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-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

Seiten: 105-108

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

HORIZON-CL3-2025-02-ECCC-06: Integration von Algorithmen der Post-Quantum-Kryptographie in High-Level-Protokolle

Erwartete Auswirkungen

Vom ECCC eingeleitete Aktion zur Übernahme der im Abschnitt "Ziel - Erhöhte Cybersicherheit" dieses Arbeitsprogramms enthaltenen Formulierung "erwartete Auswirkungen".

Erwartete Ergebnisse

Von den Vorschlägen wird erwartet, dass sie zu einigen oder allen der folgenden Ergebnisse beitragen:

- Entwurf und Implementierung mindestens eines High-Level-Post-Quantum-Kryptographie-Protokolls zusammen mit einer Sicherheitsanalyse, die zeigt, dass im Vergleich zu den verwendeten Bausteinen/Protokollen auf niedrigerer Ebene (KEMs, Signaturen, AEAD,...) keine Sicherheit verloren geht;

- Einreichung dieser High-Level-Protokolle zur Integration von PQC bei Standardisierungsgremien und/oder Einreichung der Spezifikation und Implementierung bei den jeweiligen Open-Source-Projekten;

- Anforderungsanalyse, die die Hindernisse und den Bedarf für die Entwicklung von PQC-Lösungen für fehlende Bausteine für die Migration von High-Level-Protokollen zu PQC aufzeigt.

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

Umfang

Der Übergang zur Post-Quantum-Kryptographie erfordert eine Änderung der Verwendung der meisten derzeit eingesetzten Public-Key-Kryptographie (RSA und ECC). Forschungs- und Entwicklungsanstrengungen liefern Signatursysteme und Schlüsselaustauschmechanismen, die allgemein anerkannt sind, um Angriffen mit klassischen und Quantencomputern standzuhalten. Es gibt Bestrebungen, diese in zentrale Internetprotokolle wie Transport Layer Security (TLS) zu integrieren. Dies ist zwar eine wichtige Entwicklung, doch müssen noch viele weitere Protokolle modifiziert werden, um quantenfähig zu sein und die Abwärtskompatibilität mit Altsystemen zu gewährleisten. In verschiedenen Anwendungsbereichen wie dem Internet der Dinge, Cloud-basierten Anwendungen und der Automobilindustrie gibt es Einschränkungen bei der Bandbreite oder der Verarbeitungszeit, die zu anderen Entscheidungen führen können als bei TLS. Derzeit verwendete High-Level-Protokolle können Komponenten enthalten, die spezifisch für die Elliptic Curve Cryptography (ECC) oder für Rivest-Shamir-Adleman (RSA) sind oder zusätzliche Bausteine neben oder anstelle von Signaturen und Schlüsselaustauschmechanismen erfordern. Während Anwendungen, die für Authentizität sorgen, weniger dringend migriert werden müssen als solche, die für Vertraulichkeit sorgen, haben diejenigen, die eingebettete Hardware verwenden, wie z.B. sichere Elemente, Zwei-Faktor-Authentifizierung (2FA) und Multi-Faktor-Authentifizierung (MFA) unter Verwendung von Hardware-Tokens und andere, einen sehr langsamen Umsatz und müssen ersetzt werden, bis es große Quantencomputer gibt, was eine Migration des Designs in naher Zukunft erfordert.

Die Aktivitäten sollten auf ein oder mehrere relevante High-Level-Protokolle ausgerichtet sein und deren Post-Quantum-Versionen erstellen. In der Regel kann dies durch die Kombination von aktuellen und Post-Quantum-Lösungen erreicht werden, um Abwärtskompatibilität zu gewährleisten. Atypische Lösungen mit gleichwertiger Sicherheit sind ebenfalls willkommen. Konsortien, die sich aus verschiedenen Akteuren zusammensetzen, wie z.B. Forschungseinrichtungen, relevanten öffentlichen Einrichtungen und der Industrie, um sicherzustellen, dass PQC-Lösungen den realen Sicherheitsanforderungen entsprechen und in verschiedenen Anwendungen robust getestet werden, sind ebenfalls willkommen.

Art der Maßnahme	Research and Innovation Actions
Vorläufiges Budget	*6 Mio. EUR*
Vorläufiges Budget pro Projekt	*2-3 Mio. EUR*
Zuwendungsberechtigt	Rechtsträger mit Sitz in EU-Mitgliedstaaten, assoziierten Ländern und OECD-Ländern, die nicht direkt oder indirekt von Drittländern kontrolliert werden
Abrechnung	Förderfähige Kosten werden als Lump Sums (Pauschalbeträge) gewährt
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.

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**