

Nový evropský projekt QARC zajistí kvantově odolnou bezpečnost dat

20.2.2026 - | Národní úřad pro kybernetickou a informační bezpečnost

Šestnáct partnerů z akademické sféry a průmyslu a národních úřadů pro kybernetickou bezpečnost z jedenácti evropských zemí se v průběhu tří let zaměří na zavedení postkvantové kryptografie (PQC) do praxe v reálných aplikacích a kritické digitální infrastruktury. Projektový tým ve spolupráci s národními úřady kybernetické bezpečnosti vyvine nové prototypy PQC řešení a prověří je v realistických pilotních testech. Testování proběhne v prostředí digitalizovaných systémů pro výkon veřejné správy (eGovernment), cloudových infrastruktur, služeb kyberbezpečnostních agentur i vybraných open-source softwarových ekosystémů. Výsledky projektu přispějí k tvorbě strategií a osvědčených postupů, které Evropské unii umožní plynule přejít na kryptografii odolnou vůči budoucím hrozbám kvantových technologií. Zároveň bude projekt zvyšovat povědomí o PQC pomocí seminářů a workshopů.

„Úspěch při zavádění postkvantové kryptografie vyžaduje úzkou spolupráci výzkumu, průmyslu a státních institucí. Přejít na postkvantovou kryptografii není jen technologickou modernizací, ale nezbytným krokem pro zachování dlouhodobé důvěry v digitální služby. Projekt QARC nám umožní poskytnout jasná doporučení a nové podpůrné materiály, které institucím pomohou bezpečně zvládnout změnu kryptografických standardů,“ uvedl Tomáš Rabas, vedoucí oddělení kryptologických analýz a odborný garant v projektu za NÚKIB.

Důležitou součástí projektu **QARC** je aktivní zapojení národních orgánů pro kybernetickou bezpečnost, které hrají klíčovou roli v podpoře praktického přechodu na PQC v zapojených zemích. Úřady z Estonska, Lotyšska, Slovenska, Ukrajiny a Norska budou spolupracovat na tvorbě akčních strategií a plánů implementace PQC a zároveň se podílet na řešení právních, technických i strategických výzev spojených s přechodem na nové kryptografické standardy.

Během tříletého období budou partneři projektu **QARC** vyvíjet a testovat rozsáhlé pilotní implementace PQC, které vytvoří základ pro včasný a koordinovaný vstup Evropy do kvantové éry. Zároveň také přispějí k formování standardů PQC, rozvoji potřebné podpůrné infrastruktury a zajistí dlouhodobou ochranu evropských dat a digitálních služeb.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je v projektu QARC zapojen jako klíčový partner zodpovědný za odbornou expertizu v oblasti kryptografie a koordinaci národního přechodu na postkvantová řešení. Úřad se bude aktivně podílet na vývoji a ověřování metodik pro bezpečnou implementaci post kvantové kryptografie v kritických systémech státu, testování kryptografických prototypů a na hodnocení jejich připravenosti pro praktické nasazení. Současně přispěje k tvorbě strategických dokumentů, analýz a doporučení potřebných pro přijetí PQC v českém veřejném i soukromém sektoru. Díky svému zapojení NÚKIB posiluje roli České republiky v evropském úsilí o bezpečný přechod do kvantové éry.

Bližší informace o projektu naleznete na webu: www.qarc.vut.cz.

Projekt financovaný na základě grantové dohody č. 101225691 je podporován Evropským centrem kompetencí pro kybernetickou bezpečnost (ECCC), financovaným Evropskou unií. Názory a

stanoviska vyjádřená v tomto dokumentu jsou však pouze názory autora (autorů) a nemusí nutně odrážet názory Evropské unie nebo ECCC. Evropská unie, ani poskytovatel grantu za ně nenesou žádnou odpovědnost.

<https://nukib.gov.cz/cs/infoservis/aktuality/2375-novy-evropsky-projekt-qarc-zajisti-kvantove-odolnou-bezpecnost-dat>