

Pogosta vprašanja o načrtu Evropske unije za postkvantno kriptografijo

25.5.2026 - | gov.si

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je pripravil slovensko različico dokumenta Načrt Evropske unije za postkvantno kriptografijo - pogosta vprašanja, ki se navezuje na evropski načrt za prehod na postkvantno kriptografijo (PQC). Evropski dokument je URSIV že prevedel in objavil.

Dokument s pogostimi vprašanji dodatno pojasnjuje ključne vsebine evropskega načrta, zlasti ocenjevanje kvantnega tveganja, določanje prednostnih nalog pri prehodu na PQC, pripravo popisa kriptografskih sredstev, vključevanje dobavne verige, kriptografsko prilagodljivost ter načrtovanje kvantno varnih nadgradenj.

Poseben poudarek je namenjen tveganju scenarijev »shrani danes, dešifriraj kasneje«, pri katerih lahko napadalci že danes prestrežejo šifrirane podatke in jih dešifrirajo v prihodnosti, ko bo na voljo dovolj zmogljiv kvantni računalnik. Zato dokument izpostavlja pomen pravočasnega načrtovanja, stalnega spremljanja tveganj in postopnega uvajanja kvantno varnih rešitev.

Gradivo je pomembno za zavezance po Zakonu o informacijski varnosti (ZInfV-1), organe javne uprave, ponudnike kritične infrastrukture in druge organizacije, ki morajo prehod na postkvantno kriptografijo vključiti v dolgoročno upravljanje kibernetских tveganj.

Dokument pojasnjuje tudi povezavo Načrta EU za PQC z evropskimi zakonodajnimi okviri, kot so Direktiva NIS 2, Akt o kibernetiski odpornosti (CRA), Splošna uredba o varstvu podatkov (GDPR), Akt o kibernetiski varnosti (CSA) in Akt o digitalni operativni odpornosti (DORA).

URSIV s pripravo slovenske različice dokumenta prispeva k boljšemu razumevanju evropskih usmeritev ter k pravočasni pripravi organizacij na prihodnje izzive na področju informacijske in kibernetiske varnosti.

• Načrt Evropske unije za postkvantno kriptografijo: Pogosta vprašanja

- Načrt EU za postkvantno kriptografijo FAQ maj 2026 (pdf, 2 MB)

<https://www.gov.si/novice/2026-05-25-pogosta-vprasanja-o-nacrtu-evropske-unije-za-postkvantno-kriptografijo>