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:	Additional actions for improving EU Cyber resilience
Förderthema:	2.14 Dedicated action to reinforce hospitals and healthcare providers
Seiten:	64-65

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

2.14 Gezielte Maßnahmen zur Stärkung von Krankenhäusern und Gesundheitsdienstleistern

2.14.1 Ziele

Diese Aktion zielt darauf ab, die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern zu stärken. Ziel ist es, sicherzustellen, dass Krankenhäuser und Gesundheitsdienstleister, die im Gesundheitssektor eine zentrale Rolle spielen, Cyberbedrohungen, insbesondere Ransomware, die ein erhebliches Risiko darstellen, wirksam erkennen, überwachen und darauf reagieren können, um so die Widerstandsfähigkeit des europäischen Gesundheitssystems zu verbessern.

Die Maßnahme wird einen Beitrag zum EU-Aktionsplan für Cybersicherheit in Krankenhäusern und im Gesundheitswesen leisten, der von der Kommission[1] im Januar 2025.

2.14.2 Umfang (oder Anwendungsbereich)

Mit dieser Maßnahme soll dem wachsenden Bedarf an kontinuierlicher Überwachung der Cybersicherheit, an Bedrohungsdaten und an Reaktionen auf Vorfälle in Krankenhäusern und bei Gesundheitsdienstleistern entsprochen

1 https://commission.europa.eu/cybersecurity-healthcare_en

werden, denen es häufig an spezifischen Cybersicherheitsressourcen fehlt, um sich angemessen gegen Cyberbedrohungen zu schützen.

Im Rahmen der Aktion werden Pilotprojekte unterstützt, die Akteure wie regionale und/oder nationale Verbände[2] von Krankenhäusern und Gesundheitsdienstleistern (wie nationale Gesundheitssysteme, Krankenhäuser oder Verbände von Krankenhäusern, Gesundheitsdienstleistern und/oder Berufsverbände von Angehörigen der Gesundheitsberufe) sowie Anbieter von Cybersicherheitsdiensten zusammenbringen.

Die Pilotprojekte werden den Stand der Bereitschaftskapazitäten in Clustern von Krankenhäusern und Gesundheitsdienstleistern in der Europäischen Union ermitteln, um ihre Bedürfnisse zu bewerten. Auf Grundlage dieser Analyse werden sie einen Überblick über die modernsten Cybersicherheitslösungen und benötigten Ressourcen (Technologien, Dienstleistungen, Werkzeuge, Humanressourcen, Schulungsbedarf usw.) für Krankenhäuser und Gesundheitsdienstleister erstellen, um den Umfang dieser Aktion zu erfüllen. Dazu können zum Beispiel gehören: Security Operation Centres, die Echtzeit-Überwachung, Bedrohungserkennung und schnelle Reaktion auf Vorfälle bieten, sowie fortschrittliche Cybersicherheits-Tools wie SIEM-Plattformen (Security Information and Event Management), Threat Intelligence und automatisierte Reaktionsmöglichkeiten, um nur einige zu nennen.

Die Pilotprojekte werden technische Pläne entwickeln, die auf die Bedürfnisse repräsentativer Krankenhäuser und Gesundheitsdienstleister (z. B. kleine oder große Krankenhäuser, private Gesundheitsdienstleister usw.) zugeschnitten sind und die auch Empfehlungen für die beste Umsetzung und Kostenschätzungen für eine effektive Einführung enthalten müssen.

Die Pilotprojekte werden eine Demo-Implementierung dieser technischen Pläne durchführen, um ihre Effektivität in den Betrieben der Beteiligten zu demonstrieren, wobei verschiedene Anwendungsfälle für verschiedene Nutzergruppen in kleinen, mittleren und großen Krankenhäusern und Gesundheitsdienstleistern in mindestens zwei verschiedenen Mitgliedstaaten vorgestellt werden.

Die Pilotprojekte werden als Demonstrationsprojekte dienen und darüber hinaus das Personal ihrer Partnerkrankenhäuser und Gesundheitsdienstleister in Sachen Cybersicherheit schulen, um das Bewusstsein zu schärfen und bewährte Verfahren zum Schutz sensibler Gesundheitsdaten zu gewährleisten.

Schließlich werden die Pilotprojekte in Zusammenarbeit miteinander Aktivitäten zur weiten Verbreitung bewährter Praktiken in der gesamten EU durchführen, mit dem spezifischen Ziel, die Aktivitäten der Pilotprojekte so weit wie möglich zu replizieren und auszuweiten.

2 Cluster associations' refers to any legally established group of hospitals and healthcare providers, such as regions and professional associations established in one or more Member States.

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

Die Pilotprojekte werden Gesundheitseinrichtungen bei der Einhaltung der NIS-2-Richtlinie unterstützen.

2.14.3 Zu erbringende Leistungen

- Kartierung der gemeinsamen Cybersicherheitsbedürfnisse von Krankenhäusern und Gesundheitsdienstleistern.
- Leitlinien für Gesundheitsdienstleister zur Bewertung ihres aktuellen Stands des Cybersicherheitsschutzes und des entsprechenden Bedarfs.
- Technische Cybersicherheitspläne zur Verbesserung der Abwehrbereitschaft und der Widerstandsfähigkeit: verbesserte Erkennungs- und Reaktionsfähigkeiten für Einrichtungen des Gesundheitswesens zur Minimierung der Auswirkungen von Cyberangriffen, insbesondere von Ransomware. Dazu gehören auch spezielle Schulungskurse für das Personal.
- Pilot-Demo-Installationen zur Cybersicherheit in Partnerkrankenhäusern und an Standorten von Gesundheitsdienstleistern, um sicherzustellen, dass Krankenhäuser und Gesundheitsdienstleister die Betriebskontinuität angesichts von Cybersicherheitsvorfällen aufrechterhalten können. Dies sollte durch spezifische KPIs überwacht werden.
- Breit angelegte Verbreitungskampagnen, um die Bereitschaft von Krankenhäusern und Gesundheitsdienstleistern in Europa zu erhöhen.

2.14.4 Zuschussfähigkeit von Konsortien

Zu den Konsortien gehören regionale und/oder nationale Zusammenschlüsse von Krankenhäusern und Gesundheitsdienstleistern aus mindestens zwei EU-Mitgliedstaaten (z. B. nationale Gesundheitssysteme, Krankenhäuser oder Verbände von Krankenhäusern, Gesundheitsdienstleister und/oder Berufsverbände von Angehörigen der Gesundheitsberufe), die kleine, mittlere und große Einrichtungen sowie Anbieter von Cybersicherheitsdiensten umfassen.

Art der Maßnahme	Simple grant
Vorläufiges Budget	*30 Mio. €*
Vorläufige Ausschreibungsplanung	2025
Vorläufige Projektdauer	1,5-2 Jahre
Implementierung	ECCC
Zielgruppe	Private und öffentliche Einrichtungen
Sicherheit	Aufruf eingeschränkt auf Basis von Artikel 12(5) der DEP-Verordnung (EU) 2021/69

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

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**