Kvanttiturvalliset algoritmit ja niihin siirtyminen

1 PQC-standardoinnin tilanne ja kansalliset kriteerit

Klassiset julkisen avaimen kryptografiset menetelmät ovat haavoittuvia riittävän tehokkaalle kvanttilaskennalle, joten niiden korvaamiseksi on käynnissä useita kansainvälisiä projekteja, jotka tähtäävät kvanttiturvallisten algoritmien (PQC, post-quantum cryptography) standardointiin. Nämä algoritmit perustuvat sellaisiin matemaattisiin ongelmiin, joita ei nykytietämyksen mukaan näytä olevan mahdollista ratkaista kvanttilaskennalla tehokkaasti.

Yksi PQC-algoritmien standardointiin tähtäävä hanke on yhdysvaltalaisen standardisointivirasto NIST:n vetämä projekti, jossa valittiin vuonna 2022 standardoitavaksi yksi algoritmi avainten neuvotteluun (CRYSTALS-Kyber) ja kolme algoritmia allekirjoitusten tekemiseen (CRYSTALS-Dilithium, Falcon, SPHINCS+). NIST julkaisi viime vuonna CRYSTALS-Kyberille, CRYSTALS-Dilithiumille sekä SPHINCS+:lle standardiluonnokset, joissa näitä algoritmeja kutsutaan nimillä ML-KEM, ML-DSA ja SLH-DSA.

Kansallinen kryptotyöryhmä on linjannut[1], että NIST:n standardoimat PQC-algoritmit tullaan lisäämään myös salaustuotteiden arvioinnissa hyödynnettävään kansalliseen kryptokriteeristöön. Kriteeristöä päivitetään sitä mukaan, kun NIST:n standardeja julkaistaan. On kuitenkin mahdollista, että uuden tutkimuksen myötä standardoitavien algoritmien kvanttiturvallisuus todetaan aiemmin arvioitua heikommaksi. Lisäksi näiden algoritmien turvallisuudesta voi löytyä edelleen muitakin heikkouksia, minkä takia alan tutkimusta on hyvä seurata aktiivisesti. Samasta syystä PQC-algoritmien kanssa on suositeltavaa käyttää klassisia julkisen avaimen algoritmeja silloin, kun se on mahdollista. Klassisen ja PQC-algoritmin yhdistelmää kutsutaan hybridimenetelmäksi ja niiden etuna on se, että tiedon turvallisuus ei suoraan vaarannu, vaikka toisesta algoritmista löytyisikin haavoittuvuus. Lisäksi järjestelmissä on hyvä tehdä algoritmien vaihto helpoksi, mitä kutsutaan kryptoketteryydeksi (crypto agility).

On odotettavissa, että ainakin NIST:n standardoimia algoritmeja tullaan käyttämään laajalti standardoiduissa salausprotokollissa, kuten TLS ja IPsec. Näiden standardeista julkaistiin viime vuonna päivitysluonnokset, joissa kuvataan, miten edellä mainitut PQC-algoritmit tulee toteuttaa protokolliin. Joissain sovelluksissa ja protokollissa on jo otettu käyttöön kvanttiturvallisia algoritmeja standardiluonnosten pohjalta. Tällaisia tuotteita ja protokollia ovat mm. Signal, iMessage ja SSH. Lisäksi kvanttiturvallisuuden voi joissain tapauksissa saavuttaa käyttämällä jaettua symmetristä avainta (PSK, pre-shared key) julkisen avaimen menetelmällä neuvotellun avaimen kanssa. Näin ollen salaustuotteiden valmistajilla on hyvät edellytykset saada PQC-algoritmit käyttöön mahdollisimman nopeasti sen jälkeen, kun standardit niistä saadaan valmiiksi.

2 PQC-algoritmeihin siirtyminen

Vaikka kvanttiturvallisten algoritmien standardointi etenee hyvin, liittyy niiden käyttöönottoon erilaisia haasteita, joiden ratkaiseminen edellyttää organisaatioilta jatkuvaa kehityksen seurantaa ja suunnittelua.

Koska kryptografisia algoritmeja hyödynnetään suurimmassa osassa verkkoon kytkettävistä tuotteista, uusien algoritmien tulo tarkoittaa monelle organisaatiolle

[1] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/post-quantum-crypto-aikaan-valmistautuminen-kaynnissa-myos-suomessa

hyvin laajoja järjestelmäpäivityksiä. Näiden päivitysten onnistuminen vie aikaa sekä resursseja ja vaatii tarkkaa suunnittelua. Tämän takia useissa maissa viranomaiset ovat laatineet siirtymän toteuttamiselle ohjeistuksia (esim. [1] ja [2]), joilla pyritään nopeuttamaan siirtymää ja välttämään organisaation luottamuksellisten tietojen vaarantuminen järjestelmäpäivitysten yhteydessä. Näissä ohjeistuksissa neuvotaan organisaatioita tyypillisesti tunnistamaan järjestelmässä käytetyt kryptografiset menetelmät, niiden käyttötarkoitukset sekä järjestelmässä olevat suojattavat tiedot, niiden sensitiivisyys ja suojausaika. Näin organisaatiot voivat priorisoida päivitykset kriittisimpiin kohteisiin ja vähennetään riskiä näiden kohteiden vaarantumisesta. Mitä pidempään päivitysten tekemisessä kestää, sitä enemmän salattuja tietoja voidaan kerätä myöhempää analyysiä varten.

Myös Liikenne- ja viestintävirasto Traficom suosittelee organisaatioita aloittamaan siirtymään liittyvät valmistelut niin pian kuin mahdollista. Siirtymän toteuttamisen apuna voidaan käyttää kansainvälisten viranomaisten laatimia ohjeistuksia. Ohjeistuksissa annetut askeleet siirtymälle ovat pääasiassa samankaltaisia:

1. Siirtymäsuunnitelman laatiminen: Siirtymäsuunnitelman tulee kuvata mitä, milloin ja miten organisaation järjestelmiä päivitetään. Suunnitelmaan kuuluu kryptoinventaario sekä riskiarvio, joiden perusteella laaditaan päivitysten prioriteetit ja aikataulut.

    - Kryptoinventaarion laatiminen: Kryptoinventaario on luettelo organisaation järjestelmien suojattavista tiedoista, niiden sensitiivisyyksistä ja suojausajoista sekä niiden suojaamiseen käytetyistä salausmenetelmistä. Osassa muiden tahojen julkaisuja ohjeistetaan kattavan inventaarion tekemistä ennen päivitysten aloittamista. Koska siirtymään käytetyllä ajalla on paljon merkitystä kvanttiuhkan kannalta, ei kattavan inventaarion tekeminen ole kuitenkaan välttämättä kannattavaa. Sen sijaan on tärkeää tunnistaa sensitiivisimmät tiedot mahdollisimman nopeasti sekä päivittää niiden suojaamisessa käytetyt salausmenetelmät kvanttiturvallisiksi.

    - Riskiarvion tekeminen: Riskiarviossa kuvataan tietoihin sekä järjestelmän osiin kohdistuvat riskit. Tarkoitus on tunnistaa erityisesti riskialttiit osat järjestelmässä, kuten julkiseen verkkoon näkyvillä olevat rajapinnat, joilla siirretään sensitiivistä tietoa. Lisäksi on tärkeää tunnistaa, millä salausmenetelmillä suojataan verkon yli kulkevaa sensitiivistä tietoa sekä millaisia pitkäaikaisia allekirjoituksia järjestelmässä tehdään. Näin riskialttiimpien osien päivityksiä voi priorisoida.

    - Muiden siirtymäsuunnitelmien selvitys: Organisaatioiden tulisi selvittää, millä aikataululla tiedon suojaamisessa käytettyjen tuotteiden valmistajat aikovat toteuttaa kvanttiturvalliset algoritmit tuotteisiinsa. Näitä tietoja voidaan käyttää siirtymään liittyvien päivitysten priorisoinnissa sekä riskiarvion tekemisessä.

2. Päivitysten toteuttaminen: Päivitysten toteuttaminen vaatii organisaation sisäistä koordinaatiota siten, että päivityksiin liittyvät turvallisuusriskit sekä niihin käytetty aika saadaan minimoitua. Mikäli tuotepäivitysten tekeminen on vaikeaa, tulee organisaation varautua mahdollisiin tuotehankintoihin tai muiden mitigointikeinojen toteuttamiseen.

3 Viitteet

1. TNO, AIVD, CWI. The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography. https://ir.cwi.nl/pub/32988/ (2023)

2. CISA, NSA, NIST. Quantum-Readiness: Migration to Post-Quantum Cryptography. https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF (2023)