaaten zu gewährleisten, dürfen Einrichtungen, die in einem der oben aufgeführten förderfähigen Länder ansässig sind, aber direkt oder indirekt von einem nicht förderfähigen Land oder einer Einrichtung eines nicht förderfähigen Landes kontrolliert werden, nicht an der Aktion teilnehmen.

Das Verfahren ist im Allgemeinen Anhang F beschrieben. Es gelten die folgenden Ausnahmen:

Um ein ausgewogenes Portfolio zu gewährleisten, das ein breites Spektrum an Forschungsbereichen abdeckt, werden die Zuschüsse nicht nur in der Reihenfolge der Rangfolge der Anträge vergeben, sondern mindestens auch an die beiden höchstrangigen Vorschläge, die das erwartete Ergebnis a) betreffen, und den höchstrangigen Vorschlag, der das erwartete Ergebnis b) betrifft, sofern die Anträge alle Schwellenwerte erreichen.

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

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.

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

Erwartetes Ergebnis: Die Projekte werden Technologien, Werkzeuge und Prozesse entwickeln, die die Cybersicherheit durch den Einsatz von KI-Technologien, insbesondere generativer KI, im Einklang mit den einschlägigen politischen, rechtlichen und ethischen Anforderungen der EU erhöhen.

Die Vorschläge sollten mindestens eines der folgenden erwarteten Ergebnisse ansprechen:

a. Entwicklung, Training und Test von generativen KI-Modellen für die Überwachung, Erkennung, Reaktion und Selbstheilung von digitalen Prozessen und Systemen gegen Cyberangriffe, einschließlich feindlicher KI-Angriffe.

b. Entwicklung von generativen KI-Tools und -Technologien für die kontinuierliche Überwachung, Einhaltung von Vorschriften und automatisierte Abhilfemaßnahmen. Diese sollten sowohl rechtliche Aspekte der EU und der nationalen Regulierung als auch ethische und datenschutzrechtliche Aspekte berücksichtigen.

Umfang

Der Einsatz von künstlicher Intelligenz wird bei Anwendungen, bei denen es um große Datenmengen geht, unverzichtbar. Um alle Implikationen für die Cybersicherheit zu verstehen, bedarf es einer tieferen Analyse und weiterer Forschung und Innovation.

Generative KI bietet sowohl Chancen als auch Herausforderungen auf dem Gebiet der Cybersicherheit. Dieses Thema unterstützt die Erforschung der neuen Möglichkeiten, die generative KI für Cybersecurity-Anwendungen bietet, um KI-Modelle zu entwickeln, zu trainieren und zu testen, um die Erkennung von Bedrohungen und Schwachstellen zu skalieren, die Reaktionszeit zu verbessern, die großen Datenmengen zu bewältigen und Prozesse und die Entscheidungsfindung zu automatisieren, z.B. durch die Erstellung von Berichten aus Bedrohungsdaten, das Vorschlagen und Schreiben von Erkennungsregeln, Bedrohungsjagden und Abfragen für das Security Information and Event Management (SIEM), die Erstellung von Management-, Audit- und Compliance-Berichten und das Reverse Engineering von Malware.

Vorschläge zu den erwarteten Ergebnissen a)

(a) (i) **Erweiterte Erkennung und Analyse von Bedrohungen und Anomalien**: Die derzeitigen Tools für die Cybersicherheit können mit den sich entwickelnden Taktiken der Cyberangreifer nur schwer Schritt halten. Die Entwicklung, das Training und das Testen von generativen KI-Modellen kann dazu verwendet werden, große Datenmengen zu analysieren und Anomalien und Abweichungen von normalen Verhaltensmustern genau zu erkennen, was eine effektivere Erkennung, Analyse und Reaktion auf Bedrohungen ermöglicht.

Die Tools sollten auch Fachleute für Cybersicherheit unterstützen, da es für sie schwierig sein kann, Bedrohungen durch generative KI zu erkennen und darauf zu reagieren, insbesondere da diese

Systeme immer ausgefeilter werden und schwer von echten menschlichen Aktivitäten zu unterscheiden sind.

(a) (ii) **Adaptive Sicherheitsmaßnahmen**: Cybersecurity-Tools verlassen sich bei der Erkennung von Bedrohungen oft auf statische Regeln und Signaturen, was sie weniger effektiv gegen neue und sich weiterentwickelnde Angriffsmethoden macht. Darüber hinaus sind viele Cybersecurity-Tools bei der Reaktion auf Bedrohungen immer noch auf manuelle Eingriffe angewiesen, was zeitaufwändig und ineffektiv sein kann. Generative KI kann durch die Entwicklung, das Training, die Feinabstimmung und das Testen von generativen KI-Modellen diese Tools dabei unterstützen, sich anzupassen und in Echtzeit auf neue Bedrohungen zu reagieren, was die allgemeine Sicherheitslage verbessert.

(a) (iii) **Verbesserte Authentifizierung und Zugangskontrolle**: Der Einsatz von KI-Technologien könnte die Widerstandsfähigkeit von Authentifizierungs- und Zugangskontrollsystemen gegen unbefugten Zugang und den Diebstahl von Zugangsdaten verbessern, so dass es für unbefugte Benutzer schwieriger wird, Zugang zu sensiblen Informationen oder Systemen zu erhalten.

Vorschläge zu den erwarteten Ergebnissen b)

(b) (i) Entwicklung von Tools auf der Grundlage generativer KI, die die **Anwendung der nationalen und EU-Rechtsvorschriften für digitale Systeme** analysieren und erleichtern, insbesondere das Gesetz über künstliche Intelligenz, die Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der Union (NIS2) und das Gesetz über die Cyber-Resilienz.

(b) (ii) **Anpassung an ein dynamisches Umfeld**. Unternehmen, der öffentliche Sektor und Organisationen sind mit einem sich ständig verändernden Umfeld konfrontiert, das die Einhaltung von Cybersicherheitsvorschriften zu einer Herausforderung macht. Auf der einen Seite gibt es eine Vielzahl von Vorschriften, die auf sektoraler, nationaler oder europäischer Ebene gelten und zu berücksichtigen sind. Auf der anderen Seite sind Änderungen und Aktualisierungen der IKT-Systeme in Unternehmen an der Tagesordnung. Der Einsatz von Tools, die auf generativer KI beruhen, bietet das Potenzial für eine kontinuierliche Einhaltung der Vorschriften in Unternehmen, die sonst zeitlich begrenzt sind, wenn sie nur durch menschliche Eingriffe gesteuert werden.

Von allen Vorschlägen wird erwartet, dass sie die Grundsätze der vertrauenswürdigen und verantwortungsvollen KI und des Datenschutzes beachten.

Alle Vorschläge sollten den EU-Mehrwert durch die Förderung der Entwicklung von EU-Technologien, den Einsatz von Open-Source-Technologien, sofern technisch und wirtschaftlich machbar, und die Nutzung verfügbarer EU-Daten (Data Spaces, EOSC, föderierte Daten usw.) nachweisen.

Die Vorschläge sollten wichtige Leistungsindikatoren (KPI) mit Basiszielen zur Messung des Fortschritts festlegen und aufzeigen, wie die vorgeschlagene Arbeit den Stand der Technik entscheidend voranbringen wird. Alle entwickelten Technologien und Tools sollten angemessen dokumentiert werden, um die Übernahme und Nachahmung zu unterstützen. Die Teilnahme von KMU ist erwünscht.

Von den Vorschlägen wird erwartet, dass sie der Dimension des geistigen Eigentums der Ergebnisse besondere Aufmerksamkeit widmen. Die Verwendbarkeit der Ergebnisse und Resultate nach Abschluss des Projekts wird genau geprüft.

Art der Maßnahme	Research and Innovation Actions
Vorläufiges Budget	*40 Mio. EUR*

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

Vorläufiges Budget pro Projekt	*12-14 Mio. EUR*
Zuwendungsberechtigt	Rechtsträger mit Sitz in EU-Mitgliedstaaten und assoziierten Länder, die nicht direkt oder indirekt von Drittländern kontrolliert werden
Fördervergabe-Verfahren	Förderquote 100 %. Das Verfahren ist im Allgemeinen Anhang F beschrieben. Es gelten die folgenden Ausnahmen: Um ein ausgewogenes Portfolio zu gewährleisten, das ein breites Spektrum an Forschungsbereichen abdeckt, werden die Zuschüsse nicht nur in der Reihenfolge der Rangfolge der Anträge vergeben, sondern mindestens auch an die beiden höchstrangigen Vorschläge, die das erwartete Ergebnis a) betreffen, und den höchstrangigen Vorschlag, der das erwartete Ergebnis b) betrifft, sofern die Anträge alle Schwellenwerte erreichen.
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.

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**