Ankstyvoji žinutė organizacijoms apie perėjimą prie postkvantinės kriptografijos

Kada pradėti ruoštis postkvantinei kriptografijai? Vakar!

Kvantinės technologijos atveria naujų galimybių, tačiau kartu kelia ir rimtą pavojų šiuo metu naudojamai kriptografijai. Šiandieninėje elektroninėje erdvėje (pvz. naršant internete, jungiantis prie el. pašto, el. bankininkystės, naudojant skaitmeninius parašus, virtualius privačius tinklus (VPN) ir pan., plačiai naudojami asimetriniai šifravimo algoritmai tokie kaip RSA (*Rivest–Shamir–Adleman*), DSA (*Digital Signature Algorithm*) ir ECC (*Elliptic Curve Cryptography).*

Pakankamai išvystyti kvantiniai kompiuteriai, panaudodami kvantinės mechanikos principus, šiuos algoritmus galės greitai ir efektyviai *nulaužti.* Tai reikštų grėsmę:

- **duomenų konfidencialumui** (pvz., asmens duomenys, sveikatos įrašai, verslo paslaptys);
- **pasirašymo patikimumui** (pvz., elektroniniai parašai, sertifikatai, VPN).

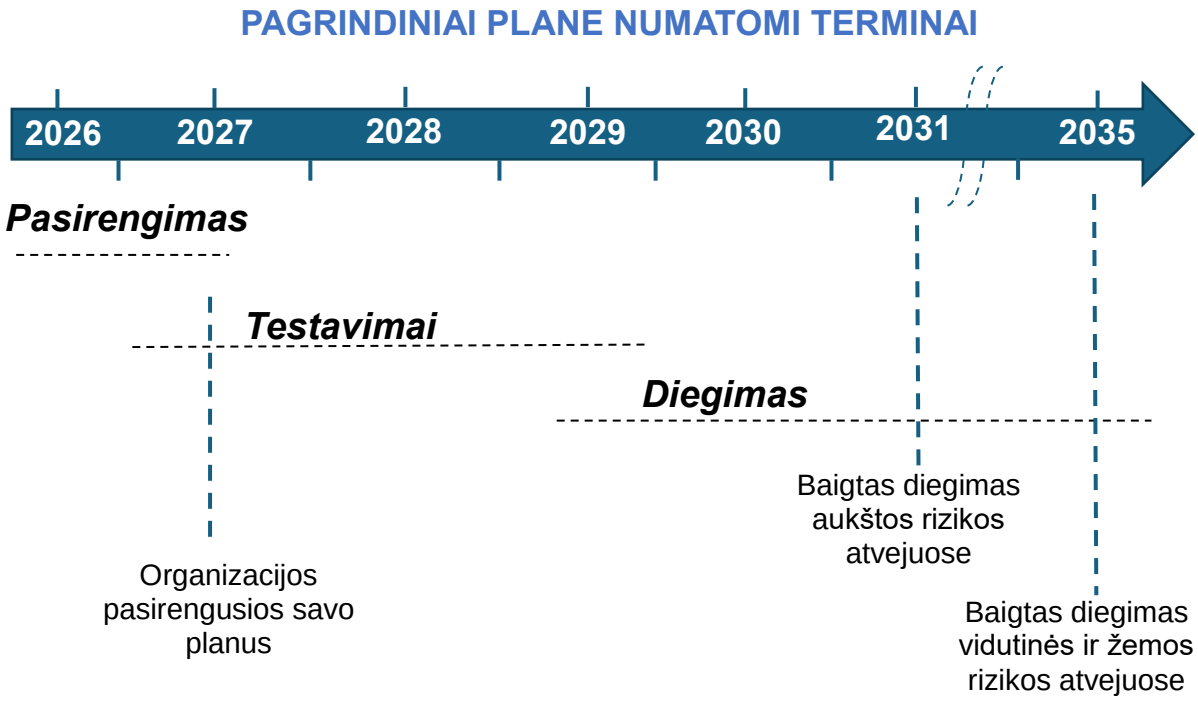
Ypatinga rizika kyla dėl „*Harvest now, decrypt later*“ scenarijaus – kuomet Jūsų duomenys gali būti surinkti dabar ir iššifruoti ateityje, todėl kiekviena delsimo diena tik didina pažeidžiamumą.

Kvantinių kompiuterių keliamą grėsmę galima suvaldyti laiku, kompleksiškai ir koordinuotai pereinant prie postkvantinės – kvantinėms grėsmėms atsparios – kriptografijos ir pakeičiant dabartines kriptografines priemones.

Reaguodama į šią grėsmę, Europos Komisija **įpareigojo ES valstybes nares iki 2026 m. pabaigos**:

1) pasirengti savo nacionalinius perėjimo prie postkvantinės kriptografijos planus;
2) pradėti šių planų įgyvendinimą.

Lietuvoje šį procesą koordinuoja Krašto apsaugos ministerija. Ministro įsakymu sudaryta Nacionalinė perėjimo prie postkvantinės kriptografijos koordinavimo darbo grupė, kuri iki 2026 m. III ketv. parengs Lietuvos perėjimo prie postkvantinės kriptografijos planą. Šis planas bus privalomas visoms organizacijoms, identifikuotoms kaip kibernetinio saugumo subjektams.



Rekomenduojame nelaukti nacionalinio plano patvirtinimo ir visiems kibernetinio saugumo subjektams **nedelsiant pradėti imtis šių** veiksmų:

1. **Informuoti vadovybę ir atsakingus IT saugumo padalinius** apie kvantines grėsmes ir artėjančią būtinybę pereiti prie postkvantinės kriptografijos;
2. **Numatyti atsakingą asmenį ar padalinį** – projekto vadovą, kuris koordinuos pasirengimą organizacijoje;
3. **Pradėti kriptografinių priemonių inventorizaciją** – sudaryti sąrašą sistemų ir paslaugų, kuriose naudojama kriptografija, įvertinti duomenų jautrumą ir ilgo saugojimo poreikius, nustatyti viešojo rakto infrastruktūros (angl. Public Key Infrastructure, PKI) naudojimą;
4. **Pradėti dialogą su tiekėjais** dėl jų pasirengimo postkvantinei kriptografijai, kriptografinio lankstumo galimybės (galimybės greitai atnaujinti algoritmus ar sertifikatus);
5. **Dalintis patirtimi ir sekti tarptautinę pažangą** – stebėti kvantinių kompiuterių raidą, postkvantinių algoritmų standartizavimą, dalyvauti konferencijose ir mokymuose.

👉 ***Laukimas – pats nesaugiausias sprendimas***