ÕPPETUND KÜBERSÕJAST: TUGEV KRÜPTOGRAAFIA ON HÄDAVAJALIK

Vene eriteenistuste eesmärk on saada juurdepääs riigile olulisele infole – nii salajasele kui salastamata teabele.

Info kaitseks tuleb kasutada metoodiliselt hinnatud tugevat krüptograafilist lahendust.

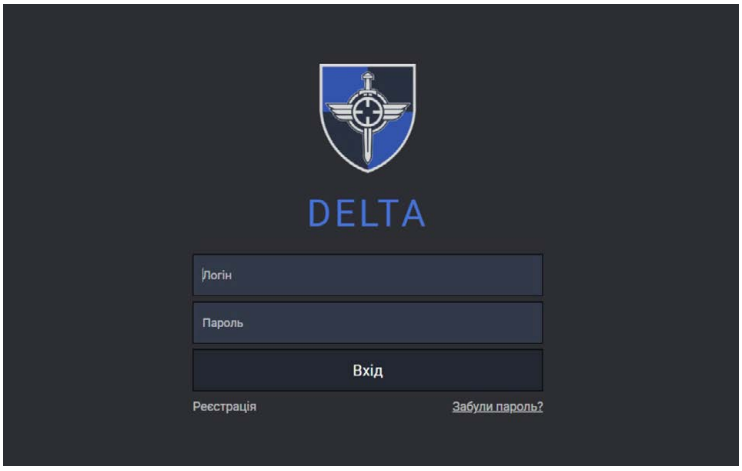
Juba täna on oluline mõelda kvantarvutitest tulenevale ohule ja võtta kasutusele postkvant-krüptograafia.

Sõjas on võidu saavutamisel kriitiliselt oluline, et info jõuaks õigel ajal õigesse kohta. Keegi ei soovi, et info, millest ta edueelist loodab, satuks tema konkurendi või veelgi halvemal juhul vaenuliku riigi eriteenistuse kätte. Teabe kaitseks tuleb teha õigeid valikuid ja leppida, et teatud juhtudel kannatab kasutajamugavus.

Vene eriteenistused teevad pidevalt katseid pääseda ligi tundlikele infosüsteemidele. Sõjas Ukraina vastu on nende fookuses ka Ukraina sõjaväe kasutatavad süsteemid, näiteks olukorrateadlikkuse platvorm Delta, mis on kättesaadav nii telefonist kui arvutist. Delta koondab kokku info lahinguvälja kohta erinevatest kanalitest: õhuseirest, satelliitidest, droonidest, turvakaameratest jm. Kui sealne info venelaste kätte jõuab, satuvad ohtu ka Ukraina sõjaväelaste elud ja sõjaline edu.

Venelased on proovinud erinevaid viise platvormile ligi pääsemiseks:

- küberründed nutiseadmetele, mida rindel olevad ukrainlased sõjapidamiseks kasutavad; võrkudele ligipääsemiseks on venelased lahinguväljalt ka füüsiliselt seadmeid varastanud;
- tehakse võltsitud veebilehti, mis näevad välja nagu päris platvormid, et peibutada sõjaväelasi sinna oma andmeid sisestama;
- proovitakse üle võtta sõjaväelaste meiliaadresse.



Delta platvorm koondab infot vaenlase paiknemise kohta paljudest allikatest (droonid, radarid, satelliidid jm) ning manab selle geolokatsiooniga interaktiivsele kaardile

Allikas: Internet

Suuremaid kahjusid saab ära hoida tundlike süsteemide nutika ülesehitusega.

Ukraina on sellised katsed tuvastanud ja võtnud kiirelt kasutusele vastumeetmed. Muuhulgas saab suuremaid kahjusid ära hoida tundlike süsteemide nutika ülesehitusega: range segmenteerituse (ligipääs ühel kasutajal on piiratud, mitte terviklik) ning teabe krüpteerimisega metoodiliselt hinnatud krüptolahenduste abil.

Ka Eesti riigiasutused ja ühiskonna jaoks olulisi teenuseid pakkuvad ettevõtted on Venemaa eriteenistuste küberluure sihtmärgiks. 2024. aasta oli Eesti jaoks märgilise tähendusega. Toimus avalik küberründe omistamine Venemaa sõjaväeluurele GRU-le. GRU sai 2020. aastal enda käsutusse kümneid tuhandeid asutusesisese kasutamise (AK) märgistusega dokumente. Jah, see ei puuduta riigisaladust, kuid oleks naiivne eeldada, et GRU analüütikud ei suuda mitmest AK märgistusega infokillust panna kokku teavet, mida me oma riigis käsitleme rangelt riigisaladusena.

MILLEKS MEILE KRÜPTOGRAAFIA?

Üks levinumaid teabe kaitse viise info turvalisuse tagamiseks on selle krüpteerimine. Krüpteerimist kasutati juba Vanas Roomas, kui edastaja pidas teavet piisavalt oluliseks, et selle sattumine vaenlase kätte oleks ohustanud isiku, tema lähedaste või Rooma impeeriumi turvalisust ja julgeolekut. Täna on kasutajale märkamatu krüptograafia kasutamine laialt levinud – mobiilsides, suhtlusrakendustes, ruuteri ja arvuti vahelises sides, andmesides internetis või ID-kaardiga teabe krüpteerimisel. See on matemaatikal ja arvutiteadustel põhinev tehnoloogia, mille eesmärk on hoida infot volitamata osapoolte eest salajas ning manipuleerimata. See võimaldab nii infot usaldusväärselt saatja ja vastuvõtja vahel liigutada kui ka määrata matemaatiliselt kindlaks saatja ja saaja enda usaldusväärsuse. Info turvalisust ohustavad ühtviisi nii ebasobivate krüptograafiliste teostuste (algoritmid, võtmepikkused, kvantkindluse puudumine) valimine ja rakendamine kui laiemalt selle olulisuse tähelepanuta jätmine infosüsteemides, nendes kasutavates seadmetes ja teenustes.

Lisaks vaenulikest eriteenistustest lähtuvale küberluureohule on viimasel ajal jõudsalt arenenud kvanttehnoloogiad, mis toovad kaasa ohu klassikalistele krüptoalgoritmidele ja nendega kaitstud teabele. Küberturvalisuse kogukonnas on tähelepanu juhitud probleemile „salvesta täna – dekrüpteeri hiljem“. See tähendab, et kui vaenulikud eriteenistused praegu infot laiaulatuslikult maha salvestavad, siis on teoreetiliselt võimalik seda tulevikus kvantarvutite abil dekrüpteerida ja sealt salastatud infot saada.

Mosca teoreem, mis hindab, millal peame üle minema kvantkindlale krüptograafiale. X – aeg, kui teave peab olema kaitstud; Y – aeg, mis on vajalik süsteemi üle viimisele kvantkindlale krüptograafiale; Z – aeg, mis kulub võimsa kvantarvuti tekkeks

Kvantarvutitest tuleneva ohu vastu tuleb kasutusele võtta postkvant-krüptograafia ehk lahendused, mis kasutavad krüptoalgoritme, mille murdmine ei ole isegi kvantarvutile jõukohane. Nii täna kasutatavaid kui ka kvantkindlaid krüptolahendusi on salastatud süsteemides kasutamiseks vajalik metoodiliselt erapooletult hinnata.

Riik peab suutma oma teabe kaitseks krüptolahendusi metoodiliselt standardiseeritult hinnata. See tähendab, et infosüsteemides kasutavatele lahendustele on kehtestatud konkreetsed nõuded ning kontrollitakse sõltumatult, kas lahendused (krüptotooted, -tarkvarad) ka päriselt nõuetele vastavad. Hinnatakse krüptoalgoritmi vastavust ning pööratakse tähelepanu ka sellele, kuidas seda toodeti, kas ettevõttes on kehtestatud ranged nõuded komponentide käitlemisele, kes on tootja ettevõtte tegelikud kasusaajad, kuidas toimub toote jõudmine tellijani. Usaldust ei tekita mitte üks ja lõplik kontrollija, vaid tunnustatud ja samadele alustele tuginev toodete usaldushindamine. Protsess võtab arvesse riigile olulise info kaitsevajadusi, turbemeetmeid ja rakendamist. Metoodiliselt hinnatud krüptolahenduste kasutamine võimaldab nii vaenulikest eriteenistustest lähtuvaid kui kvanttehnoloogiate laiema kasutuselevõtmisega seotud riske maandada.

Eesti ei ole kummagi ohu suhtes üksi ega eraldatud, vaid sarnaselt füüsilise maailmaga saame ka küberturbes tugineda rahvusvahelistele suhetele, parimatele praktikatele ning nende raames usaldusväärsust tagavatele tegevustele kriteeriumite määramisel, aga ka usalduskindluse standardiseeritud valideerimisel ehk sertifitseerimisel. Eesti on kaitstud, kui meie riigi kõige tundlikum teave on kaitstud – sellesse saab panustada, õppides süvendatult matemaatikat ning sealt edasi krüptograafiat, mis omakorda loob võimaluse töötada pikemas perspektiivis Välisluureametis paiknevas riiklikus sideturbelahenduste heakskiitmise volitatud esindaja kontoris. Lisainfot vaata VLA kodulehelt – www.valisluureamet.ee/infosec.

QBXYB HXFQPB LK LIRIFKB

Teabe kaitse on oluline = (-3) qbxyb hxfqpb lk lirifkb