Samsungi koolitusjuht: häkkerid ootavad kvantläbimurret, mis paljastab inimeste andmed

1 aasta tagasi - 06.02.2025 Autor: AM

Kvantarvutite areng võib lähiaastatel muuta senised krüpteerimismeetodid ebapiisavaks, seades ohtu kasutajate andmed. Samsung on nüüd toonud oma uude Galaxy S25 seeriasse post-kvantkrüptograafia (PQC) põhise andmekaitse, mis hoiab andmed turvalisena ka tulevikus.

Kvantarvutid suudavad teha keerukaid arvutusi kiiremini kui tänapäevased masinad. See võib tuua teaduses ja tehnoloogias suuri läbimurdeid, näiteks kiirendada ravimite väljatöötamist.

Samas kujutavad need ohtu andmeturbele, kuna suudaksid murda paljusid praegu kasutusel olevaid levinud krüpteerimisviise.

“Kui senised krüpteerimismeetodid muutuvad kvantarvutite jaoks lihtsasti murtavaks, on ohus nii isiklikud kui ärilised andmed,” selgitas Samsung Eesti koolitusjuht Alari Pennar. Tema sõnul koguvad küberkurjategijad juba täna tundlikku krüpteeritud infot lootuses, et tulevikus saab selle kvantarvutitega dešifreerida.

Samsung järgib Ameerika Ühendriikide Standardite ja Tehnoloogia Instituudi (NIST) soovitusi ning kasutab ML-KEM algoritmi, mis tagab pilveandmete turvalisuse. See lahendus kaitseb andmeedastust ja vähendab riski, et ründajad saaksid tundlikke andmeid varastada või murda. Eriti oluline on see turvalise suhtluse tagamiseks ühendatud seadmete vahel.

Pennar rõhutas, et Samsungi eesmärk on tagada kasutajatele meelerahu, et nende andmed on pilves kaitstud mitte ainult täna, vaid ka tulevikus, kus küberohud muutuvad keerukamaks. See on eriti oluline seetõttu, et seadmete omavaheline andmevahetus muutub aina tihedamaks. “NIST-i PQC standardid on loodud kaitsma erinevaid elektroonilisi andmeid – alates konfidentsiaalsetest e-kirjadest kuni e-tehinguteni,” selgitas ta.

Sel aastal välja tulnud Samsung Galaxy S25 on esimene nutitelefon, mis kasutab PQC-põhist turvalisust Samsungi pilveteenustes. See tähendab, et kui kasutaja varundab, taastab või sünkroonib oma andmeid Samsungi pilve kaudu, on need juba krüpteeritud viisil, mis peab vastu ka tuleviku küberohtudele.

- Uudised

- Androidiblog
- Mobiiltelefonid
- Turvalisus

Pilt

