Hans Lõugas

"Selles pole midagi dramaatilist", kui nähtamatu vaenlane pidevalt meie võrke kompab. "Usaldust on kerge kaotada, julgeolekus vähe võita," kui krüpteerimise tagauksega reedaksime. Nii avab Läti kaitseministeeriumi küberpoliitika juht Ieva Ilves oma seisukohti. Ta rõhutab samas, et küberilma kaitsjad teevad ründajate vastu tugevaid edusamme.

Eesti presidendi abikaasa räägib oma tööst selgelt ja täpselt ning mida edasi intervjuu küberjulgeoleku maailma lahti rullub, seda sagedamini peegeldavad säravad silmad kirge oma valdkonna vastu.

Eesti ja Läti tegelevad kübervaldkonnaga üsna sarnaselt, kuid torkab silma, et Lätis koordineeritakse kõike kaitseministeeriumis, samas kui Eestis on meil eraldi amet (riigi infosüsteemi amet ehk RIA) majandusministeeriumi juures. Miks nii? Kas te suhtute küberkaitsesse rohkem militariseeritult?

Ei, see on väga selgelt ikkagi tsiviilvaldkonnas ja kaitseministeerium oma loomult on tsiviilamet. Läti kaitseministeeriumi all tegutsev CERT (Computer Emergency Response Team, enamikus maailma riikides tegutsev küberintsidentide käsitlemise üksus – siin ja edasi autori märkused) lähtub omaette normidest ja eelarvest. See on umbes samamoodi nagu Eestis RIA-s tegutseb CERT.

Me [kaitseministeeriumis] küll valvame nende üle, aga me ei sekku nende igapäevasesse töösse. Ja see järelevalve tähendab eelarve koostamist ja eelarve suurendamist, kui seda on vaja mingis suunas teha.

See on muidugi aastate jooksul muutunud, sest küberjulgeolekuga tegelemine asus meil varem samuti transpordi- ja kommunikatsiooniministeeriumis. Ja kui Eestis koostati alguses küberjulgeoleku strateegia kaitseministeeriumis ja siis läks see majandusministeeriumi alla, siis meil on see vastupidi liikunud.

Ma arvan, et lõppude lõpuks sõltuvad need protsessid kahest asjast: rahastamine ja isiklik juhtimisvastutus. Loeb see, kui keegi mingi teema eest seisab ja võtab liidrirolli. Kui vaadata üldse, kuidas kübervaldkonnaga riikides tegeldakse, siis põhimõtteliselt koosneb see paarist alateemast: küberkuritegevus (üldiselt sise- või justiitsministeeriumi all), kommunikatsioon ja side, e-valitsemine, küberkaitse ehk julgeolek. Eri riikides langebki valdkonnaga tegelemine nende jaotuste järgi ühe või teise ministeeriumi alla, aga lõpuks sõltub rahast või juhtimisest. Näiteks Taanis on see selgelt kaitseministeeriumi teema, Norras pigem justiitsministeeriumi all ja nii edasi.

Nii et asi pole siis selles, et eelarves on vaja saada täis NATO kaitsekulutuste 2% SKT-st?

Ei, Lätis polnud see põhjuseks. Meie [kaitseministeeriumis] saime aru, et vaja on laia strateegilist juhtimist. Meil oli pisut omavahelist vaidlemist ja transpordiministeerium ei olnud nõus küberkaitse eelarvet suurendama. Meie olime. Ja nii oligi valitsuses üsna lihtne valik teha. Selgitasime isegi parlamendis, et küberkaitse jääb tsiviilvaldkonda ning CERT sai isegi omaette seaduse.

CERT Lätis monitoorib ja jälgib olukorda võrkudes, te pole ju andnud neile ikkagi nii-öelda sunnijõudu?

Me arutame praegu, kas CERT-ist piisab. Seaduse järgi on neil kaheksa ülesannet, mida on palju. Neist peamine on monitoorida võrke ja reageerida intsidentidele ning aidata neid leevendada. Aga selle põhjal on neil ka õigus teha ettepanekuid olukorra parandamiseks. Ja lisaks on neil õigus teenusepakkujaid 24 tunniks võrgust välja lülitada, kui neist lähtub ühiskonnale suurem oht. Lisaks sellele on veel hariduslikud ülesanded ja nii edasi, nii et neil on palju tööd.

CERT teeb oma tööd hästi ja Lätis on aru saadud, et CERT on väga vajalik. Kui kuskil on tulekahju, siis on ju vaja tuletõrjet. Sama seis on võrkudega ja selleks CERT.

Minu nägemuses on ressursse juurde vaja, aga me ei hakkaks ilmselt tegema uut ametkonda, vaid laiendame ja ehitame CERTi tuumiku peale. Ent loomulikult tegutseme me piiratud eelarvega.

Kuidas ja kui palju Balti riigid küberkaitses koostööd teevad?

Väga asjakohane küsimus, sest meil toimusid just kaks päeva tagasi (intervjuu toimus 1. aprillil) kolme riigi küberkaitse konsultatsioonid. Balti küberkaitse eksperdid käisid koos ja see toimub iga aastaselt.

Aga virtuaalselt teeme me palju koostööd, sest nagu vist jaapanlased ütlesid "virtuaalselt oleme me kõik naabrid". Me jagame Balti riikidega samasuguseid ohte, meil on sarnane taristu, meil on palju ühist ja see kõik on nii ka kübervaldkonnas. Poliitikakujundamine on toimunud ühiselt juba alates... iseseisvuse taastamisest, me taastasimegi ju selle ühise pingutusega.

Kübervaldkonnas on meil CERTide kokkuleppe koostööks. See on väga praktiline asi, mille me allkirjastasime alles sel aastal, kuigi seda on visandatud juba ammusest ajast. On ju väga vähe [küber] intsidente, mis on kohalikud. Noh, näiteks mõni kooliõpilane teeb nalja. Aga vähegi suuremad sündmused käivad üle riikide piiride ja siis tuleb küsida, kas naabritel toimuvad sündmused sarnaste mustrite alusel ja nii edasi.

Muide, miks selle kokkuleppe allkirjastamine nii kaua aega võttis – me tahtsime seda teha digitaalselt! See oli paras harjutus. Uskuge mind või mitte, aga sellega läks väga kaua, sest me tahtsime, et iga riigi minister saaks allkirja anda oma kabinetis istudes. Tuli välja palju tehnilisi viperusi, iga riik uuendab oma taristut ja sertifikaate omas tempos ja nõnda edasi. Aga kui mingil teemal peaks ühise digiallkirja panema, siis ometi CERTide kokkuleppele.

Eesti välisluureagentuur kirjutas hiljuti oma esimeses avalikus raportis, kuidas Eesti riigiasutuste võrke on mullu "kaardistatud", et hinnata suuremahulise rünnaku jaoks vajaminevaid ressursse. Kuidas me selliseid teateid teie arvates tõlgendama peaks? On need nagu vene hävitajate "juhuslik eksimine" meie õhuruumi või midagi tõsisemat, nagu tulevahetus piiril?

Ma arvan, et sellised raportid peavad tõstma meie kõigi teadlikkust. Me peame riske teadvustama. Minu jaoks taandub kõik riskidele. Peame aru saama, kui olulised on digitaalsed süsteemid meie riigile või majandusele. Kui mingi [organisatsioon või sihtmärk] muutub poliitiliselt või finantsiliselt suureks, kaalukaks, siis hakatakse kahtlemata kohe "kompama" ja uurima, kas selle võrku on võimalik sisse tungida. Aga meie töö on seda teha raskemaks. See on küber-heidutus, mille mõte on anda märku, et siia on väga raske sisse tungida.

Ma ei näe seda dramaatilise uudisena. See on loomulik, et mida enam meie ühiskond muutub digitaalseks, seda rohkem püüab keegi selle kaitset kombata.

Ukrainat tabas eelmise aasta lõpus maamärgiline küberrünnak ühe elektrivõrgu vastu, mis jättis sadu linnu mõneks ajaks pimedusse. Selle ja enamiku märkimisväärsete küberrünnakute puhul ei saa nimetada rünnaku autorit. Teeb see küberjulgeoleku põnevamaks või hoopis keerulisemaks... kui näiteks nonde hävitajatega võitlemise?

Jah, tõsi, praegu on veel üsna raske öelda, kes rünnakute taga on. Aga me areneme väga kiiresti.

Me õpime analüüsima korraga mitut komponenti. Esialgu oleme me tegelenud [rünnaku] tehnilise osa uurimisega, vaatame, kust rünnak pärineb ja niidiotsad kaovad. Aga nüüd me analüüsime üha paremini ka teisi osi, näiteks rünnaku poliitilist või majanduslikku motivatsiooni. Ja isegi kui me ei saa nüüd rünnakut omistada täpselt nõnda, et see inimene vastutab selle arvuti eest, siis me saame ikkagi juba päris hea hinnangu anda.

Muidugi, juriidilise vastutuse määramine on teine asi. Aga me areneme väga kiiresti, ma tõesti rõhutan, et me teeme suuri edusamme. Me saame rünnakuid suurel skaalal päris hästi omistada.

See on muide üha tähtsam ka uut tüüpi sõjategevuses, kus tank ei sõida üle piiri, vaid toimub nn hübriidne sõda. Sünkroniseeritult tehakse erinevaid asju, millel on üks poliitiline eesmärk, selle hulgas on strateegiline kommunikatsioon.

Sellega tegeleb ju Riias NATO strateegilise kommunikatsiooni keskus, mida te ka hästi tunnete?

Jah, ma juhtusin olema selle projekti juht ja mõnel ajahetkel isegi ainus inimene, kes projektiga tegeles. Mulle meeldiks öelda, et oli meeskond, keda juhtida, aga olin vaid mina... (naerab)

Aga nüüd on see projekt edukalt lõpetatud, keskus töötab ja selle asejuhiks on eestlane Aivar Jaeski.

Täpselt nii ja mul on väga hea meel, et see tehtud sai. Meil oli väga palju arutelusid, kus arvati, et see pole tähtis ja vajalik. Kui Ukraina kriis puhkes sai selgeks, kui oluline osa strateegilisel kommunikatsioonil on.

Krüpteerimine. See on kuum teema nii siin kui sealpool Atlandit, hiljuti ütles Europoli juht, kuidas krüpteerimine on oluline takistus terrorismiga võitlemisel. Mida see teie arvates tähendab, kui peaksime valima, kas oleme krüpteerimise poolt või vastu, valima turvalisuse või privaatsuse?

See on keeruline teema, mis on tihedalt läbi põimunud paljude küsimustega privaatsusest ja andmekaitsest. Aga kui minna tagasi põhialusteni, siis asi on usalduses – mida me muide ka küberjulgeoleku strateegias oleme rõhutanud.

Digitaalsete teenuste vastu on vaja usaldust. Teenus saab olla turvaline siis, kui on krüpteeritud. Kui võtta vaikimisi, et kellelgi on alati võimalus andmed dekrüpteerida, siis see mõjub usaldusele väga halvasti.

Ma mõistan teisalt väga hästi riske ja ohte, aga ma usun, et nendega saab demokraatlikul moel

tegeleda. Kas see on efektiivne viis? Noh, ei, keegi pole öelnud, et demokraatia on kõige tõhusam vahend, aga ilmselt on see siiski parim vahend.

Kui juriidiline raamistik on paigas ehk seadus lubab, siis on [võimudel] näiteks kriminaaljuurdluses õigus kellegi digitaalseid andmeid näha. Siit edasi tuleb küsimus, et kuidas seda tehniliselt teha. Kui lahenduseks oleks kujuteldav võti, mis avaks kõik krüpteeritud andmed – siis ma arvan, et see haavaks usaldust ja ka turvalisust rohkem kui tooks kasu.

Kui lugeda raporteid terrorismist, muuhulgas Brüsseli ja Pariisi rünnakutest, siis paljud neist mainivad järgmist: isegi kui digitaalsetele andmetele oleks 100% juurdepääs, oleks võimud rünnakutest vähe teada saanud või tõenäoliselt olulise käest lasknud. Krüpteeritud andmetele tagaukse loomine ei muudaks seisu eriti kuidagi paremaks, kuivõrd murendaks tugevalt usaldust.

Ma tean, et ka presidendil on selles suhtes tugevad seisukohad, millega ma kipun nõustuma.

Te olete juba jõudnud käia Eestis kooliõpilastele küberkaitsest rääkimas, on seda vaja lapsest saati õpetada?

Ma usun küll. Minu tütar pole veel kaheaastanegi ja ta juba teab, mis on puutetundlik ekraan. Kui telefon näitab PIN-koodi klahve, siis ta juba taipab, et ta peab neid nuppe vajutama. Ilmselgelt ta veel numbrikoodi ei tea, aga juba saab aru, mis tal ekraanil teha tuleb.

Ma arvan, et me peame lastele rohkem õpetama, kuidas turvaliselt internetis käia. Need on samasugused põhimõtted nagu kuidas turvaliselt tänaval olla. Me õpetame, et punase tulega peab peatuma ning teed ületades paremale-vasakule vaatame. Internet muutub sama elementaarseks osaks elust nagu liiklus. Nagu elekter, ära pane näppe pistikusse!

Me oleme muidugi üleminekuajal, mis võib väldata põlvkondi, aga me peaksime juba lapsi harima nii palju kui võimalik, kuidas turvaliselt internetis käituda. Seepärast nimetatakse seda küberhügieeniks – seda võib võrrelda terviseõpetusega, hammastepesuga, või liiklusega.

Me tegime kord ühe näitliku video selle kohta, mis juhtuks, kui inimesed teeksid tänaval sama, mida nad teevad sotsiaalmeedias. Täielik hullumaja: "Mul on uus T-särk või vaadake, laps sündis!" (naerab)

Muidugi ei saa neid üks-ühele võrrelda, aga internetis on vaja teatud hügieen luua ning lastega selleks tööd teha. Lätis oleme selle üle kõvasti vaielnud, haridusministeerium ütleb "olgu, näidake, millise õppeaine me siis praegusest kavast välja võtame, teie otsustage". Just eile lõunatasime presidendiga koos matemaatikaekspertidega, kes ütlesid, et õppekava kui selline vajab ümbermõtlemist. Nii ei saa, et võtame möödunud sajandite õpetamismeetodid ja kuhjame üha materjali juurde. Lapsed ei suuda üha rohkem teha. Kui meil on infole pidev ligipääs, siis õppimine muutub. Turvateema on aga igal pool oluline.

Artikkel Geenius.ee veebilehel .