
Riigi Infosüsteemi Amet
Küber-
turvalisuse
aastaraamat
2022



Riigi Infosüsteemi Amet

Küberturvalisuse aastaraamat 2022

Sisukord



EESSÕNA

6 **Turvanõrkustest õppimine ja rääkimine teeb tugevamaks**
Möödunud aastal tuli võidujooksus aja ja kurjategijatega vastu võtta valusaid õppetunde. Ent kõik kogemused on vajalikud ning neid tuleb jagada, leiab RIA küberturvalisuse teenistuse juht **Gert Auväärt.**

2021. AASTA ÜLEVAADE

8 **Olukorrast küberruumis: turvanõrkuste aasta**
2021 läheb küberturvalisuse ajalukku kui suurte turvanõrkuste aasta. Neist mastaapseim oli logimisrakenduses Log4j tuvastatud haavatavus, kuid oli ka neid, mis puudutasid ainult Eesti e-riiki.

14 **Kuidas häkker varastas 300 000 dokumendifotot?**
Möödunud aasta üks tõsisemaid intsidente juhtus RIA enda teenuses olnud turvanõrkuse tõttu. Ründaja laadis alla ligi 300 000 dokumendifotot, kuid ta tabati juba paar päeva pärast andmevarguse avastamist.

16 **Taakvara tõi halbu üllatusi**
Riigiportaali eesti.ee pääsuõiguste süsteem andis meile valusa meeldetuletuse, et kui muutub suhtumine andmekaitsesse, peab seda tegema ka infosüsteem.

18 **Turvauuendused: viivitamine maksab kätte**
Tänaseida toimetusi viska ikka homse varna. Eelmisel aastal nägime liiga tihti, mis juhtub, kui kriitiliste haavatavuste paikamisel lähtuda sellest elutarkusest.

20 **Log4j põhjustas IT-maavärina**
9. detsembril pidid IT-spetsialistid reageerima viimaste aastate ühele suuremale turvanõrkusele: Log4j nullpäeva veale. IT-kogukonna silmis toimus kõikjal maailmas üheaegselt ränk maavärin ning valmistuti rannikualasid laastavaks tsunamiks.

22 **2021. aastal poole rohkem ummistusründeid**
Mullu registreerisime 47 mõjuga teenusetõkestusrünnet, mida on poole rohkem kui 2020. aastal. Kevadeni tekitasid peavalu väljapressimistega ummistusründed ettevõtete vastu, sügisel said populaarseks sihtmärgiks koolid ja õppekeskkonnad.

24 **Finantspettused on muutunud mitmekesisemaks**
Lõppenud aastal saime mullusega võrreldes viiendiku võrra rohkem teateid pettustest, mille tõttu Eesti inimesed ja ettevõtted raha kaotasid. RIA näeb vaid jäämäe tippu.

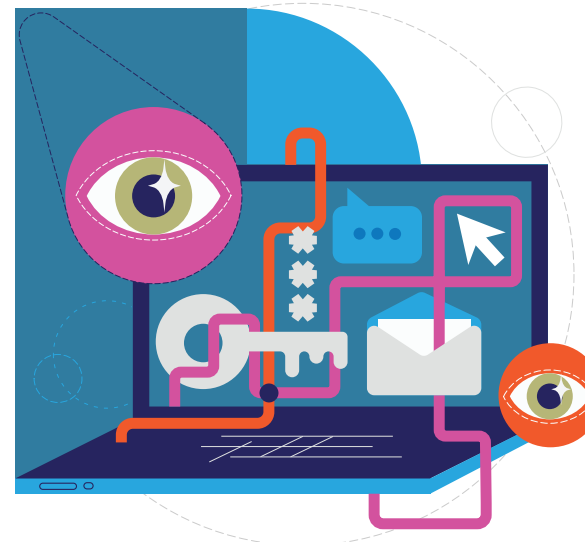
28 **Ei saa enne väravast läbi, kui värav avatud**
Oma füüsilise turbe tagamiseks järgib enamik meist lihtsaid printsiipe, kuid digitaalse vara puhul näivad paljud arvavat, et see kaitseb ennast ise, kirjutab keskkriminaalpolitsei küberkuritegude büroo juht **Oskar Gross**.

30 **Lunavararünnakud saavad harva ilusa lõpu**
Kui Hollywoodi pantvangidraamades kangelased reeglina pääsevad, siis küberruumis toimuvate pantvangivõtmistega, kus kurjategijate kätes on ettevõtte või inimese andmed, on sageli valida halbade ja väga halbade variantide vahel.

32 **Mida õppisime kohalikest valimistest?**
Avalikkuses tekitasid pahameelt mõned funktsionaalsed apsakad, kuid ühtegi märkimisväärse mõjuga intsidenti me 2021. aasta kohalike valimiste ajal ei tuvastanud.

34 **Häkkerid, tulge riigile appi!**
Töötame mudeli kallal, mis võimaldaks riigiasutusel teha koostööd häkkeritega ning maksta neile turvanõrkuse info eest tasu.





36 **Mis toimus rahvusvahelises küberruumis 2021. aastal?**
Eelmisel aastal kuulsid küberintsidentidest ja -turvalisusest ka need, kes varem polnud nende teemadega kokku puutunud. Paljud juhtumid häirisid otseselt ja suurelt inimeste igapäevaelu ning ületasid uudiskünnise.

40 **Õnneliku lõpuga intsidendid**
Küberturvalisusest rääkides on sageli fookuses olulise mõjuga intsidendid ja nende põhjustatud kahju: olgu selleks varastatud andmed, krüpteeritud süsteemid või rahakaotus. Halbade juhtumite varju jääb aga ka õnnelikuma lõpuga lugusid.

42 **Eesti elanike küberhügieen paraneb**
Eesti elanike küberhügieeni tase on kolme aastaga paranenud, kuid arenguruumi jagub, selgub koostöös statistikaametiga kogutud andmetest.

44 **Mida toob 2022. aasta küberruumis?**
Eelmine aasta tõi kuhjaga turvanõrkuseid ja lunavara-epideemia. Millega ähvardab 2022?

Turvanõrkustest õppimine ja rääkimine teeb tugevamaks

Möödunud aastat võiks pidada turvanõrkuste aastaks, kus võidujooksus aja ja kurjategijatega tuli võtta vastu valusaid õppetunde. Ent kõik kogemused on vajalikud ning neid tuleb jagada, leiab RIA küberturvalisuse teenistuse juht **Gert Auväärt.**

Minu esimesed töönädalad RIAs algasid kohe suurte krahhidega. Juulis sai ilmsiks kaks kriitilist nõrkust meie enda asutuse süsteemides, mis võimaldasid ligipääsu võõraste inimeste andmetele. Sisuliselt võib öelda, et uks küll oli lukus, aga võti oli ka seal samas lähedal.

Juba järgmisel kuul laekus info võimalikest haavatavustest teistes riigi e-teenustes, mille tulemusel olid samuti kättesaadavad inimeste andmed. Kinnisvara- ja abieluvararegistri vead parandati ning praegu pole teada, et andmeid oleks kuidagi kuritarvitatud.

TURVALISUS SÜNNIB KOOSTÖÖST

Mõlemad RIA teenustes avaldunud intsidendid, nii eesti.ee ettevõtja lehel oleva pääsuõiguse andmeleke kui ka dokumendifoto ebaseaduslik allalaadimine (mõlemat kaasust käsitleme pikemalt selles aastaraamatus) said osaliselt võimalikuks seetõttu, et uutes arendustes on jätkuvalt peidus vanad süsteemide liidesed, mis on jäänud tähelepanuta. Oleme nende juhtumite osas teinud asutuses sees korraliku analüüsi ja korrastanud protsesse, et midagi sellist enam ei juhtuks.

Mõlema juhtumi info andsid inimesed, kes ei tööta RIAs ega mujal valdkonnaga seotud asutustes. See kinnitab väidet, et riik üksi ei leia 20-aastase e-riigi nõrku kohti üles ning et turvalisust saab luua koostöös kogukonnaga. On väga tähtis, et me kõik võtame turvanõrkusi ja nende parandamist tõsiselt. Jagame infot, sest nii õpime teistelt, ega jäta vihjeid ja soovitusi tähelepanuta. Meie tegutsemise kiirusest sõltub see, kui rängad on haavatavuste tagajärjed – kas jõuame turvavead parandada enne, kui keegi jõuab neid kuritegelikel eesmärkidel ära kasutada.



GERT AUVÄÄRT
RIA küberturvalisuse teenistuse juht

HOIATUSI EI VÕETA TÕSISELT

Kui Microsoft avalikustas eelmise aasta märtsis oma Exchange'i turvanõrkuse ning selle paikamise info, mille kohta edastasime juhised ka teistele asutustele, siis nädal hiljem tehtud seire näitas, et kaks kolmandikku informeeritutest polnud võtnud vajalikke meetmeid kasutusele. Nende asutuste meiliserverid olid endiselt haavatavad ehk töötajate e-post sisuliselt kaitseta ja avatud. Hoiatust ei võetud tõsiselt.

Paikamata süsteemide tulemuseks on reeglina see, et pahategijad leiavad need üles ja paiskavad süsteemidesse pahavara, mis võimaldab näiteks ligipääsu e-kirjadele ja muudele andmetele. Küberkuritegevus on maailmas üks tulutoovamatest ning seeläbi ka kõige suurema kasvu teinud kuriteoliikidest. Kurjategija tabamine on aga kõige keerulisem, kuna mõju ja tagajärjed võivad avalduda alles aastaid hiljem ning jälgede peitmiseks on oluliselt rohkem võimalusi.

IT-süsteeme üle maailma rünnatakse kogu aeg ning avastatud ja ka avalikustatud turvanõrkustest võib olla palju kasu neilegi, kes üritavad selle arvelt rikastuda või mõju saavutada. RIA registreerib aastas üle 20 000 pöördumise ning ligi 2500 küberintsidenti, millel on reaalne mõju süsteemile või selle toimimisele. Kuigi suurem osa rünnakukatsetest ebaõnnestub, ei saa valvsust kaotada.

TURVALISEMA EESTI NIMEL

Maailmas üha sagenevad lunavararünnakud tekitavad ettevõtetele kahjusid, mis on võrreldavad keskmise Eesti riigiasutuse eelarvega. Eesti ei ole väga suure mõjuga lunavararünnakutega seni pihta saanud, kuid see on aja küsimus, kuna meie igapäevaelu, sh riigi toimimine, sõltub digitaalsetest teenustest.

Kuigi süsteemide turvalisuse eest kannab hoolt selle omanik, on turvalisus meie kõigi kätes ja meie kõigi luua. Nii nagu riik peab kaitsma oma inimesi, kes on usaldanud talle oma andmed, peab seda tegema ka mistahes teine andmekogu või teenuse omanik. Digitaalne ühiskond võrdub usaldus.

Usaldusväärsuse ja turvalisema e-riigi kaitseks oleme tõstnud ka enda võimekust RIAs – nii inimeste kui ka uuema ja moodsama seadmepargi abil. Lõime omaenda testijate tiimi, töötame välja heade häkkerite motiveerimissüsteemi, et avastada ja parandada teenuste nõrkusi, ning paigaldasime riigivõrku täiendava kaitsemüüri. Turvalisuse loomiseks ja hoidmiseks oleme astunud RIAs veel ühe olulise sammu – nimelt valmis kaua tehtud kaunikene ehk uus Eesti infoturbestandard (E-ITS). See on aabits ettevõtetele, mille järgi juhinduda ning ennetada võimalike riske. Aasta lõpus alustas ka esimene pilootrühm, mille peamine roll on töötada välja standardi rakendamise hea praktika ja valmistada ette uusi E-ITSi kogemusnõustajaid. Koos Tartu Ülikooliga valmis esmane E-ITSi-põhine küpsusmudel, mis annab organisatsioonidele kiire hinnangu nende infoturbe olukorrast ning võimaldab asutustel infoturbe taset omavahel võrrelda. Just nii, sammhaaval, turvalisemat Eestit ehitamegi.



Olukorrast küberruumis: turvanõrkuste aasta

2021 läheb küberturvalisuse ajalukku kui suurte turvanõrkuste aasta. Neist mastaapseim oli logimisrakenduses Log4j tuvastatud haavatavus, kuid oli ka neid, mis puudutasid ainult Eesti e-riiki.



Turvanõrkusi leidub peaaegu igas süsteemis, igas koodis, kui vaid piisavalt otsida ja katsetada. Suurem osa neist teadvustatakse ja parandatakse kiiresti. Infoturbe kogukondades on levinud põhimõte, et turvanõrkuse avastaja teavitab sellest süsteemi või teenuse omanikku. Ta annab piisavalt aega turvapaikade või koodiuuenduste väljatöötamiseks ning alles seejärel avalikustab haavatavuse ülejäänud maailmale.

2021. aastal avastatud suuremate turvanõrkustega alati nii hästi ei läinud. Suure mõjuga turvanõrkused on varemgi ühiskonda valusalt hammustanud, kuid 2021. aastal ei paistnud neil lõppu tulevat.

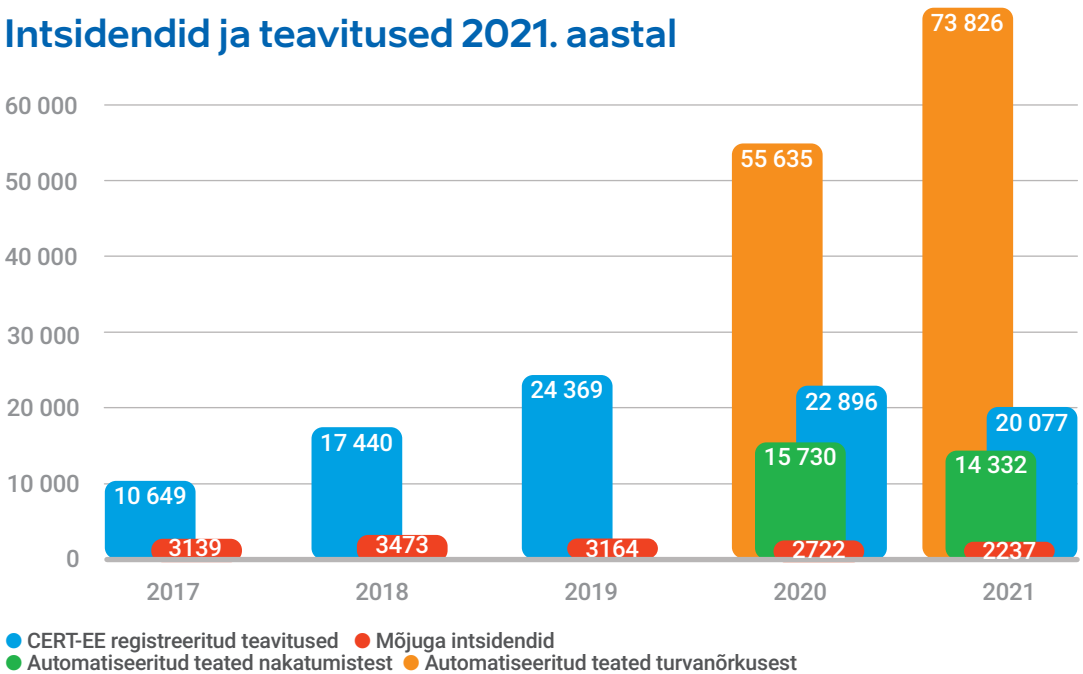
Suure mõjuga turvanõrkused on varemgi ühiskonda valusalt hammustanud, kuid 2021. aastal ei paistnud neil lõppu tulevat.

KUI SA EI TEA VEEL, ET OLED HAAVATAV

Eesti ühiskonda mõjutas 2021. aastal vast kõige valusamalt teadmine, et üks ründaja leidis turvanõrkuse RIA enda hallatavas süsteemis ning sai ligi sadade tuhandete inimeste dokumendifotodele (sellest kirjutame pikemalt lk 14).

Kuigi haavatavus andis ründajale ligipääsu pelgalt dokumendifotodele – millega pole tänapäeva digitaalsete isikutunnistuste ajastul peaaegu midagi kurja ette võtta –, tekitas see õigustatud küsimusi, kas Eesti e-riik suudab andmeid turvaliselt hoida ja varaste eest kaitsta. Kuid intsidendi käik andis märku, et e-riik ja meil kasutatav andmete lahususe põhimõte on õige. Iga päring dokumendifoto kohta jättis jälje, tänu millele oli politseil võimalik ründaja kinni pidada ja muid andmeid ta kätte ei saanud.

Turvanõrkuste all peame silmas ka seadistusvigu. Ühe sellise avastas tähelepanelik inimene eesti.ee ettevõtjatele mõeldud iseteeninduskeskkonnas, kus olid näha juriidiliste isikutega seotud enam kui 300 000 inimese ees- ja pere-



konnanimi, isikukood, töökoht ning osa puhul veel seosed varasemate ametikohtadega. Süsteem oligi algselt ehitatud nii, et volitatud isikud näeksid teiste volitatud isikute andmeid, kuid aastate jooksul oli see jäänud ajakohastamata. Sel puhul oleme ääretult tänulikud, et turvanõrkusest teavitamine toimus korrapäraselt: saime vea parandatud enne, kui laiemal avalikkusel või pahatahtlikul ründajal tekkinuks võimalus võõraid andmeid vaatama minna.

Turvanõrkust, mis on nii uus, et sellest teab vaid ründaja ja teenuse omanikul pole olnud päevagi selle paikamiseks, nimetatakse nullpäeva nõrkuseks. Kui aga haavatavale teenusele on juba uuendus olemas, on jutt teine. Pahatihti pole aga suuremate võrkude ja e-teenuste omanikel piisavalt detailset ülevaadet kõigist oma internetti avatud teenustest ning nende haavatavustest. Kaitsja peab vaatama oma IT-taristut ründaja silmadega, sest nemad käivad pidevalt ukselinke logistamas.

2020. aasta lõpus rünnati niimoodi majandus- ja kommunikatsiooniministeeriumi ning sotsiaalministeeriumi haldusala ja välisministeeriumi. Sarnase käekirjaga rünnakud jätkusid ka 2021. aastal. Sarnase käekirja all mõtleme seda, et ründaja skaneeris avalikult kättesaadavate tööriistadega veebiservereid, leidis mõned turvanõrkused, laadis üles ründekoodi ja sai niimoodi serveritele autoriseerimata ligipääsu.

Veebruaris teavitas meid kompromiteerimisest ettevõte, kes pakub pilveteenuseid ja tarkvara paljudele avaliku sektori asutustele (ministeeriumid ja kohalikud omavalitsused), ning teine, kes pakub avaliku sektori asutustele kaugligipääsu teenuseid. Ettevõtted reageerisid intsidentidele asjatundlikult ja paikasid oma teenused, teavitasid kliente ning tegid CERT-EEga koostööd.

KUI KOGU MAAILM TEAB, ET OLED HAAVATAV

Mõne turvanõrkuse tagajärgedest kuuleb avalikkus alles palju hiljem, sest nende mõju võib ilmneda kuude pärast. Märtsis avalikustas Microsoft neli nullpäeva haavatavust oma meiliserverite tarkvaras, mille kaudu said ründajad ulatusliku ligipääsu kogu serverile, sealhulgas e-kirjadele ja salasõnadele. Microsofti teadete järel ehitasid ründajad kiiresti tööriistad, mis hakkasid otsima veel uuendamata ja seega haavatavaid Exchange'i servereid üle terve maa-

ilma, leidmise korral need kompromiteeriti ja nakatati pahavaraga.

Augusti lõpus teatas maailmas laialdaselt kasutatava Confluence'i wiki-platvormi tootja Atlassian, et nendegi tootes on kriitiline turvanõrkus, mille parandamiseks oli vaja tarkvara uuendada. Confluence on kasutusel äriprotsesside dokumentatsiooniks või asutuste siseveebideks. Septembri alguseks suutsid ründajad haavatavust juba ära kasutada ning üritasid automatiseeritud süsteemide abil sisse pääseda avalikku internetti avatud Confluence'i serveritesse üle maailma, sealhulgas Eestis (neist haavatavustest loe lähemalt lk 18).

Kõige ulatuslikuma mõjuga turvanõrkus avaldati alles aasta lõpus, kui populaarses mänguplatvormis „Minecraft" hakkasid mängijad katsetama äsja avastatud turvanõrkusega, mis andis neile ootamatult võimaluse saata käsklusi mänguserverile. Üle maailma miljardites seadmetes ja tarkvaratoodetes kasutatava Java programmeerimiskeele logimisfunktsioonis Log4j tuvastatud kriitilise turvanõrkuse „Log4Shell" oli tootja küll juba paiganud, kuid needsamad miljonid seadmed ja neis käitatav tarkvara ei olnud veel uuendatud.

> Kaitsja peab vaatama oma IT-taristut ründaja silmadega, sest nemad käivad pidevalt ukselinke logistamas.

Niipea kui uudis turvanõrkusest levis, ruttasid IT-spetsialistid, arendajad ja infoturbespetsialistid üle maailma kõigepealt omaenda loodud tarkvaras Log4j funktsiooni uuendama ning seejärel kõigis oma teistes toodetes – tööstusseadmetes, võrguseadmetes, antiviiruse tarkvaras, veebiteenustes jne – tarkvarauuendusi ootama. Nii läks ka Eestis, sest paljudes Eesti e-teenustes on kasutusel ülipopulaarne Java programmeerimiskeel ning ka Log4j funktsioon.

Laiem avalikkus ei pruukinud seda näha, kuid ülemaailmse IT-kogukonna ühine pingutus haavatavuse ulatuse väljaselgitamisel ja üksteise toetamisel oli muljetavaldav. Tootjatel ununesid riigipiirid, tasuta ja tasuliste teenuste vahelised müürid, aeg-ajalt ka uni ja lähedased. Kuid „Log4Shelli" tagajärgi võib hakata nägema alles hiljem, kui selgub, kuhu ründajad selle turvanõrkuse abil enne paikamist sisse said.

KÕIK ALGAB LIGIPÄÄSUST: LUNAVARA JA TEISED INTSIDENDID

Maailmas said lunavararünnakud sel aastal õigustatult palju tähelepanu. Enim pakkus kõneainet Ameerika Ühendriikide kütusevarustajat Colonial Pipeline tabanud lunavararünnak, mille tõttu peatati USA idaranniku

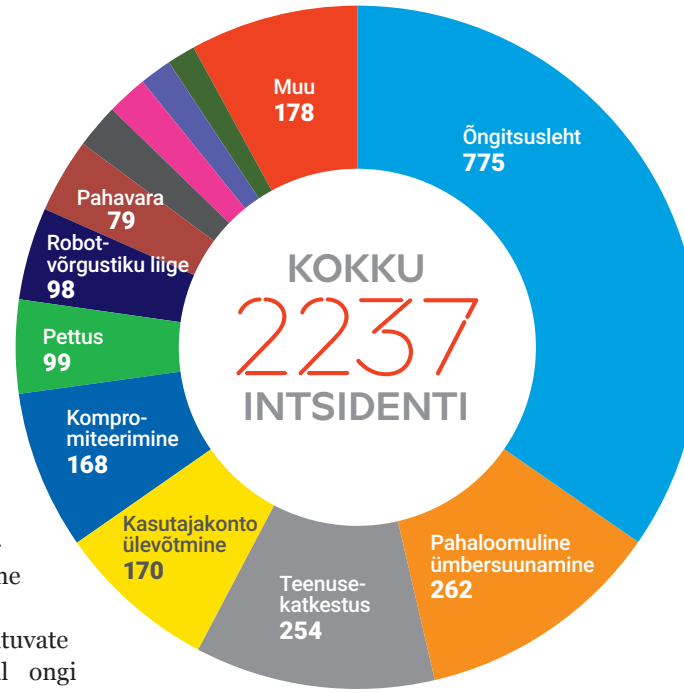
Log4j haavatavus – mis see on?

Üle maailma miljardites seadmetes ja tarkvaratoodetes kasutatava Java programmeerimiskeele funktsioonis Log4j tuvastati kriitiline turvanõrkus „Log4Shell". Turvanõrkuse tõsidus on rahvusvahelise CVE standardi järgi hinnatud kõrgeimaks võimalikuks (10 punkti 10st), see lubab ründajal haavatavas seadmes jooksutada vabalt valitud koodi.

Turvanõrkust on ründajal võimalik ära kasutada nii, et ta saadab haavatavale serverile, seadmele või süsteemile kindla formaadiga käsu (algusega „${jndi:") ja lisab sinna viite pahavarale, mis võib asuda kuskil kolmandas serveris. Haavatav server logib käskluse, Log4j otsib viidatud pahavara üles, laadib selle endale ja käitab. Sõltuvalt pahavara iseloomust võib see anda kolmandale osapoolele ligipääsu seadmele.

Mõjuga intsidendid 2021. aastal

- Teenusetõkestusrünne 47
- Kasutajaandmete leke 43
- SEO-spämm 34
- Lunavara 30



kütusetarned, kuid mitmemiljonilised lunarahanõuded ja lukustunud IT-süsteemid tekitasid ulatuslikke probleeme paljudes riikides.

Niisuguste miljonitesse eurodesse ulatuvate kahjudega lunavaraintsidentide puhul ongi enamasti sihtmärgiks USAs või laiemalt ingliskeelses ärikeskkonnas tegutsevad ettevõtted. Eestis saavad pihta väiksemad asutused, kellele esitatakse tihti „vaid" mõne(kümne) tuhande eurone lunarahanõue. Meid teavitati 2021. aastal kokku 30 lunavaraintsidendist (2020. aastal 33). Meie hinnangul on meid kaitsmas mõneti Eesti väiksus, keelekeskkond ja vaikselt, kuid kindlalt paranev küberhügieen.

Küberhügieen ja standardite järgimine on lunavararünnakute vastu suhteliselt tõhus rohi. Ka 2021. aastal jõudsid ründajad ohvrite süsteemidesse enamasti avatud kaugtöölauarakenduse kaudu (Windowsi keskkonnas *Remote Desktop Protocol* ehk RDP). Teatud versioonide puhul on tegemist avalikult teadaolevate turvanõrkustega, mõnel juhul on võimalik leida lekkinud paroolide andmebaasidest siiani kasutusel olevad salasõnad.

Kolmandatele osapooltele teenuseid pakkuvad IT-ettevõtted peaksid võimalike lunavararünnakute ennetamisele erilist tähelepanu pöörama. Aprillis saime teada juhtumist, kus lunavararünnakuga sihiti IT-teenust pakkuvat ettevõtet ning lunavara laienes selle kaudu veel nelja firmasse. Mais pääseti ligi raamatupidamisettevõttele, mille kaudu jõuti ka ühe Läänemaa vallavalitsuse süsteemidesse, kus ebaõnnestunult üritati lunavara käivitada.

CERT-EE spetsialistid on suutnud nii mõnelgi korral aidata taastada lunavaraga krüpteeritud andmeid, ilma et ohvrid peaksid lunaraha maksma. Mõnikord on lunavara jätnud suure osa andmetest kättesaadavaks (näiteks krüpteerib ära mingi osa failide algusest või lõpust), teistel kordadel on juba olemas dekrüpteerijad, mille abil saab andmed taastada. Lunavaraintsidendi puhul pöörduge kindlasti CERT-EE poole. Kurjategijatele raha makstes motiveerite neid samal alal jätkama.

MIS SAI ÕNGITSUSTE AASTAST?

2020. aastat nimetasime mulluses aastaraamatus õngitsuste aastaks – õngitsuslehtede hulk oli kasvanud viiendiku võrra ning õngitsused olid tihtipeale vahendiks, mille abil said ründajad teada mõne asutuse töötaja paroolid.

Õngitsused ei kadunud 2021. aastal kuhugi. Vastupidi: neid tuli veelgi juurde. Õngitsuslehtede intsidentide hulk kasvas nii protsentuaalselt (kõigist mõjuga intsidentidest 35% *vs* 26% aasta varem), aga ka üldarvudes (vastavalt 2021. aastal 755 ja 2020. aastal 711). Need arvud ei näita seda tohutut hulka, kui mitu korda on meile lehtedest märku antud, vaid seda, mitme õngitsuslehe mahavõtmist on CERT-EE spetsialistid nõudnud.

Olukord on sarnane aasta varasemaga ning lehed jagunevad laias laastus kaheks: pangakonto õngitsusteks ja kontoandmete õngitsusteks. Õngitsuslehed on enamasti äravahetamiseni sarnased originaalidega, vaid aadress on teine. Pangakonto õngitsuste puhul saadab ohver endalegi teadmata raha võõrale kontole, kontoandmete lehtedele sisestatud paroole kasutatakse kõige sagedamini meilikontodesse sissemurdmiseks. Reeglina päästab valele lehele sisestatud parooli kuritarvitamisest mitmeastmelise autentimise kasutamine.

Võib arvata, et mitu aastat nähtud pangakonto õngitsused on eestlastele juba tuttavad. Paistab, et kurjategijatele on tulusam ohvritele pigem helistada ja veenda neid raha saatma. Kontoandmete osas aga ei paista õngitsustel lõppu kuskilt.

ROBOTVÕRGUSTIKUD ANNAVAD TEENUSETÕKESTUSRÜNNAKUTELE UUE HOO

Ebameeldiva üllatuse pakkus 2021. aasta hajutatud teenusetõkestusrünnakute (*Distributed Denial-of-Service* ehk DDoS) suure mõjuga. Ka üldarvudes on näha kasvu: 2020. aastaga võrreldes tõusis suuremate DDoS-rünnakute hulk 32-lt 47-le (need on rünnakud, millest eraldi CERT-EE-le teada anti). Samuti oleme saanud 2020. aasta suvest parema nähtavuse väiksemate DDoS-rünnakute kohta, mis näitab samuti selget tõusutrendi.

2021. aastal nägime mitut lainet olulise mõjuga ummistusründeid. Kohe jaanuaris ja veebruaris sattusid mitmed Eestis tegutsevad pangad ja tehnoloogiafirmad selliste rünnakute alla, millega kaasnesid väljapressimiskirjad. Samadele ettevõtetele tehti sarnased rünnakud juba kolm kuud varem ja ähvarduskirjades viidatigi varasematele rünnakutele, öeldes, et „me ei ole teilt makset kätte saanud“ ja „oleme nüüd tagasi, makske ära“ ning „kui te nüüdki ei maksa, tuleme varsti taas“. Sarnased ründed toimusid ka teistes Euroopa riikides (CERT-EU andmetel vähemalt viies liikmesriigis) ning kaugemalgi.

Samuti nägime juba jaanuaris esimest rünnakut ühe Tallinna kooli vastu, mis häiris lühiajaliselt kogu linna haridusasutuste tööd. See muutus kevadel ja sügisel lausa trendiks. Alates septembrist oleme näinud pidevalt lühiajalisi rünnakuid üldhariduskoolide, kutseõppeasutuste, ülikoolide ning ka haridus- ja noorteameti hallatavate e-õppekeskkondade vastu.

Tihti on rünnakute taga kooliõpilased, kes on tellinud need suhteliselt vabalt kättesaadavatest veebifoorumitest. Sellistes kohtades pakutakse DDoS-rünnakuid kui teenust: ründaja on endale robotvõrgustikku kogunud suure hulga turvanõrkustega või nõrkade seadistustega ruutereid ja muid asjade interneti seadmeid ning püüab seesugustes foorumites väikeste summade eest seda rahaks teha.

Samas ei mõjuta need rünnakud ainult kooli enda taristut, vaid ka teisi asutusi, mis kasutavad näiteks samu nimeservereid.

Ühe maikuise teenusetõkestusrünnaku puhul tuvastasime Eestis asuva turvanõrkusega ruuteri, mis oli robotvõrgustikku liidetud ning mis osales rünnakus ühe kutseõppeasutuse vastu. Loomulikult teavitasime ruuteri omanikku ja vähemalt seda seadet pole enam võimalik võimendusründeks ära kasutada. Teenusetõkestusrünnetest loe lähemalt lk 22.

> Meie hinnangul on meid kaitsmas mõneti Eesti väiksus, keelekeskkond ja vaikselt, kuid kindlalt paranev küberhügieen.

Kuid seegi intsident näitab, et turvanõrkused, uuendamata tarkvara ja konfiguratsioonivead võimaldavad rünnakuid, millel on suur mõju meie igapäevaelule. Seetõttu on seadmete ja süsteemide omanikel äärmiselt oluline pöörata päriselt tähelepanu turvapaikadele ja teavitustele turvanõrkustest (muu hulgas ka CERT-EE kord ööpäevas saadetavatele teavitustele). Nii hoolitsed selle eest, et sinu ruuter, nutiteler või -külmkapp ei annaks ründajatele võimalust häirida Eesti elu.

Kuidas häkker varastas 300 000 dokumendifotot?

Möödunud aasta üks tõsisemaid intsidente juhtus RIA enda teenuses olnud turvanõrkuse tõttu. Ründaja laadis alla ligi 300 000 dokumendifotot, kuid ta tabati juba paar päeva pärast andmevarguse avastamist.

21. juulil tuvastas CERT-EE, et isikut tõendavate dokumentide andmekogust on ebaseaduslikult alla laaditud 286 438 dokumendifotot. Neid oli massiliselt alla laaditud 9000-lt Eesti ja välismaa IP-aadressilt alates 12. juulist. Seda võimaldas turvanõrkus pilte vahendavas teenuses (nn pilditeenuses), mida kasutatakse, kui inimene soovib alla laadida enda dokumendifoto.

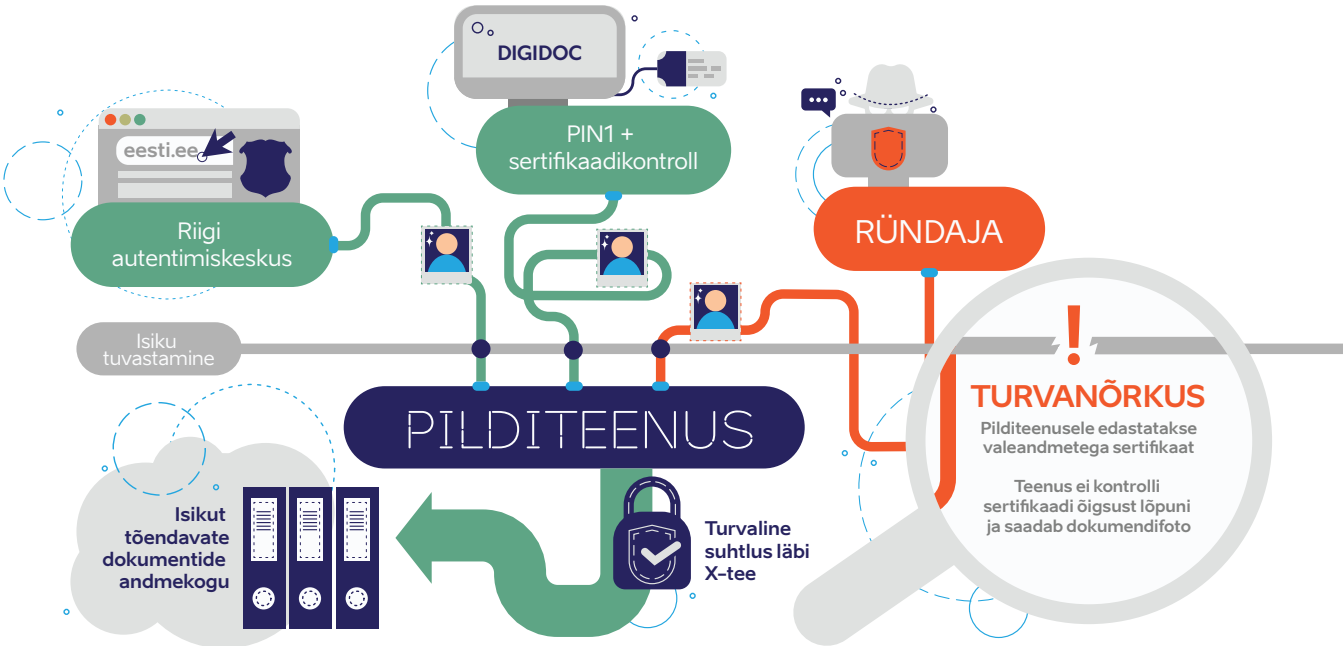
Oma dokumendifotot saab alla laadida kas otse riigiportaalist või DigiDoci rakenduse kaudu. Mõlemal juhul peab inimene end enne autentima. Kui ta on vastava päringu teinud, küsib süsteem fotot seda vahendavalt teenuselt ehk nn pilditeenuselt, mida haldab RIA. Pilditeenus pärib fotot üle X-tee isikut tõendavate dokumentide andmekogust, mis kuulub politsei- ja piirivalveametile (PPA), ja saadab selle küsijale tagasi. Ründe avastamise järel sulges RIA ajutiselt selle funktsiooni DigiDoci jaoks.

KUIDAS RÜNDAJA FOTOD KÄTTE SAI?

DigiDoc teeb päringuid üle avaliku URLi ehk veebiaadressi. Sellega manipuleerides õnnestus ründajal jätta pilditeenusele mulje, et päring tuleb autenditud kasutajalt, kes soovib alla laadida enda dokumendifotot. Tegelikult oli päringu taga aga ründaja, kes pöördus otse pilti

Fotovarguse õppetunnid

RIA analüüsis ja täiustas oma tööprotsesse, et niisugustest turvanõrkustest põhjustatud intsidente tulevikus vältida. Lisaks andis see juhtum hoogu riikliku ***bug bounty*** ehk nii-öelda heade häkkerite motiveerimise programmi loomisele. See tähendab, et tulevikus võivad riigi süsteemidest turvanõrkusi avastanud häkkerid riigilt ka tasu saada. Seda aga juhul, kui tegutsetakse paika pandud reeglite ja tingimuste järgi. Praegu preemiaprogrammi kallal veel töötatakse.



vahendava teenuse poole, kasutades selleks võltsitud ehk enda loodud sertifikaate (vt joonist). Võltsitud sertifikaatide loomiseks pidid ründajal olema inimeste isikukoodid ja nimed.

Pilditeenus oleks pidanud ära tundma, et ründaja kasutatud sertifikaatide väljastaja pole SK ID Solutions, vaid et need on võltsitud. Ehkki ründaja oli petteks ka enda loodud sertifikaatide väljastajaks kirjutanud SK ID Solutions, oleks nende „sisse vaatamine“ näidanud, et tegelikult on see mujalt pärit. Turvanõrkuse tõttu teenus seda ei teinud.

Rünnaku tagajärjel ei pääsenud kurjategija isikut tõendavate dokumentide andmebaasi, vaid tal õnnestus päringutega sealt kätte saada ainult dokumendifoto. Paar päeva pärast avastamist sai turvanõrkus parandatud ning RIA taasavas pilditeenuse DigiDoci jaoks, et inimesed saaksid taas selle kaudu oma dokumendifoto alla laadida.

KUIDAS SEE NÕRKUS TEKKIS?

Teadaolevalt tekkis ründaja poolt kuritarvitatud turvanõrkus fotosid vahendavas teenuses 2018. aasta novembris. Tõenäoliselt oli see seotud ID-kaartide sertifikaatide vahetusega, mistõttu tehti muudatusi infosüsteemides, et need toetaks uute sertifikaatidega autentimist.

CERT-EE analüüsis logisid alates 30. juunist 2018 ega tuvastanud muid anomaaliaid. See lubab järeldada, et fotosid vahendava teenuse turvanõrkust ei olnud enne 2021. aasta juulit kuritarvitatud. Politsei pidas kahtlustatava kinni paar päeva pärast intsidendi avastamist ja konfiskeeris alla laaditud andmed. Esialgne info lubas arvata, et fotod ei jõudnud kahtlustatava arvutist kaugemale. Riigiprokuratuuri juhitav menetlus käib endiselt.

> Politsei pidas kahtlustatava kinni paar päeva pärast intsidendi avastamist ja konfiskeeris alla laaditud andmed.

Pole just tavaline, et küberintsidente tekitanud ründajad nii kiiresti kätte saadakse. Sageli asuvad nad välismaal ja nende jälgi on keeruline – kui mitte võimatu – tuvastada. Kõnealuse juhtumi puhul oli lahenduse võtmeks politsei, CERT-EE ja prokuratuuri kiire ning tõhus koostöö.

Taakvara tõi halbu üllatusi

Möödunud suvel saime valusa meeldetuletuse, et kui muutub suhtumine andmekaitsesse, peab seda tegema ka infosüsteem.

6. juulil andis ettevõtja meile teada, et riigiportaali eesti.ee ettevõtja lehel on pääsuõiguste haldussüsteemi (AAR) iseteeninduskeskkonnas autenditud kasutajale kättesaadav andmebaas 336 733 andmereaga. Näha oli inimeste ees- ja perekonnanimi, isikukood, töökoht ning osal juhtudel seos eelnevate ametikohtade ja rolliga (nt ametinimetus, töösuhte algus- ja lõpukuupäev). Andmebaasis oli isikuid nii avalikust kui ka erasektorist.

Need andmed olid näha asutuse või ettevõtte esindajaks määratud inimestele ehk kõigile neile, kelle enda kohta oli samas andmebaasis rida. Kõik andmeread tulid otsijale nähtavale, kui ta tegi nn tühja ehk parameetriteta otsingu. Otsija nägi teiste andmeid ka siis, kui ta otsis näiteks isikut „Ants“ – sel juhul kuvati talle kõik andmebaasis olevad Antsud.

Mis on AAR?

AAR ehk pääsuõiguste haldussüsteem on asutuse ja ettevõtte volitatud isikutele mõeldud süsteem, milles nad saavad teistele anda ligipääsu erinevatesse teenustesse. Näiteks saab ettevõtte juht anda seal õiguseid raamatupidajale, et too saaks edastada töötajate andmed maksu- ja tolliameti hallatavasse töötajate registrisse.

Tegemist polnud klassikalise küberintsidendiga – süsteemi ei rünnatud ega ei läinud see ka katki. Ometi poleks tohtinud need andmed sellisel viisil nähtavad olla. Milles siis asi?

SÜSTEEM JÄI AJALE JALGU

Kogu pääsuõiguste haldussüsteem – sh selle riigiportaalis olev iseteeninduskeskkond – oligi algusest peale mõeldud ja ehitatud nii, et kõik andmed on kõigile andmebaasis olevatele inimestele näha. Maailm selle süsteemi ümber on muutunud, eriti lähenemine andmekaitsele. Nii muutus ka selline ülesehitus kohatuks.

Oli selge, et seesuguse süsteemiga ei saa jätkata. RIA sulges juulis riigiportaalis pääsuõiguste süsteemi iseteeninduskeskkonna. See tähendas, et rollide ja ligipääsude andmiseks peab sellest ajast peale pöörduma RIA kasutajatoe poole aadressil help@ria.ee. Kui enne said kliendid ligipääsusid anda kiirelt ja vahetult ise, siis nüüd on see muutunud veidi ebamugavamaks. Volituse koostamine, digiallkirjastamine, RIA-le saatmine ja vastuse saamine võtab rohkem aega ja vaeva.

Me ei pidanud otstarbekaks panustada vana süsteemi põhjalikku arendamisse, et iseteeninduskeskkond seal taas avada. Üks oluline argument oli see, et RIA-l on juba töös uue pääsuõiguste haldussüsteemi Pääsuke arendamine. Teine oluline argument oli see, et vanade süs-



teemide ehk nn *legacy* muutmine ei pruugi olla niisama lihtne.

LAIEM PROBLEEM

Legacy ehk taakvara on süsteem, tehnoloogia või tarkvara, mis endiselt töötab, kuid on tegelikult vananenud ning muutub ajaga järjest rohkem haavatavaks. Taakvara vaevab paljusid pikka aega tegutsenud ettevõtteid ja asutusi. Näiteks ei pruugi kümme aastat tagasi arendatud süsteemi praegustel omanikel olla täielikku teadmist selle ülesehitusest ega funktsioonidest. Organisatsioonid muutuvad ajas, inimesed vahetuvad ning pahatihti ei ole kunagi kasutusele võetud lahendused „järeltulijatele“ korralikult dokumenteeritud. Seetõttu pole sageli täpselt teada, millise dominoefekti võib ühe osa uuendamine kuskil süsteemi teises otsas kaasa tuua.

Riik panustab taakvara probleemi lahendusse

2022. aasta riigieelarvest eraldati täiendavalt 14,4 miljonit eurot vananenud infosüsteemide ja platvormide uuendamiseks ning ülalhoiuks. Lisaks eraldas valitsus reservfondist 500 000 eurot täiendavateks investeeringuteks riigiportaali eesti.ee vananenud infosüsteemide kiirkorras uuendamiseks ja vajadusel sulgemiseks. Varasema alarahastatuse tõttu on tekkinud taakvara probleem, mis muudab e-teenused haavatavaks.

Vanu süsteeme on kasutusel nii avalikus kui ka erasektoris. See on paljuski mõistetav, sest taakvarast loobumine on kulukas, ajamahukas ning võib kaasa tuua ka harjumuspäraste funktsionaalsuste muutuse. Millest siis alustada? Esimene samm võiks olla oma asutuse või ettevõtte taakvara tundmaõppimine. Nii tekib arusaam, mis seisus süsteem on, mis funktsioone see üldse pakub, kus on selle nõrgad kohad ja ristsõltuvused.

Millest siis alustada? Esimene samm võiks olla oma asutuse või ettevõtte taakvara tundmaõppimine.

Just sel moel on talitanud ka RIA. Oleme senisest veelgi põhjalikumalt tundma õppinud oma taakvara, välja selgitanud erinevate teenuste seoseid ja seadnud sisse protsessid, et meie süsteemid arengutest maailmas enam sellisel moel maha ei jääks.

Turvauuendused: viivitamine maksab kätte

Tänaseida toimetusi viska ikka homse varna. Eelmisel aastal nägime liiga tihti, mis juhtub, kui kriitiliste haavatavuste paikamisel lähtuda sellest elutarkusest.

2. märtsil 2021. teatas Microsoft, et populaarses meiliserveri tarkvaras Exchange Server on neli nullpäeva haavatavust, mille kaudu said ründajad paigaldada ohvri serverisse pahavara ning selle kaudu ligipääsu neis olevatele e-kirjadele, kontaktidele, salasõnadele ja administraatori õigustele. Sama teatega avaldas Microsoft ka turvapaigad, mis nõrkused parandas, ning palus need kiiremas korras paigaldada.

Kiirus loeb

Selles, et tarkvarades leitakse kriitilisi turvanõrkusi, pole midagi uut, kuid enneolematu on tempo, millega küberrühmitused ja üksikürita-jad paikamata süsteemid tuvastavad ja kompromiteerivad. Kui varem võis selleks kuluda nädalaid, siis nüüd päevi või tunde. Küberturbe eest vastutajad peavad tõusnud tempoga sammu pidama ja paikama ohtlikud turvanõrkused esimesel võimalusel, selmet lükata need tegemist vajavate tööde üha pikemaks veniva järjekorra lõppu.

Kui seni teadsid haavatavustest vähesed (Microsofti sõnul kasutas neid rünnakuteks Hiina riikliku taustaga küberrühmitus HAFNIUM), siis 2. märtsist oli info kõigile huvilistele kättesaadav. Algas võidujooks ajaga – kas enne jõuavad kohale ründajad, kes asusid automatiseeritud tööriistadega haavatavaid meiliservereid otsima ja ründama, või serverite omanikud ja haldajad, kellel olid nüüd vahendid turvaaugu lappimiseks.

MAÑANA-SUHTUMINE EI AITA

Sageli võitsid ründajad. 3. märtsil teatas Microsoft, et ohvreid on „piiratud arv“, 8. märtsil oli neid juba rohkem kui 60 000. Päev pärast haavatavuste avalikustamist tuvastas CERT-EE Eesti küberruumist enam kui 80 mainitud nõrkustega meiliserverit. Teavitasime nende omanikke ja haldajaid, informeerisime avaliku sektori turvajuhte ning elutähtsa ja olulise teenuse osutajaid. Kui 10. märtsil seiret kordasime, avanes nukker pilt: kaks kolmandikku serveritest olid endiselt paikamata tarkvaraga ja seetõttu rünnakutele avatud. Kui üle ilma paigati nädalaga kolmveerand haavatavatest serveritest, siis Eestis vaid kolmandik.

Rekordarv haavatavusi

- USA riikliku standardite ja tehnoloogia instituudi (NIST) haavatavuste andmebaasis NVD (National Vulnerability Database) registreeriti 2021. aastal 20 046 haavatavust (2020. aastal 18 351, 2019. aastal 17 382 ja 2018. aastal 17 252).
- 90 protsenti haavatavustest olid sellised, mille ärakasutamiseks polnud ründajal vaja häid tehnilisi oskusi.
- 61 protsenti haavatavustest ei vajanud rünnaku läbiviimiseks ohvri poolt mingit tegevust: lingil vajutamist, paroolide jagamist, tarkvara käivitamist ega muud taolist.



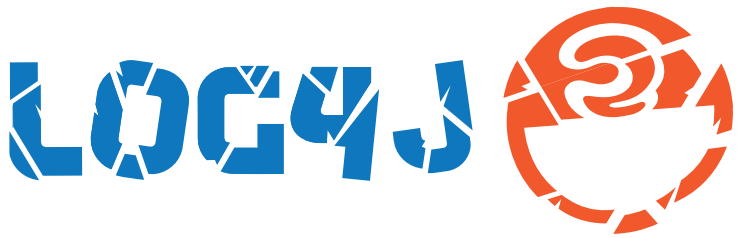
Seetõttu ei tulnud teated kompromiteeritud meiliserveritest meile üllatusena. Ohvrite seas oli kohalikke omavalitsusi ja eraettevõtteid, pihta sai meditsiinisektor ja haridusasutus.

TEINE TARKVARA, SAMA SKEEM

Sarnane sündmustejada keris end lahti augusti lõpus ja septembri alguses. 25. augustil teatas wiki-platvormi tootja Atlassian, et nende Confluence'i tarkvarades on koodi kaugkäivitust võimaldav kriitiline haavatavus. Selle abil sai autentimata kasutaja tungida ettevõtte või asutuse Confluence'i, seal andmeid muuta, lisada, kustutada ja/või kopeerida. Lisaks oli selle kaudu võimalik paigaldada ohvri süsteemidesse pahatahtlik kood, mille abil kaevandada krüptoraha või luua tagauks, mille kaudu viia läbi uusi rünnakuid. Atlassian hindas nende haavatavuste ohtlikkust kümnesel skaalal 9,8-ga.

Confluence pole küll nii levinud kui Microsoft Exchange, kuid seda kasutavad ka paljud Eesti riigiasutused ja eraettevõtted siseveebi platvormina. Septembris saime teada, et mainitud turvanõrkuse kaudu on rünnatud kolme riigiasutust. Tänu sissetungijate varasele avastamisele jäi suurem kahju sündimata, kuid tarkvara kiire uuendamise korral olnuks need rünnakud väldatavad.

Ohvrite seas oli kohalikke omavalitsusi ja eraettevõtteid, pihta sai meditsiinisektor ja haridusasutus.



Log4j põhjustas IT-maavärina

9. detsembril pidid IT-spetsialistid reageerima viimaste aastate ühele suuremale turvanõrkusele: **Log4j nullpäeva veale**. IT-kogukonna silmis toimus kõikjal maailmas üheaegselt ränk maavärin ning valmistuti rannikualasid laastavaks tsunamiks.

Java on üks enimkasutatavatest tarkvaraarendusplatvormidest. Selle vabavaraline Apache Log4j logimisfunktsioon on väga levinud – miljardid arvutid kasutavad seda äppide ja teenuste töös hoidmiseks. Seda funktsiooni kasutavad Apple, Steam, Twitter, Amazon, Tesla, IBM, Minecraft, LinkedIn ja tuhanded teised tuntud ja vähem tuntud ettevõtted.

MIS ON LOG4J FUNKTSIOON?

Iga tarkvara logib ehk talletab andmeid moel või teisel selleks, et oleks ülevaade, mis tarkvaraga toimub. See on vajalik laias laastus kolmel põhjusel: tarkvara töös hoidmiseks, arendamiseks ja turvalisuse tagamiseks. Logimine ehk andmete talletamine on hädavajalik.

Logimist võib võrrelda ühe linna peatänaval ja -väljakul asuva targa kaameraga. See annab linnavõimudele võimaluse kontrollida, kas jõulukuusk on ikka püsti, kas tänavad on lumesaju tõttu lumme mattunud või kas mõni muu linna teenus toimib nagu peab. Lisaks aitab see analüüsida, kuidas inimesed sealkandis talitavad: kas nad kasutavad olemasolevaid kõnniteid ja ülekäiguradu või „lõikavad“. Kui piirkonnas juhtub liiklusõnnetus, saavad politseinikud salvestist vaadates õnnetuse asjaoludes selgusele. Umbes sedasi toimib ka logimine.

Kui aga üks hetk võimaldab kaamera turvanõrkus üle võtta kogu linnavalitsuse infosüsteemid ja andmebaasid, on olukord võrdväärne Log4j kriitilise nõrkusega, mis annab kurjategijatele võimu mitte ainult selle konkreetse funktsiooni (kaamera), vaid kogu taristu üle.

KUIDAS TURVANÕRKUST KURITARVITATAKSE?

Kuigi pärast nõrkuse ilmsiks tulekut oodati suurt veeuputust ning valmistuti Noa laevale minekuks, siis praegu pole IT-maailma lõpp kätte jõudnud. Kuna turvanõrkus on väga ulatuslik, võib nõrkuse mõju avalduda alles aastate pärast. Praegu me ei tea veel, kas ja kuhu enne turvauuenduste paikamist sisse tungiti.

Ründaja sai turvanõrkust ära kasutada nii, et

saatis internetist kättesaadavale haavatavale serverile, seadmele või süsteemile kindla formaadiga sõnumi ja lisaviite pahavarale, mis asus kuskil kolmandas serveris. Haavatav server luges sõnumist välja käskluse, Log4j otsis viidatud pahavara üles, laadis alla ja käitas selle. Nagu inimene lööks iseennast oimetuks. Pahavara iseloomust sõltuvalt võib see anda kolmandale osapoolele ligipääsu seadmele.

Turvanõrkus mõjutab eeskätt ettevõtteid ja asutusi, sest nende süsteemidesse on võimalik potentsiaalselt sisse murda. Kui turvanõrkust hakkavad ära kasutama kurjategijad ja neil õnnestub paigaldada pahavara populaarsetesse teenustesse, võib see mõjutada ka tavakasutajaid.

2021. aasta lõpu seisuga ei ole turvanõrkuse massilist ärakasutamist Eestis ega maailmas toimunud, kuid nagu kirjutasime, võib selle mõju olla väga pika vinnaga. Kurjategijad seiravad praegu aktiivselt internetis olevaid teenuseid, et leida süsteeme, kus pole nõrkust kõrvaldatud. Haavatavaid seadmeid otsitakse ka Eestist.

MIDA TEHA?

Kõigepealt tuleks üle vaadata oma teenuseportfelli kuuluvad, Java platvormile ehitatud teenused. Jälgige, kas teie kasutuses olevatele toodetele on väljastatud uuendusi. Kui on, paigaldage need võimalikult kiiresti, sest need paikavad kriitilise turvanõrkuse. See on eriti oluline nende süsteemide puhul, mis on kättesaadavad internetis.

Pärast uuendust ei tohi jääda loorberitele puhkama. 28. detsembril avastati ühes Log4j versioonis väiksema mõjuga turvanõrkus. IT-spetsialistid peavad pingsalt jälgima, mis toimub selle turvanõrkuse ümber ning olema valmis, et uuendus vajab samuti uuendamist. Tuleb ka arvestada, et kõikide teenuste jaoks pole turvapaiku veel välja töötatud.

Mida tegi RIA?

- 10. detsembril teavitasime Eesti avalikkust turvanõrkusest ja selle mõjust.
- 13. ja 19. detsembril saatsime avalikule sektorile ja elutähtsate teenuste osutajatele täiendavat infot turvanõrkuse kohta.
- 22. detsembril avaldasime RIA blogis turvanõrkusele keskenduva postituse.
- Selgitasime välja RIA teenused, mis on nõrkusest mõjutatud. Paigaldasime uuendused või vastumeetmed.
- CERT-EE jälgib 24/7 Eesti küberruumis toimuvat ja otsib rünnakukatseid.

Haavatavus ei pruugi kunagi realiseeruda, kui haavatav teenus ei ole internetti avatud või on keelatud seadmetel internetti pöörduda.

OLUKORD EESTIS

CERT-EE tuvastas turvanõrkuse avalikustamise järgsetel päevadel Eesti ettevõtteid ja asutusi, mis olid nõrkusest ohustatud ning palus vastavad teenused uuendada või sulgeda. CERT-EE jätkab uute juhtumite otsimist, sest kõik teenusekasutajad pole veel nõrkust paiganud. Kõikidele teenustele pole turvapaika veel olemaski.

RIA-le pole teatatud tõsiste tagajärgedega Log4j haavatavuse kaudu tehtud rünnakutest. Küll aga on Eestis nõrkuse kaudu paigaldatud arvutitesse pahavara, mis kaevandab krüptoraha. Kuna see pahavara on koormav ja muudab teenused aeglasemaks, on need krüptokaevurid kiiresti üles leitud ja eemaldatud.

Välismaal on tulnud teateid, et nõrkuse kaudu on proovitud ette valmistada lunavararünnakuid. Kui kurjategijad on süsteemis käivitanud pahavara, mida on raske kohe avastada, võivad andmelekked ilmneda palju hiljem.

Kõigepealt tuleks üle vaadata oma teenuseportfelli kuuluvad, Java platvormile ehitatud teenused.

2021. aastal poole rohkem ummistusründeid

Mullu registreerisime 47 mõjuga teenusetõkestusrünnet, mida on poole rohkem kui 2020. aastal. Kevadeni tekitasid peavalu väljapressimistega ummistusründed ettevõtete vastu, sügisel aga said populaarseks sihtmärgiks koolid ja õppekeskkonnad.

Ühel veebruari külmal keskpäeval saabus Eestis tegutsevasse kommertspanka ähvardava sisuga e-kiri. Kandke kaks Bitcoini (toonases vääringus ligi 56 000 eurot) kirjas toodud kontole või korraldame teie vastu massiivse teenusetõkestusründe, mis halvab ettevõtte tegevuse. Samasisulise kirja ja nn näidisrünnaku oli pank saanud ka neli kuud tagasi.

Kui tavaliselt antakse reageerimiseks rohkem aega, siis sel korral algas rünnak kümme minutit hiljem. Kõige raskemal hetkel polnud kättesaadavad ei internetipank, kaardimaksed ega panga siseteenused. Ehkki rünnak kestis vahelduva intensiivsusega sama päeva õhtuni ja selle mõju tundsid nii panga kliendid kui ka töötajad, aitasid kaitsemeetmed halvima ära hoida.

> Selleks, et ohutu väljanägemisega seadmed ei muutuks mõne küberkurjategija käes ohtlikuks ründerelvaks, tasub nende tarkvara uuendada.

VÄLJAPRESSIMISTEGA RÜNDED LÕPPESID

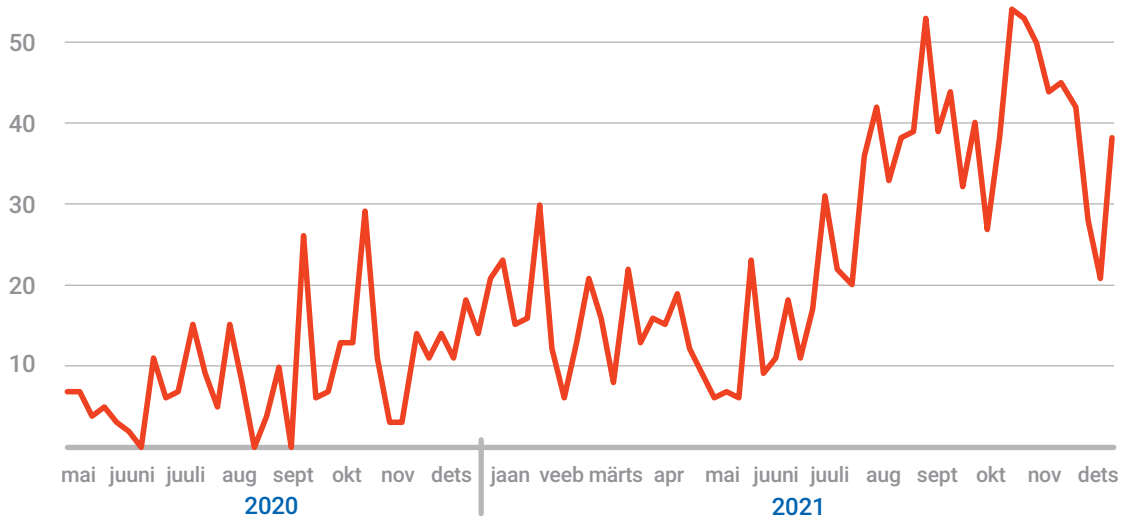
Säärased väljapressimistega ummistusründed naasid Eesti küberruumi 2020. aasta sügisel ja jätkusid 2021. aasta alguses. Sihtmärkideks olid mitmed tehnoloogiavaldkonnas ja finantssektoris tegutsevad ettevõtted, kel on e-teenuste katkemisest palju kaotada, kuid kes on tänu sellele ka keskmisest parema küberturbe tasemega.

Nendeni, keda sügisel rünnati, jõuti mõne kuu pärast tagasi. Enamasti mängiti vaid hirmul, aga oli ka erandeid. Näiteks kirjutas üks ummistusründe korraldanud väljapressija, et vajab raha tütre operatsiooniks ning muud ideed vajaliku summa teenimiseks on tal otsas.

Ründemeetodid, maht ja mõju erinesid, kuid ohvreid ühendas otsus väljapressimisele mitte alluda. Asjaolu, et kurjategijate äriplaan end ei õigustanud, oligi tõenäoliselt põhjus, miks väljapressimistega ummistusründed pärast esimest kvartalit peaaegu täielikult kadusid.

Teenusetõkestusrünnete hulk kasvab

2020. a suvest kogume automaatteavitusi ka olulise mõjuta ummistusrünnetest, mis on selges tõusutrendis.



RÜNNAKUD KOOLIDE VASTU

Nende asemel tõstis pead uus probleem: rünnakud koolide ning õppeinfosüsteemide Tahvel ja Moodle vastu. Neid ei kannustanud rikastumissoov – meile pole teada ühtki haridusasutuste vastu sooritatud rünnakut, millega kaasnes rahaline nõue –, vaid pigem on põhjust kahtlustada sama kooli mõne vähem usina õpilase hirmu ees ootava kontrolltöö või koolitunni ees.

Rünnakud koolide või õppeinfosüsteemide vastu toimusid reeglina õppetöö ajal. Nädalavahetusteks ja koolivaheaegadeks kadusid need kui vits vette, et siis koolipäevadeks taas naasta.

Septembris muutusid teated ummistusrünnetes koolide või õppekeskkondade vastu peaaegu igapäevaseks. Vahel polnud neil olulist mõju, kuid osa rünnakuist häiris siiski koolide igapäevatööd: polnud võimalik lisada ega vaadata tunniplaane, hindeid, puudumisi, õppematerjale, sooritada teste. Oli ka rünnakuid, mis mõjutasid lisaks sihtmärgiks valitud koolile ka teisi asutusi, mis kasutasid sama võrku või nimeservereid.

Kui mõni Juku võis arvata, et tellides oma kooli vastu rünnaku, pääseb ta sellega kontrolltööst või tema puudumine jääb registreerimata, siis Juhan teab, et nii need asjad ei käi.

Kui mõni Juku võis arvata, et tellides oma kooli vastu rünnaku, pääseb ta sellega kontrolltööst või tema puudumine jääb registreerimata, siis Juhan teab, et nii need asjad ei käi.

RÜNDAVAD KA EESTIS ASUVAD SEADMED

Enamasti osalevad meie e-teenuste vastu suunatud ummistusrünnetes välismaised seadmed, kuid intsidente analüüsides oleme leidnud ründajate ridadest ka Eesti IP-aadresse. Omanikud ei pruugi teadagi, et nende ruuter, printer või valvekaamera on nakatunud pahavaraga, liidetud mõnda robotvõrgustikku ja püüab „maha joosta“ tema kodupanka või laste kooli. Selleks, et ohutu väljanägemisega seadmed ei muutuks mõne küberkurjategija käes ohtlikuks ründerelvaks, tasub nende tarkvara uuendada.

Finantspettused on muutunud mitmekesisemaks

Lõppenud aastal saime mullusega võrreldes viiendiku võrra rohkem teateid pettustest, mille tõttu Eesti inimesed ja ettevõtted raha kaotasid. RIA näeb vaid jäämäe tippu, sest seda tüüpi pettuste puhul pöörduvad inimesed esmajoones politsei poole.

Kui ettevõtteid püütakse jätkuvalt tüssata erinevate arvepettustega, siis läinud aasta paistis silma just eraisikutele suunatud pettuste arvukuse ja kahjude poolest. Põhjuseid võib otsida pandeemiaolukorras tekkinud säästudest, pensionireformi tulemusel vabaks saanud rahast ja huvi suurenemisest krüptovaluutade vastu. Ennekõike aga asjaolust, et ka petturid arenevad kiiresti, kasutavad edukalt psühholoogilise mõjutamise võtteid ning on alati osanud muutlikest oludest kasu lõigata.

PETUKÕNED PANGAST JA POLITSEIST

Meieni jõudvatest teadetest eraisikuid puudutavate finantspettuste kohta on suur osa endiselt seotud petukõnedega panga nimel. Enamasti on helistajaks vene keelt kõnelev isik, kuid aasta lõpus oli ka selline laine, kus vestlust alustati eesti keeles ning alles seejärel anti üle venekeelsele „klienditeenindajale“. Kõnede eesmärk on PIN-koodide teada saamine ja nende abil pangakonto tühjendamine.

Ehkki nii politsei kui pangaliit on näinud vaeva probleemi teadvustamisega (vaata näiteks kampaanialehte eiaitah.ee) ning ka meedias on seda korduvalt kajastatud, on kahjuks jätkuvalt palju inimesi, kes kõnesid uskuma jäävad ning seeläbi oma säästud kaotavad. Arvud kõnelevad iseenda eest: politsei andmetel peteti aasta esimese kümne kuuga inimestelt sel moel välja 2,8 miljonit eurot, eriti aktiivselt just sügisel.

2021. aasta lõpus algas ka politseid imiteerivate kõnede laine: helistaja väidab end olevat Eesti politseist ja informeerib kõne saajat, et tema nimel olevat võetud suur laen, või siis küsib infot kellegi kolmanda isiku kohta ning annab teada, et kõne saaja pangakontoga on manipuleeritud. Kõne eesmärk on isikukoodi ja muude andmete õngitsemine, mis olevat vajalikud, et laen või ülekanded tühistada ja säästa inimene edasistest probleemidest.

Petturid proovivad enda usaldusväärsuse suurendamiseks erinevaid võtteid, näiteks nimetavad oma ametitunnuse (niinimetatud politseižetooni) numbri. Petukõnede taga on aga rahvusvaheliselt organiseeritud võrgustik, mille kõnekeskustest tehakse tuhandeid kõnesid päevas ja tulu teenimiseks püütakse neid järjest usutavamaks kohandada.



KRÜPTORAHAPETTUSED ON TÕUSEV TREND

Tõusev trend oli möödunud aastal erinevad krüptorahadega seotud pettused, mille kahjud ulatusid mõnesajast eurost ligi 100 000 euroni. Kõige tüüpilisemad olid juhtumid, kus inimene oli loonud konto ja alustanud tegevust mõnel krüptorahaga kauplemise platvormil, kust aga hiljem enam raha välja võtta ei õnnestunud. Tagantjärele selgus sageli, et tegemist oli libaplatvormiga ehk kurjategijate poolt spetsiaalselt loodud ajutise keskkonnaga, kuhu meelitati inimesi tehinguid tegema. Mõne aja pärast platvorm aga suleti ning raha omastati.

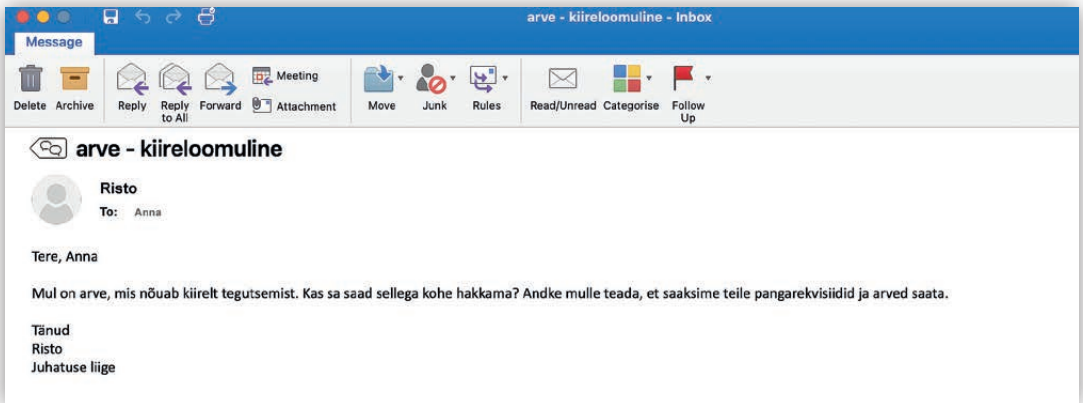
Seda tüüpi petuskeemide läbiviimine on suhteliselt lihtne, sest krüptoraha puudutav regulatsioon on kogu maailmas alles arenemisjärgus (Eestis vastavat valdkonda korrastav

Petuskeemidel on ka kaudsed ohvrid

Lisaks otsesele rahas mõõdetavale kahjule võivad arvepettustel olla ka kaudsed ohvrid, kelle äritegevus või maine saab ajutiselt kannatada. Toome siinkohal näite ühest meditsiinisektori ettevõttest, kelle nime ja rekvisiite võltsides hakati laiali saatma libaarveid sama valdkonna koostööpartneritele. See rikkus ajutiselt ettevõtte head nime ning põhjustas ka viivitusi makselaekumistel, kuna koostööpartnerid ei teadnud enam, milliseid saadud arveid usaldada, milliseid mitte.

Tõusev trend oli möödunud aastal erinevad krüptorahadega seotud pettused, mille kahjud ulatusid mõnesajast eurost ligi 100 000 euroni.

Näide petukirjast



seaduseelnõu loodetakse heaks kiita sel aastal). Praegu võib pea igaüks endale luua või osta krüptoga kauplemise keskkonna, osta sellele näilisi kasutajaid ja jälgijaid, teha ja suunata reklaami mõjukates sotsiaalmeediakanalites. Ehkki esmane soovitus enne mistahes krüptovääringu soetamist või vastava keskkonnaga liitumist on alati teha põhjalik taustauuring, ei pruugi ka sellest lõpuni abi olla – libaplatvormide puhul võivad olla võltsitud ka kasutajate arvustused ning negatiivne info petta saanud klientidelt jõuab foorumitesse alles siis, kui platvorm on tegevuse lõpetanud. Lisaks leidub ka foorumites sulisid, kes rahast ilma jäänutele „appi tõttavad“ ning neid uutele õngitsuslehtedele või libakeskkondadesse suunavad.

Libaplatvormide kõrval saime teateid ka juhtumitest, kus kurjategijatel õnnestus sisse murda inimese krüptorahakotti (rakendusse, kus krüptovara hoiustati) ja nad selle sisust ilma jätta. Keskmine raporteeritud kahju oli mõne tuhande euro ringis. Tuntumad rakendused, nagu näiteks MetaMask, ei ole iseenesest ebaturvalised, ent need on siiski haavatavad tavapärastele ohtudele nagu liiga nõrk parool, seotud rakenduste, näiteks veebibrauserite turvanõrkused või on kasutaja hoopis ise oma krüptovõtmed kogemata mõnele õngitsuslehele sisestanud. Kui pankade puhul on panga enda vastutus raha hoiustamisel väga selgelt reguleeritud ja hoiustajaid kaitseb seadus, siis vargus krüptomaailmas tähendab üldjuhul oma varast lõplikult ilma jäämist.

INVESTEERIMISNÕU TINDERIST?

Mitmed meile teadaolevad pettused olid seotud ühe kindla skeemiga. See toimib nii, et tutvumiskeskkonnas – sageli Tinderis või Facebook Datingus – leitud uus tuttav, näiteks kaunis asiaadist neiu või prantsuse noormees, hakkas mõne aja pärast rääkima investeerimisvõimalustest, millega ta ise on oma elujärge parandanud ja mille kohta on ta nõu saanud „finantsvaldkonnas töötavalt sugulaselt“.

Jutt ei pruukinud üldse olla pealetükkiv ning oli põimitud muu vestluse sisse oma igapäevastest tegemistest, oodati pigem vestluspartneri huvi ja lisaküsimusi. Tutvuse edenedes ja usalduse kasvades oli uus tuttav nõus oma häid investeerimissoovitusi ka jagama, aitas luua

Upistic kadus koos investorite rahaga

Aasta kahel viimasel kuul saime teateid keskkonna upistic.com kohta, mis reklaamis end Eesti juhtiva krüptoinvesteerimisteenuse pakkujana ning meelitas investoreid üle terve maailma. Keskkond aga lakkas tegutsemast ning investorid, enamasti välismaalased, jäid oma rahast ilma. Meile teadaantud juhtumite puhul olid kahjusummad mõnesajast mõne tuhande euroni.

konto mõnes spetsiaalselt selle jaoks loodud keskkonnas ning näitas, kuidas investeeritud summad justkui suurt kasumit teenisid.

Seejärel julgustati aina suuremate summadega edasi proovima, kui aga inimene soovis tehtud investeeringut välja võtta, osutus see võimatuks. Tegemist oli investeerimispettusega, ent agressiivse telefonimüügi asemel kasutatakse siin tutvumiskeskkondi, õpitakse ohvrit tundma ja tegeletakse temaga pikaajaliselt.

LIBAARVEID MAKSTI EELMISEL AASTAL VÄHEM

Läinud aasta purustas rekordi kahe Eesti mõistes väga suure arvepettuse katsega, mis aga õnneks ainult katseteks jäidki. Nendest suurim toimus varasuvel, kui kurjategijad asusid jälgima ühe Eesti suurettevõtte meilivahetust välismaal asuva koostööpartneriga. Sobival hetkel nad sekkusid ja esitasid näiliselt koostööpartneri nimel võltsitud arveid kokku mitme miljoni euro eest.

Ettevõtte meilifiltrisüsteemi abil saadi pettusele küllalt kiirelt järele ja kahju jäi olemata. Samuti ei leidnud Eesti ettevõte oma meilisüsteemist sissemurdmise jälgi, mistõttu võis oletada, et kompromiteeritud oli Kesk-Euroopas asuva koostööpartneri postkast.

Teine juhtum leidis aset aasta alguses, kui ühe ehitusettevõtte tähelepanelikud töötajad suutsid ära hoida sarnaselt läbi viidud arvepettuse katse 900 000 euro ulatuses. Öeldakse, et suur tükk ajab suu lõhki, ent need juhtumid näitavad, et õigesti valitud kaitsemeetmed ja töötajate teadlikkus levinumatest petuskeemidest tõesti tasuvad ära.

Mõned arvepettused läinud aastal siiski õnnestusid ja meile teadaolevalt suurim sel moel kaotatud summa oli 35 000 eurot.

Lisaks ülal kirjeldatud viisile, kus pettus viiakse läbi süsteemi sisse murdmise ja meilivahetusse sekkumise kaudu, ei ole kadunud ka klassikaline tegevjuhi petuskeem. Aasta viimasel kuul andis tosinkond ettevõtet meile teada, et nende raamatupidaja on justkui tegevjuhilt või juhatuse liikmelt saanud kirja palvega teha kiireloomuline ülekanne välispanga kontole. Vähemalt ühel juhul see ülekanne ka tehti ning 15 000 eurot jõudis petturi kontole. Üldine teadlikkus seda tüüpi pettustest on aga aastatega kasvanud ja suurt rahalist kahju toonud juhtumeid on vähem.

Ühe pettuse lugu

Martin on keskealine edukas ettevõtja, kes töötab konsultatsioonivaldkonnas ja suhtleb tööga seoses väga paljude inimestega Eestis ja välismaal. Ühel päeval sai ta Facebookis sõbrakutse naisterahvalt, kes esitles end rahvusvahelise moetööstuse esindajana, oli käinud Eestis puhkamas ning otsis siin turunduskontakte. Tema suhtlemisstiil oli viisakas ja professionaalne, ta saatis ka oma erialase tööga seonduvaid materjale ega käitunud kuidagi pealetükkivalt. Naine rääkis ka enda taustast, saavutustest ning saatis pilte, kõik tundus usutav ja usaldusväärne.

Kui suhtlus oli kestnud juba mitu nädalat, rääkis uus tuttav muu hulgas oma kogemustest krüptoraha turul ning plaanidest konkreetsete tehingute osas. Kuna ka Martin tundis selle valdkonna vastu huvi, küsis ta lähemalt ning sai viiteid ja linke erinevatele keskkondadele, kusjuures Martin kontrollis neid ega leidnud kuskilt viiteid, et keskkonnad oleks seotud petuskeemidega. Seejärel otsustas Martin investeerida krüptorahasse 1000 eurot, see hakkas kasumit teenima ning esialgu oli tal ka võimalik oma investeeringuga edasi toimetada. Positiivsest kogemusest innustunult tegi ta veel kaks lisainvesteeringut.

Ühel hetkel Martinil aga oma sõnul „ärkas intuitsioon“ ning kui ta püüdis teenitud raha oma krüptokontole tagasi kanda, see enam ei õnnestunud. Kokku kaotas Martin 8000 eurot, mille tagasi saamiseks politsei lootust ei anna ning Martin võtab seda kokkuvõtteks õppetunnina. Mis puudutab raha ja investeerimist, siis tema soovitus on olla väga ettevaatlik igasuguste uute kontaktidega ning mitte nende nõuandeid usaldada, ükskõik kui oskuslikult need on esitatud.

Ei saa enne väravast läbi, kui värav avatud*

Oma füüsilise turbe tagamiseks järgib enamik meist lihtsaid printsiipe, kuid digitaalse vara puhul näivad paljud arvavat, et see kaitseb ennast ise, kirjutab keskkriminaalpolitsei küberkuritegude büroo juht **Oskar Gross**.

Aasta tagasi kirjeldasin RIA küberturvalisuse aastaraamatus politsei rolli küberintsidentide uurimisel ning selgitasin, miks on oluline oma süsteeme uuendada ja pidada logisid. Nagu mullu, tuleb ka praegu tõdeda, et küberturvalisuse põhimõtted, nagu ka trendid küberkuritegevuses, ei ole ajas muutunud. Sel põhjusel on paslik seda „mantrat" korrata.

Helistasin eksprompt kolleegile CERT-EEst ja esitasin lihtsa küsimuse: kui ettevõttel puudub igasugune küberturve, siis mis on need kolm asja, mida minimaalselt peaks ära tegema, et end kaitsta? Vastus oli täpselt sama, mida oleks ka politsei omalt poolt pakkunud.

1. Tea, mis süsteeme sa kasutad ja mis andmed seal on.
2. Uuenda oma süsteeme regulaarselt.
3. Koolita oma kasutajaid, et nad teaks ohte märgata.

Päris „Tätte topeltgarantiid" anda ei saa, et neid kolme reeglit järgides oled kõigi küberohtude eest täielikult kaitstud, kuid tõenäosus ohvriks sattuda langeb siiski suurusjärkude võrra.

KAHJUD ON SUUREMAD KUI ESIALGU PAISTAB

Küberturvalisus ei erine teistest olukordadest, kus iga inimene teeb ise palju ära, et ohvriks mitte sattuda. Oma füüsilise turbe tagamisel järgime ju igapäevaselt lihtsaid printsiipe, et vara oleks kaitstud. Teame, kus asuvad aknad ja uksed meie kodus ja lahkudes veendume, et need oleksid lukus. Väärtuslikke asju hoiame seifis (punkt 1). Kui ukselukk katki läheb, vahetame luku välja (punkt 2). Lastele õpetame samuti, kuidas ust lukustada (punkt 3).

Me ei jäta katkist ukselukku vahetamata põhjusel, et see on tülikas või maksab raha. Meie kodu ja asjad seal on meile kallimad kui uue ukseluku maksumus ning julgen väita, et sama kehtib ka meie digitaalsete andmete kohta.

Probleeme süsteemide uuendamiste ja logide olemasoluga näevad küberkuritegude uurijad oma igapäevatöös aga väga tihti. Ka inimlikud eksimused on sagedased – ei osata ära tunda õngitsuskirja, paroole korduvkasutatakse.

Nii otsesed kui ka kaudsed kahjud, mis küberkuriteo järel võivad saabuda, on märkimisväärselt suuremad kui esialgu paistab. Tagajärg võib

* Eesti vanasõna

olla suur rahaline kahju eraisikule või ettevõttele ning tuleb arvestada, et kui pangaarvelt on raha varastatud, siis raamatupidamislikust kasumist kellelegi palka maksta ei saa.

Politsei poolt püüame oma koostööpartneritega alati kannatanul aidata raha tagasi saada, kuid tuleb arvesse võtta, et raha liigub erinevate riikide vahel kiiresti ning pole harvad juhud, kui see on ammu juba sularahana mõnes riigis välja võetud enne, kui kannatanu üldse aru saab, et midagi juhtunud on.

EELMISE AASTA OLULISEMAD UURIMISED

Küberkuritegevusest rääkides ei saa mainimata jätta möödunud aasta olulisi uurimisi – enam kui 280 000 dokumendifoto allalaadimine ja rahapesu teenuse pakkumine küberkurjategijatele.

Esimesel juhul on märkimisväärne, et koostöös partneritega tuvastasime kahtlustatava juba 24 tunni jooksul pärast rünnaku avastamist. Kiirele kinnipidamisele aitas kaasa asjaolu, et tegu pandi toime Eestis. Küberkuritegude puhul on rahvusvaheline element pigem reegel kui erand.

Ka rahapesu teenust pakuti Eestist, sedapuhku kurjategijatele välismaal ning kahtlustuse järgi teeniti sellega ligi 1,5 miljonit eurot.

Võib tekkida õigustatud küsimus, miks küberpolitsei uurib rahapesijaid, mitte häkkereid? Uurime loomulikult klassikalisi arvutikuritegusid, kuid lähtume ka siin põhimõttest, et kuritegevus ei tohi ära tasuda.

> Nii otsesed kui ka kaudsed kahjud, mis küberkuriteo järel võivad saabuda, on märkimisväärselt suuremad kui esialgu paistab.

Arvestades, et küberkuritegusid pannakse toime valdavalt finantsilistel motiividel, siis sellest tulenevalt mängib ka rahapesu uurimine olulist rolli. Pingutame, et küberuurimise võimet tõsta ning valdkonna interdistsiplinaarsuse tõttu vajame lisaks IT-teadmistega inimestele üha enam tööle muude valdkondade spetsialiste.



Lunavararünnakud saavad harva ilusa lõpu

Kui Hollywoodi pantvangidraamades kangelased reeglina pääsevad, siis küberruumis toimuvate pantvangivõtmistega, kus kurjategijate kätes on ettevõtte või inimese andmed, on sageli valida halbade ja väga halbade variantide vahel.

CERT-EE registreeris 2021. aastal 30 lunavararünnakut (2020. aastal 32). See arv ei tundu suur, aga tuleb arvestada, et lunavararünnaku tagajärjed on ühed raskemad: need rünnakud on seisanud päevadeks ettevõtete tootmisliinid ning nende kaudu on kaotatud kogu ettevõtte digitaalne paberimajandus ühes klientide andmetega.

Isegi kui pahavara saadaks süsteemidest välja ja masinad uuesti tööle, võivad failid olla igaveseks kadunud. Siin ei tasu loota filmilikku ilusat lõppu, pigem ootavad ees suured kahjud ja halvemal juhul pankrot.

KAKS MILJONIT VÕI MUIDU...

2020. aasta detsembris sai kaugtööd võimaldava RDP-protokolli kaudu lunavararünnakuga pihta kaubandusettevõte, kelle töö rünnaku tagajärjel seiskus. Kurjategijad panid firma andmed – muu hulgas klientide nimekirja ja aruanded – CryLocki-nimelise pahavaraga lukku ning nõudsid nende vabastamise ja mitte müümise eest 100 Bitcoini. Toonases väärингus oli see ligi kaks miljonit eurot.

2021. aasta jaanuaris teatas IT-teenuseid pakkuv firma, et nad avastasid serverites lunavara, mis järjest andmeid krüpteeris. Ettevõtte IT-spetsialist suutis rünnaku peatada, kuid selleks ajaks olid pooled serverid juba krüpteeritud. Firma varundas oma andmeid regulaarselt ning nad said failid koopiatest taastada.

Ühel veebruaripäeval avastas hulgimüügiga tegeleva ettevõtte töötaja, et tal puudub ligipääs serveris töötavatele süsteemidele. Lähemal uurimisel selgus, et sealsed failid, e-posti server, varukoopiad jmt olid lunavaraga krüpteeritud ning kausta oli jäetud lunarahanõue. Ettevõte eraldas vanad süsteemid võrgust, puhastas seadmed ja paigaldas uuesti tarkvara. Selliste rünnakute vältimiseks muutsid nad töökorraldust ja paigaldasid uued turvalahendused.

Veebruari teises pooles tabas lunavararünnak Harjumaal tegutsevat hooldekodu, mille server krüpteeriti Phobose lunavaraga. Kolm päeva pärast rünnakut õnnestus hooldekodul süsteemid tööle saada. Meie teada tasus ettevõte lunavaranõude ning märtsi alguseks õnnestus neil kõik failid dekrüpteerida.

Märtsis teatas Tallinnas elektritöid pakkuv ettevõte, et kaugtöölaua protokolli ehk RDP kaudu pääsesid ründajad nende serverisse. Lunavara avastati, kui ühel töötajal ei avanenud Microsoft Office. Selgus, et nende andmed krüpteeriti Lockbiti lunavaraga. Ettevõte eemaldas



Kuidas end kaitsta?

Lunavaraga nakatumise ennetamiseks ja tagajärgede leevendamiseks on mõned lihtsad reeglid, mida järgida:

- kasuta viimast tarkvaraversiooni ning veendu, et kõik uuendused on paigaldatud,
- tee regulaarselt varukoopiad,
- piira süsteemi kasutajate õigusi,
- koolita personali küberohtude teemal.

Loe RIA kodulehelt, kuidas kaitsta ettevõtet lunavararünnakute eest:

võrgust servereid ja alustas seadmete puhastamist. Osa andmetest oli varundatud kolm kuud tagasi, mistõttu polnud võimalik kõiki andmeid taastada.

Aprillis teatas äritarkvara pakkuv ettevõte, et nad said RDP kaudu lunavararünnakuga pihta ning selle tulemusena võisid nakatuda ka neli nende klienti sama pahavaraga. Rünnak viidi läbi Lockbiti lunavara uuema versiooniga ning sellega krüpteeriti ettevõtte failiservereid ja virtuaalserverid.

Juulis saime teate, et IT-teenust pakkuva ettevõtte kaudu tabas kohtutäituri seadet lunavararünnak ja kurjategijad nõudsid kohtutäiturilt raha. Meile teadaolevalt ei jõutud krüpteerida tagavarakoopiaid.

Novembris teatas lunavararünnakust tööstusettevõte. Pahavaraga krüpteeriti failide hoidmiseks mõeldud server, kus oli ka ettevõtte raamatupidamistarkvara. Esialgse info põhjal krüpteeriti ka tagavarakoopiad.

Need näited on vaid osa CERT-EE-le teada antud lunavararünnakutest.

KURJATEGIJATELE MAKSTA EI TASU

Maksmine annab kurjategijatele indu juurde. Seda raha kasutatakse pahavarade ja kuritegevuse edasiarendamiseks: see tähendab, et rünnakud muutuvad veel ohtlikumaks ja lunarahanõuded suuremaks. Raha maksmine ei garanteeri andmete vabastamist ega tagastamist. On teada juhtumeid, kus pärast lunaraha maksmist paisati ohvri käest varastatud andmed müüki.

Kui langed lunavararünnaku ohvriks, teavita meid sellest aadressil cert@cert.ee. Saame nõustada, kuidas konkreetses olukorras kõige paremini toimida, kuidas tuvastada ründevektorit, ründajat, millist pahavara on kasutatud, kas andmeid on varastatud ning mida teha, et samalaadne intsident ei korduks. Paljud andmeid lukustavad lunavarad on nüüdseks juba lahti murtud. See tähendab, et on võimalik lukustatud andmed avada ilma, et peaks selleks kurjategijaid nuumama.

Kui langed lunavararünnaku ohvriks, teavita meid sellest aadressil cert@cert.ee.

Mida õppisime kohalikest valimistest?

Avalikkuses tekitasid pahameelt mõned funktsionaalsed apsakad, kuid ühtegi märkimisväärse mõjuga intsidenti me 2021. aasta kohalike valimiste ajal ei tuvastanud.

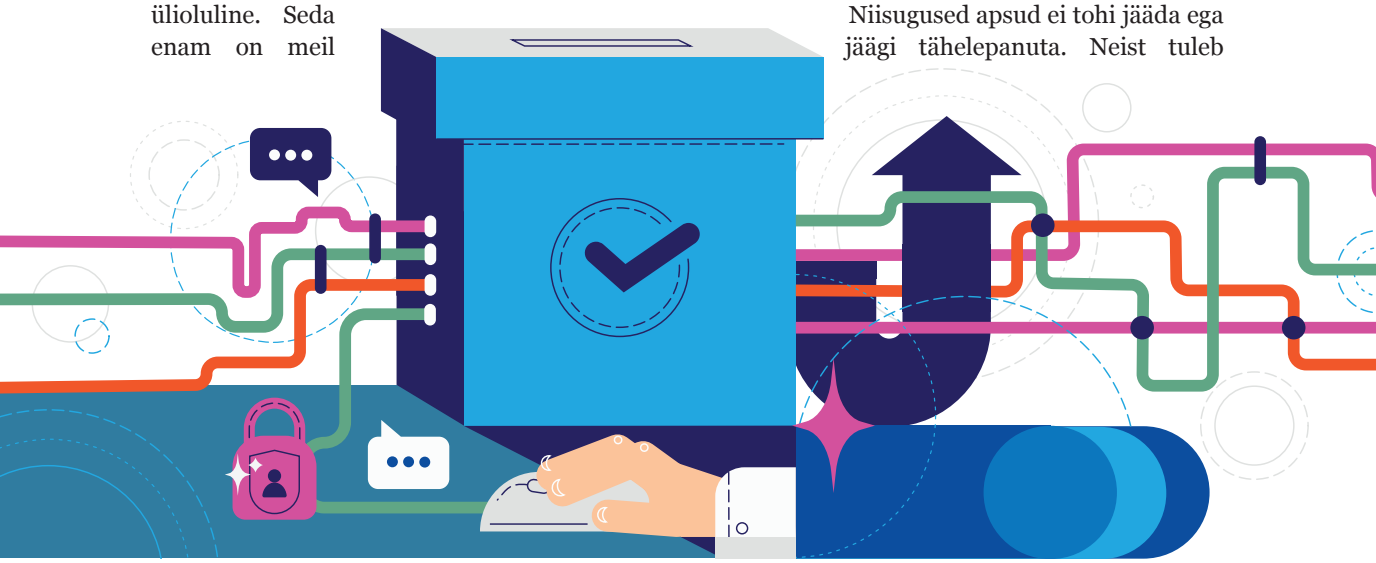
Riigi valimisteenistuse kõrval oli RIA-l kaks suuremat ülesannet: jooksutada valimiste jaoks vajalikke süsteeme (valimiste infosüsteem VIS3 ja e-häälte kogumiskast nimega Koguja) ning hoolitseda kogu valimiste küberturvalisuse eest.

Eesti on ainus riik maailmas, kus tänu e-riigi taristule on võimalik korraldada e-valimisi. Olukorras, kus ka kõik paberil antud ja käsitsi üle loetud hääled salvestatakse infosüsteemidesse ja edastatakse avalikkusele digitaalselt, on küberturvalisus ülioluline. Seda enam on meil hea meel raporteerida, et ühtegi märkimisväärse mõjuga intsidenti me valimiste ajal ei tuvastanud.

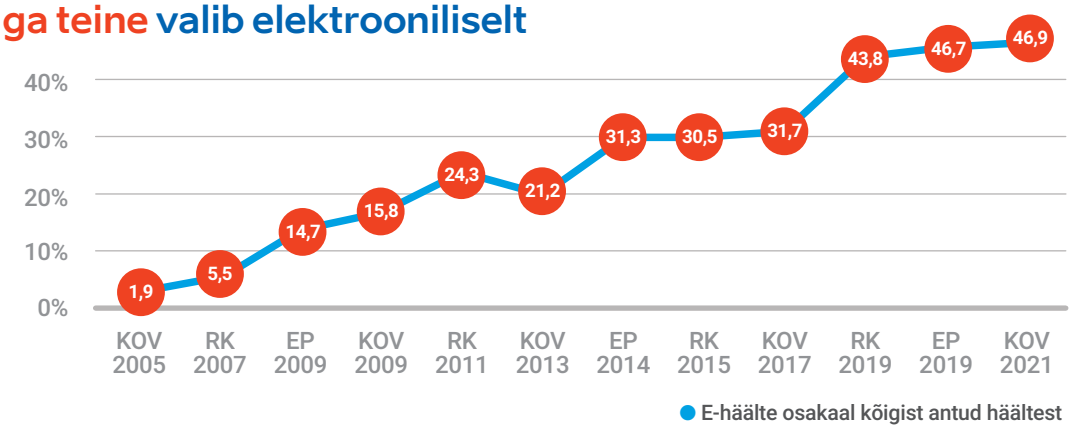
KÕIK POLNUD VEATU

Valimisnädala alguses tekitasid avalikkuses pahameelt mõned funktsionaalsed apsakad. Teatud MacOS versiooni kasutajatel ei teinud valijarakendus ID-kaardiga koostööd; e-hääletuse rakenduse dokumentatsioonis leidus apse; avalikkus taasavastas, et populaarse Smart-ID-ga pole võimalik e-häält anda.

Niisugused apsud ei tohi jääda ega jäägi tähelepanuta. Neist tuleb



Iga teine valib elektrooniliselt



õppida ja võtta arvesse järgmiste valimiste eel. Valimistulemustest selgus, et e-valimiste mainele ja usaldusväärsusele need sügavat jälge ei jätnud: e-hääletus tegi järjekordse rekordi nii e-häälte osakaalu kui ka üldarvu poolest.

Ühestki valimistega seotud intsidendist polnud näha viiteid pahatahtlikule tegevusele, samuti polnud neil mõju häälte konfidentsiaalsusele ega süsteemi või andmete terviklusele. Vaid valimisnädala laupäeval tekkis suurem tõrge, kui liiga kangeks keeratud teenusetõkestusrünnaku kaitse tõttu ei saanud jaoskondade töötajad umbes poole tunni jooksul VIS3-le ligi. Kuid ka siis jätkus hääletamine ning valijad registreeriti infosüsteemis tagantjärele.

TURVALISUS OLI FOOKUSES

Kunagi varem pole me pööranud valimiste turvalisusele nii palju tähelepanu kui 2021. aastal. Turvatestimised, riskianalüüsid, ohuhinnangud ja teadlikkuse tõstmine kõikvõimalikel tasanditel pani küberturvalisuse küsimuse valimiste fookusesse. Tegime koostööd erakondadega, teiste riigiasutustega, valimisjaoskondade töötajatega ja rahvusvaheliste partneritega, et valmistuda potentsiaalseteks riskistsenaariumiteks.

Järgmised, riigikogu valimised toimuvad 2023. aasta kevadel. Me juba hakkame sättima. 2021. aasta sügisestest valimistest on meil olemas järjekordne kogemus vajalikest tegevustest, et järgmist kokkuvõtet tehes saaksime taas kord öelda: ühtegi märkimisväärse mõjuga intsidenti valimiste ajal me ei tuvastanud.

RIA tegevused 2021. aasta KOV valimistel

Riigi valimisteenistuse (RVT) ülesandeks on valimiste (sealhulgas e-hääletuse toimimine ja valimiste infosüsteemi kasutus) üldine korraldamine. RIA on koostöölepingu alusel RVT partner.

RIA majutas e-häälte kogumislahendust Koguja, arendas koos arenduspartneritega RVT tellimusel järgmist versiooni valimiste infosüsteemist VIS3, pakkus kliendituge ja korraldas küberturvalisuse tegevusi:

- tehniliste lahenduste turvatestimise korraldamine ja koordineerimine,
- riskianalüüside ja ohupildi koordineerimine,
- küberhügieeni koolitused VIS3 kasutajatele,
- küberhügieeni Digitesti pakkumine valimisjaoskondade töötajatele,
- tööjaamade vahendamine valimisjaoskondadele ning nende seire (koostöös RIKiga),
- erakondadele meili- ja veebiserverite turvalisuse ülevaade,
- tehnoloogia ja küberturvalisuse tiimide 24/7 valmisolek valimisnädalal,
- valimisnädalal ülejäänud Eesti küberruumi jälgimine kõrgendatud valmisolekus.

Lisaks aitasime RVT-l korraldada e-hääletuse teavituskampaaniat „Lase oma e-häälel kõlada!“, mis keskendus uue e-hääletuse perioodi ning olemasolevate turvalisuse meetmete teadlikkusele.



Häkkerid, tulge riigile appi!

RIA eksperdid töötavad mudeli kallal, mis võimaldaks riigiasutusel teha koostööd häkkeritega ning maksta neile turvanõrkuse info eest tasu. Eelmisel suvel jäi üks sarnane koostöö pooleli ning esialgu lubatud preemia välja maksmata.

Bug bounty nime kandev koostöövorm (maakeeli puugipreemiajaht) on levinud paljudes riikides, sh USAs, Prantsusmaal, Suurbritannias ja naaberriigis Soomes. Selle eesmärk on teha koostööd sõltumatute ekspertidega, kes otsivad teenustest võimalikke nõrkusi ning edastavad selle info teenuse haldajale, kes maksavad nõrkuse tuvastamise eest honorari. USA ekspertide väljatöötatud mudel on eeskujuks RIA sarnasele süsteemile. Esimese õnnestunud lepinguni loodame jõuda selle aasta kevadel.

ESIMENE ÕPPETUND

Vaatamata poolikule süsteemile soovis RIA tasuda häkkerile honorari juba läinud aasta augustis, kui asutuse üldmeilile laekus info võimalikust turvanõrkusest riiklikes e-teenustes, sealhulgas

RIA hallatavas riigiportaalis eesti.ee. RIA eksperdid kontrollisid saadud infot ning tuvastasid kaks võimalikku nõrkust registrite ja infosüsteemide keskuse (RIK) e-teenustes (e-kinnistusraamatus ja abieluvararegistris) ning edastasid selle info koos teataja saadetud materjalidega RIKi spetsialistidele. RIKi töötajad kinnitasid turvanõrkuste olemasolu ning kõrvaldasid need. Riigiportaalis eesti.ee turvanõrkust ei tuvastatud.

RIKi teenuste nõrkus seisnes selles, et kinnistusregistrist ja abieluvararegistrist oli võimalik kätte saada infot ilma end vastavas teenuses autentimata. Ühegi inimese andmete kuritarvitamisest teatatud ei ole. Nende nõrkuste teataja pidi olema esimene, kellele RIA oli valmis tasuma honorari. Esimene väljamakse pidi jääma 3000–4000 euro vahele. Kuigi kogu süsteemi väljatöötamine oli alles algusjärgus ning seda toetavad õiguslikud alused kirjeldamata ja kinnitamata, proovisime siiski leida võimalusi honorari maksta. Selle eelduseks olid aga mõned tingimused.

Üheks tingimuseks oli see, et turvanõrkus pidi olema kriitilises teenuses ning selle avastamiseks ei ole kasutatud ega laaditud alla rohkem andmeid, kui on nõrkuse dokumenteerimiseks otstarbekas. Samuti eeldab selline koostöövorm konfidentsiaalsust mõlemalt osapoolelt – reeglina tuleb leidjal hoiduda kommentaaridest järgneva 90 päeva jooksul, et teenuste omanikud jõuaksid turvanõrkused üle kontrollida, parandada ja teha täiendavaid analüüse. Kuna teataja rikkus kõiki eeltoodud tingimusi ning tekitas edasise käitumisega kahtlusi enda motiivides, otsustas RIA honorari mitte maksta. RIA asejuht tunnistab, et asutus saanuks olla selgem sõnumikandja.

RIA TÕSTAB VÕIMEKUST

2022. aasta veebruaris hakkas RIA küberintsidentide käsitlemise osakonnas (CERT-EE) eraldi üksusena tegutsema meeskond, kelle ülesandeks on testida asutuse teenuseid ning leida neist võimalikud nõrkused enne, kui nendeni jõuavad küberkurjategijad. Kui varasemalt kaasas RIA oma teenuste testimiseks erinevaid Eesti tipptegijaid, siis tänavu tugevdab asutus tagalat sellega, et kaasab lisaks välistesijatele enda eksperte. Esialgu töötab testijate tiim (õppustel reeglina RedTeamina tuntud üksus) RIA teenuste kallal. Tulevikus on plaanis laiendada meeskonna haaret nii palju, et pakkuda testimistuge ka teistele riigiasutustele.

Kuid turvalisuse tõstmiseks inimestest üksi ei piisa. Ka tehnikapark vajab pidevat täiendamist ja arendamist. Aasta alguses sai CERT-EE tiim enda käsutusse demoseadmed, et testida nende tööd riigivõrgus. Seadmete eesmärk on tõhustada riigivõrgu kaitset. Seega võib loota, et riigivõrgus olevate riigiasutuste ja kohalike omavalitsuste võrk on tulevikus oluliselt paremini turvatud. ●

Täna käituksime teisiti



GERT AUVÄÄRT
RIA peadirektori asetäitja

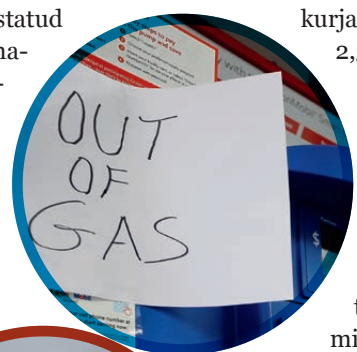
Riik üksi ei leia e-riigi kõiki kitsaskohti üles, seetõttu on koostöö kogukonnaga hädavajalik. RIA on teinud koostööd mitme teadlase ja eksperdiga, kelle kaasabil on lahendanud hulk suuremaid ja väiksemaid intsidente. Ka sel korral soovisime jõuda eduka koostöö tulemuseni ning maksta soovitud honorari. Kuid me ei saanud tormata lepingusse üleöö, sest sellised tehingud nõuavad terve rea tingimuste ja protseduuride täitmist, nagu info valideerimine, turvariskide kriitilisuse hindamine, logide analüüs jms. Selgitasime seda ka teatajale.

On asju, mida oleksime saanud teha teisiti. Sellist koostööd pole riik varem teinud, mistõttu kulges suhtlus kohati konarlikult ning oli hetki, kus pidime hoo maha võtma, et vaadata, kuidas sobivad kokku see, mida tahame teha, ning see, mida võimaldavad teha seadused. RIA oleks saanud selgemalt sõnastada, et tasu maksmine on võimalik ainult siis, kui kõik kokkulepitud tingimused on täidetud. Oleme järgmisel korral targemad ning loodame *bug bounty* esimese lepingu sõlmida selle aasta kevadel.

Mis toimus rahvusvahelises küberruumis 2021. aastal?

Eelmisel aastal kuulsid küberintsidentidest ja -turvalisusest ka need, kes varem polnud nende teemadega kokku puutunud. Paljud juhtumid häirisid otseselt ja suurelt inimeste igapäevaelu ning ületasid uudiskünnise.

Mööndunud aasta üks enim kajastatud küberintsidentidest oli lunavararünnak USA energiaettevõtte **Colonial Pipeline** vastu. Ettevõtte ligi 9000 kilomeetri pikkuse torujuhtme kaudu liigub ligi pool kogu USA idarannikul kasutatavast kütusest. Rünnaku tagajärjel peatati torujuhtme töö peaaegu nädalaks, mistõttu seisid mitu osariiki silmitsi kütusepuudusega. Süsteemide taastamiseks maksis Colonial Pipeline ründajatele – Venemaal tegutsevale küberrühmitusele Darkside – 75 Bitcoini, toonases vääringus 4,4 miljonit dollarit. Ehkki krüptoraha jälitamine on äärmiselt keerukas, õnnestus USA föderaalsel juurdlusbürool (FBI) kurjategijatele makstud rahast 2,3 miljonit dollarit tagasi saada.





Colonial Pipeline polnud ainus ettevõte, mis ründajatele lunaraha maksis. Seda tegi ka maailma suurim lihatöötleja **JBS**, mida tabas lunavararünnak, mille taga Venemaal tegutsev rühmitus REvil. Ettevõte maksis rühmitusele dekrüpteerimisvõtme eest 11 miljonit eurot, et vältida potentsiaalset kahju restoranidele, toidupoodidele ja talunikele.

Kuid oli ka neid, kes ei maksnud. Mais sai lunavaraga pihta Iirimaa tervishoiusüsteem, kuhu kurjategijad süstisid Conti lunavara. Krüpteeritud süsteemide tõttu oli takistatud juurde-



pääs diagnostikale ja meditsiinilistele dokumentidele. Lisaks varastasid ja avalikustasid ründajad patsientide tundlikke andmeid. Süsteem õnnestus peaaegu täielikult taastada alles mitu kuud hiljem septembris.

Paljude niivõrd tõsiste tagajärgedega lunavararünnakute tõttu hakati möödunud aastal küberturvalisuse ringkondades aina aktiivsemalt rääkima lunavara epideemiast. Sellele andis hoogu juulis tarkvarafirma **Kaseya** suunas tehtud lunavararünnak, mille taga oli Venemaal tegutsev rühmitus REvil. See mõjutas rohkem kui tuhandet ettevõtet 17 riigist, mis kasutasid Kaseya pilvepõhist lahendust IT-süsteemide kaughalduseks. Rünnaku üheks ohvriks oli Rootsi COOPi kauplusekett, mis pidi sulgema 800 kauplust, sest nende arveldussüsteem ei töötanud.





VENEMAA JA SOLARWINDS

Lisaks küberkurjategijatele oli tihe aasta ka küberluurajatel. Vahetult enne möödunud aasta algust ehk 2020. aasta detsembris sai teatavaks tarneahelarünnak USA ettevõtte **SolarWinds** pihta, mis pakub IT-halduse ja monitoorimistarkvara Orion. Ründe ja selle järelmite uurimise taktis kulges 2021. aasta esimene pool.

Aprillis omistasid USA ja liitlased (sh Eesti) SolarWindsi rünnaku Venemaa välisluure teenistuse SVR küberrühmitusele APT29 (tuntud ka kui Nobelium). Kompromiteeritud tarkvarauuenduste abil said nad ligi SolarWindsi tarkvara kasutavate asutuste ja ettevõtete süsteemidele. Ohvreid oli üle maailma 18 000, sealhulgas mitu USA ministeeriumit ja valitsusasutust, aga ka näiteks Taani keskpank. Venemaa eitab igasugust süüd.

HIINA JA MICROSOFT EXCHANGE

Maailm polnud SolarWindsi juhtumist jõudnud toibudagi, kui juba avastati teine suure mõjuga intsident. Nimelt teatas märtsi alguses **Microsoft**, et tuvastas ja parandas oma meili-

serveritarkvaras Exchange Server neli nullpäeva haavatavust, mille kaudu olid ründajad pääsenud ligi serverites olevatele e-kirjadele, salasõnadele ja administraatori õigustele.

Kohe kerkis ka kahtlus, et ründe taga on luurajad. Suvel esitasidki USA ja selle liitlased (sh Eesti) ametliku süüdistuse Hiina Rahvavabariigi suunal mitme küberrünnaku tõttu, sealhulgas ka Microsoft Exchange'i kompromiteerimise eest (rühmitus Hafnium). Hiina valitsusega seotud häkkerid olevat viinud läbi ka mitmeid lunavararünnakuid ja teisi küberoperatsioone mitte ainult luure eesmärgil, vaid ka raha teenimiseks. Hiina eitab süüd.





Pärast lääneriikide ühist avaldust teatas Prantsuse küberamet (ANSSI), et mitmed Prantsuse organisatsioonid on Hiina riiklike sidemetega küberrühmituse APT31 rünnaku all. APT31 on oma tegevuses keskendunud küberspionaažile, andes infot Hiina valitsusele ja riigiettevõtetele, et saavutada poliitilist, majanduslikku ja sõjalist edumaad. Märkimist väärib ka see, et küberturvalisuse ettevõte Positive Technologies teatas, et APT31 sihtmärgiks oli esimest korda ka Venemaa.

VENEMAA JA GHOSTWRITER

Euroopas tekitas pingeid ka **Ghostwriteri**-nimeline küberohustaja, mis on mitme riigi hinnangul seotud Venemaa sõjaväeluurega (GRU). Küberturbeettevõtte Mandiant teatel on Ghoswriteri taga Valgevene. Juunis olid Ghostwriteri sihtmärgiks Poola poliitikud ja ametiasutused. Ründajad pääsesid ligi peaministri büroojuhi ja teiste valitsusliikmete isiklikele Gmaili kontodele. Osa varastatud e-kirjadest lekitati.

Sügisel teatas Saksamaa, et Ghostwriter proovib varastada nende parlamendiliikmete andmeid. Nimelt olevat Ghostwriter juba kuid proovinud õngitsuskirjade abil pääseda ligi Bundestagi ja Landtagi liikmetele, sihtmärgiks põhiliselt Kristlik-Demokraatlik Liit (CDC) ja Sotsiaaldemokraatlik Partei (SPD).

Peagi esitas ametliku süüdistuse Venemaa aadressil ka Euroopa Liit. Venemaad süüdistati pahatahtlikus kübertegevuses, millega sekkutakse ELi liikmesriikide valimistesse ja poliitikasse. ELi teatel ründas Venemaa Ghostwriteri-nimelise kampaaniaga liikmesriikide parlamente, ametnikke, poliitikuid, ajakirjanikke ja tsiviilisikuid. Häkkerid tungisid sisse sihtmärkide arvutisüsteemidesse ja isiklikesse kontodesse ning varastasid andmeid, eesmärgiks desinformatsiooni levitamine ja infoga manipuleerimine.

VALGEVENE AKTIVISTIDEST HÄKKERID

Ent poliitilised tõmbetuuled väljendusid küberruumis ka teisel moel. Näiteks teatasid Valgevene kohaliku protestiliikumise häkkerid (**Cyber Partisans**) oma Telegrami kanalil, et nad pääsesid ligi Valgevene riiklikele andmebaasidele. Oma sõnul said nad infosüsteemist Pass enda käsutusse Valgevene inimeste nimed, passinumbrid, töökohad, vanemate nimed jm. Nende seas olid ka KGB töötajad ja informaatorid. Häkkerid võitlevad Valgevene praeguse režiimi vastu. Mullu avaldas rühmitus oma Telegrami kanalil ka plaani, milles lubati „momendil X" palju tegevusi „fašistliku režiimi" kõrvaldamiseks. End apoliitiliseks nimetav rühmitus soovib uusi, vabasid ja demokraatlikke valimisi.

OHTRALT ANDMELEKKEID

Andmeleketega pidid rinda pistma paljud organisatsioonid nii avalikust kui ka erasektorist. Näiteks pääsesid häkkerid ligi maailma ühe suurima veebimajutaja ja domeenide registreerija **GoDaddy** võrku. Nii lekkis 1,2 miljoni GoDaddy kliendi e-posti aadress ja kliendinumber. E-posti aadressi lekkimine soodustab õngitsusrünnete tegemist. Lekkis ka hulgaliselt inimeste terviseandmeid.

Näiteks teatas andmelekkest USAs Utah' osariigis asuv radioloogiakeskus (**UIA**). Avalikuks sai 582 170 inimese isiklik info: patsientide ees- ja perekonnanimi, e-posti aadress, sünnikuupäev, isikukood, tervisekindlustuse poliisi number, meditsiiniline info (diagnoosid, ravi, retseptid).

Häkkerid viisid endaga kaasa ka teisi tundlikke andmeid. Näiteks ilmusid veebifoorumisse müüki Leedu välisministeeriumi e-kirjad. Samuti said häkkerid ligi USA kaitsetööstuse ettevõtte **Electronic Warfare Associates** (EWA) meilisüsteemile. Seda, kas ründajad pääsesid ligi ka konfidentsiaalsetele tehnilistele dokumentidele, ettevõte ei avalikustanud.

VAHISTATI KÜBERKURITEGUDES KAHTLUSTATAVAD

Möödunud aastal oli õiguskaitseorganitel küberrindel mitu õnnestumist. Peagi pärast Colonial Pipeline'i ründamist lõpetas tegevuse lunavararühmitus **Darkside**. Sügisel panid USA võimud välja 10 miljonit dollarit info eest, mis viib Darkside'i liikmeteni.

Sügisel teatas USA justiitsministeerium, et lunavararühmituse **REvil**i kaks liiget on arreteeritud ja neile süüdistus esitatud. Üks neist oli Poolas vahistatud Ukraina kodanik Jaroslav Vasinskyi, kes olevat ka Kaseyat tabanud lunavararünnaku taga. Teine vahistatu oli Vene kodanik Jevgeni Poljanin, kellele laekunud 6,1 miljonit dollarit lunaraha võimud konfiskeerisid.

Arreteerimisi oli veel. Muuhulgas viis näiteks Interpol läbi rahvusvahelise operatsiooni, mille tulemusel arreteeriti 1003 isikut, kes on kahtlustuse kohaselt seotud paljude küberkuritegudega. Näiteks armupettustega, investeerimiskelmustega, rahapesu ja ebaseaduslike hasartmängudega. Võimud külmutasid 2350 pangakontot ja üle 27 miljoni dollari. Juunist septembrini läbi viidud operatsioonis osales 20 riigi politsei (nt Hiina, India, Rumeenia, Sloveenia, Angola, Kolumbia).

Suvel tekkis uus lunavararühmitus **BlackMatter**, ent juba sügisel teatas seegi, et lõpetab





võimude ja õiguskaitseorganite surve tõttu tegevuse. Ehkki küberkuritegevus vohab endiselt, võib neid arreteerimisi pidada siiski olulisteks töövõitudeks. ●

Noppeid üle ilma

- Detsembris avastati Java programmeerimiskeele logimisfunktsioonis **Log4j** kriitiline turvanõrkus, mis mõjutab miljoneid seadmeid üle maailma. Loe lähemalt lk 20.
- Juulis tunnistas Eesti kodanik **Pavel Tsurkan** end USAs Alaska kohtus süüdi arvutikuritegude toimepanemises. Tsurkan haldas robotvõrgustikku ehk botnetti „Russian 2015", milles oli üle tuhande kompromiteeritud arvuti ja ruuteri.
- Oktoobris kutsus insuliinipumpade tootja **Medtronic** küberohu tõttu tagasi osade oma insuliinipumpade kaugjuhtimiseks mõeldud puldid. Turvanõrkust ära kasutades saaks pulti kaugelt kontrollida, nt alustada või peatada insuliini pumpamist või muuta pumbatavat kogust.
- Vene tehnoloogiahiiglane **Yandex** teatas, et augustis ja septembris nende pihta tehtud teenusetõkestusrünnak (DDoS) oli ajaloo võimsaim. Rekordhetkel tehti 22 miljonit päringut sekundis.
- Iisraeli ettevõte **NSO** aitas oma klientidel luurata ajakirjanike, poliitikute ja aktivistide järele. Selleks kasutati NSO loodud Pegasuse tarkvara, millega nakatudes saab käivitada sihtmärgi telefoni kaamera ja mikrofoni, samuti pääseb ligi sõnumitele, fotodele, e-kirjadele ja saab salvestada kõnesid.

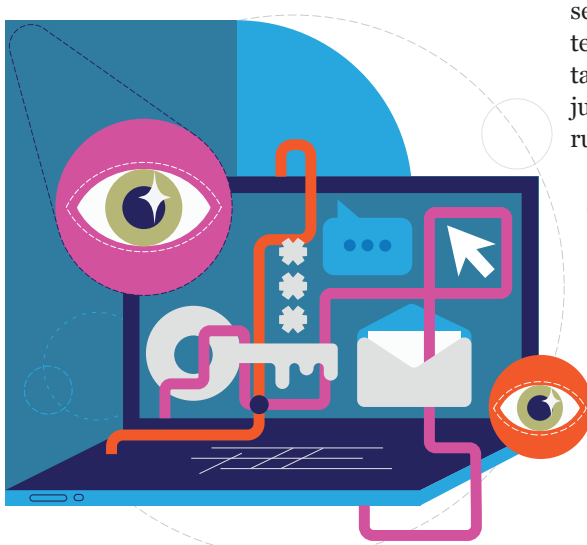
Õnneliku lõpuga intsidendid

Küberturvalisusest rääkides on sageli fookuses olulise mõjuga intsidendid ja nende põhjustatud kahju: olgu selleks varastatud andmed, krüpteeritud süsteemid või rahakaotus. Halbade juhtumite varju jääb aga ka õnnelikuma lõpuga lugusid.

Need on juhtumid, kus inimeste küberteadlikkus ja tehnilised meetmed on aidanud ära hoida suurema kahju. „Lohutuseks“ ja motiveerimiseks tasub suunata pilk ka õnnestumistele.

TÄHELEPANELIKKUS TOOB EDU

Suvel prooviti ühelt elektriettevõttelt arvepettuse teel välja petta miljoneid eurosid. Nimelt õnnestus kurjategijatel (tõenäoliselt koostööpartneri meilisüsteemi kompromiteerimise tõttu) hakata jälgima ettevõtte kirjavahetust välismaal asuva koostööpartneriga. Kui meilivahetus jõudis arvete saatmise ja tasumiseni, võtsid petturid kirjavahetuse üle ning hakkasid edastama libaarveid. Õnneks saadi ettevõtte meilifiltrisüsteemi abil pettusele jälile. Ehkki postkasti kompromiteerimine ja selle kaudu meilivahetuse jälgimine on juba tõsine konfidentsiaalsuse rikkumine, õnnestus suur rahaline kahju ikkagi ära hoida.



Sama hästi ei läinud kahjuks mõnel teisel ettevõttel. Mitmel korral õnnestus petturitel kirjavahetust jälgida ja „õigel“ ajal sekkuda ning arvetel arvelduskonto numbrit muuta. Kusjuures alati ei pruugi arveid vahetanud osapooled sellest kohe aru saada, et nendevahelisse suhtlusesse on sekkunud keegi kolmas. See teadmine jõuab kohale pahatihti alles siis, kui tasu ootaja arve tasumisele uuesti tähelepanu juhib. Ent kui raha on juba üle kantud, on keeruline seda tagasi saada.

Seega on oluline olla teadlik niisuguse pettuse ohust ning enne arveldamist alati veenduda andmete õigsuses. Nagu näha, võib nii säästa miljoneid eurosid.

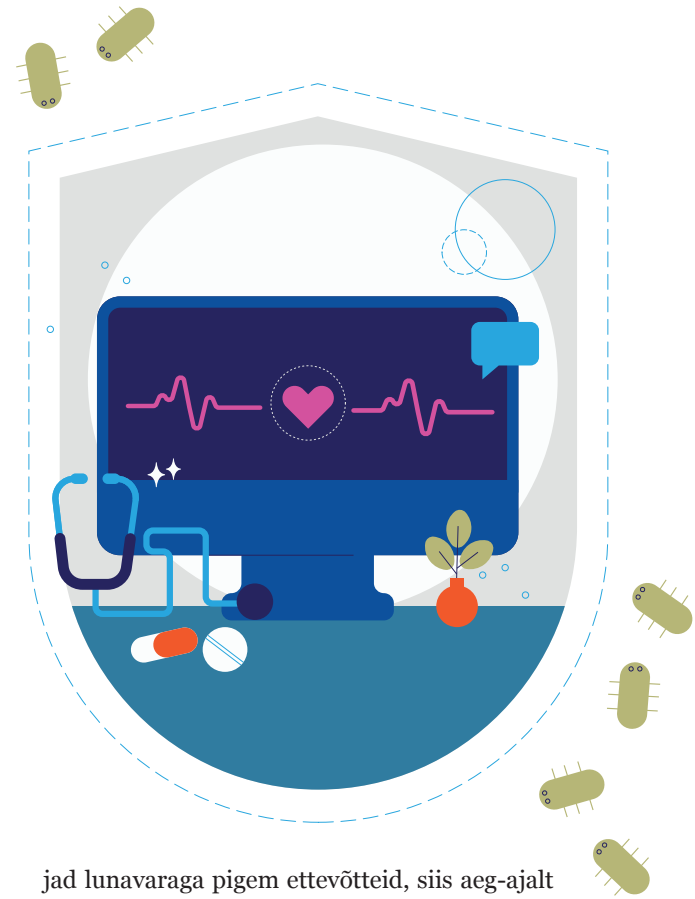
MÕJUTA UMMISTUSRÜNDED

Tähelepanelikkus on alati omal kohal, kuid sageli aitavad suurema kahju vastu tõhusad ja õigesti seadistatud süsteemid. Eelmisel aastal nägime tihti, kuidas

ummistusrünnete (DDoS) puhul aitasid automaatsed kaitsemehhanismid, nt DDoS-kaitse või tulemüür. Automaatne kaitse aitas tõhusalt tõrjuda ummistusründeid riigiportaali eesti.ee ja mitme avaliku sektori asutuse vastu.

Ummistusründe puhul n-ö ujutatakse süsteem või veebileht päringutega üle, nii et see muutub töövõimetuks. Kui kaitset poleks olnud ja ründed oleksid õnnestunud, olnuks veebilehtede töö tavapärasest oluliselt aeglasem või katkenuks sootuks.

Avaliku sektori asutustel tasub kaaluda liitumist riigivõrguga, mis pakub kõikidele klientidele DDoS-kaitset.



VARUKOOPIA AITAB

Absoluutset kaitset lunavararünnakute eest pole kellelgi. Küll aga saavad inimesed, asutused ja ettevõtted teha midagi selleks, et pihta saamine võimalikult valutult mööduks. See tähendab, et andmed peavad olema hajutatud, varundatud ja taastatavad. Nii et kui süsteemid on lunavaraga krüpteeritud, siis kurjategijatele maksmise asemel oleks võimalik dokumendid ja failid varukoopialt kätte saada.

Näiteks teatas üks ettevõte, et lunavara tabas nende raamatupidaja arvutit, kust liikus edasi teistesse arvutitesse. Ühtekokku krüpteeriti andmed kuues seadmes. Varukoopiast õnnestus andmed taastada. Sarnaseid lugusid on palju – tänu varukoopiale säästeti aega ja raha.

Mõistagi on edulugude kõrval ka omajagu õnnetuid näiteid. Kui üldiselt sihivad kurjategijad lunavaraga pigem ettevõtteid, siis aeg-ajalt saavad pihta ka eraisikud. Näiteks andis üks video- ja fototöötlusega tegelev inimene teada, et kaks tema kõvaketast on krüpteeritud. Paraku polnud tema materjale varundanud.

> Tähelepanelikkus on alati omal kohal, kuid sageli aitavad suurema kahju vastu tõhusad ja õigesti seadistatud süsteemid.

Kuna lunavara püüab krüpteerida faile nii kohalikul kettal, välistel andmekandjatel kui ka võrguketastel, peab varukoopia asuma eraldi, muidu võib seegi „lukku“ minna. Üht varukoopiat tasub hoida *offline*-režiimis.

TEADLIKKUS ON VÕTI

Kaitsemeetmete ja teadlike arvutikasutajate abil ära hoitud kahju on keeruline hinnata ja arvutada. Pole teada, kui paljudel pahatahtlikel linkidel on keegi jätnud klõpsamata või mitmele õngitsuslehele andmed sisestamata. Võib aga kindel olla, et suurem teadlikkus küberruumis varitsevatest ohtudest ja võimekus nendega toime tulla aitab edulugusid juurde tuua.

Küberhügieen paraneb

Eesti elanike küberhügieeni tase on kolme aastaga paranenud, kuid arenguruumi jagub, selgub koostöös statistikaametiga kogutud andmetest.

2019. aastal väitis 64 protsenti vastanutest, et nad kasutavad miinimumnõuetest tugevamaid paroole või eri paroole eri kohtades. 2021. aastal oli samamoodi vastanuid juba 69 protsenti, seejuures oli suurim tõus vanuserühmas 65–74, kus see näitaja kerkis 33 protsendilt 42 protsendi peale.

PALJUD RÜNNAKUD ALGAVAD NÕRGAST SALASÕNAST

Uuringu tulemused on meie jaoks rõõmustavad eelkõige selle tõttu, et oma teavituskampaaniates, avalikes sõnumites ja ennetustegevustes oleme pööranud väga palju tähelepanu paroolidele ja mitmeastmelisele autentimisele. Just korduvkasutatavad ja nõrgad salasõnad ning mitmeastmelise autentimise puudumine annab ründajatele esialgse ligipääsu seadmetele ja süsteemidele.

Vastajate hulk, kes on teinud oma paroole tugevamaks, on kolme aastaga kasvanud kõikides vanuserühmades. Noorte hulgas oli baastase juba kõrge (82,5 protsenti 16–24-aastastest nimetas seda varianti 2019. aastal ja 87,1 protsenti 2021. aastal), kuid tase tõusis märgatavalt ka vanemaealiste hulgas (55–64-aastastel tõusis 47,2 protsendilt 2019. aastal 54,5 protsendile 2019. aastal, 65–74-aastaste hulgas 33,1 protsendilt 42,1 protsendile).

2019. aastal korraldasime teavituskampaania vanemaealistele internetikasutajatele, et rõhutada küberhügieeni olulisust. Selle ja 2020. aastal venekeelsetele elanikele suunatud jätkukampaania mõju hakkamegi küsitlustulemustes nägema alles nüüd.

EAKATE TEADLIKKUS ON ENDISELT MADAL

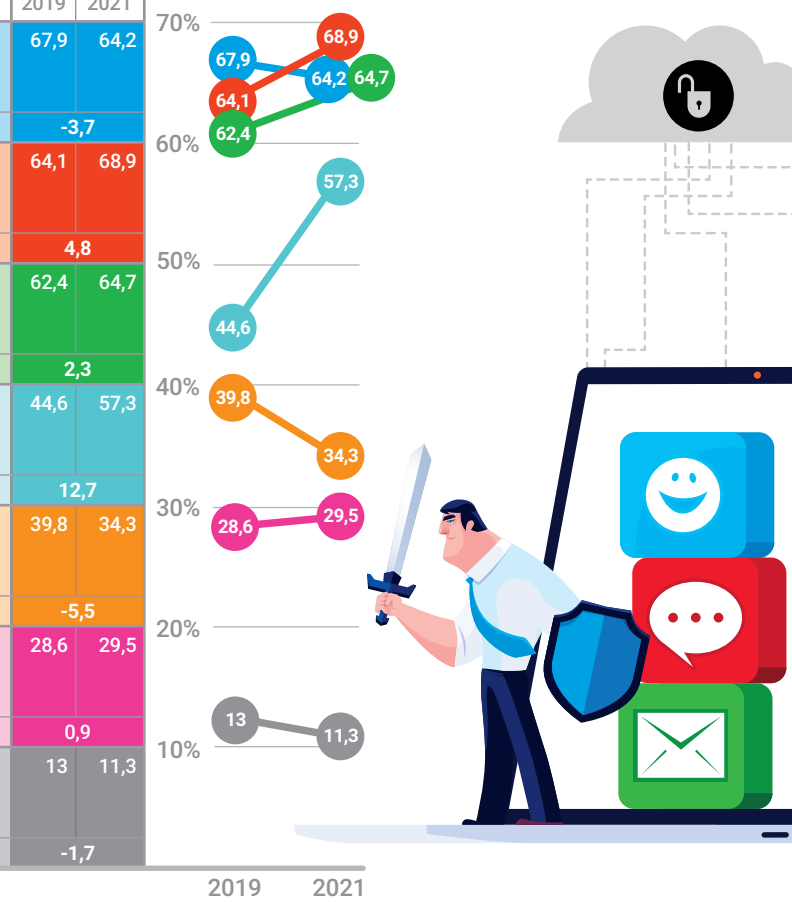
Jätkuvalt on vanemaealiste küberhügieen selgelt madalam kui noorematel. Küll aga teeb head meelt, et nende vastajate hulk, kes ütlesid, et nad ei tee ühtegi pakutud tegevustest, on langenud 13 protsendilt 11,3 protsendile. Seda langust on just vedanud vastajad vanuses 45+.

Mõnes valdkonnas näeme liikumist ka teises suunas. Võrreldes 2019. aastaga vastas enam kui 5 protsenti vähem inimesi, et nad teevad enne uue seadme, äpi või teenuse kasutamist sellele taustauuringu, 3 protsenti vähem ütles, et nad kasutavad turvalisuse programme või äppe. Kas või kuidas võivad need teemad mõjutada Eesti inimeste küberturvalisust, alles selgub.

Üks väga selge tegur, mis mõjutas küberhügieeni taset, oli vastajate rahvus. Muust rahvusest Eesti elanikud nimetasid oluliselt vähem tegevusi, mida nad enda turvalisuse nimel teevad. Kui paroolide tugevdamist nimetas 72 protsenti eestlastest, siis muu rahvuse esindajatest vaid 61 protsenti. Kahtlastel linkidel klikkimise puhul olid tulemused vastavalt 68 ja 55 protsenti. Tõsi, ka muust rahvusest vastajate küberhügieen on kolme aastaga paranenud peaaegu kõigis valdkondades.

KÜSIMUS: mida olete internetis või äpis isiklikul eesmärgil teinud turvalisuse või privaatsuse tagamiseks?

	2019	2021
Turvalisuse programmide või äppide kasutamine (nt viirusetõrje, nuhkvaratõrje, tulemüür)	67,9	64,2
Muutus	-3,7	
Paroolide tugevamaks tegemine või eri paroolide kasutamine (sh miinimum-nõuetest pikemad ja keerulisemad paroolid, regulaarne muutmine vms)	64,1	68,9
Muutus	4,8	
Ootamatutes või tundmatult saatjalt saadud kirjades ja sõnumites linkide ja manuste üle kontrollimine enne nende avamist	62,4	64,7
Muutus	2,3	
Võõra arvuti või nutiseadmega interneti kasutamise vältimine	44,6	57,3
Muutus	12,7	
Ettevõtte/teenusepakkuja tausta põhjalik uurimine internetis, enne nende uue seadme/äpi/teenuse kasutamist/tellimist (nt e-pood, taksoäpp)	39,8	34,3
Muutus	-5,5	
Internetibrauseri/sotsiaalvõrgustiku/äppide turvasätete muutmine	28,6	29,5
Muutus	0,9	
Ei ole teinud ühtegi neist	13	11,3
Muutus	-1,7	



Allikas: statistikaamet

Mida teeb RIA ühiskonna küberhügieeni tõstmiseks?

Avaliku sektori ja kriitilise taristu küberturvalisuse kõrval võtsime 2018. aasta riikliku küberturvalisuse strateegiaga RIA-le veel laiema eesmärgi: et Eesti inimesed oleksid järjest küberoskuslikumad.

Valitsuses heaks kiidetud strateegias oli selle jaoks sõnastatud ka meetod: „Laiemale ühiskonnale on vaja järjepidevalt teadvustada valitsevaid riske, jagada nõuandeid riskide maandamiseks ja rõhutada, et küberturvalisusalaste teadmiste ja oskuste arendamine on kõigi küberruumis tegutsejate ühine vastutus. /--/ RIA võtab küberturvalisuse seaduse jõustumise järel keskse rolli küberhügieeni, riiklike ennetustegevuste ning ühiskondliku teadlikkuse kasvatamisel. Sarnaselt PPA ja päästeametiga korraldatakse mahukad ennetus- ja teadlikkuskampaaniad küberohtude teadvustamiseks erinevatele sihtrühmadele, sealjuures ettevõtjatele."

Aasta hiljem korraldasime esimese üleriigilise kampaania „Ole IT-vaatlik!" vanemaealistele elanikele, seejärel pandeemia alguses jätkukampaania, 2020. aasta sügisel IT-vaatliku teavituskampaania ettevõtetele ja erinevaid lisanduvaid teavitustegevusi vene keelt kõnelevale elanikkonnale. Ka tänavu on plaanis teavitustegevused.

Kampaaniate ja teavituste puhul on alati keskne küsimus, kuidas mõõta nende mõju. Iga kampaania järel mõõdetakse muidugi üle, mitu silmapaari nägi telereklaami ja mitu klikki tuli sotsiaalmeedias. Kuid küberhügieeni taseme mõõtmiseks otsustasime 2018. aastal hakata koostööd tegema statistikaametiga, kes igal kevadel viib Eesti elanike hulgas läbi küsitluse „Infotehnoloogia leibkonnas".

Mida toob 2022. aasta küberruumis?

Eelmine aasta tõi meile kuhjaga turvanõrkuseid ja lunavara-epideemia. Millega ähvardab 2022?

Turvanõrkuste aasta saab järje

Eespool nimetasime 2021. aastat turvanõrkuste aastaks. See pikeneb aastasse 2022, täpselt nagu COVID mõjutab juba kolmandat aastat järjest meie elusid. Detsembris 2021 maailma vallutanud Log4j põhjustatud probleeme tuleb välja kogu aasta vältel. Tuleb teateid uutest suurtest, Exchange'i või Confluence'i haavatavustega võrreldavatest nõrkustest.

Kui vaadata ringi kodumaiste prillidega, peab olema valmis järgmisteks taakvarast põhjustatud intsidentideks, mis võivad lõppeda veelgi tõsisemate tagajärgedega kui suvel 2021 RIAs või sügisel 2020 majandus- ja kommunikatsiooniministeeriumi haldusalas aset leidnud juhtumid. Probleeme jäävad tekitama nn *anti-patcher*'id – turvajuhid või administraatorid, kes ei uuenda oma asutuses kasutatavat tarkvara, kui selles on avastatud haavatavused ja tootja on need paiganud. Selliseid leidub kahjuks nii meie riigiasutuste kui elutähtsate ja oluliste teenuste osutajate palgal. Olgu siinkohal veel kord palutud: RIA-lt tulnud ohuteavitustele ning paikamisjuhistele tuleb reageerida viivitamatult! Pätid ei maga ja magada ei tohi ka kriitiliste infosüsteemide turvalisuse eest vastutajad.



Riiklike sidemetega toimijad (APT) muutuvad aina julgemaks

2020. aastal aset leidnud ning 2021. kevadel USA ja liitlaste poolt Venemaale omistatud SolarWindsi intsident, mille käigus õnnestus häkkeritel sisse murda mh USA jõuministeeriumitesse ja suurkorporatsioonidesse, ei jää suurimaks omasuguseks. On ainult aja küsimus, millal tugeva kübervõimekusega riikide juhtimisel või tellimusel tegutsevad rühmitused sarnase suurusega skalbi skoorivad. Olgu siin veel rõhutatud, et SolarWindsi nimetatakse Ühendriikides „IT Pearl Harbouriks". Kuni avastatakse uusi turvanõrkusi, mida samas paraku otsekohe ei paigata, on sarnase mõjuga ründevektori avastamine väga ja väga reaalne.



Lunavararünnakute arvukus ja kahju maailmas kasvavad

Lunavarast põhjustatud väga mastaapseid intsidente on aasta-aastalt aina rohkem ning kasvasid ka nende põhjustatud kahjud. Kui ikka USA idarannikul päevade kaupa bensiini või Rootsis Coopist toidukaupu osta ei saa või kui töö lõpetavad liri haigekassa IT-süsteemid, on asi selgelt enam kui tõsine. Eesti on seni suurmatest paukudest pääsenud, abiks nii meie väike keel kui ka tõik, et Eesti ettevõtted ei ole oma sektoris maailma suurimad ja rikkaimad. Arvatavasti jätkub Eestis lähemas tulevikus senine stabiilne olukord, mis väljendub kahes-kolmes CERT-EE-le teavitatud lunavaraintsidendis iga kuu. Maailma skaalal ent on oodata aina uusi ja suuremaid intsidente ning välistada ei saa ka inimelude kadu, kui mõni tervishoiuasutus tõsiselt pihta peaks saama.

Õngitsemine ja petukõned ei kao kuhugi

2019. ja 2020. aastat domineerinud ning 2021. aastal järjekordse arvukusrekordi saavutanud õngitsuskatsed ei kao kuhugi. Nii pangakonto kui meilikontode õngitsuslehed saavad ajapikku aina tõetruumana väljanägemise ning aina korralikuma eesti õigekirja, mistõttu langevad meie inimesed endiselt kurjategijatest raha- ja andmekalastajate ohvriks.

Pangakonto õngitsuste mündi teise ja praeguseks juba rohkem kahju toova külje moodustavad aina populaarsemaks saavad venekeelsed petukõned kas „pangast" või „politseist". Samuti on tõusuteel krüptorahadega seotud skeemid (nii telefonikõnede kui õngitsuskirjade näol), mille puhul on eraisikud kandnud kahju isegi viiekohalise arvu eurode väärtuses. Politsei- ja piirivalveameti andmetel kaotati 2021. aastal erinevate petukõnede tõttu kokku viis miljonit eurot.





RIA küberturvalisuse teenistuse reageerimiskiirus ja -võimekus kasvavad

RIA KTT võimekus on viimase umbes viie aasta jooksul püsinud üsna samasugune, ent 2022. aastal teeme arenguhüppe, nagu ka eespool lugeda saab. CERT-EE saab mitu uut tööriista ning kasvavad ka järelevalve, analüüsi ja kriitiliste infrastruktuuri kaitsega tegelevate üksuste ressursid.

Loomulikult võtab uute võimekuste loomine oma aja, kuid aasta vältel peaksime hakkama ohte aina kiiremini avastama ning kogukonda, ettevõtteid, riigiasutusi ja avalikkust aina nobedamalt neist teavitama ja asjakohaste vastumeetmete osas juhendama. Koos Eesti elanike järjekindlalt kasvavate teadmistega küberhügieenist viib see loodetavasti selleni, et meie inimesed, ettevõtted ja asutused on küberruumis senisest paremini kaitstud.

Küberturvalisuse aastaraamat 2022

Väljaandja: **Riigi Infosüsteemi Amet**
Pärnu mnt 139a, 11317 Tallinn
Kujundus: **Martin Mileiko** (Profimeedia OÜ)
Illustratsioonid: **Linda Vainomäe** (Profimeedia OÜ), **iStock**
Fotod: **Seiko Kuik, Scanpix**
Trükk: **Ecoprint AS**

Riigi Infosüsteemi Amet

Euroopa Liit
Euroopa struktuuri- ja investeerimisfondid

Eesti tuleviku heaks

See reklaam ei lahenda probleemi. Aga mine vaata eits.ria.ee



Eesti Infoturbestandard

Eesti infoturbestandardi ja sellega seotud dokumendid on koostanud KPMG Baltics OÜ, Cybernetica AS ja Tallinna Tehnikaülikool Riigi Infosüsteemi Ameti tellimusel Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.