UE își consolideaza securitatea cibernetica cu ajutorul criptografiei post-cuantice

Statele membre ale UE, sprijinite de Comisie, au publicat o foaie de parcurs și un calendar pentru a începe sa utilizeze o forma mai complexa de securitate cibernetica, așa-numita criptografie post-cuantica, se arata într-un comunicat al Executivului comunitar.

"Pe masura ce intram în era cuantica, criptografia post-cuantica este esențiala pentru a asigura un nivel ridicat de securitate cibernetica, consolidând sistemele noastre împotriva amenințarilor viitoare. Foaia de parcurs privind criptografia post-cuantica ofera o direcție clara pentru a asigura securitatea solida a infrastructurii noastre digitale", a declarat Henna Virkkunen, vicepreședinta executiva pentru suveranitate tehnologica, securitate și democrație.

Tehnologiile cuantice pot îndeplini sarcini complexe și pot conduce la soluții pentru provocarile globale actuale, inclusiv schimbarile climatice, detectarea dezastrelor naturale și gasirea de noi soluții în domeniul asistenței medicale. Potențialul tehnologiei cuantice de a aduce beneficii societale este însoțit de riscuri pe care utilizarea sa abuziva le poate prezenta pentru securitatea cibernetica a comunicațiilor și a infrastructurii noastre conectate. O soluție eficienta la aceste provocari este criptografia post-cuantica, care utilizeaza metode de criptare bazate pe probleme matematice complexe pe care chiar și computerele cuantice le gasesc dificil de rezolvat.

Toate statele membre ar trebui sa înceapa tranziția catre criptografia post-cuantica pâna la sfârșitul anului 2026. În același timp, protecția infrastructurilor critice ar trebui sa treaca la PQC cât mai curând posibil, cel târziu pâna la sfârșitul anului 2030, informeaza Executivul comunitar.

Ca raspuns la recomandarea Comisiei publicata la 11 aprilie 2024, Grupul de cooperare NIS a elaborat strategia, reflectând necesitatea ca Europa sa acționeze acum, pe masura ce dezvoltarea calculatoarelor cuantice avanseaza rapid.