Kas tervishoid on küberkurjategijate lihtsaim sihtmärk?

Hannes Krause – Riigi Infosüsteemi Ameti juhtivanalüütik

Eelmise aasta lõpus tabas Eestit suuremahuline kampaania, kus asutuste või kodanike arvutitesse jõudsid arvutiviirused, mis muutsid seal olnud andmed kasutuskõlbmatuks või siis ähvardasid seda teha, ning mille puhul nõuti arvutikasutajalt enamasti lunaraha. Selliseid juhtumeid oli eelmisel aastal Eestis 150 ning selliseid arvutiviirusi tuntakse spetsialistide hulgas ka kui „lunavara".

Tegu on järjest tõsisema ohuga, millega peavad arvestama kõik Eesti tervishoiuasutused. Eesti meditsiinis, mis teadagi kasutab infotehnoloogiat järjest kasvavas mahus, võivad küberkurjategijate edukuse tagajärjel sattuda ohtu ka inimelud. Riigi Infosüsteemi Ameti (RIA) küberturvalisuse teenistust teavitati sellistest juhtumitest mitmes kiirabiasutuses ja ka haiglas. Seega on tegu Eesti tervishoiu seisukohalt vägagi reaalse riskiga ning selle vältimisele tervishoiujuhtide vaatepunktist ongi alljärgnevalt keskendutud.

ÜLEMAAILMNE OHT

Küberkurjategijate võimalik edu justnimelt tervishoiuasutuste ründamisel on üle maailma järjest suurem risk. Kui 2015. aastal suurenes erinevat tüüpi lunavara levik oluliselt, siis selle aasta alguses on küberkurjategijad suutnud edukalt lunaraha kätte saada mitmete tervishoiuasutuste käest üle maailma. Samuti on mitmete asutuste tööd suudetud tõsiselt häirida.

Kõige enam ülemaailmset tähelepanu pälvinud juhtum leidis aset Los Angeleses asuvas Hollywoodi Presbüteri haiglas, mille infosüsteemidesse pääses lunavara 5. veebruaril 2016. See muutis haigla arvutites olnud andmed kasutuskõlbmatuks, sundides haiglat järgnenud nädalavahetuse jooksul võtma taas kord kasutusele paberi ja pliiatsi ning suunama enam kui 900 patsienti teistesse haiglatesse (1). Esmaspäeva hommikuks oli haigla maksnud kurjategijatele 40 virtuaalset bitimünti (ingl *bitcoin*), praeguses väärtuses umbes 23 500 eurot. Presbüteri haigla maksis kurjategijate nõutud summa, selleks et tagada haigla normaalne töö, ja alles seejärel võeti ühendust õiguskaitseorganitega (2).

Vaid mõni nädal hiljem tabas sarnane pahavara ka mitmeid haiglaid Saksamaal, kus kurjategijatel ei õnnestunud küll meedia kinnitusel teha samasuguse ulatusega kahju kui Los Angeleses. Siiski peatusid arvutiviiruse tõttu röntgeniaparaadid (3), vereanalüüse tuli registreerida käsitsi (4) ning mitmeid plaanilisi operatsioone tuli edasi lükata. Märtsi algul sai sarnase juhtumi läbi kannatada ka üks suurhaigla Kanada pealinnas Ottawas (5), kus suudeti suuremaid kahjusid kiire tegutsemisega väidetavalt küll vältida. Mai keskpaigas juhtus koguni ka nii, et USAs Kansase osariigis tegutseva südamehaigustele keskendunud haigla kaotas oma andmed kurjategijatele, otsustas maksta neile lunaraha, kuid sellele järgnes uus nõue, kus küsiti järgmist summat (6). See oli kindlasti õppetund neile, kes arvavad, et raha maksmine on kindel tee küberkurjategijate küüsist pääseda.

Kuigi Saksamaa ja Kanada tervishoiuasutused olid kirjeldatud juhtudel kurjategijate rünnaku korral USA kolleegidest ilmselt paremini ette valmistatud ning suutsid haiglate normaalse töö ilma lunaraha maksmiseta taastada, võib, arvestades küberturvalisuse maailma kuldreegleid tegelike kannatanute hulga kohta, eeldada, et ilmselt on küberkurjategijate poolt tervishoius tekitatud kahju nii Euroopas kui ka Ameerikas palju suurem kui need meedia tähelepanu pälvinud juhtumid.

Justnimelt tervishoidu on küberturvalisuse eksperdid hiljuti hakanud pidama ka valdkonnaks, mida rünnates on küberkurjategijatel ilmselt kõige kergemini võimalik raha teenida. Seda äärmiselt lihtsal põhjusel: just tervishoiu toimimine sõltub väga suurel määral püsivalt saadaolevast värskeimast infost patsientide kohta. Olgu selleks väljakirjutatud ravimite ajalugu või tehtud uuringute tulemused, mille kasutuskõlbmatuks muutumise korral – kas või üsna väikeseks ajaks – võib teatud määral peatuda kogu organisatsiooni põhitegevus ehk arstiabi osutamine. Loomulikult võivad sattuda ohtu inimelud või tekkida tervisekahjustuste tekke risk, tuues kaasa hilisemad kohtuhagid patsientidelt (7).

Seega on kurjategijad tõenäoliselt jõudnud tõdemuseni, et üks oma andmed kaotanud tervishoiuasutus võib langetada otsuse lunaraha maksta ilmselt kergemini kui mõni teine asutus mõnes teises valdkonnas.

KAS OHUSTATUD ON KA EESTI?

Eesti on üle maailma tuntud oma digitaalsete teenuste poolest, mille puhul ei ole kindlasti erandiks ka tervishoid. Tervishoiuvaldkonna oluliseks riskiks ei ole siiski

mitte niivõrd meie maailmaklassis e-teenuste võimalik katkestus, vaid arstiabi enda katkemine, mis võib tuleneda häiretest või katkestustest asutuse infotehnoloogilistes (IT) süsteemides.

Nagu on näidanud sellel aastal USA ja Saksamaa juhtumid, sõltub tänapäevane tervishoiuprotsess otseselt IT-süsteemide toimimisest. Lihtsaima näitena võiks tuua vereanalüüsi andmisel info liikumise, mille korral analüüsi tegijalt arstini jõuab teave infosüsteemi kaudu mõne minutiga. See kehtib ka röntgenipiltide või muude andmete puhul, mille olemasolust või millele ligipääsetavusest tervishoiuteenus praegu igapäevaselt ja otseselt sõltub. Sama lugu on erinevate aegkriitiliste andmete liikumisega valvearstideni, sest ühenduse katkemisel võivad kohe sattuda ohtu ka inimelud. Võime eeldada, et rünnak, mille ohvriks on sel aastal langenud tervishoiuasutused USAs ja Saksamaal, võib ka mõne Eesti tervishoiuasutuse puhul kaasa tuua kogu asutuse tegevuse katkemise.

Statsionaarne eriarstiabi ja kiirabiteenus on Eestis kehtiva hädaolukorra seaduse kohaselt elutähtsad teenused, mille osutajad peavad RIAt teavitama kõikidest infoturbeintsidentidest ning mille tagamiseks tuleb neil teha küberturvalisuse vallas riigiga koostööd. Nii tänu sellele kohustusele kui ka tänu infoturbeekspertide omavahelisele heale infovahetusele Eestis on RIA viimase poole aasta jooksul saanud teada mitmetest säärastest juhtumitest Eesti tervishoiusüsteemis – nii kiirabiasutustes kui ka haiglates. Kahjuks on RIA olnud tunnistajaks ka sellele, et meditsiinilised uuringutulemused on muutunud kasutuskõlbmatuks, ning sellisel juhul on tervishoiusüsteemis olemas ka reaalne rahaliselt mõõdetav väärtus. Nendesse juhtumitesse tuleb suhtuda kui otsestesse ohumärkidesse selle kohta, et tervishoiuteenuse katkemine Eestis on kehvasti korraldatud infoturbe tõttu juba reaalne risk.

MIDA SAAB TEHA IGA TERVISHOIUASUTUSE JUHTKOND?

Küberjulgeoleku valdkonnas on pidevalt uusi pahavarasid ning ründemeetodeid arendavad pahategijad alati sammukese eespool vastumeetmete loojatest ja kaitse korraldajatest. Eesti tervishoiu praegust olukorda arvestades on esmane, mida iga tervishoiuasutuse juhtkond riskide maandamiseks teha saab, tagada toimiva ja kvaliteetse IT-teenuse olemasolu asutuses. Kuigi iga tervishoiuasutuse esmane ülesanne on pakkuda kvaliteetset arstiabi, on selge, et IT-teenus ei ole üheski valdkonnas enam pelgalt tugiteenuse tähendusega, vaid ilma selle olemasoluta ei saa ka asutuse põhitegevuses enam kindel olla. Piiratud ressursside kontekstis kõikides tervishoiuasutustes on väga oluline tagada võimalikult kvaliteetne teenus, investeerides selleks kas asutuse IT-personali ja -vahenditesse või ostes teenust sisse. Nii mõnelgi juhul võib olla kõige õigemaks lahenduseks see teenus tervishoiuasutusse sisse osta, et asutus saaks ise keskenduda oma põhitegevusele, kuid ka siis on peamine teha seda targalt.

Praegusaja Eestis on kvaliteetse IT-teenuse puudumise risk kõige suurem just väiksemates tervishoiuasutustes ja nende puhul oleks kõige õigem korraldada IT-teenuste sisseostmist ühiselt, sest just nii on kõikidel osapooltel lootust saada endale kvaliteetsem teenus, mis ka reaalsete küberohtude vastu mingit kaitset pakuks. Kuna tervishoiuasutuse peamine pädevus ei ole IT-teenuste valdkond, on selge, et selle teenuse sisseostmine sellisel kujul, et riskid oleksid maandatud ning seda kannataks välja ka asutuse eelarve, ei pruugi tervishoiuasutusele olla sugugi lihtne. Sellisteks olukordadeks on RIA koostanud näidiseks hulga raamdokumente (8), mis aitavad igal tervishoiuasutusel kvaliteetse IT-teenuseni jõuda. Samuti saab vajaduse korral alati küsimuste esitamiseks ja nõuannete saamiseks RIA poole pöörduda. Korralikult tagatud IT-teenus on iga tervishoiuasutuse jaoks esmane eeldus, et mitte langeda küberkurjategijate kätte ning et tagada arstiabi toimepidevus.

Kui IT-teenuse toimimine on tagatud, on nüüdisaja ohumaastikku silmas pidades tervishoiuasutuste juhtkondade vaatepunktist veel mitmeid teisi asju, mille tagatuses täpsemalt veenduda tasub. Krüpteeriva lunavara sattumist asutuse süsteemidesse või selle võimalike kahjude minimeerimist nakatumisel korraldavad igas asutuses ennekõike IT-spetsialistid, kellele annab RIA pidevalt ka erinevaid juhiseid (9), kuid on ka asju, mida saavad jälgida ja kontrollida tervishoiuasutuste juhid ja peaarstid. Näiteks peaks iga tervishoiuasutuse juhtkond olema veendunud, et asutuse andmetest oleksid olemas varukoopiad ning neid tehtaks tervishoiu eripärasid arvestades vähemalt korra ööpäevas. Samuti tuleks kindlustada, et andmetest tehtavaid koopiaid hoitaks üksteisest eraldi ja selliselt, et peamisesse infosüsteemi sattunud pahavara ei pääseks rikkuma andmetest tehtud varukoopiaid.

Enamasti pääseb andmeid kasutuskõlbmatuks muutev lunavara tervishoiuasutuse infosüsteemi arsti või õe kasutuses olevast arvutist, liikudes sealsete andmete krüpteerimise järel edasi nende andmete juurde, millele ligipääs talle võimalikuks on jäetud. Seega on teiseks oluliseks viisiks küberohtude vastu valmistumise vahendina selge ja piiratud kontroll infosüsteemide kasutajaõiguste üle ning garantii, et iga arsti või õe arvutist ei oleks võimalik teha muudatusi andmekandjatel või serverites, kuhu salvestatakse asutuse kriitilisi andmeid või mille töökindlusest võib sõltuda meditsiiniseadmete töö. Näiteks on Eestis tervishoiuasutuse keskse andmehoidla rike toonud kaasa plaaniliste operatsioonide edasilükkumise – kokkuvõtvalt elutähtsa teenuse katkemise. Seda meeles pidades on igal tervishoiujuhil oluline olla kindel, et ühe tavalise kasutaja arvutist ei saaks sinna pääsenud lunavara ligi

asutuse toimepidevuse seisukohalt olulistele andmekandjatele.

Kolmandaks tervishoiuasutuste juhtide meelerahu tagajaks saab olla teenuse toimepidevuse tagamine juhtudeks, kui asutuse infosüsteemid langevad ühel või teisel põhjusel rivist välja või asutuse andmed muutuvad kasutuskõlbmatuks. Ehk laiemalt on küsimus iga tervishoiuasutuse valmisolekus erinevate kriisistsenaariumide realiseerumisel jätkata osutatava teenuse pakkumist. Siin ei ole oluline mitte ainult plaanide olemasolu paberil, vaid ka nende reaalne läbiharjutamine asutustes. Kui USAs ja Saksamaal sundis lunavara võtma muidu kõrg- ja infotehnoloogiaga harjunud asutusi järsku kasutusele fakse ning paberit-pliiatsit, selleks et üldse arstiabi jätkuda saaks, siis kas Eestis oleksime sellises olukorras suutelised samamoodi toimima?

MIDA TEEB RIIK?

Isegi kõige kvaliteetsema infoturbe ja IT-teenuse korral on ja jääb kõige nõrgemaks lüliks küberturvalisuse tagamisel tavaline arvutikasutaja ja tema teadlikkus selle kohta, kuidas küberohtusid vältida, sest just tema käitumine mängib enamasti kõikide küberohtude realiseerumisel suuremat või väiksemat rolli. Siinkohal on tervishoiutöötajad eriti ohustatud, kuna Eestis kasutavad patsiendid järjest rohkem arstidega suhtlemisel internetti. Tervishoiutöötajal Eestis ei ole paljuski alternatiivi kõikide laekuvate e-kirjade avamisele, saadetavate failide, piltide jm peal klikkamisele, mis kõik võivad tuua kaasa pahavaraga nakatumise ja kehvemal juhul seada ohtu ka kogu arstiabiteenuse osutamise. Sellest lähtudes ongi riik otsustanud tõsta arstide, õdede ja teiste tervishoiu valdkonna töötajate teadlikkust küberohtude vältimise kohta. Nüüdseks on RIA organiseeritud infoturbe teadlikkuse suurendamise koolituse läbinud juba enam kui 400 tervishoiutöötajat üle Eesti ja koolitused jätkuvad. Ootame kindlasti Eesti tervishoiuasutuste tagasisidet toimunud koolituste kohta ning samuti seda, et meile antaks teada asutuste koolitusvajadusest, et saaksime seda infot kasutada oma edasise tegevuse kavandamisel.

KOKKUVÕTE

Küberturvalisus Eesti tervishoius saab sündida ainult teenuseid pakkuvate tervishoiuasutuste ja riigi aktiivses ning pidevas koostöös. Kuigi kogu maailmas on riskid tervishoiuasutustele muutunud viimase poole aasta jooksul järjest reaalsemaks, algab kõik sellest, et Eesti tervishoiuasutused võtaks neid riske senisest tõsisemalt, küsiks vajaduse korral nõu spetsialistide käest ning annaks kõikidest infoturbeintsidentidest teada aadressil cert@cert.ee või kiik@ria.ee. Nii nagu on Eesti tervishoiuteenuse osutajad, on ka Eesti küberturvalisuse tagajad valmis teile abi pakkuma ööpäev läbi.

KIRJANDUS

1. Balakrishnan A. The hospital held hostage by hackers. http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html.
2. Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.
3. Steffen S. Hackers hold German hospital data hostage. http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030.
4. IT-Sicherheit: Computervirus legt krankenhäuser lahm. http://www.spiegel.de/netzwelt/web/it-probleme-in-nrw-computervirus-legt-mehrere-krankenhaeuser-lahm-a-1077469.html.
5. Ottawa Hospital targeted by cyberattack. http://www.cbc.ca/news/canada/ottawa/hospital-cyber-attack-1.3489388.
6. Kansas Heart Hospital hit with ransomware; attackers demand two ransoms. http://www.networkworld.com/article/3073495/security/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html.
7. Why hospitals are the perfect targets for hansomware. https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.
8. IT-halduse raamdokumentide näidised. Lisatud 17.09.2012. Uuendatud 05.04.2016. https://www.ria.ee/ee/raamdokumentide-naidised.html.
9. Veldre A. Lunavarajuhtumi ennetamine. https://blog.ria.ee/lunavarajuhtumi-ennetamine/.

LÜHIDALT

Ravi opioididega ei ole piisavalt tõhus kroonilise mittespetsiifilise nimmevalu korral

Mittespetsiifilise nimmevalu – nii ägeda kui ka kroonilise vormi – ravis kasutatakse sageli opioide. Näiteks määratakse Austraalias nimmevalu raviks oksükodooni 12%-l, tramadooli 2,8%-l, paratsetamooli kodeiiniga 12%-l kõigist nimmevalu puhul määratud ravimitest. Samas ei ole kindlaid andmeid opioidide tõhusama toime kohta nimmevalu ravis.

Austraalia uurijad analüüsisid rahvusvahelistes andmebaasides aastatel 2000–2014 avaldatud artikleid, kus oli käsitletud opioidide toimet ägeda ja kroonilise nimmevalu ravimisel. Kokku analüüsiti 20 artikli andmeid, mis hõlmasid ligemale 8000 vaatlusalust. Neist 13 artiklis leiti opiaatide lühiaegne positiivne mõju kroonilise nimmevalu korral. Pooled osalejatest olid katkestanud ravi kas kõrvaltoimete või liiga väikse toime tõttu. Ravi mõjusus ei sõltunud oluliselt ka kasutatud opioidide annusest.

Uurijad järeldasid, et opioidid annuses 40–240 morfiiniekvivalenti ei taganud kroonilise nimmevalu korral kliiniliselt olulist valu vähenemist (valu vähenes keskmiselt 20 punkti võrra 0–100 punkti skaalal). Analüüsitud materjalide põhjal ei olnud võimalik teha kindlaid järeldusi opioidide tõhususe ja eeliste kohta ägeda mittespetsiifilise nimmevalu ravis. Samuti ei saanud teha kindlaid järeldusi pikemaaegse ravi tõhususe kohta kroonilise nimmevalu korral.

REFEREERITUD

Abdel Shaheed C, Maher CG, Williams KA, Day R, McLachlan AJ. Efficacy, tolerability, and dose-dependent effects of opioid analgesics for low back pain: a systematic review and meta-analysis. JAMA Intern Med 2016;176:958–68.