Erinumber: küberturvalisus Tallinn Digial Summitil

2021-09

Jätkusuutlik rahastus kui usaldusväärse ühendatuse alustala

Reflektsioon Tallinn Digital Summiti avakõnede ning minister Sutti küberturbe rahastamise initsiatiivi üle.

Hüpe vastupidavamasse küberruumi

Kokkvõte küberturvalisuse arutelust digiministrite vahel. Arutelu juhtis Raul Rikk.

Vaata kõiki esinemisi ja paneele järele siit!

Majandus- ja Kommunikatsiooni-ministeerium

Jätkusuutlik rahastus kui usaldusväärse ühendatuse alustala

Martin Paluoja

Kui selleaastase digimaailma suursündmuse Tallinn Digital Summiti võtmeteemat valiti, käis vaieldamatult laualt läbi hulk omadussõnu. Tark ühendatus, kiire ühendatus, tänapäevane ühendatus, globaalne ühendatus. Maanduti aga usaldusväärsel ühendatusel. Zeitgeist.

Kui rääkida targast, kiirest, tänapäevasest ja globaalsest ühendatusest, siis pole keeruline leida otsest majanduslikku (võib isegi öelda ärilist) põhjendust nende maksiimide poole liikumiseks. Kiired ühendused loovad alused uutele kasutoovatele teenustele, globaalne ühendatus võimendab kaubandust - need ideed justkui tasuvad iseenese eest. See-eest oleme viimaste aastatega õppinud, et kiiruse, mugavuse ja efektiivsusega teeb ära vaid pool rehkendust. Kaubanduskeskuses käigu pealt inimesi vaktsineerides jõuame vaid poolele teele. Ülejäänud tee tuleb käia usalduse loomise käänulisel rajal.

Usaldus teenuse või toote, aga ka institutsiooni vastu nõuab läbipaistvust ja avatust, nii avaliku kui erasektori puhul. Kaja Kallas nimetas avakõnes usaldusväärset ühendatust millekski, mille ideoloogiline tuum on meie ühised demokraatlikud väärtused: avatus, läbipaistvus ja üksikisiku õiguste kaitse. Euroopa ülemkogu eesistuja Charles Michel väljendas omakorda vajadust ühiste väärtuste ja standardite järele Euroopas, millest saaksid juhinduda ka kõik meie partnerid. Need standardid peavad olema juurutatud ühistesse väärtustesse: usaldusse ja läbipaistvusse. USA kaubandusminister Gina Raimondo lähenes oma kõnes ühendatusele andmete liikuvuse vaatepunktist: andmete liikuvus tagab nii ühendatuse kui innovatsiooni, kuid mida rohkem andmed mööda maailma rändavad, seda enam on tarvis teha pingutusi nende kaitseks ja nende kasutamise läbipaistvuse tagamiseks.

Kui esinejate sõnumeid kuulata ja lahata, siis küberturvalisuse valdkonnas tegutseva inimesena jäi minu peas kõlama üks võtmetähtsusega, kuid vähe välja öeldud sõnum: see kõik nõuab meilt palju rohkem kui me praegu arvata võime.

Minister Sutt sedastas oma kõnes, et regulatsioonid - nii kohalikud kui Euroopa Liidu tasandil - ei saa omama tuntavat mõju ilma selleta, et rahastus küberturbesse märkimisväärselt kasvaks. Seda sõnumit saab tõlgendada mitmeti. Ühelt poolt, kui näha küberturvalisust kui mingit sorti avalikku teenust või hüve, mida reguleeritav teenuseosutaja või riigiasutus rahvale pakub, võiks näha siin üleskutset iga korralduse või regulatsiooniga anda kaasa ka rahapakk selle rakendamiseks. Kui riik tahab, et bussiliin Palivere ja Koluvere vahel edasi sõidaks, peab ta selle eest ka maksma. Loogiline ju - tegemist on teenusepakkuja jaoks puhta kuluga.

Teiselt poolt nähtuna pole küberturvalisuse kui ühekordse arenguhüppe rahastamine kuskilt otsast piisav lahendus. Suurimad augud küberturbe baashügieenis seisnevad kroonilises alarahastatuses ja kuhjuvates investeeringuvajadustes, alustades taakvarast ja lõpetades puuduliku (või puuduva) turvatestimisega. Sellest vaatest on kriitilise tähtsusega, et me ei otsiks küberturbe rahastamise kasvu riigi-poolsetest rahasüstidest (kuigi need võivad olla vajalikud aktsepteeritava baastasemeni jõudmiseks), vaid kahest fundamentaalsest muutusest mõtlemises ja juhtimises.

Esmalt on vaja hakata nägema küberturvalisuse rahastamist asutuses sellena mis ta tegelikult on: vältimatu ja püsiv kulu, ilma milleta ei saa toimetada. Tõsi, pakendada võib seda kindlustusmaksena, mille alternatiiviks võib olla tulevikus sadades kordades rohkema raha välja käimine, kuid lõpptulemus on see, et samamoodi nagu tehase juhtkond ei saa hakata arutama, kas ja kui palju nad parajasti on nõus elektrisse või käibemaksu investeerima, ei tohiks vajalikud kulud küberturbesse olla küsimuse all.

Esimese sammu saavutamiseks on vaja ka teist: küberturvalisus peab olema juhtide 'asi'. Kui vastutus lasub mujal ja juhini jõuab vaid küsimus kas sel aastal paigutada X eurot serveripargi uuendamisse või uute toodete arendamisse, siis ei saa olla juttu jätkusuutlikust küberturbe rahastamisest ega ka küberturbekultuurist. Nii raha kui ka vastutus on traditsiooniliselt ettevõtete ja asutuste juhtide käes, ning küberturvalisusega ei saa olla teisiti.

See viib meid ministri poolt välja käidud võtmesõnumini, mis sai Tallinn Digital Summitil avalikkuse ette toodud ning mis tõotab saada oluliseks majakaks küberturvalisuse arengus lähitulevikus: **küberturvalisuse kulud peavad olema otseses võrdelises seoses IKT kuludega, ning meie peame seadma selle standardi.**

Nii minister Sutt kui ka Riikliku küberturvalisuse osakond on võtnud üheks oma põhifookuseks küberturvalisuse jätkusuutliku rahastamise, ja seda selle kõige laiemas tähenduses. Mitte ainult selleks, et auke lappida ja vana võlga tasa teha, vaid selleks, et tagada jätkusuutlik rahastus homseks ja ka ülehomseks.

Hüpe vastupidavamasse küberruumi

Osalised: Raul Rikk (juhataja, riikliku küberturvalisuse juht), Andres Sutt (Eesti ettevõtlus- ja infotehnoloogiaminister), Margarete Schramböck (Austria digiminister), Ossian Smyth (Iirimaa digiminister), Oliver Dowden (Ühendkuningriigi digiminister), Josephine Teo (Singapuri digiminister).

Raul Rikk: Ülesandeks on meie digitulevikku kujundada ja ta turvaliseks muuta. Paari aasta eest korraldasime küsitluse, millises Eestis meie rahvas elada tahaks ning vastuste esikolmiku moodustasid „turvaline", „vaba" ja „naturaalne". Üllatav oli, et „tõhusus" ja „innovatiivsus" olid edetabeli teises otsas. Eks ikka innovatsiooni tahetakse, aga selle aluseks peab olema usaldusväärsus. Mis on viimasel ajal olnud kõige olulisem küberintsident, mis on teie mõtlemist ja teie riigi küberpoliitikat muutnud? Milline on küberohtude maastik teie jaoks?

Ossian Smyth: Kui sarnane küsitlus Iirimaal korraldada, siis „turvalisus" ilmselt esikohal ei oleks, Iirimaa asub sedavõrd perifeerias, isegi roomlased ei suvatsenud meid väisata. Iirimaa kaugus ja varasem vaesus on ilmselt paar põhjust, miks paljud meie kallale pole kippunud. Küberrünnakute kontekstis pole aga enam vahet, keda ja kustkohast rünnata. Geograafiline eraldatus meid enam ei kaitse. 2021.a mais rünnati Iiri tervishoiusüsteemi - kõik arvutid ja serverid lakkasid töötamast. Poola kolleegid olid selle kuritegeliku rühmitusega kokku puutunud ja tulid meile appi. Rühmitus nõudis $20 mln lunaraha, millest meie ei maksnud sentigi. Rünnak ise läks meile maksma vähemalt viis korda rohkem. Pääsesime sellest, et me andmed oleks avalikuks tehtud või hävitatud. Igaüks meist võib hommikul ärgates avastada, et mingit olulist osa taristust on rünnatud. Meie kogemus näitab, et ennetus on tõhusam ja soodsam kui ravimine.

Margarete Schramböck: 2020.a jaanuaris rünnati Austria välisministeeriumit. IT-sektoris töötades puutusin kokku suhtumisega, et küberturvalisus on meeletu kulu — reaalsuses on see samasugune kulu nagu kindlustuse eest maksmine. Muretsen väikeste ja keskmiste ettevõtete (VKE) pärast, kel puudub vajalik oskusteave. Suvel rünnati meie piimatööstust, SalzburghMilchi. Olukorra parandamiseks lõime regionaalsed digiinnovatsiooni keskused, kuhu VKE-d pöörduda saavad. Kasutame ka investeerimisboonust: 14% küberturbe investeeringutest maksame ettevõtetele tagasi.

Oliver Dowden: Ühendkuningriigil on riiklik küberkaitse keskus, kuhu oleme siiani £2 mld investeerinud. Olulisemgi veel on mõelda ettevõtetele ja muudele institutsioonidele. Väljakutse on panna inimesi mõistma, et küberrünnakud on neile ohuks. Kel on iganenud IT-varustus, on haavatav. VKE-dele on vahel vaja kõige elementaarsemaid asju selgeks teha: uksed ju paneme instinktiivselt lukku, olgugi et see on tüütu. UK-s keskendume selle sõnumi edastamisele ja ka legislatiivsetele sammudele.

Josephine Teo: Singapuri kodanikud on harjunud turvalisusega. Mõistagi siis küberturvalisuse pärast südant ei valutata. See hakkas muutuma, kui 2018.a rünnati ka meie tervishoiusüsteemi ja varastati tundlikke isikuandmeid. Küberturvalisus on nurjatud probleem: seda ei saa lõplikult lahendada. Esiteks on asümmeetria kaitsjate ja ründajate vahel: kaitsta tuleb kõike, aga ründajatele piisab ühest avausest. Teiseks ei tunne küberrünnakud riigipiire ja vastutuse omistamine on keeruline. Rünnakud ei käi üksnes informatsiooni infrastruktuuri pihta, vaid ka ops tech'i pihta (nt Colonial Pipeline). Singapur on võtnud suhtumise, et küsimus pole, **kas** küberrünnak tuleb, vaid **millal** ta tuleb. Eeldame, et meie süsteemidesse on juba tungitud ning tegeleda tuleb ohuseirega. Lisaks ennetamisele töötame välja reageerimismehhanisme, et rünnakuga kiirelt toime tulla. Valitsused võlgnevad selle oma kodanikele. Viimaks oluliseks tegevuseks on kommunikatsioon ja kodanike usalduse säilitamine.

Andres Sutt: 2007.a pronksiöö küberrünnak

Eesti pihta pälvis maailma tähelepanu. Eestis on üksikute eranditega (ID-kaardi tõrked, andmelekked) olnud võrdlemisi rahulik olukord. Kuid see toonitab Josephine'i argumenti, et tuleb valvel olla ja valmistuda, nii avalikus kui erasektoris. Eestile tehakse u 300 küberrünnakut päevas. Mulle näib, et küberruum on muutumas aina vaenulikumaks. Niimoodi siin kohapeal nendest ohtudest rääkides saab publik aimu, et küberohud on reaalsed. Usaldus ja läbinähtavus on hirmolulised. Eesti tunneb vastutustunnet ja seepärast vaatan küberinvesteeringute formaliseerimise poole. Investeeringud digipöördesse ei tohi unustada investeeringuid küberturvalisusse.

Raul Rikk: Kuidas küberturvalisuse taset siis tõsta? Eestis on ID-kaart ja X-tee olukorda hoopis turvalisemaks muutnud. Kas lahendus peitub regulatsioonides, tehnoloogias, koostöös või mujal?

Ossian Smyth: Kui ennetus on odavam ravimisest, siis on olulisim haridus. On tarvis küberhügieeni harjutada. Iga asutus või organisatsioon peaks üritama omaenda süsteemi sisse muukida. Isegi IT-ettevõtetes läheb tubli 5% töötajatest phishing-meilide õnge. Kui nii juhtub, on küsimus, kui kiirelt ründaja tuvastatakse ja kui sügavale ta tungib. Hävitustöö ennetamiseks on vaja mitmekihilist kaitset. EL-i tasandilt on meil võrgu- ja infoturbe (NIS) direktiiv, varsti avaldatakse uus. Arendame taastemehhanisme kriisidest toibumiseks. Nüüdseks on meie politsei ka IE tervishoiusüsteemi rünnanud rühmituse kodulehti ja pangakontosid kinni panema hakanud.

Margarete Schramböck: Vajame rahvusvahelist koostööd, kuna oht ei ole isoleeritud. Kõigi kodanike digioskused peavad paranema, alustada tuleb juba kooliajal. Inimesed ise on küberriskide keskmes. Lisaks on geopoliitiline aspekt: Austria hinnangul toimub ca neljandik küberrünnakutest mõne riigi toega.

Oliver Dowden: Nägime enne Eesti küsitlusest, et „turvalisus" on kodanike esimene prioriteet. See turvalisus kehtib küberruumile, andmete jagamisele ja laste interneti kasutamisele. Rahvusvahelise koostöö kontekstis on tarvis suurendada meie võimekust kurjategijate identiteet tuvastada ja ka meie julgust seda avalikult välja öelda. UK-s peab valitsus oma IT-taristut uuendama.

Josephine Teo: Küberturvalisus on jagatud vastutus. Meie kui ministrite pingutustest ei piisa. Vastutus algab indiviidiga, kasvõi parooli valimisest. Ettevõtetel on vastutus oma klientide ja aktsionäride ees. Hiljutine uuring Singapuris osutas, et 80% kohalikest ettevõtetest on koroonapandeemia ajal pidanud oma digitaliseerimisplaane kahe aasta jagu varasemaks tõstma. Meie hinnangul aga pole piisavalt panustatud küberturvalisusse. Paljud ettevõtteid ei teagi, kuidas sellega pihta hakata. Singapur arendab VKE-dele tööriistakasti, mis neid aitab. Ühtlasi koostame akrediteerimismehhanismi, mis VKE-dele küberhügieeni õpetab. Küllap on ekslik eeldada,

et üks riiklik küberturvalisuse keskagentuur suudab kõigile väljakutsetele vastata. Oleme siin võtnud sektoripõhise lähenemise: igat tööstust nõustab omaette agentuur. Nii saab arvesse võtta iga sektori eripärasid. Tuleb küsida, kas ka kübervallas on reeglitepõhine multilateraalne maailmakord? Kiidame Eestit, et te küberturvalisuse ÜRO Julgeolekunõukogus lauale panite. Singapur panustab järgmise viie aasta jooksul aktiivsemalt ÜRO-s toimuvatele küberturvalisuse ettevõtmistesse. Viimaks on suutlikkuse suurendamine (capacity-building) ja rahvusvaheline infovahetus.

Andres Sutt: Arutelu käigus on ilmnenud, kui tihedalt ühendatud inimesed ja maailm on. Küberkaitse algab ekraani taga istuvast üksikisikust ning tema oskustest ja suhtumisest. Seda kujundatakse kodus, koolis ja tööl. Kui ka digiruum reeglitele allutada, siis hakkab asi juba ilmet võtma. Küberkuritegudele peab kehtima nulltolerants.

Raul Rikk: Kuidas suhtute küberinvesteeringute formaliseerimisse?

Ossian Smyth: Investeerimine on oluline, aga tarvis on mõõta väljundit, mitte sisendit.

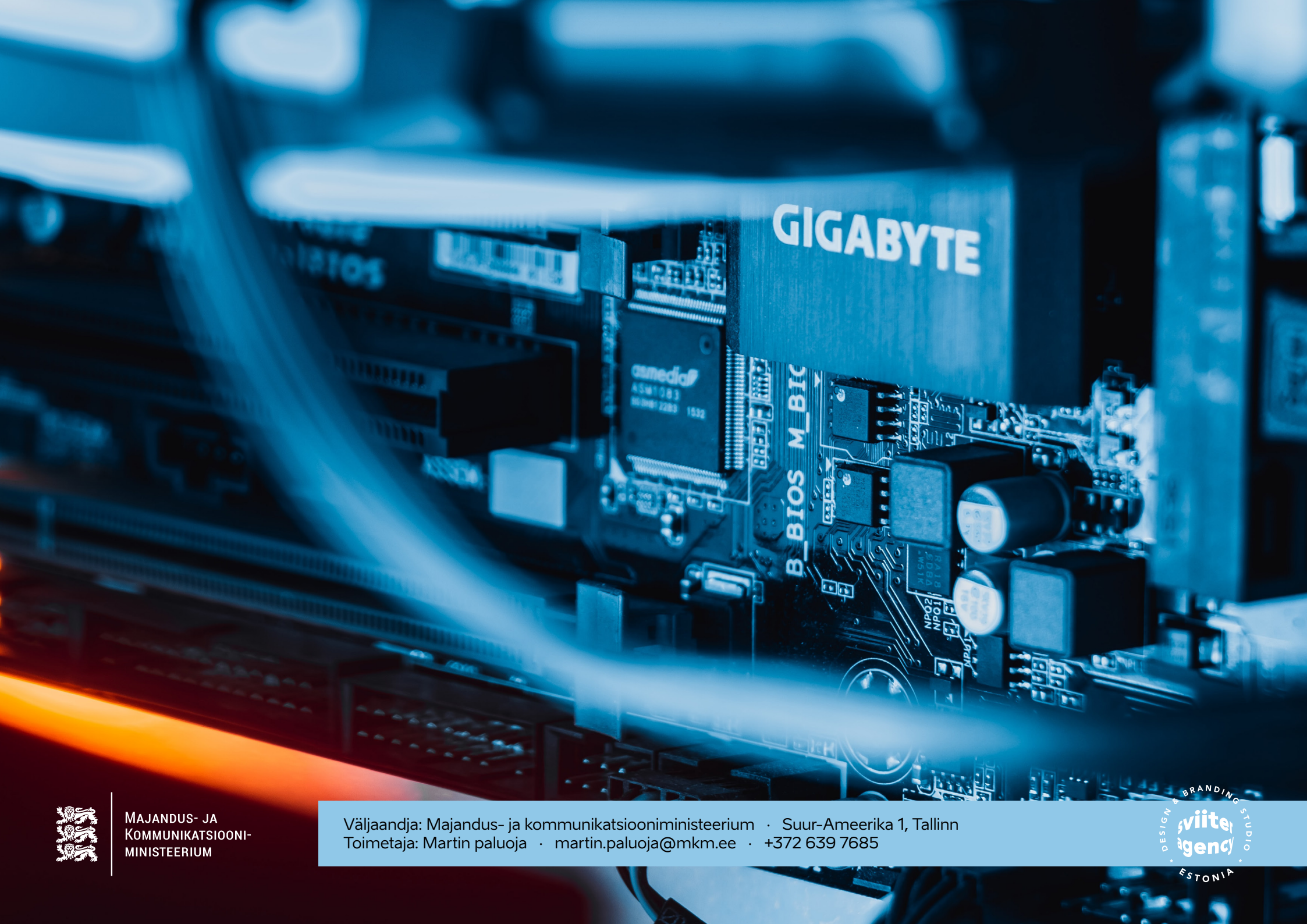
Lunaraha ei tohi maksta, krüptovaluuta muidugi aitab jälgi peita. IT-taristule tuleb kehtestada standardid, et hinnata ühe või teise asutuse või ettevõtte nõrkusi. Ja kui sellist auditit too asutus eirab, siis on vastutus nende õlul. Peame arendama võimekust oma süsteeme uuesti üles ehitada, selleks on vaja võrgust välja lülitatud tagavarasid.

Josephine Teo: Ka meie anname ettevõtetele nõu, et lunavara ei tohi maksta. Ei ole garantiid, et andmed tagasi või süsteemid korda saab. Toetan mõtet, et mingi protsent mingist eelarvest pandaks kõrvale küberturvalisuse jaoks. Teisalt peavad asutuste ja ettevõtete juhid ise aduma oma ainulaadset riskiprofiili. Protsent on hea alguspunkt, aga sellest on vaja enamat. Ei tasuks soodustada ebakriitilist kuuletumist: „linnuke kirjas, probleem lahendatud". Eelistame riskipõhist lähenemist.

Margarete Schramböck: Kalleim lahendus pole tingimata parim lahendus, raha kulutamine lihtsalt kulutamise pärast probleemi küüsist ei päästa. Investeerimisele lisaks on vaja jagada parimaid tavasid ja lahendusi. Küberturvalisuse tõstmise protsess peab olema kaasav.

Oliver Dowden: Idee on huvitav. See töötab hästi, kui selle eest vastutab riik ise, nagu NATO kaitsekulutuste puhul, kus investeeringud on umbes võrdelised väljundiga. Kui protsessis osalevad nii avalik kui erasektor, on vaja natuke enamat. Me ei maksa lunaraha, kui inimesi pantvangi võetakse, miks me seda küberrünnakute puhul teeme? Demokraatiate ülesanne on alati olnud omavahel reeglid kokku leppida ja siis neid kogu maailmas levitada. Digiajastul pole me selle ülesandega veel hakkama saanud. 21. sajandi alusväärtused peavad olema meie väärtused.

Sutt: Väljundit on kindlasti vaja paremini mõõta ja lähenemine peab olema riskipõhine. Meie asi on nüüd lükata see lumepall veerema ja vaadata, kui kaugele välja jõuame!



Majandus- ja Kommunikatsiooni-
ministeerium

Väljaandja: Majandus- ja kommunikatsiooniministeerium · Suur-Ameerika 1, Tallinn
Toimetaja: Martin paluoja · martin.paluoja@mkm.ee · +372 639 7685

Design & Branding Studio Estonia