Riigi Infosüsteemi Amet

Riigi Infosüsteemi Amet
Küberturvalisus 2019

Sisukord

Sissejuhatus. Tugevam e-riik 4
Olukord küberruumis
Olukord Eesti küberruumis 6
Trendid ja tähelepanekud 8
Tehniline näpuviga katkestas ühenduse häirekeskusega 21
Kuidas toimub finantspettus. 23
Küberkogukond aitas parandada haavatavuse riigiportaalis . . 26
RIA tegevused küberturvalisuse parandamisel
Automatiseeritud seirelahendus S4a 28
Valimiste küberturvalisus 30
Küberturvalisuse baasstandard saab uue sisu 32
Turvatestimine pole must maagia 34
EL kutsus eestlased küberturvalisust arendama 36
KüberSIIL tuleb tagasi 38
Küberturvalisus sõltub igaühest
Politsei: kuidas ennetada küberkuritegevust 40
Kübersuursaadik: küberruumis peavad kehtima reeglid 43
Vaated välismaalt 44
Turvaline identiteet
Eestis käib töö kvantarvutite turvamiseks 46
Kuidas sündis uus ID-kaart 49
Küberturvalisuse strateegia aastatel 2019—2022 52

OLUKORD KÜBERRUUMIS AASTAL 2018

SISSEJUHATUS

Tugevam e-riik

Kett on täpselt nii tugev, kui tugev on selle nõrgim lüli. 2018. aastal juhtus mõndagi, mis seda ütlust kinnitab.

Mitukümmend Eesti ettevõtet kirjutasid korstnasse kokku sadu tuhandeid eurosid arvepettuste tõttu. Maakataster pääses napilt maani maha põlemisest. Mitmel korral kadus kogu riigis võimalus pangakaardiga maksta, häirekeskuse liinid olid terve päeva tummad ühe suure mobiilsideoperaatori klientidele, kopamehed lõikasid ära Baltikumi suurima tanklaketi kõik automaattanklad. Lekkisid delikaatsed isikuandmed sõjaväelaste ja koolilaste kohta, pandi toime rünnakuid meediaportaalide vastu, pressiti lunavara välja suurettevõtteilt ja perearstikeskustelt. Intsidentide loetelu võib jätkata pikalt — registreerisime 17 000 pöördumist, mida on enam kui 60 protsenti rohkem kui aasta varem.

Uku Särekanno
RIA küberturvalisuse teenistuse juht

Ometi oli 2018. aasta hea ja turvaline aasta. Hüppeliselt kasvanud pöördumiste arvule vaatamata registreeriti kriitilisi intsidente kokkuvõttes vähem kui aasta varem. NotPetya ja Wannacryga võrreldavaid suuri ja rahvusvahelisi kampaaniaid ei kordunud. E-riigi alustalad, nagu ID-kaart ja X-tee, toimisid stabiilselt ja suuremate tõrgeteta.

Politsei- ja piirivalveamet sulges mais 11 000 ID-kaarti e-teenuste kasutamiseks ning RIA eksperdid murdsid lahti vigase kiibiga ID-kaardi. Sellega sai sisuliselt punkti 2017. aasta ID-kaardi kriis. Õppetunnid olid käes, uusi turvanõrkusi pole ilmnenud ning aasta lõpust asuti väljastama juba täiesti uut ja seni Eesti ajaloo kõige turvalisemat ID-kaarti.

2018. aastal said paika mitmed eeldused, et Eesti e-riik püsiks turvalistel alustel. Korrastus õiguslik raamistik ning valitsus otsustas eraldada IKT valdkonnale oluliselt lisaraha: 2019. aastal 21 miljonit ning järgmise nelja aasta jooksul kokku 118,4 miljonit eurot. Euroopa Liidu tasandil jõustus andmekaitse üldmäärus (GDPR) ning võrgu- ja infoturbe direktiiv (NIS), Eestis aga küberturvalisuse seadus ja isikuandmete kaitse seadus.

Võeti vastu küberturvalisuse strateegia aastateks 2019–2022, mille kolm peamist fookust on uue infoturbestandardi väljatöötamine, riikliku küberturbekeskuse loomine ning süsteemne ennetustegevus. Kogu uut strateegiat kannab arusaam, et investeering halva ära hoidmisse on mitu korda odavam kui tagajärgedega tegelemine. Täpselt nii, nagu politsei pöörab tähelepanu kuriteo ennetusele ja päästeamet tuleohutusele. Riskide väljaselgitamine ja nende maandamine on kokkuvõttes tulemuslikum ja odavam.

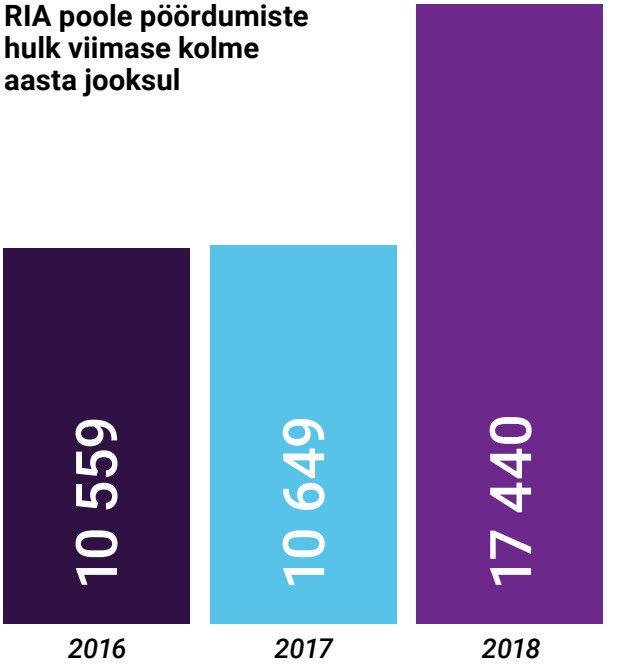
RIA ülesandeks on seadusest tuleneval maandada riske, tõsta teadlikkust ja tagada e-riigi võtmekomponentide turvaline toimimine. Me pakume 400 asutusele Eesti kõige turvalisemat riigivõrku, 15 suurele ettevõttele võrguseire teenust, kümnetele ettevõtetele turbeteste ning sadadele ohuteateid. Kõikidele Eesti kodanikele ja asutustele aga turvalisi lahendusi autentimiseks, digitaalallkirjastamiseks ja andmevahetuseks.

Seda kõike on üksjagu, ent mitte piisavalt. Üle kõige on vaja laiemat suhtumise muutust — arusaama, et küberturvalisus väärib tähelepanu ning see pole IT-osakonna või tehnikute asi. See on ennekõike juhtkonna asi, kes otsustab äriportsessi ja investeeringute üle. Vastasel juhul kannatavad tooted/teenused, kaob maine, kliendid ja raha. Juht annab tegevustele suuna, tunnetuse ja prioriteedid. RIA saab olla siinkohal hea partner ja konsultant. Ent vajadust ja vastutust peab mõistma iga juht ise. Ei tasu olla nõrgim lüli.

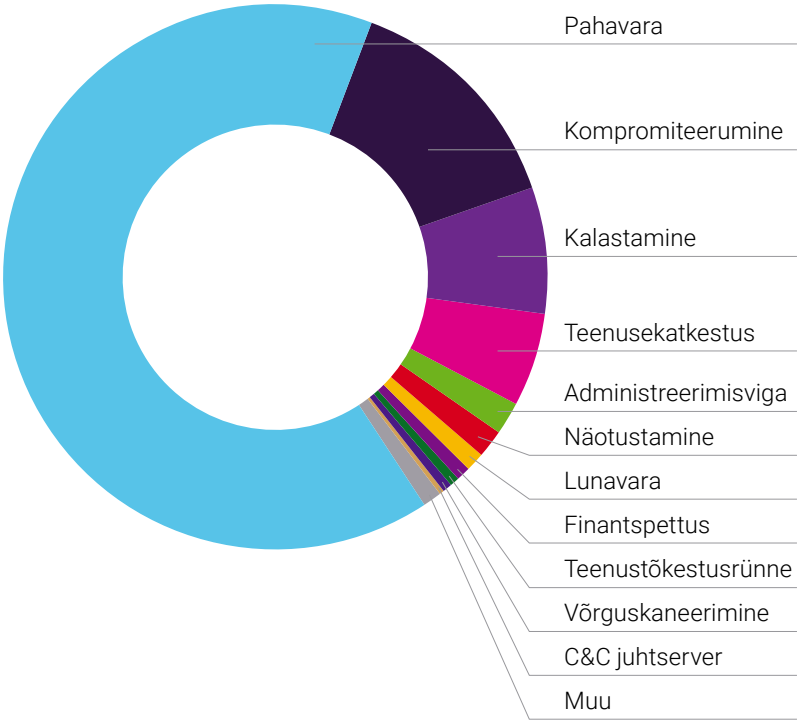
Olukord Eesti küberruumis

2018. aastal jõustunud uued küberturvalisuse ja andmekaitse regulatsioonid andsid meile süsteemsema pildi olukorrast Eesti küberruumis. Võrreldes aasta varasemaga saime pea kaks korda enam teavitusi (17 440 teavitust), mille hulgas registreerisime 3390 andmeid või infosüsteeme mõjutanud intsidenti.

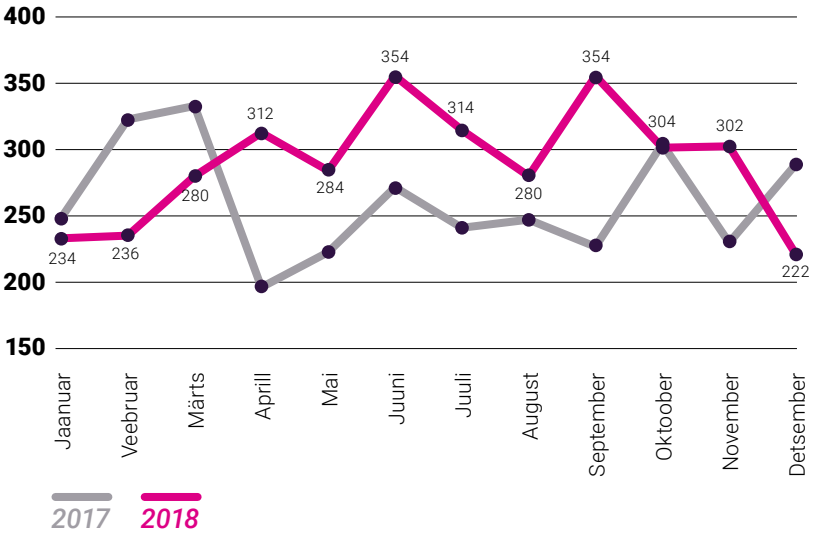
RIA poole pöördumiste hulk viimase kolme aasta jooksul



2018. aastal registreeritud intsidentide osakaal liigiti



Registreeritud mõjuga intsidentide hulk 2018. aastal kuude kaupa



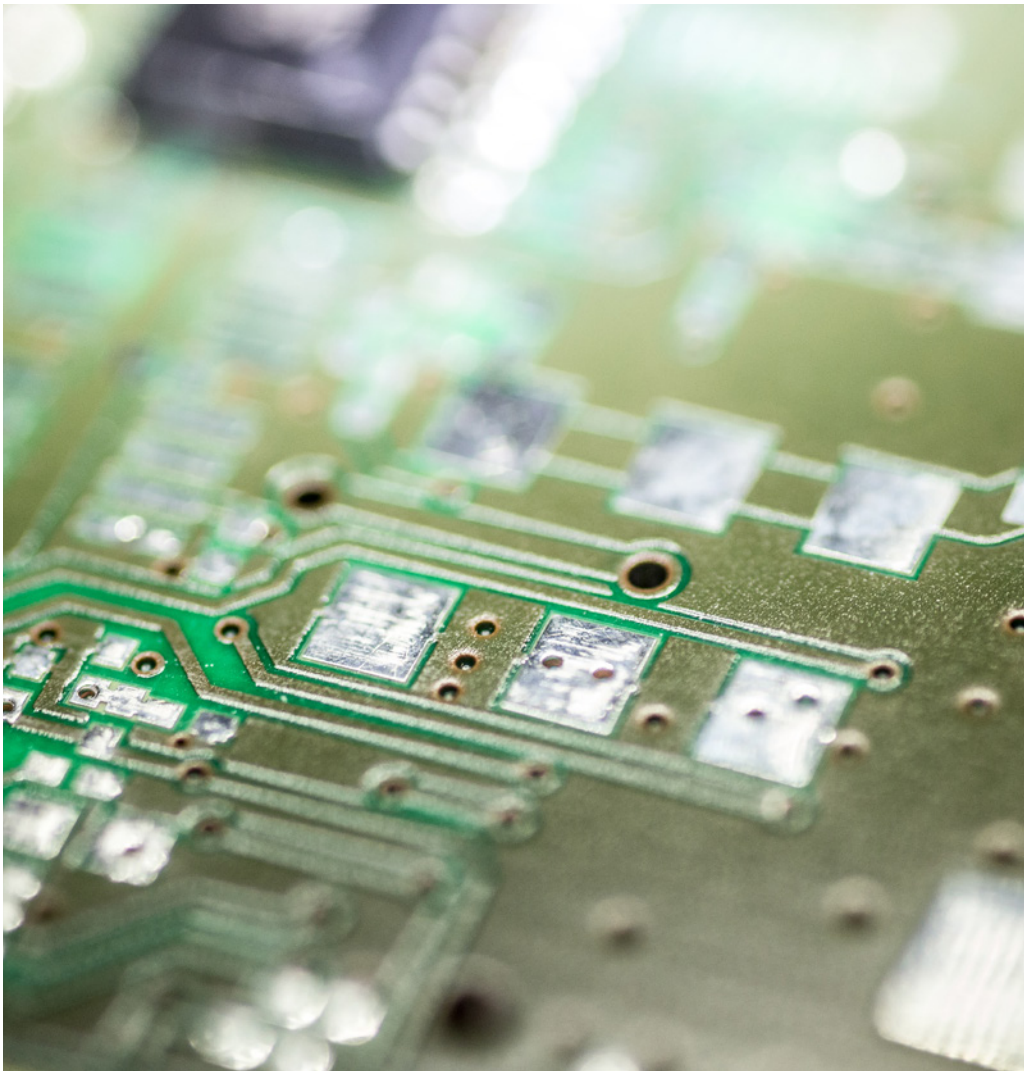
Küberturvalisus tähendab igapäevast tööd

MULLU KIRJUTASIME: ***Turvanõrkused laialdaselt kasutatavas tehnoloogias ei ole ühekordne šokk, vaid keskkonnale iseloomulik, ja selge on, et ilmnenud nõrkusi püütakse ära kasutada. Turvalisus ei lõpe infosüsteemi valmimise või seadme soetamisega, selle hoidmine tähendab järjepidevat tööd ning esmavastutus oma seadme või süsteemi turvalisuse eest on omanikul endal.***

OLUKORD 2018. AASTAL: 2018. aastal jätkus trend, et kui seadmed on haavatavad, siis seda haavatavust kasutatakse ära. Mullu suvel avastati, et teatud väikeettevõtetele ja kodukasutajatele mõeldud internetiruutereid saab kasutada pahatahtlike tegevuste peitmiseks, informatsiooni varastamiseks ja samamoodi näiteks krüptoraha kaevandamiseks. Andsime välja sellesisulise hoiatuse eesmärgiga teavitada kasutajaid vajadusest uuendada tarkvara. Suvel välja antud hoiatustest hoolimata oleme korduvalt näinud era- ja avalikes võrkudes seadmeid, mis kasutavad sama haavatavat, uuendamata tarkvara.

Samuti nägime, et suurt osa Eesti ettevõtete ja asutuste meilikontosid on jätkuvalt võimalik lihtsasti võltsida ning niimoodi pahavara levitada või paluda valedele kontodele raha saata. Mõned e-postiserverite turvalisuse jaoks mõeldud turvalisusprotokollid ja tehnoloogiad on aastaid vanad, kuid jätkuvalt rakendamata.

Samamoodi kompromiteeritakse veebiservereid ja -lehekülgi, millel pole tarkvara uuendatud või turvastandardeid rakendatud.



Kui on välja töötatud uus turvastandard, on vastutustundetu jätkata varasema versiooniga.

KUIDAS EDASI: Küberturvalisuse hoidmine Eestis nõuab pidevat tööd ja juhtide tähelepanu. Uuendused on olulised, standardid samuti, nagu on ka vaja investeerida uuendustesse ja standarditesse aega ja raha. Selleks, et suudaksime Eestis ka edaspidi vältida suure mõjuga küberintsidente, tuleb see töö ära teha. Kui välja töötatakse uus tarkvaraversioon või kui uuendatakse turvastandardit, on vanema versiooni kasutusele jätmine pigem vastutustundetu ning seab ohtu kogu organisatsiooni. See kehtib nii meilikontode, veebiserverite kui ka operatsioonisüsteemide ja sidekanalite kohta.

Nõrkust otsitakse kõikjalt

MULLU KIRJUTASIME: ***Küberründe oht ei sõltu sellest, kas sinu andmed on väärtuslikud kurjategijale, vaid sellest, kas need on väärtuslikud sinule. Enamik küberründeid ei pööra mingit tähelepanu kasutaja isikule, vaid sihivad valimatult kõiki kaitsmata seadmeid ja kasutajakontosid.***

OLUKORD 2018. AASTAL: 2018. aastal Eestis meilikontode kaaperdamise tagajärjel majanduslikku kahju saanud ettevõtted ei olnud ühe kindla valdkonna ettevõtted või kuidagiviisi omavahel seotud: kui ettevõtte meilikontode hulgas oli üks eriti nõrga parooliga kasutaja, saadi just tema kaudu serverisse.

Samuti ei näinud me kindlat mustrit nende lunavaraohvrite seas, kes olid oma serverisse jätnud kaugtöölauaprotokolli kaudu ligipääsu avatuks – kui niisugune võimalus serverist avastati ja leiti üks nõrga parooliga konto, sai just see organisatsioon pihta.

Laiemalt levinud pahavarakampaaniate puhul ei paistnud kurjategijatel samuti väga palju vahet olevat, millise ettevõtte töötaja õngitsuskirjas lingile vajutab ja pahavara endale arvutisse tõmbab. Veelgi suurema võrgu viskasid välja need kurjategijad, kes lootsid lihtsalt hirmutada kasutajaid jutuga, et nende veebikaamerast on neid jälgitud.

Üha rohkem seadmeid on võrkudesse ühendatud, mis tähendab omakorda rohkem riske.

KUIDAS EDASI: Ka praegu hakkab keskmine Eesti ettevõte küberturvalisusele, oma andmete kaitsmisele ja süsteemide toimepidevusele mõtlema enamasti siis, kui intsident on juba toimunud. Riigile oluliste ja elutähtsate teenuste puhul sunnib nüüd regulatsioon juba ennetavaid meetmeid kasutusele võtma. Suurte ettevõtete puhul sunnib neid selleks risk mainele või sissetulekule. Neil on tihtipeale ka ressursse riskide maandamiseks.

Väiksemate ettevõtete ja kodukasutajate jaoks on aga internetti ühendatavad seadmed ja süsteemid muutunud üha taskukohasemaks. IT-võrgu haldamine ja turvamine (ehk inimressurss) muutub aga järjest nõutumaks ja seetõttu kallimaks. Selline olukord võib tekitada lähiajal palju uusi nõrku kohti, mida kurjategijad hakkavad avastama ja ära kasutama.

Küberintsidendid teevad jätkuvalt haiget

MULLU KIRJUTASIME: ***[Wannacry ja NotPetya] pahavarakampaaniad põhjustasid maailmas miljarditesse ulatuvat majanduskahju ning kätkesid endas ka vahetut ohtu inimeste elule ja tervisele. Eestis oli kahju minimaalne; olime ohust sammu ees nii tänu turvapaigatud süsteemidele kui operatiivseirele ja kiirele infoedastusele. Viidatud kampaaniad ei jää aga viimaseks.***

OLUKORD 2018. AASTAL: Pahavarakampaaniad ei ole ainsad, mis inimestele ja ettevõtetele kahju teevad. Väikese viitajaga jõudis Eesti kasutajateni maailmas palju kahju teinud ettevõtete meilikontode kaaperdamise kampaania (Office 365 meilikontode kompromiteerimine), niinimetatud *sextortion*-kampaania, kaugtöölaua (Remote Desktop Protocol) kaudu lunavara paigaldamise kampaania, aga ka Loki-Bot pahavarakampaania.

Tegevjuhi petuskeemi kaudu ja meilivestluste kaaperdamisest alanud finantspettuste tagajärjel said Eesti väike- ja keskmise suurusega ettevõtted 2018. aastal vähemalt 600 000 eurot kahju. Kogusummast olulisem on see, et väikesele Eesti ettevõttele on ka 10 000- või 20 000-eurone väljaminek kurjategijatele märkimisväärne kaotus – selliseid kahjusummasid nägime keskmiselt korra nädalas. Ettevõtted kaotasid eelmisel aastal ka kliente ja käivet nendel päevadel, kui nad parasjagu lunavaraintsidentide tõttu oma andmeid taastasid.

Võime olla kindlad, et eelmainitud summad ei peegelda kogu kahju Eesti majandusele, sest kindlasti oli kannatanuid, kes teavitasid ainult õiguskaitseorganeid. Koostöös politsei- ja piirivalveametiga saatsime eelmise aasta lõpus kõigile Eesti ettevõtetele välja ka kirja, mis küberpettuste eest hoiatas. Täname kõiki ettevõtjaid, kes meid juhtunud küberintsidentidest mullu teavitasid, sest vaid nii on võimalik saada tõepärane pilt ohtudest ja kahjudest Eesti küberruumis.

KUIDAS EDASI: Me ei kavatse sellise olukorraga leppida. Kurjategijate elu saab teha kas väga lihtsaks või keerulisemaks kui see praegu on. Ka küberturvalisusele palju tähelepanu pöörav ettevõte võib saada kahju oma äripartneri tõttu, kes seda teinud ei ole. Kurjategijad otsivad kõige nõrgemat lüli ning selle leidnud, püüavad kõiki andmeid enda jaoks rahaks teha.

Jätkame igapäevast teavitustööd, kus pöörame tähelepanu elementaarsele küberhügieenile. Selle kõrval vaatame tänavu eraldi, kuidas on võimalik meil kõige paremini Eesti ettevõtete küberturvalisust arendada. Ootame ka ettevõtete juhtidelt ja IT-personalilt tagasisidet, kuidas saame neid paremini aidata.

Eesti ettevõtjad said palju kahju välispartnerite meilikontode kompromiteerimiste tõttu.

Kriitilised andmed vajavad kriitilist tähelepanu

MULLU KIRJUTASIME: ***Iseäranis tervishoiuvaldkonna küberturvalisus vajab tõhusamat tuge. Olukorras, kus haiglad ja perearstikeskused töötlevad meie kõigi delikaatseid isikuandmeid ja nende töö sõltub suurel määral digitaalsete süsteemide toimimisest, ei tohi neid jätta olukorda, kus küberturvalisus konkureerib ressursi pärast tervishoiuteenuse osutamisega.***

OLUKORD 2018. AASTAL: Nägime ka mullu küberintsidente tervishoiuvaldkonnas ja terviseandmete lekkeid. Näiteks ühe perearstikeskuse infosüsteemid krüpteeriti lunavaraga, mis häiris oluliselt patsientide vastuvõtmist. Riigi enda dokumendihaldussüsteemides olid valesti märgitud ja seetõttu avalikult nähtaval kaitseväelaste terviseandmed ja koolilaste terviseandmed. See ei ole ainult Eesti küsimus – tervise- ja delikaatsete isikuandmete lekkeid nägime igal pool üle maailma.

Samas tegime pidevalt tööd selle nimel, et tervishoiuvaldkond suudaks informatsiooniga turvalisemalt ümber käia. Korraldasime tervishoiutöötajatele kümneid koolitusi, millel on osalenud sadu tervishoiutöötajaid üle Eesti. Perearstid said eelmisel aastal oma oskuste arendamiseks küberhügieeni digitesti, mida nad on ka tublisti kasutanud. Tellisime eraldi analüüsi perearstide kasutatavatele üleriigilistele infosüsteemidele, mille kaudu terviseandmeid töödeldakse ja tööd korraldatakse.

Nüüdisaegse meditsiini protsessid sõltuvad püsivast ligipääsust erinevatele terviseandmetele.

KUIDAS EDASI: Isikuandmete lekkimise vältimise juures on esimene oluline samm küberturvalisuse tagamine. See tähendab selleks vajalike meetmete süsteemset rakendamist, millele peavad taas kord tähelepanu pöörama organisatsioonide juhid. Isikuandmete talletamise ja käitlemise süsteemid vajavad järjepidevat riskide maandamist, tarkvarauuendusi ja uutele turvalisematele standarditele üleminekut organisatsiooni suurusest hoolimata.

Näiteks tervishoiusektoris peavad lisaks haiglatele 2022. aastaks ka väikse meeskonnaga perearstikeskused enda küberriskid välja selgitama ja oskama neid maandada – seda nõuab küberturvalisuse seadus. Selle jaoks pakume perearstikeskustele koolitusi, kus saame neid toetada vajalike ja sobivate meetmete väljatöötamisel. Samuti jätkame tervishoiutöötajate küberhügieenikoolitustega.

Selgem regulatsioon seab selgemad kohustused

MULLU KIRJUTASIME: ***Küberturvalisuse seadus toob suurema õigusselguse, ent seadus ei lahenda kõiki haavatavate valdkondade muresid. Uus küberturvalisuse seadus korrastab rollid, mõisted ja vastutuse Eesti küberturvalisuse korraldamisel, ent seaduse rakendamise kõrval jääb oluliseks tihe partnerlus riigi- ja erasektori asutustega.***

OLUKORD 2018. AASTAL: 2018. aasta keskel võttis riigikogu vastu küberturvalisuse seaduse, millega kehtestati tugevamad nõuded ettevõtjatele ja riigiasutustele nii küberohtudeks valmistumiseks, infosüsteemide ja andmebaaside haldamiseks kui ka küberintsidentidest teavitamiseks. Kõige otsesemalt mõjutas seadus teenusepakkujaid, kes osutavad elutähtsaid teenuseid, nagu näiteks elektriga varustamine, arstiabi või ID-kaardi isikutuvastuse tagamine.

Oma klientide andmete küberturvalisuse tagamist peavad pingsamalt hakkama järgima ka kõik digitaalse teenuse osutajad, olgu selleks siis e-poed või ka otsingumootorid, kes meie küberruumis tegutseda soovivad. Seaduse rakendamiseks valmis mullu suvel ka määrus, mis pani paika riskide väljaselgitamise ja turvameetmete täpsemad nõuded.

2018. aasta lõpus kiitis valitsus heaks ka küberturvalisuse strateegia aastateks 2019–2022, mis sõnastas eesmärgid nii meile kui teistele riigiasutustele ja valitsusega seotud sihtasutustele. Strateegiat tutvustame täpsemalt veel siin aastaraamatus.

KUIDAS EDASI: Küberturvalisuse seadus pani konkreetselt paika, kes milliseid nõudeid täitma peavad. Eelmisel aastal pidid selle seaduse kohuslased oma riskid ära hindama ja kirja panema, kuidas nad neid riske maandavad. Need tegevused on nüüd vaja ellu viia. Tänu senisest paremale ja selgemale süsteemile võime eeldada, et oluliste ja digitaalsete teenuste osutajad on tänavu paremini kaitstud. See uus süsteem täiustab meie teadmist selle kohta, mis Eestis toimub, mistõttu võime oodata sel aastal veelgi suuremat hulka registreeritud intsidente.

Ühiskonnale oluliste teenuste pakkujate küberturvalisus on meie kõigi ühine mure.

Tähelepanekud 2018. aasta intsidentidest

SUURIM OSA INTSIDENTIDEST

Pahavara ja robotvõrgustikud

Kõige enam on mõjutatud infosüsteemide terviklikkus (mis tähendab, et infot või infosüsteemi on keegi loata muutnud). Enamik neist on robotvõrgustikuga nakatunud seadmed, millest oleme kirjutanud ka varasemates aastaraamatutes. Hoolimata regulaarsetest teadetest nakatunud seadmete omanikele, nägime siiski, kuidas 2018. aastal võtsid tuhandetelt IP-aadressidelt seadmed korduvalt robotvõrgustikuga ühendust.

Kuidas robotvõrgustikke kuritegevuses ära kasutatakse

Robotvõrgustikku kuuluvat liiget võib ära kasutada nt teenustõkestusrünnakutes, pahavara levitamiseks (nt pangaandmete varastamiseks). Samuti renditakse robotvõrgustikku välja kurjategijatele, kes soovivad laiendada oma pahavara saajate ringi (pahavara platvormi kui teenuse kasutamine ehk *crimeware-as-a-service infrastructure*.)

Avalikus sektoris tuvastatakse pahavaraga nakatumine kiiresti. Enamikul juhtudel on robotvõrgustiku liige (ehk nakatunud seade), mis tuvastatakse avaliku sektori haldusalas, tegelikult eraisiku nakatunud arvuti, mida ta on otsustanud tol hetkel kasutada mõnes avalikus wifi-võrgus, mis annab talle siis avaliku sektori IP-aadressi.

Erasektori võrkudes avastatud, robotvõrgustikuga nakatunud seadme puhul teavitatakse esmalt internetiteenuse pakkujat, kuid see informatsioon ei pruugi alati jõuda lõpptarbijani, ning isegi kui jõuab, ei pruugi lõppkasutaja aru saada, mida see mõjutab ja kuidas oma arvutit kaitsta.

ENIM RAHALIST KAHJU TOONUD INTSIDENDID

Tegevjuhi petuskeem

Finantspettus, kus ettevõtte tippjuhi nimelt saadetakse raamatupidajale lühike ja lakooniline küsimus, kas on võimalik kiiresti saata mingi summa võõrale arveldusarvele. Enamasti kasutatakse võõrast meiliaadressi, mille omanikuks on lihtsalt lisatud tippjuhi nimi.

Ettevõtete meilikontode kompromiteerumisest alguse saanud finantspettused

Mullu sügisel hakkasime taas saama teateid mõne aasta vanusest petuskeemist, kus kurjategijad püüavad ettevõtetelt raha välja petta, kasutades ära kompromiteeritud meilikontode ja meilivestluste sisu. Pikema meilivestluse ühes etapis palub kompromiteeritud partner muuta ettevõtete omavahelise ülekande jaoks pangakonto andmeid. See tähendab aga, et ühe lühikese perioodi jooksul ei tea kumbki osapool, et meilivestlused on kaaperdatud.

MÄRGATUD, KUID ENAMASTI EI JÕUDNUD KAHJU TEKITADA

Sekspressimiskirjad (*sextortion*)

2018. aasta suvel levis üle maailma väljapressimiskirjade laine, kus kurjategijate eesmärk on hirmutada kirja saajat väitega, et neil on ligipääs ohvri IT-seadmetele ning ülevaade veebilehtedest, mida inimene on külastanud. Selleks, et väljapressimiskiri oleks usutav ja tõsiseltvõetav, on kurjategijad kasutanud aastate jooksul lekkinud paroole ning lisanud kirjale ohvri kunagise parooli, e-posti aadressi või telefoninumbri. Suurem osa paroolidest, mida kurjategijad kasutavad, on lekkinud mitu aastat tagasi.

ENAMASTI MÄRKAMATULT KAHJU TEKITANUD

Arvutiressursi kasutamine krüptoraha kaevandamiseks

Krüptoraha populaarsuse (ja hinna) kasvuga 2017. aasta lõpus püüdsid kurjategijad leida üha paremaid viise, kuidas seda koguda – enamasti nõuab selle „kaevandamine" elektrit ja protsessorite ressursse. Avalikult teadaolevate haavatavustega seadmed (näiteks kodukasutuses olevad ruuterid), millel ei ole uuendatud tarkvara, andsid ründajatele lihtsaid viise teiste inimeste arvutiressursside kasutamiseks. 2018. aasta esimeses pooles erakordselt silma jäänud trend.

KUST INTSIDENDID TIHTIPEALE ALGUSE SAID

Õngitsus- ja pahavara levitavad kirjad

Nägime mitmeid kampaaniaid, kus tuntud ettevõtete nimede alt saadeti pahavara sisaldavaid kirju või õngitsuskirju. Meile on teada vaid üksikud nakatumised – kasutajate teadlikkus võõrastest kirjadest leitud failide avamisel on tõusnud ja pahavarakaitsed tihtipeale ei lubagi selliseid kirju läbi. Samas langevad kasutajad jätkuvalt tihti õngitsuskirjade kaudu kasutajaandmete varguse ohvriks. Valesse kohta sisestatud paroolid viisid tihtipeale uute küberintsidentideni, nagu järgmiste õngitsuskirjade väljasaatmine, finantspettused ja pahavara levitamine.

MILLEL OLI MÕJU KÕIGE SUUREMALE HULGALE INIMESTELE

Teenusekatkestused

Eesti ühiskond on digitaalsetest teenustest üsna tugevasti sõltuvuses – alates autentimisest kuni tervishoiuteenusteni. Seetõttu mõjutasid kõige suuremat hulka inimesi lühikesed teenusekatkestused just avalikus sektoris, mis omakorda olid tihtipeale põhjustatud administratiivsetest vigadest.

Tehniline näpuviga katkestas ühenduse häirekeskusega

2018. aasta kõige suurema mõjuga intsident juhtus kohe aasta alguses, kui 24. jaanuaril ei olnud suurel hulgal Elisa Eesti klientidel võimalik helistada hädaabinumbrile 112. Kaheksa ja poole tunni jooksul püüdsid 151 abivajajat teha kokku umbes 600 kõnet ega saanud häirekeskusega ühe ndust. Õnneks lõppes juhtum tõsiste tagajärgedeta.

Kuigi esimene ebaõnnestunud kõne Elisa võrgust tehti häirekeskusele hommikul kell 10.40 (112-le helistanud kuulsid vastuseks teadet „Number ei ole kasutusel"), tuvastati rike alles kaheksa tundi hiljem. Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT)

töötajad said rikkest teada kella 18 paiku, kui üks politsei infotelefonile helistanud Elisa klient andis neile teada, et tal ei ole võimalik hädaabinumbrile helistada.

SMITi tehnikud teavitasid Elisat ning alles paar tundi hiljem sai veast teada häirekeskus. Veerand tundi pärast rikkeinfo saamist muutis Elisa tehnik võrgu konfiguratsiooni, mille tulemusel õnnestus viga kella 19ks parandada.

Rikke põhjustas samal hommikul tehtud võrgu konfiguratsiooni muudatus. Ühe varasema vea parandamise käigus aga ei märgatud, et see mõjutab ka helistamist numbrile 112. Viga ei mõjutanud kõiki Elisa kliente, vaid ühe keskjaamaga ühendust võtvaid mobiilikasutajaid, sealhulgas välismaa operaatorite kliente, kes kasutasid Elisa *roaming*-teenust. Samas ei ole teada, kui palju hätta jäänud klientidest leidis abi saamiseks alternatiivseid võimalusi – kõne tegemist teise telefoni kaudu, SIM-kaardi eemaldamist või pöördumist politsei poole, helistades numbrile 110.

Juhtum näitas ilmekalt, kuidas ühest väikesest administreerimisveast võib tekkida olukord, mis mõjutab otseselt inimeste elu ja tervist.

Elisa ise päeva jooksul probleemi ei märganud ja sai intsidendist teada vaid tänu SMITile.

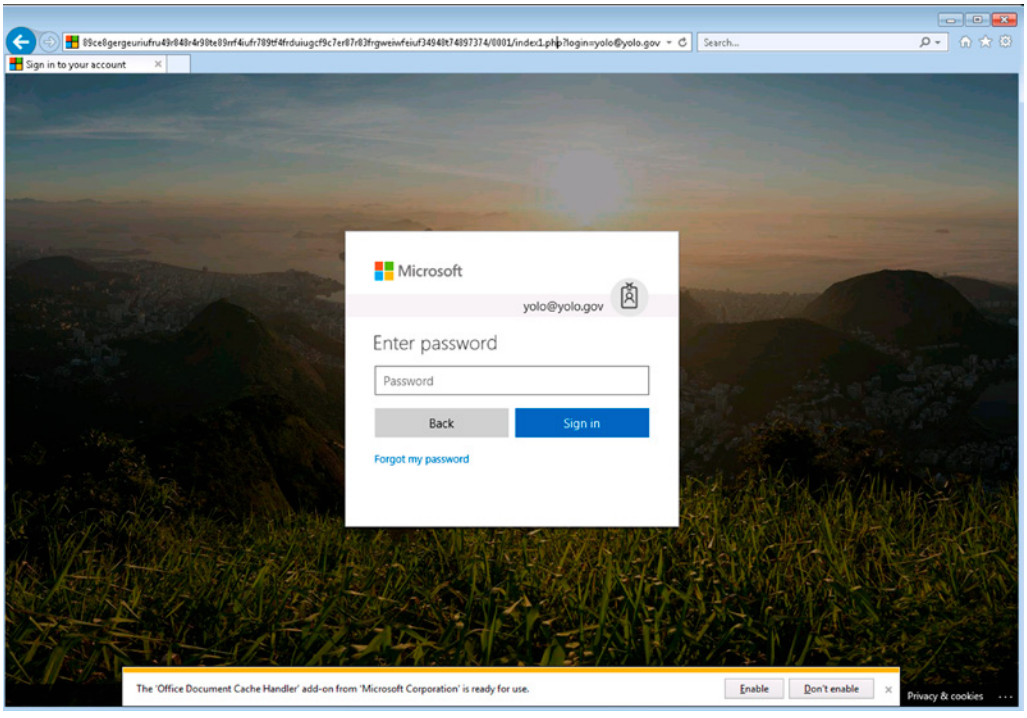
Kriitiline intsident oli proovikivi Elisale, kuidas tõsta asutuse sees rikete tuvastamise ja teavitamise võimekust ning töötada välja need meetmed, mis välistaksid tulevikus sarnaste olukordade tekkimise. 2018. aastal nägime selgelt, kuidas Elisas teadlikkus erinevatest riskidest kasvas ja astuti samme sarnaste olukordade vältimiseks tulevikus.

Elisa Eesti ASi kommunikatsioonijuht Marika Raiski: 2018. aasta alguse juhtum tekkis inimliku vea tõttu ning kahetsusväärselt on ettevõttel end nende vastu kõige keerulisem ja raskem kaitsta. Selliste juhtumite valguses vaatame alati üle ettevõttesisese rikketeavituse ja info liikumise protsessi ning õpime vigadest, koolitades ja õpetades Elisa töötajaid lähtuvalt kogetust.

Vältimaks sama olukorra kordumist, oleme parendanud muudatuste planeerimist. Näiteks testime nüüdsest muudatused, mis võivad mõjutada häirekeskusesse või teistesse prioriteetsesse kohtadesse helistamist, alati eelnevalt läbi. Samuti planeerime enne muudatuse tegemist süsteemi taastetegevused, mis võimaldab probleemi tekkimisel kiiresti taastada muudatuseelse olukorra.

Kuidas toimub finantspettus

Eelmisel aastal tekitasid kõige enam majanduslikku kahju erinevad finantspettused. Osa neist olid lihtsasti võltsitud meilid palvega, kas raamatupidaja võiks tundmatule arvele raha saata. Teistel puhkudel sai finantspettus alguse lihtsast õngitsuskirjast, mille kaudu sai kurjategija ligi töötaja meilikontole.



Selle ettevõtte töötajale saabus 9. juulil kiri, kus paluti „kinnitada" oma meilikontoandmed, vajutades meilis olevale lingile. Töötaja selle lingi ka avas, mis viis ta pealtnäha Microsoft Office 365 sisselogimislehele ning sisestas sinna oma kasutajanime ja parooli. Töötaja sai seejärel teate, mis kinnitas, et andmed on korras.

Pea kolm nädalat hiljem, 25. juuli tööpäeva lõpus paljastasid kurjategijad oma tegevuse ja saatsid sellelt kompromiteeritud meilikontolt 18 minuti jooksul välja ligikaudu 600 õngitsuskirja. Ettevõtte IT-juht blokeeris töötaja meilikonto, muutis parooli, kontrollis arvutist pahavara ning seda leidmata avas meilikonto uuesti. Tegu oli siiski vaid kurjategijate pettemanöövriga.

Alles kaks kuud hiljem teatas ettevõtte äripartner neile, et nad on alates 17. juulist suhelnud võõra isikuga, kes esines ettevõtte töötajana. Selgus, et kurjategijad salvestasid juulis kompromiteeritud meilikonto vestlused ning asusid äripartneriga meilivestlusesse, esinedes just nimelt selle ettevõtte töötajana. Sealjuures eksitati äripartnerit tegema (märkimisväärse suurusega) ülekanne kurjategija antud arvelduskontole.

MIDA TEHA, KUI SINU ETTEVÕTTE MEILIKONTODELE LIGI PÄÄSETI

Arvestades meilikontode ärakasutamise trende, soovitab RIA ettevõtetel ja asutustel väga tõsiselt pöörata tähelepanu kõikidele juhtumitele, kus töötajate meilikontodele on ligi pääsetud.

Teavita oma koostööpartnereid

Kurjategijad võivad oodata mitu kuud, enne kui hakkavad uuesti sinu asutuse nime ära kasutades sinu partneritelt raha välja petma. Kui sinu asutuse töötaja meilikonto kompromiteeritakse, anna kohe oma koostööpartneritele märku, et oled langenud kuriteo ohvriks, mis võib partnereid hiljem mõjutama hakata – näiteks hoiata neid selle eest, kui teie poolt hakkab keegi rääkima pangakonto detailide muutmisest. Selline põhimõtteline muutus tuleks kindlasti mitme kanali kaudu üle kinnitada. Nii näitad sa ka oma partneritele, et pöörad turvalisusele tähelepanu.

Hoolitse oma nime eest

Isegi kui SPF poliitika, DKIM tempel ja DMARC protokoll tunduvad liiga tehniliste kontseptsioonidena, on need ekspertide jaoks lihtsad ja odavad viisid, kuidas vähendada võimalust, et kurikaelad püüavad just sinu nime kasutades õngitsuskirju või pahavara laiali saata.

Tee kurjategijatel elu oluliselt keerulisemaks!

Otsi võimalusi rakendada mitmefaktorilist autentimist

Mõtle läbi, kuidas oleks sinu ettevõttes võimalik kasutada mitmefaktorilist autentimist, nii et võõrast arvutist meilidele ligi pääsemine oleks võimalikult keeruline. Suurte pakkujate kõrval on ka mitmed Eesti teenusepakkujad kaheastmelise autentimise võimalikuks teinud.

Sarnaseid juhtumeid, kus meilivestluseid on pikemalt jälgitud ning vestlusesse vahele segatud just ülekannete tegemise hetkel, et anda ülekandeks uued pangakonto andmed, nägime mullu sügisel pidevalt. Ohvriteks olid nii Eesti ettevõtted kui ka nende äripartnerid teistes riikides. Seetõttu saatsime koos politsei- ja piirivalveametiga aasta lõpus kõigile Eesti ettevõtetele välja sellesisulise hoiatuskirja.

LUNAVARARÜNNAKUD HÄIRISID ETTEVÕTTEID KA MULLU

Finantspettuste kõrval mõjutasid Eesti ettevõtteid ka lunavararünnakud, mille tagajärjel kaotasid asutused eelkõige võimalikke kliente, aga ka väärtuslikke töötunde. Lunavararünnakud on saanud viimastel aastatel palju tähelepanu, mullu nägime ka olukordi, kus ettevõtete turvameetmed aitasid võimalikku kahju vältida.

Näiteks Eesti suurim bürootarvete, -tehnika ja -mööbli müüja Büroomaailm sai mullu taas kord lunavararünnakuga pihta, kuid oli selleks valmis. „Meid rünnati üle kaughalduseks kasutatava RDP protokolli ja saadi ligipääs terminalserverile. Läbi selle pandi käima krüptoviirus," rääkis Büroomaailma IT-juht Sebastian Sõeruer.

„Probleem oli tegelikult ühes meie vanas terminalserveris, millele ei rakendatud enam meie ettevõtte turvapoliitikat, kuid see oli jäänud veel tööle. Seetõttu oli võimalik seda serverit ka kergelt rünnata ja ligipääs saada," ütles ta. „See on viimase kolme aasta jooksul kolmas sarnane juhtum, kus oleme krüptoviirusega pihta saanud."

Just varasemad kogemused on loonud valmisoleku, nii et sellised intsidendid ettevõtte IT-süsteemidele tõsisemat kahju teha ei saa. Sõeruer ütleb, et seekordse rünnaku põhjustatud kahjuks oli ligi kuus tema enda töötundi ja paar puuduvat rida Excelis.

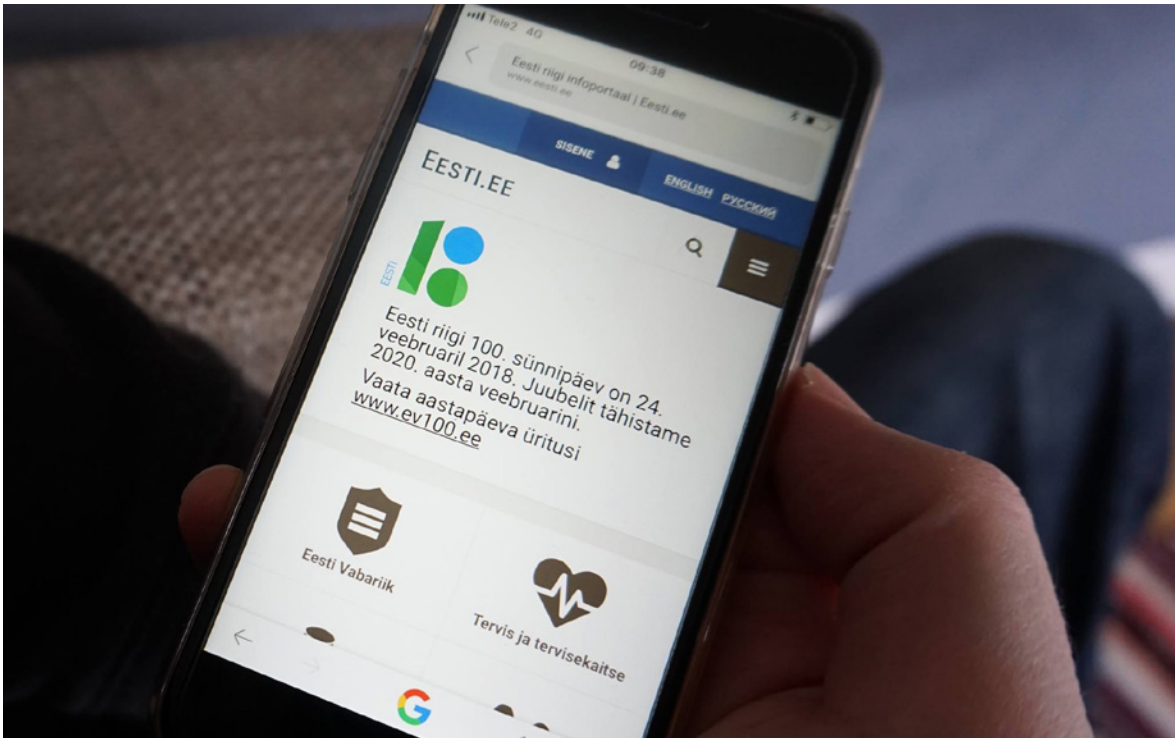
Esimene abinõu end igasuguste intsidentide vastu kindlustada on Sõerueri sõnul varukoopiate tegemine, ja seda soovitavalt mitmesse asukohta. Sõeruer on loonud mitmeastmelise varundamise süsteemi – virtualiseeritud serverite kopeerimine, regulaarne varundamine füüsiliselt teises asukohas olevatele välistele kõvaketastele, pilvekeskkonna kasutamine jne. „Varundamise tähtsust on raske ülehinnata," ütles ta. Teiseks on tema sõnul oluline range kontroll kasutajate õiguste üle – ühe kasutaja vale otsus ei tohi halvata kogu süsteemi.

Tänu küberkogukonnale parandasime aastaid riigiportaalis peitunud autentimisnõrkuse

29. juunil teavitasid ühe Eesti asutuse küberturvalisuse eksperdid meid riigiportaali eesti.ee turvanõrkusest, mille ärakasutamisel oli võimalik pangalingi abil portaali sisse logida teise kasutajana. Saades aru olukorra tõsidusest, sulgesime riigiportaali sisenemise pangalingi kaudu ning asusime tuvastatud viga parandama ja riski maandama, mis võttis meil aega neli päeva.

Turvanõrkus seisnes selles, et eesti.ee portaal ei kontrollinud pangalingi kaudu saadud autoriseerimispäringu puhul, kas see oli allkirjastatud panga antud võtmega ning kas see vastas pangalingi tehnilisele kirjeldusele. Leitud viga võimaldas portaali sisenemist teise inimese nimel juhul, kui sisselogija lõi pangalingi tehnilise kirjelduse järgi ebakorrektse pangapoolse kinnituse ise ja suutis selle saata eesti.ee portaalile sisselogimise kinnituseks. Teisisõnu – rünnak oleks eeldanud korralikke tehnilisi teadmisi ja oskusi.

Viga tulenes eesti.ee aegunud platvormist ega olnud seotud ühegi panga ega teise e-teenusega. Hilisemal uurimisel selgitasime välja, et kirjeldatud viga tekkis ilmselt 2015. aasta oktoobris portaali baastarkvaras tehtud muudatuste ja uue pangalingi kasutuselevõtmise käigus. Tegemist ei olnud pahatahtliku veaga, vaid arendaja ja RIA kui tellija hooletusega.



Pangalinkide kasutamine moodustab eesti.ee kõikidest sisselogimistest umbes 30 protsenti ehk ühes kuus logitakse pangalingi kaudu sisse umbes 100 000 korda.

Võimalike kahjude või pahatahtliku tegevuse väljaselgitamiseks kontrollisime üle riigiportaali sisenemise logid alates kirjeldatud muudatuse tegemisest. Mitu päeva kestnud logide kontrollimise tulemusel ei tuvastanud me midagi, mis viitaks sellele, et turvanõrkust oleks ära kasutatud. Kellegi andmed ei olnud kättesaadavad ning kellegi teise nimel sisselogimisi ei fikseeritud. Pärast mitmepäevast intensiivset tööd ja ka välisekspertide läbiviidud turvateste taastasime 4. juulil uuesti riigiportaali sisenemise pangalingi kaudu.

Juhtum näitas, et vigu infosüsteemide arendamisel teeme ka me ise ja intsidendist saadud õppetundide põhjal viisime oma arendusprotsessi sisse mitu muudatust, et samasuguseid olukordi ei saaks enam tekkida. Nimetatud turvaviga tuvastati ainult tänu Eesti küberturvalisuse ekspertide kogukonnale väljaspool RIAt, kes hoiab valvsalt pilku peal, et ehitaksime jätkuvalt turvalist digitaalset riiki. Me täname!

KUIDAS TEHA ELU TURVALISEMAKS

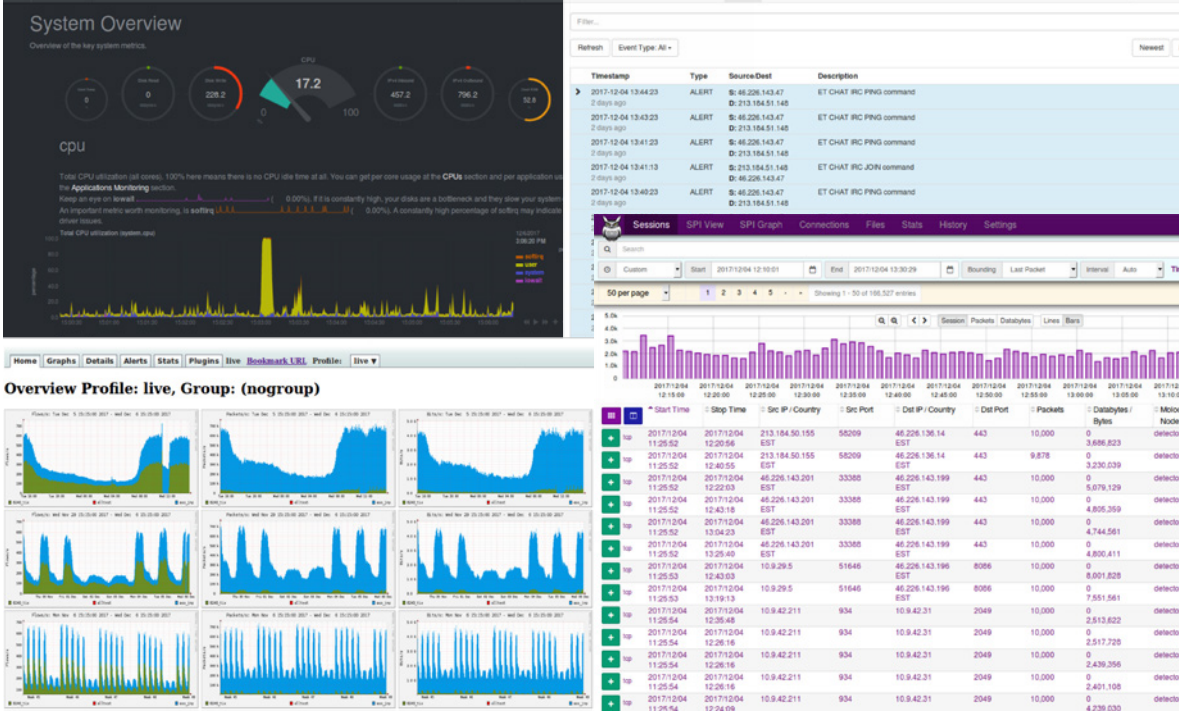
Automatiseeritud seirelahendus S4a valvab sinu võrke meie toega

Selleks, et vähendada küberintsidentide tuvastamise ja neile reageerimise aega Eestis, oleme Euroopa Liidu toel välja töötanud ja hakanud ettevõtetele pakkuma automatiseeritud võrguseirelahendust Suricata-4-all (S4a). Selle süsteemi abil saame võimalikult kiiresti jagada oma klientidele meile teadaolevaid ründeindikaatoreid ja toetada asutusi pahaloomulise võrguliikluse avastamisel.

S4a on vabavaral põhinev võrguliikluse analüüsi süsteem, mis võimaldab avastada ründeid ja pahavara ning mõningatel juhtudel ka haavatavusi ja konfiguratsiooniprobleeme. Reegleid – ehk sisuliselt neid indikaatoreid, mida süsteem peaks tuvastama – uuendame regulaarselt vastavalt ohupildile maailmas.

S4a nimi tuleneb selle põhikomponendi, vabavaralise sissetungituvastussüsteemi Suricata nimest, mis kasutab rünnete tuvastuseks reegli-/signatuuripõhist meetodit. Suricata on küll vabalt kättesaadav ja võimalik oma võrgus ise püsti panna, kuid selle monitoorimine ja sissetungi tuvastamise indikaatorite uuendamine võib võtta ülemäära palju raha ja aega.

See ongi koht, kus tuleme lähtuvalt tuvastatud riskidest oma teadmistega Eesti ettevõtetele ja teenusepakkujatele appi. S4a lahendus koosneb CERT-EE juures asuvast kesksest süsteemist ja sensoritest, mida võrkude omanikud saavad paigaldada oma ettevõtte või asutuse juurde. Kesksüsteem jagab sensoritele reegleid (mille põhjal toimub rünnete tuvastus) ning sensorid saadavad



Illustratsioon erinevatest tööriistadest, mis S4a ettevõtete võrkude seiramisel pakub.

omakorda kesksüsteemile teated, kui nad on tuvastanud pahaloomulist liiklust.

Lisaks sissetungi tuvastusele annab süsteem võimaluse võrguliiklust salvestada, indekseerida ja analüüsida. See annab sensori paigaldanud asutusele võimaluse probleemide korral võrguliiklust analüüsida või küsida selle jaoks meie tuge.

Sissetungi tuvastuse süsteem tuvastab esialgse ründevektori ning talletab pahaloomulise võrguliikluse kohta fragmente, mis vastavad reeglites kirjeldatule. Võrguliikluse täiendava analüüsi abil on aga võimalik detailsemalt näha ründajate tegevust, mida pelgalt sissetungi tuvastuse süsteem tavapärasest võrguliiklusest ei erista.

Turvalisus algab vastutuse võtmisest

Küberturvalisus algab alati iga organisatsiooni vastutusest oma riskide väljaselgitamise ja maandamise suhtes. Eestis olulisi teenuseid pakkuvatel asutustel lasub tulenevalt küberturvalisuse seadusest riskide maandamise ja intsidentidest raporteerimise kohustus. S4a annab asutustele täiendava turvalisuse kihi ja parandab pilti olukorrast Eesti küberruumis.

Süsteemiga liitumiseks tuleb soovijal hankida nõuetele vastav riistvara ning küsida sensori paigaldustarkvara **cert@cert.ee** käest. Kirjuta ja küsi nõu, kas S4a automatiseeritud võrguseire on sinu ettevõtte jaoks kasulik lahendus.

Valimiste küberturvalisus tähendab enamat kui vaid e-hääletuse turvalisus

2019 on Eestis valimiste aasta – valiti nii riigikogu kui valitakse Euroopa Parlamenti. Mullune valimistevaheline aasta andis võimaluse vaadata natuke süsteemsemalt otsa valimistel kasutatavate tehnoloogiliste lahenduste turvalisusele. Nii valmis 2018. aasta juunis Euroopa NIS direktiivi koostöögrupi egiidi all, eestlaste ja Tšehhi NUKIB analüütikute juhtimisel Euroopa valimisteks mõeldud valimisturvalisuse käsiraamat, mis koosneb praktilistest soovitustest ja näidetest, kuidas seni on hääletamist turvatud.

Eesti valimisteenistuse ja RIA jaoks on valimiste küberturvalisus seni tähendanud suuresti diskussiooni e-valimiste turvalisuse üle. Avalikult on diskuteeritud selle üle, kui läbipaistev see protsess on tavalisele valijale; kuidas saaks kindlustada, et sinu hääl ikka kindlasti registreeritakse; kuidas tagada vaatlejatele võimalust kogu protsessi jälgida.

Kuid e-hääletusega valimiste turvalisus ei piirdu. USA ja Prantsusmaa kogemused 2016. ja 2017. aasta presidendivalimistel näitasid, et rünnaku alla sattusid pigem kandidaadid. Bulgaaria ja Tšehhi nägid 2015. ja 2017. aastal teenustõkestusrünnakuid oma valimisteenistuste kodulehekülgedele. Lisaks on haavatavad igasugused meediaväljaanded ja -platvormid, mille kaudu üritatakse levitada valesid ja millel on kriitiline roll valimistulemuste avalikustamisel.

Eelmainitud valimistehnoloogiate turvalisuse käsiraamat vaatas metoodiliselt kõiki valimiste etappe alates kandidaatide registreerimisest ja valijate nimekirjadest (mis tuginevad samuti elektroonilistele kanalitele) kuni valimistulemuste teatavakstegemise platvormide kaitsmiseni välja. 2019. aasta valimiste turvalisusele lähenesime lähtuvalt Euroopa parimast praktikast ehk oma partnerasutuste kogemustest.

Näiteks eraldas valitsus ligi 304 000 eurot valimiste infosüsteemide info- ja küberturvalisuse taseme tõstmiseks. Selle hulgas telliti riigivõrgule teenustõkestusrünnete kaitsemeetmed, suurendati testimiste mahtu ja soetati riistvara, et suurenenud koormuse tingimustes e-hääletus sujuks.

Koostöös valimisteenistusega pakkus RIA küberhügieeni koolitusi kandidaatidele ja kampaaniameeskondadele. Neljal korral (kolm korda Tallinnas ja üks kord Tartus) käisime rääkimas, kuidas valimisi võidakse ohustada ja kuidas kaitsta oma meili- ja sotsiaalmeediakontosid.

E-hääletajate osakaal kõigist valijatest kasvab jätkuvalt.

Koostöös valimisteenistusega pakkusime Eesti erakondadele võimalust kontrollida oma koduleheküljegede ja meiliserverite turvapilti ehk kuidas paistavad serverid võimalikele ründajatele. Kõik parlamendis esindatud erakonnad otsustasid võimalusest kinni haarata. Igaühele saatsime kinnise ümbriku, kus pöörasime vajadusel tähelepanu turvastandardite kasutamisele, näiteks meiliserveri võltsimiskindlust parandavate protokollide nagu SPF seadistamisele, HTTPS kasutamisele ja teistele võimalustele rünnete ennetamiseks.

2019. aasta jooksul on meie roll olla valimisteenistusele partner, kes ei hoia püsti ainult e-hääletust, vaid kes on võimeline vaatama valimiste küberturvalisust laiemalt. Järgmisteks plaanideks on uuendada valimiste tulemuste sisestamise rakendust ehk valimiste infosüsteemi, mille uus versioon peaks olema valmis ja testitud 2021. aasta kohalike omavalitsuste valimisteks.

Küberturvalisuse baasstandard muutub paremini rakendatavaks

Küberturvalisuse nõuded, mis on kohustuslikud kõigile riigiasutustele ja kohalikele omavalitsustele, on ajale jalgu jäänud ega pruugi päriselulistes olukordades küberturvalisuse tagamisele kaasa aidata. Selleks, et kaitsta väärtuslikke andmeid ja infosüsteeme, kirjutame Eestis kasutatava turvastandardi ISKE ümber selliselt, et seda oleks lihtsam ja praktilisem igapäevaselt kasutada.

ISKE on 2008. aastast valitsuse määruse alusel kohustuslik andmekogusid kasutavatele riigi- ja kohaliku omavalitsuse asutustele. ISKEs kirjeldatud turvameetmed on grupeeritud liikide kaupa (organisatoorsed, füüsilised ja infotehnoloogilised) ja nende rakendamise vajadus sõltub andmekogu turbeastmest (madal, keskmine, kõrge). Kuna ohte ja riske on palju, on ka meetmeid palju ning see muudab standardi üsna mahukaks ja kohmakaks.

Nii on jõutud olukorrani, kus ISKE rakendamine on pigem formaalsus kui igapäevase turvalisuse tagamise alus. Tartu linna IT-pealik Rein Lindmäe nendib, et tema jaoks on ISKE oluline eelkõige nendel hetkedel, kui on vaja taas tellida ISKE audit. „ISKE ei ole üks sellistest raamatutest, mis oleks iga päev laual," ütleb ta. „Kui see oleks inimkeelsem või kui sellega oleks lihtsam igapäevaselt seostuda, oleks see palju mugavam ja paremini kasutatav."

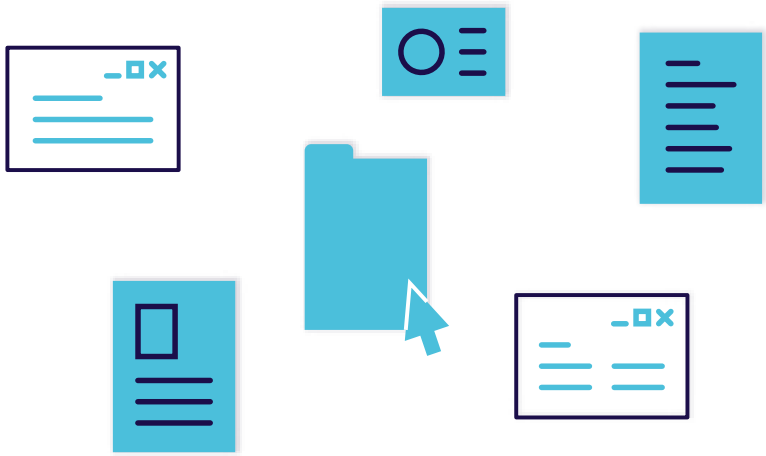
Ta rõhutab, et ei ole põhimõtteliselt niisuguse baasstandardi vastu. „ISKE põhitõed on õiged, kuid praegu tunnistan, et enamasti hindame oma riske veidi teistsugustele auditite tuginedes."

Näiteks tellib ta oma organisatsiooni küberturvalisuse hindamiseks pigem ründeauditeid, mitte ISKE-le vastavuse kontrollimist. Tartu linnal on Lindmäe arvates ressursse ja võimalusi oma riske ise piisavalt hinnata, väiksemates asutustes ja omavalitsustes ei pruugi seda võimalust olla. Seetõttu kulub ISKE Lindmäe hinnangul neile kindlasti ära.

„ISKE võiks lihtsamaks muuta, et see oleks elavam dokument," ütleb ta, „niimoodi saaks sellest päriselt kasu. Ei saa öelda, et me ISKEt pidevalt „kasutame". Jah, me tellime auditi, aga igapäevaste tegemiste puhul ei kontrolli me küberturvalisust ISKE vastu."

Riskianalüüs olgu kõige alus

ISKE nõue on kehtinud kümme aastat. Selle aja jooksul on seda regulaarselt uuendatud ja täiendatud. IT valdkonna kiire areng on endaga kaasa toonud uusi ohte ja riske, mis vajavad uusi meetmeid ja lähenemisi ning neid on ISKEsse pidevalt sisse viidud. Lisaks IT valdkonna kiirele arengule on aga ka organisatsioonid arenenud, paljud neist on muutunud küpsemaks ja võimekamaks. See tähendab, et Eestis on juba hulk organisatsioone, kes oleksid võimelised rakendama rohkem riskipõhist lähenemist ning ise täpsemini hindama oma kaitsevajadusi ja -võimalusi.



Seetõttu oleme alustanud uue infoturbestandardi väljatöötamist, mis arvestab rohkem asutuste suuruse, eripärade, võimekuste ja võimalustega. Pöörame selles rohkem tähelepanu riskianalüüsile, mis erinevalt senisest etalonturbe põhimõttest võimaldab suuremat paindlikkust. Uue standardi aluseks on taas Saksamaa vastav standard, mis on põhjaliku uuenduskuuri juba läbinud ja mida juba rakendatakse. Kuigi uues standardis on palju struktuurilisi uuendusi ja sisulisi muudatusi, ei ole infoturbe põhimõtetes väga palju fundamentaalseid muudatusi: lukus tuleb ikka hoida nii uks kui arvuti.

Turvatestimine pole must maagia

Küberturvalisuse hetkeolukorrast igas organisatsioonis annab väga hea pildi turvatestimine, mis ei tohiks uute teenuste turule toomise jooksul ära ununeda.

Juba kuus aastat oleme Eesti küberturvalisuse tagamiseks korraldanud oluliste teenuste osutajatele turvatestimisi. Teste viivad läbi riigihanke võitnud eraettevõtted, mullu tellisime turvatestid niimoodi kuuele asutusele. Tänavu on kavas testida seitsme ettevõtte või asutuse infosüsteeme.

Näiteks pakub Eestis juba kaheksa aastat niisugust teenust Clarified Security, mida juhib Mehis Hakkaja. „Oluline on arvestada, et kui tellida infosüsteem ja sellele läbistustest ehk *pen(etration)* test, peaks see olema tellija, mitte hanke võitnud arendaja otsene kulu. Turvalisuse valideerimine peab olema erapooletu hindaja tehtud," annab Hakkaja soovituse turvalise IT-projekti edukalt läbiviimiseks. „See on just nagu ehitusjärelevalve hoone ehitamisel – klient peab selle eraldi tellima."

Hakkaja sõnul liiguvad Eesti avaliku sektori infosüsteemide tellijad õiges suunas, aga vaadelda tuleb kogu arenduse elutsüklit ja mis seda mõjutab. „Vahel on nii, et väga mahuka arendusprojekti lõpus tehtava turvatesti tulemiks on pikk raport, kus on enne toodangusse minekut ka suurem hulk kiiret lahendamist vajavaid leide. Tähtajad ning äripool aga nõuavad juba järgmise suure osa funktsionaalsuse valmimist," toob ta tüüpilise näite, et turvalisuse valideerimine on vaid väike osa kogu ahelast.

Manuaalse turvatestimise kõrval on oluline ka ründaja jäljendamine ehk *red-teaming*. Eesmärgiks pole siin mitte kõikide vigade, vaid just lihtsaima vastupanutee leidmine ründaja peamiste eesmärkide saavutamiseks.

„Ühe suure välismaa kliendi puhul esitasime näiteks tõestusena edukast ründevõimalusest ettevõtte veel avaldamata börsiaruande. See ning meie raportid, kuidas me märkamatult sellisel tasemel juurdepääsu saavutasime, aitasid sel börsiettevõttel teadvustada oma turvalisuse tõsiseid puudujääke," selgitab Hakkaja *red-teaming*'u mõtet. „Aasta hiljem üle kontrollides oli selle ettevõtte kaitsevõime ning eelkõige just monitooring juba oluliselt parem."

Ohud muutuvad

Hakkaja hoiatab, et ohud muutuvad maailmas üha keerulisemaks ja globaalsemaks. „Võtame kasvõi meie e-residentsuse programmi, millega igaüks üle maailma võib saada ligipääsu meie infosüsteemidele. Paljud süsteemid on üles ehitatud eeldusega, et kiipkaardiga sisselogija on meie kodanik, kes saab kasutada mingit e-teenust. Infosüsteemides kasutatakse pahatihti „kombelõdvalt" ka isikukoodi – päringud toimuvad isikukoodi põhjal ja mõnikord on unustatud lisakontrollid, kas päringu tegija tohiks selle isikukoodi kohta andmeid saada," toob Hakkaja näiteid leitud vigadest, mis muudavad meie infoühiskonna sihitud rünnetele haavatavamaks. „Piltlikult öeldes jagame võtmeid oma imelahendustesse üle maailma, aga kas me suudame neid lahendusi ka suurema huviliste ringi eest kaitsta?" viitab ta laienenud horisondile.

Clarified Security juhatuse esimees Mehis Hakkaja

Euroopa Liit saatis eestlased Aasiasse ja Aafrikasse küberturvalisust arendama

Euroopa Liidu tellimusel oleme 2018. aasta algusest koos partnerasutustega Ühendkuningriigist ja Hollandist toetanud nelja Aafrika ja Aasia riigi küberarengut. Projekt „Cyber Resilience for Development" (Cyber4Dev) kestab 2021. aasta juunini.

Missiooni eesmärk on suurendada riikide küberturvalisuse teadlikkust, aidata välja töötada küberstrateegiad ja tegevuskavad, tõsta intsidentide käsitlemise meeskondade võimekust ning jagada kogemusi elutähtsate teenuste pakkujate ja riigiasutustega. Tegevust on alustatud neljas riigis: Mauritiuses, Sri Lankas, Ghanas ja Botswanas.

Riikide küberturvalisuse tase on erinev: kui Sri Lankas ja Mauritiuses on CSIRT meeskonnad juba mõnda aega tegutsenud, siis näiteks Botswanas CSIRT alles loodi. Neljast riigist sarnaneb Eestiga kõige rohkem Mauritius. Väikese, 1,3 miljoni elanikuga saareriigi ambitsioon on olla selles India ookeani piirkonnas kübervaldkonna eestvedaja.

Koolitame ja nõustame

Kõigis neljas riigis on IT ja küberturvalisuse valdkonnas inimeste puudus – oskustöötajaid on vähe ja minnakse sinna, kus makstakse rohkem. Samuti on elanikkonna teadlikkus küberohtudest madal, riigi ja erasektori koostöö elutähtsate teenuste kaitsel vajab parandamist ning CSIRTide võimekuse kasvatamine toetamist.

Projekti käigus hindasime kõigi riikide küberturvalisuse taset – iga riigi kohta koostati raport, milles soovitati, mida võiks parandada. Sri Lankas ja Mauritiuses kohtusime ka CSIRTidega ning analüüsisime, milliseid koolitusi oleks seal edaspidi vaja. Koolitusi ja töötubasid oleme nendes riikides juba ka korraldanud.

Sel aastal jätkame koolitustega kõigis riikides. Suuremat tähelepanu pöörame CSIRTide ülesehitusele, kriitilise informatsiooni infrastruktuuri kaitsele ja regulatsioonile, riskihaldusele ja kriisiõppustele, küberseadustele ja -strateegiatele, küberhügieenile ja -teadlikkusele. Samuti tutvustame erinevaid lahendusi, mis aitavad Eestis küberturvalisust tagada ja mis on valminud koostöös Eesti ettevõtetega. Sri Lanka ja Mauritius on tundnud huvi Eesti e-riigi kogemuste vastu, sealhulgas elektroonilise identiteedi kasutamise vastu – nende riikide eksperdid ja poliitikud on külastanud ka Eestit, et meie kogemusega lähemalt tutvuda.

Projektis osalevate riikide eksperdid on käinud külas ka Tallinnas, et tutvuda meie e-lahendustega.

KüberSIIL tuleb tagasi

2018. aasta mais mängiti Eesti kaitsejõudude suurõppusel Siil Eesti metsades ja lagendikel läbi sõjalist konflikti Murinuse ja tema vasallriikidega, kes üritasid Läänemere idakaldal oma mõjusfääri laiendada. Sellega ühel ajal, 7. ja 8. mail toimus küberturvalisuse tagajate õppus KüberSIIL, millel mängiti läbi olukord, kus Eesti territooriumil toimuva sõjategevusega samaaegselt tabasid küberründed ka mitmeid Eesti olulisi asutusi ja teenusepakkujaid.

Tulenevalt laiapindse riigikaitse põhimõtetest ja Eesti julgeolekupoliitika alustest peab küberjulgeolekut korraldama samade struktuursete lahendustega nii rahuajal kui ka sõjaolukorras. Seega on küberturvalisuse tagajate tööd sõjaolukorras ja koostööd Eesti sõjalist kaitset korraldavate üksustega vaja ka regulaarselt harjutada. Just seda kaitseväe suurõppuse raames tehti.

Näiteks said õppuse käigus rünnakutega pihta Ida-Viru keskhaigla, Pärnu haigla, maksu- ja tolliamet, Pärnu sadam ja Alexela, kes kõik said lahendada tulnud olukordadega hästi hakkama.

Intsidentidele reageerimist harjutatakse pea igal küberõppusel. KüberSIILi muutis eriliseks aga see, et harjutati infovahetuse toimimist Eesti territooriumil toimuva sõjalise operatsiooni juhtimise ja küberruumis toimuva vahel. Eesti sõjalist kaitset juhtiva staabi jaoks on kriitiliselt oluline olla reaalajas teadlik, milliseid Eesti olulisi teenuseid on parajasti tabanud küberründed ja mis on nende mõju.

Pikas perspektiivis on ülimalt oluline küberjulgeoleku nõukogus heakskiidu saanud otsus, et üleriigilised küberõppused peavad hakkama toimuma ühel ajal iga-aastaste kaitseväe suurõppustega. Seda rõhutas ka riigikogu riigikaitsekomisjon.

KÜBERÕPPUSED TEEVAD TUGEVAMAKS

Lauri Luht, NATO küberkaitsekeskuse õppuste juht

Küberkriiside lahendamise võti on valmisolek, ja valmisolek tuleb ainult harjutades. NATO küberkaitsekoostöökeskus (CCDCOE) on oma loomisest alates korraldanud küberõppusi võimalikult realistlikes tingimustes. Iga-aastaselt Tallinnas toimuv maailma suurim rahvusvaheline õppus Locked Shields on suure tähelepanu all. Vähem on räägitud keerukast, kuid madala profiiliga tehnilisest õppusest Crossed Swords (ee ristatud mõõgad, lühendiga XS), mis eelneb Locked Shieldsile.

XS on üks kõige suurema väljakutsega küberõppusi mitte oma suuruse, vaid selle tõttu, kui palju erinevaid keerukaid ja interdistsiplinaarseid tegevusi on vaja teha. Õppus viib osalejad pidevalt muutuvasse keskkonda, kus neil on vaja reageerida vaenulikele vastastele ja hulgale samal ajal juhtuvatele intsidentidele, püüdes samas vastase võrkudesse sisse tungida.

XSil osalejad peavad suutma täita ülesandeid ühtse meeskonnana, tegema koostööd erinevate agentuuridega ning suutma aimata vastase mõttemaailma. Et lahendada missioone, peavad nad hakkama saama

kõikvõimalike küberoperatsioonide läbiviimisega, ning seda kõike koostöös eriüksuste ja luurajatega. Muu hulgas peavad osalejad kübervahenditega takistama kineetilisi rünnakuid.

XS õppuse eesmärk on olla võimalikult realistlik ja pakkuda tervet hulka ründevektoreid, mis võivad tänapäeval maailmas esineda. Sõjaline vastus ei ole ainus viis, kuidas küberrünnakutega hakkama saada, sest küberkriisid võivad mõjutada sõjaliste objektide kõrval ka tsiviilisikuid või mõlemaid. Niisuguse kõikehõlmava ja päevakajalise õppuse väljatöötamine on väljakutse, mis nõuab koostööd CERT.LV, Tallinna tehnikaülikooli ja Eesti küberväejuhatuse ekspertidega.

CROSSED SWORDS

KÜBERTURVALISUS SÕLTUB IGAÜHEST

Ohumärkide tunnetamine aitaks küberkuritegevust ennetada

Kurjategijad tegutsevad kübermaailmas nutikalt, kasutades ära inimeste väheseid teadmisi ja süsteemide nõrkusi. Politsei suurimad ülesanded on leida ressurssi raskete ehk sihitud ja suure mõjuga küberrünnete tõkestamiseks ning tõsta inimeste teadlikkust.

Keskkriminaalpolitsei küberkuritegude büroo juht Oskar Gross nendib, et kuigi kuritegevust ei ole võimalik välja juurida, saab elu piiratud võimalustega turvalisemaks muuta.

Mis on kuritegevuse vaates politseile praegu kõige suurem murekoht?

Ilmselt siiski nn tänavaküberkuritegevus ehk laiahaardelised ja võrdlemisi lihtsa toimemehhanismiga küberkuriteod, nagu õngituskirjad ja erinevad arvepettused, mille õnge on väheste teadmiste tõttu lihtne langeda ning mille puhul kannatanud politsei poole kõige rohkem pöörduvad.

Kindlasti peaksime sellele teadliku ennetusega rohkem tähelepanu pöörama. Ühelt poolt seetõttu, et neid juhtumeid on kriminaalmenetluslikult võrdlemisi keeruline uurida ja tulemusi toob see harva, kuid samas tekitab ühiskonnas kõige rohkem ebakindlust. Kui suudaksime ühiskonnas harjutada inimestele sisse ohumärkide tunnetamise, hakkaksid sellised kuriteoliigid oma ebaefektiivsuse tõttu vähenema ning politsei saab suunata rohkem ressurssi

keerukamate juhtumite ehk sihitud ja suure mõjuga küberrünnete uurimisele.

Kas ja mis teeb küberkurjategija tuvastamise võrreldes mõne teise kuriteoliigiga keerulisemaks?
On teatud aspektid, mis teevad küberkuritegevuse muudest kuriteoliikidest erinevaks. Näiteks küberkeskkonna reeglid on füüsilise maailma omadest erinevad ning samuti on uurimise rõhuasetus tõenäoliselt mujal kui muude kuriteoliikide puhul. Küberkuritegude uurimine eeldab väga head klassikalise kriminaalpolitsei töö oskusi ja väga head tehnilist taipu. Minu hinnangul ei ole võimalik lahendada keerulisi kuritegusid vaid ühe kompetentsiga.

Keskkriminaalpolitsei küberkuritegude büroo juht Oskar Gross

Milline võiks olla lähiaastate prognoos, kas trendid kuidagi muutuvad?
Kuna valdkond muutub püsivalt, tuleb kindlasti mingeid üllatusi. Küberkelmuste osas samamoodi. Kui ühel hetkel ei ole enam praegused kalastamiskampaaniad piisavalt efektiivsed, mõeldakse välja midagi uut. Hoiame silmad lahti ja püüame operatiivselt reageerida.

Kuidas paremini ennetada, mis on ju kriminaalmenetlusest oluliselt lihtsam ja odavam?
Meie jaoks on ennetuse puhul suur küsimus see, kuidas jõuda õige sihtgrupini. Kindlasti on meedia üks oluline kanal, mille kaudu inimesi teavitada, kuid isiklikult tunnen, et kuna tänapäeva ühiskonnas on tähelepanu hajuv, oleks vaja meetodit, mis paneks inimesed korraks tõsisemalt süvenema.

Näiteks katsetasime aasta lõpus koos RIAga ettevõtete juhtidele otsepostituste edastamist, milles hoiatasime levivate arvepettuste eest. Kuigi seda oleks saanud kindlasti teha nüansirohkemalt, oli tagasiside valdavalt väga positiivne. Tuleviku perspektiivist võiks mõelda riikliku teavitussüsteemi peale, mis võimaldaks kindla sihtgrupi teavitamist.

Kas Eesti eristub küberkuritegude poolest kuidagi muust maailmast?
Küberkuritegude vaates Eesti väga oluliselt tegelikult ei eristu. Ühe erisusena võib ilmselt välja tuua asjaolu, et tänu Eesti ID-kaardi süsteemile on pankade klientide vastu ründeid tõenäoliselt vähem kui mujal.

KÜBERKURITEGUDE EDUKAS UURIMINE EELDAB RIIKIDE ÜHIST ARUSAAMA OLUKORRA TÕSIDUSEST

Piret Paukštys, riigiprokurör

Küberkuritegevus on üha levinum kuriteoliik, mis ei tunne riigipiire ning millega on võimalik teenida väga suures ulatuses kriminaaltulu. Kurjategija võib olla sülearvutiga Itaalia kohvikus ning minutitega mõjutada servereid hoopis Ameerika Ühendriikides või mujal maailmaosades. Sellise kuriteo menetlemiseks on rahvusvaheline koostöö ja kiire infovahetus määrava tähtsusega.

Rahvusvaheliste küberkuritegude menetlemine eeldab riikidelt ühist arusaama, et tegemist on prioriteetse valdkonnaga, millega on vaja tegeleda. Ühine arusaam probleemidest on väga oluline, et oleks võimalik edasi liikuda. 2016. aastal loodi Eurojusti juurde küberkuritegudega tegelevate prokuröride võrgustik European Judicial Cybercrime Network, milles ka Eesti annab oma panuse. Võrgustiku eesmärk on muuta riikide koostöö kiiremaks, otsida ühiselt lahendusi küberkuritegude menetlemisel tekkivatele probleemidele ning jagada kogemusi, kuidas uue tulevikukuriteoliigiga tegeleda.

Lisaks pakkus Euroopa Komisjon juba eelmisel aastal välja, et tegelikult võiks politseil ja õiguskaitseasutustel olla võimalik saada kiiremini elektroonilisi tõendeid, kui neil oleks võimalik taotlused edastada otse teenusepakkujale. Töö vastavate seaduste väljatöötamisel jätkub aktiivselt ka sellel aastal ning lisaks otsitakse lahendusi krüpteerimisega seotud probleemidele, näiteks kuidas pääseda ligi krüpteeritud andmetele.

Prokuratuur paneb aasta aasta järel küberkuritegude menetlemisele järjest enam rõhku. Kõige enam väljendub see kasvõi menetlusotsuseid saanud inimeste arvus, keda 2018. aastal oli 27 ja aasta varem hoopiski 18. Suurem osa kriminaalasjadest on aga n-ö kohalikud – võõraste interneti kasutajakontodele sisenemised ning seal andmete kustutamine või kopeerimine.

21. sajandil peavad õiguskaitseasutused arvestama uute tehnoloogiliste väljakutsetega, millega kurjategijaid tabada. Küberkuriteo tõendamiseks on vajalikud elektroonilised tõendid, kuid alati peab meeles pidama, et neid tõendeid on võimalik vaid ühe klahvikombinatsiooniga „ära kaotada".

VALMISOLEK KÜBEROPERATSIOONE OMISTADA ON KÜBERRUUMIS STABIILSUSE JA USALDUSE ALUS

Heli Tiirmaa-Klaar, küberjulgeoleku erivolitustega diplomaatiline esindaja

Viimaste aastatega on küberjulgeolekust kujunenud oluline valdkond välis- ja julgeolekupoliitikas. Järjest enam on vaja rõhutada riikide vastutustundlikku käitumist küberruumis, mis eeldab rahvusvahelisest õigusest, kübernormidest ja usaldusmeetmetest kinnipidamist. On riike, kes seda ei tee, ning seetõttu on üha olulisem kutsuda riike üles järgima reegleid küberruumis.

Riikide korraldatud või soodustatud küberoperatsioonide ennetamiseks ja heidutuseks valmistati 2018. aastal ette ja võeti selle aasta algul valitsuses vastu küberoperatsioonide omistamise tegevusjuhis, mis koosneb poliitilistest, tehnilistest ja õiguslikest elementidest ning selgitab asjassepuutuvate Eesti ametkondade pädevuse omistamise läbiviimisel. Eesti toetab ka ELi ja NATO küberoperatsioonide vastumeetmete raamistikke ja aitab ELi kübersanktsioonide režiimi väljatöötamise, kollektiivse omistamise ja teiste vastumeetmete rakendamisega kaasa stabiilse küberruumi arengule.

Järjest suurenevate küberväljakutsete, suureneva digiteerumise ja geopoliitiliste konfliktide taustal on ka välispoliitiline huvi Eesti valdkondlike kogemuste vastu üha suurem. Lähiaastatel tugevdab Eesti suhteid kübervaldkonnas peamiste liitlasriikidega ning küberjulgeolekualgatusi rahvusvahelistes organisatsioonides. Samuti pöörame järjest rohkem tähelepanu arengukoostööle kübervaldkonnas.

Eesti on juba praegu väga suur eeskuju nendele riikidele, mis alles ehitavad oma e-riiki ja küberturvalisust, ning me kavatseme jätkata oma kogemuste jagamist. Lisaks arendame edasi Eesti ekspertiisi rahvusvahelise õiguse osas ning koostöös Eesti ülikoolide ja teiste akadeemiliste asutustega on plaanis luua rahvusvahelise küberõiguse kompetentsikeskus. Vajadus õigusalase ekspertiisi järele kübervallas üha suureneb ja Eestil on, mida teiste riikidega jagada.

CSIRT VÕRGUSTIK PANUSTAB TUGEVALT EUROOPA KÜBERTURVALISUSESSE

Otmar Lendl, Austria CERT.at juht

2016. aastal Euroopa Liidus vastu võetud NIS direktiiv algatas Euroopas uue koostööplatvormi, mille liikmeteks on kõik riiklikud küberturbemeeskonnad (CSIRT) ja lisaks CERT-EU. Praeguseks on CSIRT võrgustik toimiv koostöövorm, mis iga päev panustab kogu Euroopa küberturvalisusesse. Meie Euroopa Liidu Nõukogu eesistumise trio (Eesti, Bulgaaria ja Austria) õlgadele langes ülesanne panna see koostöö toimima võrgustiku algusaastatel. Lisaks olime esimene kolmik, kes pani paika küberturvalisuse valdkonnas just eesistumise jaoks olulised prioriteedid ja mõtted. Kuna poliitilisel tasandil oli küberturvalisus tugevasti toetatud, võtsid Eesti, Bulgaaria ja Austria CERTi meeskonnad selle võrgustiku käimalükkamise enda peale.

CERT-EE suhtus oma rolli äärmiselt tõsiselt kogu meie trio eesistumiste aja. Minu hinnangul tegid nad palju rohkem, kui formaalselt tegelikult nõutud. Eesti panustas üleeuroopalisse võrgustikku näiteks sellega, et pakkus CSIRT võrgustikule kasutada oma Mattermost koostööplatvormi taristut. Esimest korda osutus see eriti kasulikuks 2017. aasta Wannacry ja NotPetya kampaaniate ajal, kui kõik Euroopa küberturbemeeskonnad kogunesid selle virtuaalse lõkkeplatsi ümber, et arutada oma tegevusi ja saada olukorrast ühine arusaam.

Teine panus Eesti poolt oli inimeste tööaeg. CERT-EE eksperdid ei piiranud kunagi oma osalemist projektides nende kuue kuuga, mil Eesti oli ametlikult eesistuja rollis. Eesti eksperdid aitasid ehitada vajalikud tööriistad CSIRT võrgustiku jaoks, aitasid luua sellele võrgustikule vastava juhtimisstruktuuri mudeli ning panustasid oluliselt Cyber Europe 2018 õppusesse. Tänan Klaid Mägi, Andres Ellikut, Hannes Krauset ja Sille Laksi Eestist, kellest igaüks andis väga korraliku panuse, et Euroopa CSIRT võrgustik oleks Euroopa küberturbemeeskondadele efektiivne informatsiooni jagamise platvorm – mul oli väga hea meel nendega koostööd teha.

RIIKLIK KÜBERTURVALISUSE KESKUS – OLULINE SAMM HOLLANDI JAOKS

Michel Van Leeuwen, Hollandi justiits- ja julgeolekuministeeriumi küberpoliitika osakonna juhataja

Hollandi küberturvalisuse keskse olukorrapildi ja ekspertiisi keskus on riiklik küberturvalisuse keskus (NCSC). Selle keskuse missioon on Hollandi ühiskonna vastupanuvõime tõstmine küberruumis toimuvate intsidentide osas, mis aitab kaasa turvalise, avatud ja stabiilse ühiskonna loomisele. NCSC on digitaalsete ohtude ja küberturvalisuse intsidentide puhul ka rahvusvaheline partnerasutus. NCSC aitab koordineerida suuremate küberkriiside operatiivset lahendamist ning on CERT tiimiks Hollandi keskvalitsusele ja kriitilise infrastruktuuri asutustele.

Hiljuti avaldasime oma küberturvalisuse strateegia, kus panime paika meetmed, kuidas niisuguste ülesannetega hakkama saada. Nende hulgas on näiteks üleriigiline küberturvalisuse võrgustik, kus on võimalik jagada efektiivsemalt informatsiooni küberturvalisuse kohta avaliku sektori ja erasektori parterite vahel.

Holland toetab ka tugevamat küberkoostööd Euroopas ja loodab sel tasandil Eestiga rohkem koostööd teha. Eesti paistab selles valdkonnas olevat loomulik koostööpartner – mõlemad riigid on arenenud digitaalse, avatud ja konkurentsivõimelise majandusega. NCSC on RIA ja CERT-EEga juba aastaid koostööd teinud nii operatiivsetes küsimustes kui ka poliitika kujundamises. Kahepoolsete suhete kõrval oleme nendes valdkondades teinud tööd ka Euroopa Liidu raames, mis on viinud küberturvalisuse koostöö uuele tasandile.

Eesti võttis digiteerumise ette üsna varakult ja on (turvalise) digitaalse valitsemise mõttes Euroopas esirinnas. Et üleeuroopalise võrgustiku professionaalsust ja arengut stimuleerida, tuleb veelgi intensiivsemalt otsida koostöökohti. Küberruumis kasvavad ohud ning kodanike üha kasvav sõltuvus tehnoloogilistest lahendustest nõuab üha tõhusamat küberturvalisust üle terve Euroopa – näiteks paremat informatsiooni- ja teadmistevahetust, võimalikele kriisidele reageerimise võimet, õppusi ja partnerite võimete arendamist.

TURVALINE IDENTITEET

Eestis käib töö kvantarvutite turvamiseks

Tartu ülikooli krüptograafiaprofessor Dominique Unruh ütleb, et avaliku võtme taristuga turvasüsteemid, näiteks Eesti ID-kaart, on kvantarvutitega murtavad. Kuigi sellist arvutit veel polegi, peavad turvalised lahendused valmis olema juba enne.

Professor Unruh, kui kaugel me töötavast kvantarvutist oleme? Ja kuidas me saame valmistuda selleks, mida veel pole?
Tänapäeval eksisteerivad veel väga piiratud kvantarvutid ja need pole kasulikud krüptosüsteemide ründamiseks. Kuigi on väga raske ennustada, millal täisfunktsionaalne kvantarvuti valmib, edeneb teadustöö nende loomiseks. Aga oleks viga oodata kvantarvuti ilmumiseni, enne kui me hakkama tegelema millegi sellisega, mida nimetatakse post-kvantkrüptograafiaks. See on krüptograafiline süsteem, mis kvantarvutite suhtes turvaline.

Uue krüptograafilise süsteemi uurimine, arendamine ja laialdaselt kasutusele võtmine võtab aastaid, ilmselt isegi kauem kui kvantarvuti enda arendamine. Kui me probleemi tõsiselt ei võta, võidakse meist mööda minna, nii et kvantarvutid saavad valmis juba enne kui turvalahendused.

Õnneks on võimalik kvantarvutite tulekuks valmistuda kvantarvutit kasutamata. Me küll ei tea, kuidas kvantarvuti täpselt ehitatakse, aga meil on selle toimimise ja põhimõtteliste piirangute kohta olemas matemaatilised mudelid. Nii saamegi hakata matemaatiliselt analüüsima, kas kvantarvutiga saaks murda mõnda krüptosüsteemi, ilma et me oleks sellisel arvutil nuppugi vajutanud.

Tartu ülikooli krüptograafiaprofessor Dominique Unruh.

Sellisel moel püüamegi me täna luua krüptosüsteeme, mis suudaks vastu seista homsetele kvantarvutitele.

Millist riski võiks kvantarvutid kujutada meie praegustele krüptosüsteemidele?

Kogu maailmas levinud avaliku võtme taristu – millel põhineb ka Eesti ID-kaart – on kvantarvutite suhtes haavatav.

Kuigi me teame, et avaliku võtme taristule on alternatiive, pole need nii hästi uuritud ega ka tõhusad ning seetõttu praktikas kasutusel.

Nii et jah, kui kellelgi on täielikult töötav kvantarvuti, saaks ta täiesti murda enamiku tänapäevasest avaliku võtme taristust.

Kui me tahaksime täpselt analüüsida, mis riske see meie igapäevaelule kujutab, on meil vaja teada, kui kallis selline kvantarvuti oleks ja kas see oleks kättesaadav ka näiteks kuritegelikele jõududele. Seda on praegu veel raske ennustada.

Saite mullu Euroopa teadusnõukogult viieks aastaks üle 1,7 miljoni euro suuruse uurimisgrandi. Mis on teie uurimistöö eesmärk?

Kui analüüsida krüptograafilisi süsteeme, olgu need tavalised või kvantsüsteemid, kasutame nende turvalisuse uurimiseks matemaatilisi tõestusi.

Aga matemaatilised tõestused on väga keerulised ja inimestel on väga lihtne neid kirjutades või kontrollides vigu teha. Põhimõtteliselt on nii, et kui ainult inimesed kontrolliks keerukat matemaatilist tõestust, siis me ei teaks ikkagi, kas see tõestus on korrektne.

Formaalne verifitseerimine on meetod, millega kontrollitakse tõestusi arvuti abil – inimene võib olla või mitte olla tõestuse kirjutanud, aga me kasutame arvutit selle kontrollimiseks.

Kuna arvutitel ei ole piiratud tähelepanuväli nagu inimestel, sobivad need hästi selleks, et vaadata läbi megabaitide kaupa tõestusi ja leida vähimgi viga.

Minu uues Euroopa teadusnõukogu projektis töötame välja formaalse verifitseerimise meetodi just kvantkrüptograafiale. Ja me kasutame seda selleks, et kvantkrüptograafiliste süsteemide turvalisust kontrollida. See annab kvantkrüptograafia arendamisele tugevama matemaatilise vundamendi.

Minu uurimisrühmas on praegu üks järeldoktoriõppe ja kolm doktoriõppe üliõpilast, aga Euroopa teadusnõukogu rahastusega kasvab see hulk kahe- või kolmekordseks. Meie igapäevane töö on matemaatiliste tõestuste kontrollimine ja formaalse verifitseerimise meetodite arendamine, esmalt paberil ja siis tarkvaras. Aga lisaks tegeleme ka õpetamisega, et kasvatada järgmine põlvkond kõrgetasemelisi krüptograafiaeksperte.

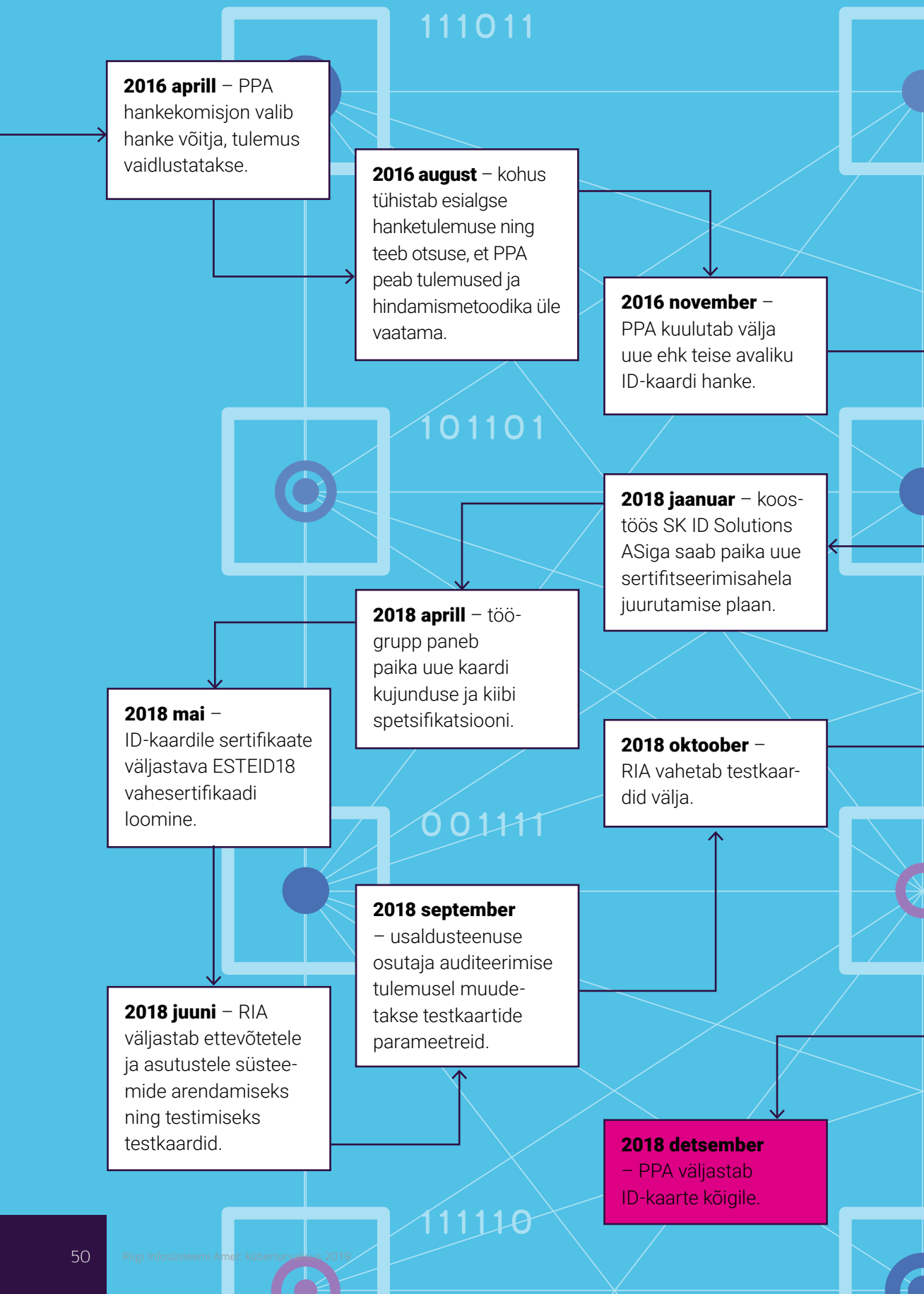
Uue ID-kaardi ajarännak

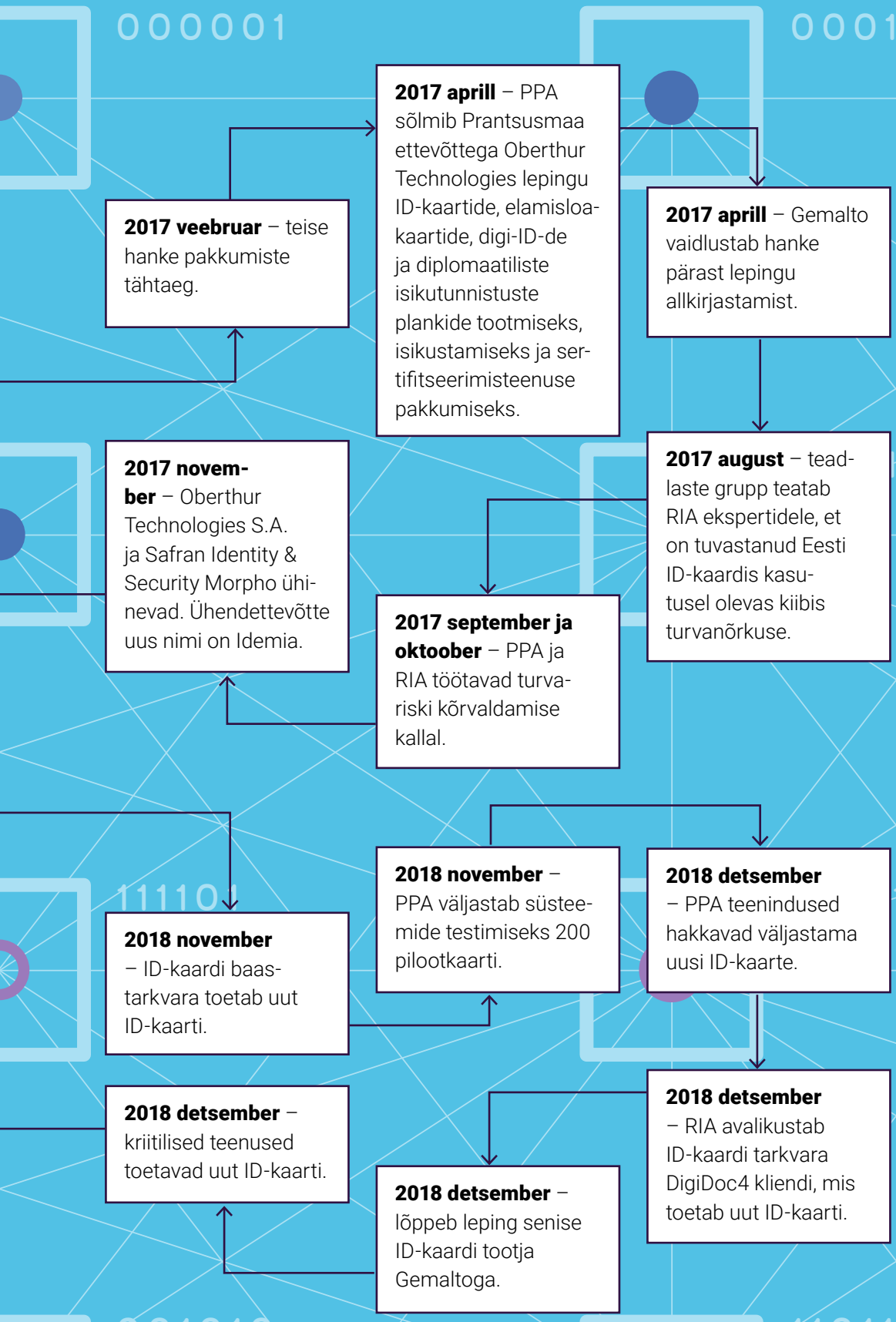
2018. aasta detsembrist väljastab politsei- ja piirivalveamet (PPA) uue kiibi, turvaelementide ja kujundusega ID-kaarte. Iga niisugune uuendus nõuab aga aega: vaja on kiipe testida ja sertifikaate uuendada.

2015 jaanuar – PPA ja RIA alustavad ettevalmistustega uue ID-kaardi hankelepingu sõlmimiseks.

2015 november – kuulutatakse välja esimene hange.

2016 veebruar – pakkumiste esitamise tähtaeg. Pakkumuse esitasid senine kaarditootja Gemalto A.G, Oberthur Technologies S.A. ja Safran Identity & Security Morpho.


111011
2016 aprill – PPA hankekomisjon valib hanke võitja, tulemus vaidlustatakse.
2016 august – kohus tühistab esialgse hanketulemuse ning teeb otsuse, et PPA peab tulemused ja hindamismetoodika üle vaatama.
2016 november – PPA kuulutab välja uue ehk teise avaliku ID-kaardi hanke.
101101
2018 jaanuar – koostöös SK ID Solutions ASiga saab paika uue sertifitseerimisahela juurutamise plaan.
2018 aprill – töögrupp paneb paika uue kaardi kujunduse ja kiibi spetsifikatsiooni.
2018 mai – ID-kaardile sertifikaate väljastava ESTEID18 vahesertifikaadi loomine.
2018 oktoober – RIA vahetab testkaardid välja.
001111
2018 september – usaldusteenuse osutaja auditeerimise tulemusel muudetakse testkaartide parameetreid.
2018 juuni – RIA väljastab ettevõtetele ja asutustele süsteemide arendamiseks ning testimiseks testkaardid.
2018 detsember – PPA väljastab ID-kaarte kõigile.
111110


2017 aprill – PPA sõlmib Prantsusmaa ettevõttega Oberthur Technologies lepingu ID-kaartide, elamisloa-kaartide, digi-ID-de ja diplomaatiliste isikutunnistuste plankide tootmiseks, isikustamiseks ja sertifitseerimisteenuse pakkumiseks.
2017 veebruar – teise hanke pakkumiste tähtaeg.
2017 aprill – Gemalto vaidlustab hanke pärast lepingu allkirjastamist.
2017 august – teadlaste grupp teatab RIA ekspertidele, et on tuvastanud Eesti ID-kaardis kasutusel olevas kiibis turvanõrkuse.
2017 november – Oberthur Technologies S.A. ja Safran Identity & Security Morpho ühinevad. Ühendettevõtte uus nimi on Idemia.
2017 september ja oktoober – PPA ja RIA töötavad turvariski kõrvaldamise kallal.
2018 november – PPA väljastab süsteemide testimiseks 200 pilootkaarti.
2018 detsember – PPA teenindused hakkavad väljastama uusi ID-kaarte.
2018 november – ID-kaardi baastarkvara toetab uut ID-kaarti.
2018 detsember – RIA avalikustab ID-kaardi tarkvara DigiDoc4 kliendi, mis toetab uut ID-kaarti.
2018 detsember – kriitilised teenused toetavad uut ID-kaarti.
2018 detsember – lõppeb leping senise ID-kaardi tootja Gemaltoga.

Küberturvalisuse strateegia 2019–2022

2018. aasta oktoobris kiitis valitsus heaks küberturvalisuse strateegia aastateks 2019–2022. See on nägemus, kuhu Eesti järgmise nelja aasta jooksul küberturvalisuse valdkonnas liigub.

VISIOON

Eesti on kõige küberturvalisem digitaalne riik. Eesti suudab küberohtudega tõhusalt toime tulles tagada digitaalse ühiskonna turvalise ja tõrgeteta toimimise, toetudes riigiasutuste ühisele võimekusele, teadlikule ja osalevale erasektorile ning väljapaistvale teaduskompetentsile. Eesti on küberturvalisuse valdkonnas rahvusvaheliselt hinnatud suunanäitaja, mis toetab riigi julgeolekut ja aitab kaasa valdkonnas tegutsevate ettevõtete globaalse konkurentsivõime kasvule. Ühiskond tervikuna tajub küberturvalisust ühise vastutusena, kus igaühel on täita oma roll.

Visiooni elluviimiseks lähtub Eesti küberturvalisuse tagamisel järgmistest aluspõhimõtetest.

- Peame põhiõiguste ja -vabaduste kaitset ja edendamist internetis sama oluliseks kui füüsilises keskkonnas.
- Kohtleme küberturvalisust Eesti kiire digitaalse arengu võimaldaja ja võimendajana, mis on Eesti sotsiaal-majandusliku arengu aluseks. Turvalisus peab toetama innovatsiooni ja innovatsioon turvalisust.
- Teadvustame, et krüptograafiliste lahenduste turvakindluse tagamine on Eesti jaoks unikaalselt oluline, kuna sellele tugineb kogu meie digiriigi ökosüsteem.
- Digiriigi toimimise aluseks on läbipaistvus ja avalik usaldus. Selle hoidmiseks peame kinni riigipoolse avatud kommunikatsiooni põhimõttest.

EESMÄRK: Eesti on jätkusuutlik digitaalne ühiskond, millel on tugev tehnoloogiline vastupanuvõime ja valmisolek kriisidega toimetulekuks

- Riigi infosüsteeme ja digitaalseid teenuseid tuleb arendada algusest peale turvaliselt, arvestades nii tehnoloogilisi kui ka organisatsioonilisi nõudeid, põhimõtteid ja standardeid.
- Võtmetähtsusega on see, et riigiasutused ja avalik sektor järgiksid infoturbestandarditest lähtuvaid baasturbenõudeid vähemalt seadusega ette nähtud tasemel.
- Tagatakse Eestile oluliste digitaalsete varade (põhiandmed kodanike, territooriumi ja õigusloome kohta) kaitse. Samuti on oluline üle vaadata turvaline andmeside riigiasutuste vahel nii tava- kui kriisiolukorras.
- Tehniliste seireandmete süsteemseks analüüsimiseks tuleb arendada tööriistad, et luua reaalajalähedane pilt, mis mõõdab tehnilist küberturbe taset Eesti arengu näitamiseks.
- Selgitatakse välja erinevate asutuste küberturvalisuse võimed ning nende põhjal pannakse kokku riiklik olukorrapilt ja riigivõrkude turbe korralduse juhtimine, luues RIA küberturvalisuse teenistuse baasil riigiülese küberturvalisuse keskuse (NCSC).
- Tugev, sidus ja kogukonnakultuuril põhinev igapäevane koostöö on olnud aluseks Eesti senisele edule küberturbe tagamisel ja laialdaste tagajärgedega intsidentide ärahoidmisel ning seda praktikat jätkatakse ja tugevdatakse ka uuel strateegiaperioodil.

EESMÄRK: Eestis on tugev, innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbesektori ettevõtlus ning teadus- ja arendustegevus, mis katab riigi jaoks olulised võtmekompetentsid

- Tulemusliku koostöö võimaldamiseks on juba loodud erasektori, akadeemilise kogukonna ja riigi koostööd toetav info- ja küberturbe klaster Eesti Infoturbe Assotsiatsioon (*Estonian Information Security Association*, EISA).
- Küberturvalisuse teadussuundade ühtsema arengu osas on vaja järgmiseks defineerida küberturbe valdkonna teadus- ja arendustegevuse fookusvaldkonnad. Ekspordipotentsiaali võimendamiseks süstematiseerib riik küberturbega tegelevate (väike)ettevõtete parema kaasamise äridiplomaatia visiitidel ja delegatsioonide külastusel.
- Startup Estonia jätkab kogukonna edendamist koostöös majandus- ja kommunikatsiooniministeeriumiga, et liikuda piisava arengutaseme saavutamisel edasi kübervaldkonna ettevõtete kiirendi loomise suunas ja pakkuda ka esmase arengufaasi läbinud ettevõtetele väärtust globaalseks kasvuks.

EESMÄRK:
Eesti on arvestatav ja tugev partner rahvusvahelisel areenil

- Oluline on jätkata senist rahvusvahelist koostööd kübernormide, usaldusmeetmete ja rahvusvahelise õiguse valdkonnas.
- Eesti huvides on tagada ka küberrünnakute edukas menetlemine, mille jaoks on omakorda vaja hoida ja edendada piiriülest koostööd, sealjuures tagada menetlusteabe kiire ja tõhus kättesaamine teistest riikidest, ning tugevdada üldist infovahetust ja koostööd.
- Ajakohase küberkompetentsi hoidmiseks tuleb soodustada diplomaatide ja ametnike rotatsiooni asutuste vahel ning teadmiste ja oskuste jagamist.
- Oluline on süsteemne küberkoostöö erinevate võtmeriikide ja neis paiknevate küberagentuuridega.
- Eesmärgiks on arendada välja toimiv küberrünnakute omistamise protseduur Eestis nii poliitilisel kui tehnilisel tasandil ning osaleda aktiivselt samameelsete riikide heidutus- ja omistamisalastes koostööformaatides. Oluline on panustada NATOs käimasolevasse diskussiooni kollektiivkaitsest küberruumis.
- Eesti jaoks on oluline süsteemselt toetada kübervõimete arendamist väljaspool ELi ja NATOt ning selleks tuleb näiteks osaleda ELi küberabivõrgustiku loomises, et arendada välja konkurentsivõimeline ja jätkusuutlik küberabi osutamise võime, mis omakorda kinnistaks Eesti kuulumist juhtivate küberriikide hulka.

EESMÄRK: Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide järelkasv

- RIA võtab küberturvalisuse seaduse jõustumise järel keskse rolli küberhügieeni, riiklike ennetustegevuste ja ühiskondliku teadlikkuse kasvatamisel. Eri ametkondade koostöös tagatakse laiema avalikkuse teadlikkus küberohtudest: nii oskus end ohtude eest kaitsta kui ka teadmised, kuidas pärast küberrünnet käituda.
- Riigiasutuste küberhügieeni taseme tõstmiseks muudetakse küberturvalisust puudutavate testide läbiviimine riigiasutuste ja KOVide töötajatele kohustuslikuks.
- Õpilaste ja õpetajate küberturvalisusalaseid teadmisi ja oskusi mõõdetakse süsteemselt ning üldharidus- ja kutsekoolide õpetajatele tagatakse küberturvalisuskoolituste pakkumine.
- Küberturvalisus tuleks lõimida informaatika ainekavasse ning toetada küberkaitse süvaõppe jõudmist võimalikult paljudesse gümnaasiumidesse, luues nii eeldused küberspetsialistide järelkasvuks formaalharidussüsteemi kaudu.
- Akadeemiline välispoliitika kompetents, mis on juba Eestis hästi, tuleks liita kübervaldkonnaga. Selle kõrval tuleks luua võimalused õigusekspertide järelkasvu tekkeks ja kinnistada Eesti küberõigusalane kompetents osalemisega rahvusvahelistes projektides.

Fotode autorid:
Lehekülјed 4, 41, 49: Politsei- ja Piirivalveamet
Lehekülјed 9, 13, 55: Renee Altrov
Lehekülg 11: Raul Mee
Lehekülg 15: Põhja-Eesti Regionaalhaigla
Lehekülg 17: Taaniel Malleus
Lehekülg 21: Häirekeskus
Lehekülјed 23, 27, 29, 37: Riigi Infosüsteemi Amet
Lehekülg 31: Rasmus Jurkatam
Lehekülg 35: Clarified Security
Lehekülg 39: NATO küberkaitsekeskus
Lehekülg 47: Andres Tennus, Tartu ülikool
Lehekülg 54: Reimo Roonet