Riigi Infosüsteemi Amet

KÜBER-TURVALISUSE AASTARAAMAT 2023

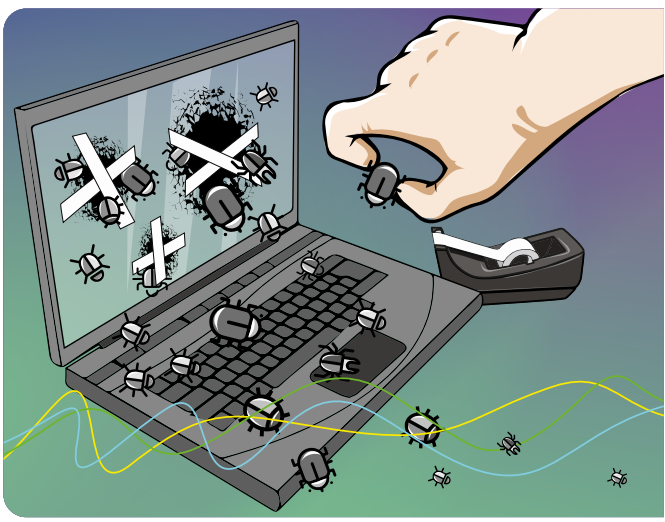
Riigi Infosüsteemi Amet

Küberturvalisuse aastaraamat 2023

Sisukord

EESSÕNA

2022. AASTA ÜLEVAADE



TURVALISEM KÜBERRUUM

KÜBER-TURVALISUS on riigikaitse ja sisejulgeoleku osa

Eelmine aasta meenutas, et vabadust, sõltumatust ja turvatunnet ei saa võtta iseenesest mõistetavalt ning et küberruum pole midagi füüsilisest maailmast eraldi seisvat. Tagamaks ühiskonna normaalselt toimimist ka kriisides, peame käsitlema küberturvalisust osana laiapindsest riigikaitsest ja sisejulgeolekust, leiab RIA peadirektori asetäitja küberturvalisuse alal **Gert Auväärt.**

Eelmise aasta jaanuaris sai selgeks, et kuumenenud olukord küberruumis nõuab kogu meie riigilt senisest suuremat tähelepanu ja valmisolekut digitaalse elukeskkonna säilitamiseks. Eesti vabariigi aastapäeval alanud Venemaa sõda Ukrainas kinnitas (küber)julgeoleku haavatavust ning tõi taas teemaks küsimuse, kas ja kuidas saame hakkama, kui meie infosüsteeme tabavad rünnakud, mis jätavad meie inimesed ilma elektrist, sidest, veest või muust eluks vajalikust.

Foto: Seiko Kulk

Gert Auväärt

Olen siiralt tänulik meie Ukraina kolleegidele, kes kriitilisel ajal, kui riik teeb kõike selleks, et päästa oma inimeste elusid, on jaganud meiega oma valusaid kogemusi ja vajalikku infot rünnakute kohta. Need on aidanud meid paremini ette valmistada – leida vahendeid, tänu millele oleme suutnud kaitsta teenuseid suuremate rünnakute eest.

See on praegune pilt, mis võib aga kiiresti muutuda. Töö selle nimel, et see pilt ei muutuks, käib iga päev ja 24/7. Nagu juba varasemalt kinnitanud oleme, teeb Eesti kõik, mis inimlikult meie võimuses, et aidata Ukrainal sõda võita, ja seda ka küberruumis.

RÜNNAKUD USALDUSVÄÄRSUSE VASTU

Vaatamata asjaolule, et meie teenuste ja süsteemide pihta pole tõsisemate tagajärgedega rünnakuid õnnestunud läbi viia, võin kinnitada, et sellised katsetused käivad pidevalt. Kõige suurema rünnakulaviini all olime kevadel ja sügisel, kui riigi jaoks olulisi veebilehti ja teenuseid tabasid rekordilised teenusetõkestusründed. Rünnakuid oli sedavõrd palju, et nendest liitlastele rääkides kergitas nii mõnigi neist kulme.

Mõnel juhul olid teenused osaliselt kättesaamatud, veebilehed maas, kuid ulatuslikke katkestusi, mis võinuks mõjutada inimeste heaolu või turvalisust, need kaasa ei toonud.

See, kui edukad on pahategijad meie elu kibedaks muutmisel, sõltub nii IT-lahenduste arendajatest, haldajatest kui ka nende kasutajatest. Iga lüli tarkus on vajalik, et hoida kurjategijad eemal meie andmetest, delikaatsest infost ja rahast. Riigil on kaitsemeetmete ja ka ohuteadlikkuse tõstmisel suur roll ning selle täitmiseks on RIA inimesed oluliselt pingutanud.

MAAILMAS AINULAADNE KÜBERRESERV

Aasta jooksul oleme võtnud kasutusele uusi tööriistu, mis kindlustavad parema kaitse rünnete eest, tõstavad seirevõimekust ning aitavad ohte ennetada ja intsidentidele kohe reageerida. RIA valmisoleku taset tõstame taas peagi algavatel riigikogu valimistel – nagu varasemalt, on valimiste turvalisus meie jaoks absoluutne prioriteet.

Oleme koos teiste ühiskonna jaoks vajalike teenuste pakkujatega kaardistanud riskid ning moodustanud riigi IT-majade ja Kaitseliiduga küberreservi, et kaasata suurema küberintsidendi lahendamiseks nii palju eksperte, kui olukord seda parajasti nõuab. See reserv sai mööda aasta lõpus õppuste käigus esimest korda ka ristsed. USA partnerite kaasabil oleme pakkunud maailmatasemel koolitusi küberreservi liikmetele ning elutähtsa ja olulise teenuse osutajatele, sh energeetikutele. Selliseid koolitusi teeme ka sel aastal.

Ülevaadete ja ohuhinnangutega oleme varustanud regulaarselt nii valitsuse liikmeid, riigi tippjuhte laiemalt kui ka IT-sektorit, kübervõrgustikku ja ettevõtteid. Oktoobris ja novembris korraldasime teavituskampaania, et rõhutada IT-vaatliku käitumise olulisust kõigile Eesti inimestele. Oleme järjepanu kasvatanud järelevalve haaret ning piloteerinud mitmekümne asutusega uue infoturbe standardi käima lükkamist. Sellega jätkame tööd alanud aastal.

Aasta alguses jõustunud uus infoturbe standard on väljakutse u 3500 asutusele, kes täidavad avaliku sektori ülesandeid või pakuvad kriitilisi teenuseid. Standardi rakendamine on üks teenuste kaitsmise moodus. Sellest, kui hästi on läbi mõeldud asutuse protsessid, välja selgitatud ohukohad, koostatud plaanid ja määratud ära infoturbe tase, sõltub asutuse käekäik laiemalt, sest intsident IT-süsteemides võib seisata kogu organisatsiooni töö. Neid juhtumeid oleme näinud ka Eestis.

PINGED PÜSIVAD HARIPUNKTIS

2022. aasta avas paljude silmad. Venemaa invasioon Ukrainas jätkub ning pinged küberruumis püsivad haripunktis.

Maailmas on vähe riike, kus saab päriselt digiriigi ja riigi vahele tõmmata võrdusmärgi. Eestis on need ühe mündi kaks külge. Küberruumis toimuv mõjutab meid igal sammul. Mul on palve headele lugejatele võtta RIA ohuhinnanguid, teavitusi ja soovitusi tõsiselt kuulda ja

> Iga meie soovitus sisaldab ka konkreetseid samme, mida saab süsteemide kaitseks ette võtta.

astuda operatiivselt samme, et end kaitsta. Iga meie soovitus sisaldab ka konkreetseid samme, mida saab süsteemide kaitseks ette võtta.

Elu on näidanud, et edukaks rünnakuks pole tihti vaja muud kui tahet ja kaitsmata tagalat, näiteks uuendamata arvutit. Iseenda kaitsmine küberruumis nõuab pingutust ning selleta pole võimalik küberturvalisust saavutada.

Mul on hea meel, et tänu meie pingutustele on RIA küberturvalisuse teenistus aastaga kasvanud päriselt riigi tsiviil-küberi kompetentsikeskuseks. Kasv jätkub ning sinu teadmised võivad olla need, mida järgmisena vajame. Kirjuta personal@ria.ee ja näeme kontoris!

Olukord küberruumis: UMMISTUS-RÜNNETE AASTA

Lootus, et pärast kaht pandeemia-aastat tuleb 2022 tavapärane, suri 24. veebruari varahommikul, kui Venemaa alustas täiemahulist sõda Ukraina vastu. Konflikt kandus küberruumi ja tõi Eestile ennenägematu hulga ummistusründeid.

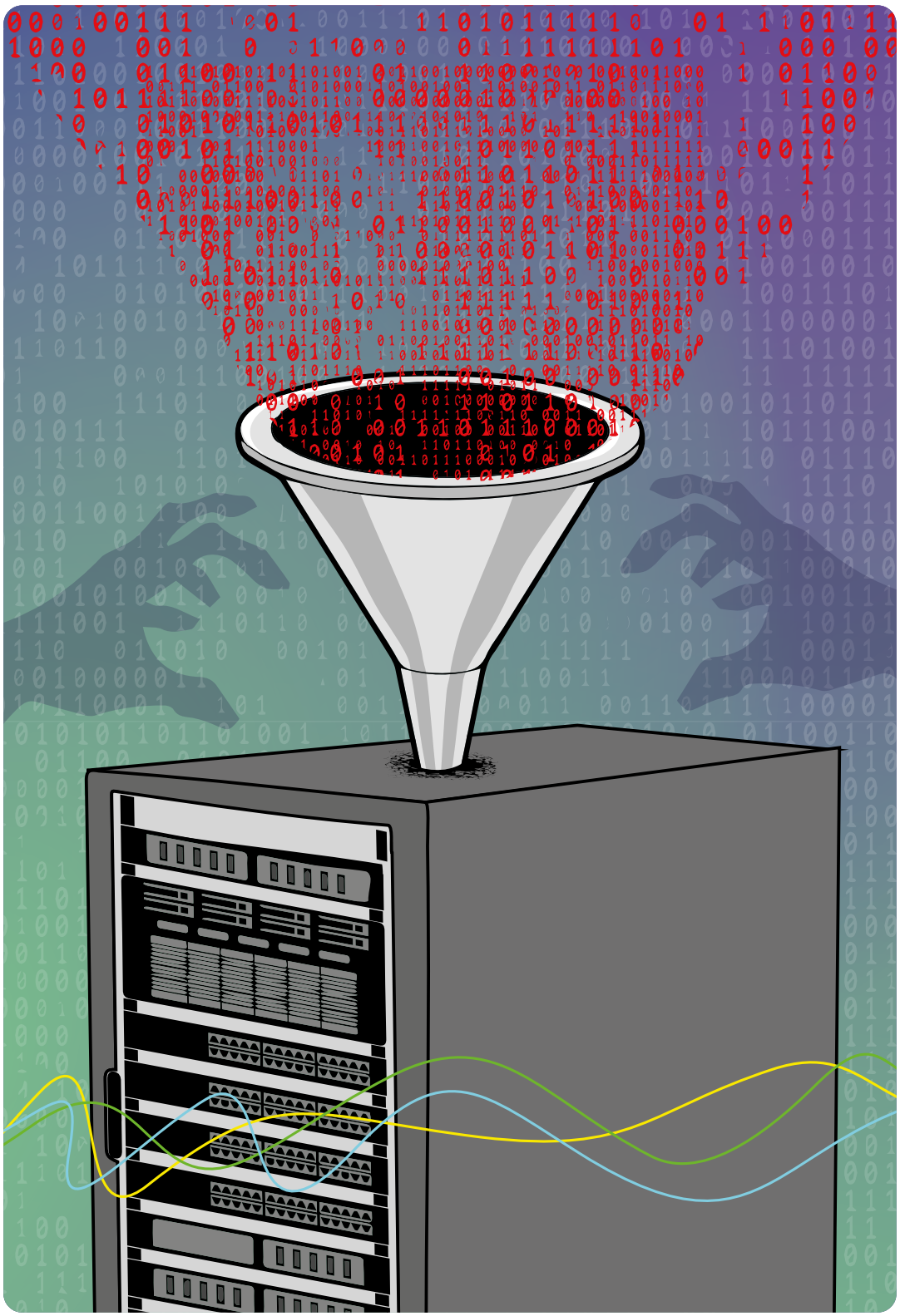
Tavapärastele hõlptulu otsivatele küberkurjategijatele lisandusid möödunud aastal poliitiliselt motiveeritud ründed, mille taga olid Kremli-meelsed häktivistid ja rühmitused.

Samuti täheldasime, et kutsumata külalised uurisid Eesti küberruumis asuvaid veebilehti ja teenuseid tavapärasest aktiivsemalt. Otsiti kõike, mis võimaldaks kutsumata külalisel kergemini sisse murda: kas kuskil on mõni turvaauk, oluline tarkvara jäänud uuendamata või lihtsalt midagi valesti seadistatud. Selline eelluurega kogutav info annab ründajatele hea ülevaate, kas ja kuhu tasub juba tõsisemate kavatsustega tagasi tulla.

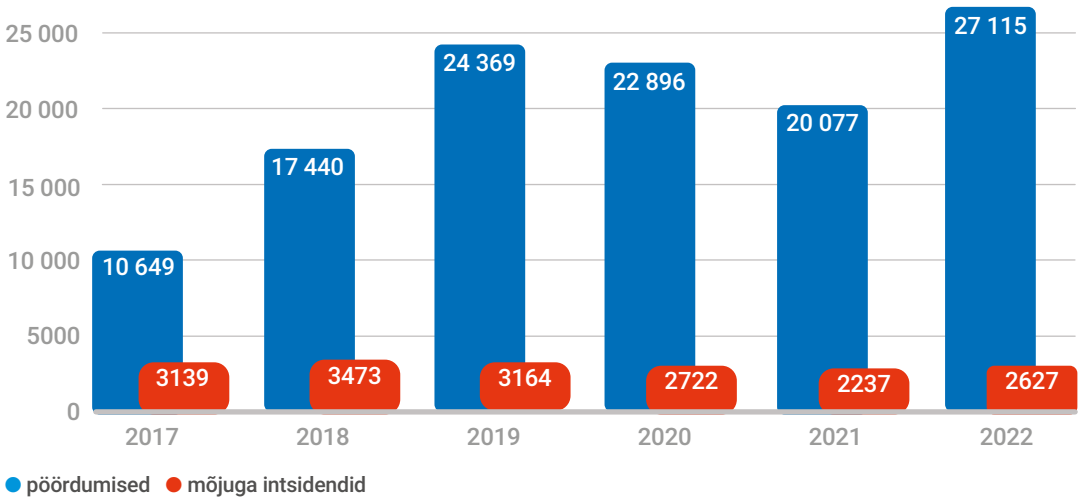
Ennetamaks suure mõjuga intsidente ja vajadusel neile kiiresti reageerida, tegutseb RIA eelmise aasta jaanuarist tõstetud valmisolekus. Teisisõnu: kohandasime oma igapäevatöö muutunud ohupildile vastavaks. Samuti tõhustasime eelmise aasta alguses tehnilisi kaitsemeetmeid, mida riigiasutustele pakume, sealhulgas kaitset teenusetõkestusrünnete vastu. Nagu järgnenud kuud näitasid, kulusid need marjaks ära.

ÜKS LAVIIN AJAS TEIST TAGA

Selle väljaande ajaloos on olnud aegu, kui oleme pidanud pikalt mõtlema, millise märksõna või lühikese pealkirjaga möödunud aasta kokku



Intsidentide ja CERT-EE poole pöördumiste hulk



võtta. Tänavu seda muret polnud. 2022 tõi Eestile ummistusrünnete lained, millesarnaseid pole me varem näinud.

Rünnakute mahud olid kohati üle saja korra suuremad kui 2007. aastal, mil pronkssõduri eemaldamise järel idanaaber meie e-teenuste tööd ja selle kaudu igapäevaelu masspäringutega häiris. Viisteist aastat tagasi olid nad selles edukamad, eelmise aasta rünnakuid tavakasutaja enamasti ei märganud. Vahel toimis mõni oluline veebileht või teenus tavapärasest aeglasemalt või katkes selle töö lühikeseks ajaks, kuid suurem osa teenusetõkestusrünnakutest õnnestus tõrjuda nii, et avalikkus ei pannud tähelegi, et olulised lehed või teenused olid massiivse rünnaku all.

Rünnakute mahud olid kohati üle saja korra suuremad kui 2007. aastal, mil pronkssõduri eemaldamise järel idanaaber meie e-teenuste tööd ja selle kaudu igapäevaelu masspäringutega häiris.

Toome näite 18. oktoobrist, kui riigikogu võttis vastu avalduse, milles mõistis hukka Ukraina territooriumi annekteerimise ja kuulutas Venemaa režiimi terroristlikuks. Sellele järgnes ummistusrünne riigikogu.ee vastu – ööpäeva jooksul tehti lehe vastu rohkem päringuid kui tavaolukorras 7,5 aasta jooksul. Lehe külastajad aga rünnakut ei märganud, sest tänu kaitsemeetmetele toimis see nii, nagu poleks midagi erilist juhtunud.

Kui tavapärasel ajal registreerime alla kümne märkimisväärse ummistusründe kuus, siis 2022. aasta aprillis 25, augustis 66, novembris 43. Kaheteistkümne kuuga kogunes neid 302, mis tähendab aasta võrdluses neljakordset kasvu. Neist mõjuga rünnakuteks lugesime sadakond. Cloudfare'i andmetel olime 2022. aasta teises kvartalis rakenduskihi vastu suunatu ummistusrünnete arvu poolest maailmas 7. kohal. Taustaks teadmine, et rahvaarvu poolest asume 150 piirist allpool.

Ründajate lemmiksihtmärgid olid ootuspärased: valitsus.ee, riigikogu.ee, president.ee, eesti.ee, politsei.ee, id.ee, aga sihiti ka transpordisektorit ja meediaettevõtteid.

Kui varasematel aastatel nägime teenuse-

tõkestusründeid, mille taga oli rahaline motivatsioon (maksa, muidu ründame suurema mahuga ja kauem!), siis mullu olid enamiku ummistusrünnete taga Kremli-meelsed häktivistid, kes sel moel oma rahulolematust väljendasid. Küll pahandas neid Narva tankimonumendi teisaldamine, küll ei meeldinud Vene telekanalite edastamise peatamine ega meie toetus Ukrainale.

Kui 2021. aastal olid ummistusrünnete sihtmärgiks sageli ka õppeinfosüsteemid ja koolid, siis eelmisel aastal nägime neid varasemast vähem. Nende rünnete ajastust ja käekirja vaadates võib arvata, et enamasti olid nende taga õpilased ise.

Ummistusrünnetest kirjutame pikemalt lk 18.

KUI TELEFON JÄÄB TUMMAKS

Kui ummistusründed jäid enamikule märkamata, siis osa teenusekatkestusi, mis ei tulenenud rünnakust, vaid inimlikust veast, kadunud elektriühendusest, riistvara- või tarkvararikkest, tajusid ilmselt kümned tuhanded inimesed.

15. veebruari hilisõhtul algas Telia võrgus ulatuslik kõneside- ja M2M teenuste rike. M2M lahendusi kasutatakse näiteks väravate ja parklate tõkkepuude avamiseks ning m-parkimise alustamiseks ja lõpetamiseks.

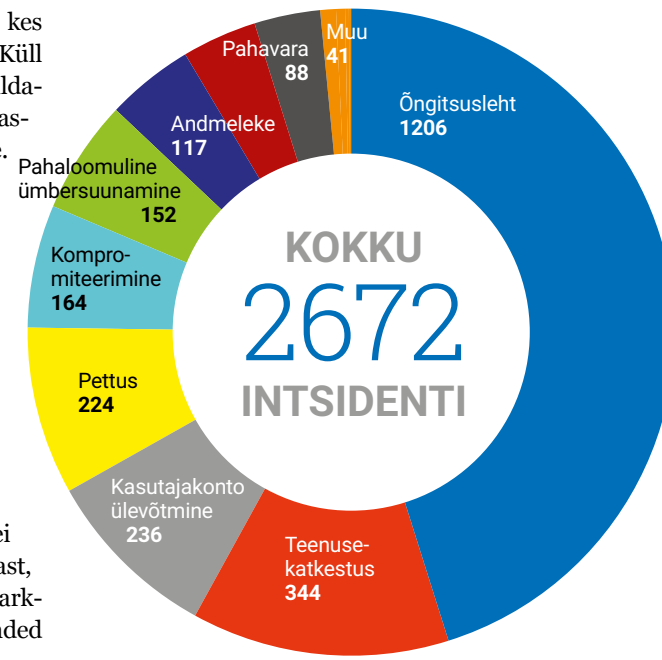
Parkimisega seotud hädad võisid tuju rikkuda, aga ohtlikum oli see, et katkestus mõjutas ka kõnesid hädaabinumbrile 112. Olukorras, kus su mobiilioperaatori võrgus on tõrked, aga on vaja kiirelt abi kutsuda, tasub telefonist eemaldada SIM-kaart või teha seadmele taaskäivitus ning PIN-koodi sisestamise asemel helistada hädaabinumbrile – sel juhul kasutab telefon 112 kõne tegemiseks mõne teise operaatori võrku.

Kui enamasti ei kesta sellised probleemid pikalt, siis sel korral saadi kõik teenused taas töökorda alles järgmiseks õhtuks.

Paraku polnud see ainus kord, kui Telia kliendid hätta jäid. 23. augustil katkes taas kõneside ja mobiilne andmeside – sel korral umbes tunniks. Rike mõjutas inimesi üle Eesti, ligikaudu kolmandik kõnedest jäi sel ajal alustamata või katkesid.

Kõne- ja andmesidekatkestusi oli ka detsembris, kui Saaremaad ja Hiiumaad tabas

Mõjuga intsidendid 2022. aastal

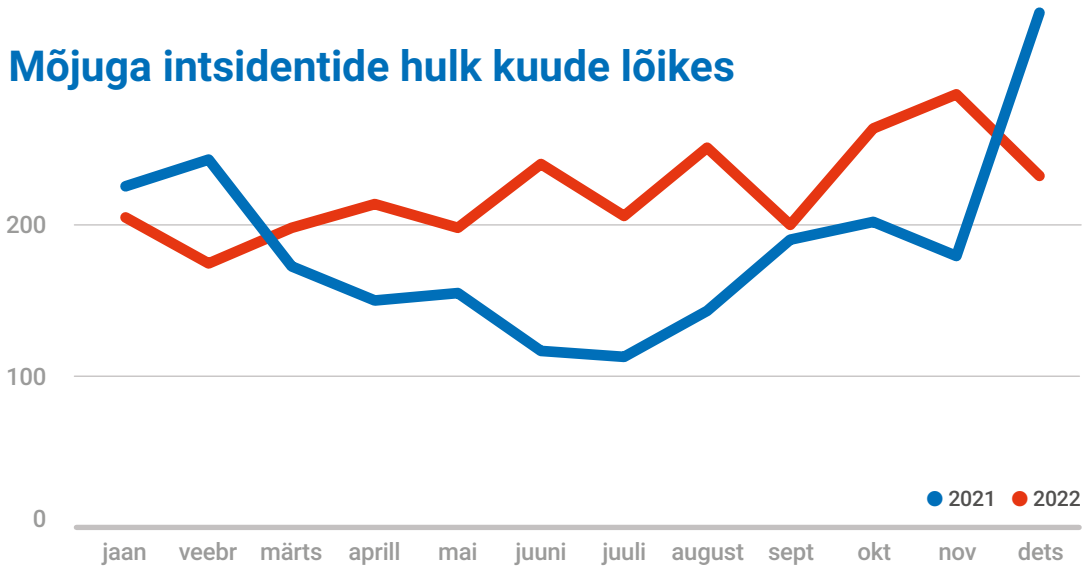


● Kättesaadavus - teenusetõkestusrünne

lumetormi tõttu elektrikatkestus. See mõjutas kõikide operaatorite tööd. Paljude mastide juurde olid küll paigutatud akud, millelt need elektriühenduse katkemise järel edasi toimisid, kuid need said tühjaks. Avariibrigaadid püüdsid mastide juurde viia mobiilseid generaatoreid, aga vahel osutus see võimatuks, sest teed polnud tiheda lumesaju tõttu läbitavad.

Korduvalt tuli katkestusi ette ka eID vahendite töös. Neist üks ebamugavamaid oli 30. augustil juhtunu, kui samaaegselt olid kolme tunni jooksul rivist väljas kõik SK ID Solutionsi teenused, sealhulgas kolm autentimisvahendit: ID-kaart, mobiil-ID ja Smart-ID. Selle juhtumi järel alustas RIA ettevõtte suhtes järelevalvemenetlust. Järelevalve kohta loe lähemalt lk 48.

Tehnika vedas alt ka üht Tallinna perearstikeskust, kus lõpetas töö hiljuti soetatud server, viies endaga kaasa nii andmebaasis olnud andmed kui ka värsked varukoopiad. Viimane toimiv varukoopia oli pool aastat vana ning vahe- →



pealset tööd polnud võimalik taastada. Mõistagi tekitas see perearstikeskuse töös suurema segaduse.

Kuid oli tõrkeid ka teenustes, mille toimepidevus ei sõltu Eesti ettevõtetest ega asutustest, kuid millel on siin palju kliente. Gmaili meiliserveri vea tõttu ei jõudnud 10. detsembril osa kirju adressaadini ja osa hilines. Eestis mõjutas see ligi 180 000 kasutajat.

ANDMED, MIS VAJASID PAREMAT KAITSET

Möödunud aasta üks olulisemaid andmelekkeintsidente seostub logistikaettevõttega Itella Smart Post. 6. novembri hilisõhtul hakkas sotsiaalmeedias levima info, et üks kasutaja on kätte saanud ligikaudu 10 000 Itella Smart Posti kaudu pakke saatnud või saanud inimese ja ettevõtte andmed: nimed, telefoninumbrid, e-postiaadressid, osa saadetiste puhul uksekoodid ja pakiautomaadid, kuhu pakk saadeti. Lisaks neile sai ründaja enda kätte äriklientide kasutajanimed. Ta proovis, kas mõned neist kasutavad oma kasutajanime ka paroolina ja paraku oli mitmekümnel juhul vastuseks jah.

Miski ei õigusta tuhandete inimeste andmete vargust, kuid õpikohti on siin ka ettevõtte jaoks. Andmed polnud piisavalt turvaliselt kaitstud ja selline leke olnuks lihtsalt välditav. Politsei alustas juhtumi uurimiseks kriminaalmenetlust.

Väiksemaid andmelekkeid jagus igasse kuusse. Näiteks maksete tarkvara uuenduse järel selgus, et sisestades kommertspanga äpis maksete lehel otsingusse kolmanda isiku nime, kuvab rakendus temaga seotud viimased maksed. Pank parandas vea mõne tunni jooksul.

Lisaks saime infot Eesti elanike pangakaardiandmete lekkest. Tõenäoliselt olid need kogutud pikema aja jooksul õngitsuslehtede kaudu. Teavitasime pankasid ja palusime lekkinud andmetega kaardid vajadusel sulgeda, et kurjategijad ei saaks neilt raha varastada.

PETTUSED JA ÕNGITSUSED

Pettuste ja õngitsuste osas eelmine aasta suuri muutusi ega uuendusi ei toonud. Õngitsused moodustasid jätkuvalt konkurentsitult suurima osa CERT-EE registreeritud intsidentidest. Traditsiooniliselt püüti heausksetelt kasutajatelt välja petta nende paroole, pangakaardiandmeid ja raha.

Küünilisemad petturid kasutasid ära inimeste heatahtlikkust ja soovi toetada Ukrainat – petukirjas lubati, et annetatud raha liigub heategevusorganisatsioonile ja sealtkaudu Ukrainasse, aga tegelikult jõudis see kurjategijate kätte.

Laialt levisid eelmisel aastal kullerifirmade nimel saadetud õngitsuskirjad ja -sõnumid. Neis teavitati, et paki kättesaamiseks on vaja tasuda kullerifirmale paar eurot. Kirjas või sõnumis olnud link viis ehtsa lehega äravahetamiseni sarnasele petulehele, kuhu paluti sisestada panga-

kaardi andmed. Kes seda tegid, avastasid peagi, et nende kontolt ei lahkunud kaks, vaid 200 või 2000 eurot. Alles pärast seda meenus paljudele, et nad ei oodanud kullerifirmalt ühtki pakki.

Samuti saime sadu teavitusi inimestelt, kes leidsid oma postkastist justkui politseilt saabunud kirja, milles neid informeeriti menetluse alustamisest lapsporno omamise, seksuaalkuriteo toimepanemise või muu taolise eest. Kirja saajal paluti kahe ööpäeva jooksul saata oma põhjendused viidatud aadressile ja ähvardati vastamata jätmise korral „viivitamatu vahistamise" ja toimepandud tegude avalikustamisega.

Selliseid kirju päris politsei ei saada. Tegu oli andmete ja raha väljameelitamiseks loodud pettusega. Kirjale vastates sai inimene edasised juhised, kuidas „rahatrahvi" tasumise abil pääseda pikast ja ebamugavast kohtusaagast. Pettustest ja õngitsustest loe pikemalt lk 20.

VÄHEM LUNAVARAINTSIDENTE

Kui mujal maailmas toimus taas mitmeid ränga mõjuga lunavararünnakuid, siis Eesti neist pääses. Eelmisel aastal registreerisime 21 lunavaraintsidenti, mida on poole vähem kui aasta varem. Rõõmu teeb see, et enamikul ohvritel olid andmetest varukoopiad, tänu millele sai asutuse või ettevõtte töö taastada, kuid nukraks asjaolu, et sageli muudetakse ründajate elu liiga lihtsaks, jättes kaugligipääsuks mõeldud RDP-ühendus avatuks kogu maailmale. Eelmisest aastast on näiteid, kus rünnak toimus vaid mõni tund pärast seda, kui kaugtööle suundunud kolleegi jaoks avati RDP-ühendus.

Tehnilistesse lahendustesse investeerimise kõrval ei tohi aga unustada, et sageli on nõrgim lüli nn tavaline arvutikasutaja.

Eriti ettevaatlikud peaksid olema IT-teenuste pakkujad, kellel on ligipääs ka oma klientide süsteemidele. Kui pole loodud piisavaid kaitsevalle, võib ohtlik pahavara kiirelt levida ka nendeni. Lunavararünnakutest loe lk 24.

2022. AASTA ARVUDES

- 2022. aastal laekus RIA intsidentide käsitlemise osakonda CERT-EE 27 115 pöördumist. See on keskmiselt 74 pöördumist päevas.
- 2672 neist olid mõjuga intsidendid, mille tõttu olid häiritud teabe või süsteemide konfidentsiaalsus, terviklus või kättesaadavus.
- Saime teateid 1206 õngitsuslehest. Seda on poole rohkem kui 2021. aastal.
- 344 puhul saime teate mõne teenusekatkestuse kohta. Katkenud teenuseid oli seinast seina, kõnesidest digiretseptini.
- 263 korral teavitati meid kasutajakonto ülevõtmisest, enamasti olid nendeks sotsiaalmeediakontod.
- 21 juhul saime infot Eesti ettevõtteid või inimesi tabanud lunavararünnakust. Nende arv langes ligi poole võrra.

IGA KLÕPS LOEB

Pole alust eeldada, et pingeline julgeolekuolukord meie piirkonnas sel aastal leeveneks. See tähendab senisest kõrgemat ohutaset ka küberruumis ja suuremat tõenäosust, et juhtub mõni ränkade tagajärgedega ja suurt osa ühiskonnast mõjutav küberintsident.

Kremli-meelsed häktivistid ja end sellistena näidata püüdvad rühmitused jätkavad Eesti ja teiste Ukraina toetajate ründamist. Suhteliselt lihtsakoeliste ummistusrünnete kõrvale tekivad keerukamad ja ohtlikumad ründed.

Eesti jaoks tähendab see üha kasvavat vajadust panustada küberturvalisusesse. Tehnilistesse lahendustesse investeerimise kõrval ei tohi aga unustada, et sageli on nõrgim lüli nn tavaline arvutikasutaja. Ükskõik kui head on viirusetõrjed, tulemüürid ja muud tehnilised kaitselahendused, võib üks vale hiireklõps või õngitsuslehele sisestatud salasõna liblika tiivalöögina vallandada sündmuste ahela, mille lõpus ei taha meist keegi olla. Ole IT-vaatlik!

VENEMAA AGRESSIOON UKRAINAS: sõda küberruumis

24. veebruaril 2022 alustas Venemaa täiemahulist sõda Ukraina vastu. Kineetilise sõjategevuse kõrval käis vilgas tegevus ka küberruumis, kus sihtmärgiks olid Ukraina valitsusasutused, kriitiline taristu, kohalikud omavalitsused, julgeoleku- ja kaitsesektor ning ettevõtted.

Päeval, mil Vene väed ületasid mitmest küljest Ukraina piiri, kadus seal tundideks KA-SAT satelliitsideühendus. Põhjuseks oli ettevõtte KA-SAT vastu suunatud küberrünnak, mis hiljem omistati Vene sõjaväeluurele. Lisaks Ukrainale oli selle küberründe mõju tunda ka mujal Euroopas – näiteks Prantsusmaal, Saksamaal, Itaalias ja Poolas –, kus satelliitside oli mõneks ajaks häiritud.

Invasiooni algusest alates üks ulatuslikema mõjuga rünnak toimus märtsis Ukraina suurima telekomiettevõtte Ukrtelekom vastu, mille tõttu jäi ligi 80 protsenti klientidest tundideks internetita. Telekommunikatsioonisektori vastu on toimunud ka teisi, väiksema mõjuga küberründeid ning mõistagi tekitas teenusekatkestusi ka otsene sõjategevus. Nii oli ka mõnest küberründest taastumine raskendatud, sest osale seadmetele pidi füüsiliselt ligi pääsema, kuid sõjategevuse tõttu olnuks see töötajatele eluohtlik.

Sihtmärgiks oli ka Ukraina energiasektor. Aprillis proovis väidetavalt Vene sõjaväeluure rivist välja lüüa suurt Ukraina energiaettevõtet, aga ebaõnnestus. Häkkerid proovisid elektrialajaamade töö katkestada, kasutades pahavara Industroyer2. Seda tööstuslike juhtimissüsteemide ründamiseks loodud pahavara kasutas Vene sõjaväeluure ka 2016. aasta detsembris Ukraina elektrisüsteemi vastu tehtud rünnakus, mis jättis osa Kiievi elanikest elektrita. Mullu aga õnnestus CERT-UA-l koostöös küberturbeettevõttega ESET rünne energiaettevõtte vastu aegsasti tuvastada ja võrku kaitsta.

HIRMUTAMINE INVASIOONI EEL

13. jaanuaril näotustati kümnete Ukraina valitsusasutuste veebilehed ehk ründajad asendasid nende sisu oma sõnumiga. Veebilehtedelt võis ukraina, vene ja poola keeles lugeda: „Ukrainlane! Kõik sinu isikuandmed on laaditud avalikku

võrku. Su arvutis olevad andmed on hävitatud, neid on võimatu taastada. Kogu teave sinu kohta on avalikuks tulnud, karda ja oota halvimat. See on sinu minevik, olevik ja tulevik."

Ukraina valitsus teatas järgmisel päeval, et enamik mõjutatud veebilehti on taastatud ning isikuandmeid pole lekkinud ega muudetud. Veebilehtede näotustamine on tehniliselt suhteliselt lihtsakoeline küberrünne, kuid sel võib siiski olla oluline mõju: ärevuse tekitamine, Ukraina võimude autoriteedi õõnestamine, uurijate aja raiskamine jm.

UMMISTUSRÜNDED SAID IGAPÄEVASEKS

Enne invasiooni tabasid Ukrainat ka jõulised teenusetõkestusründed. Näiteks olid maas Ukraina riigile kuuluvate pankade (Privatbank ja Ošadbank) e-teenused ning kaitseministeeriumi ja relvajõudude veebilehed. Pankade veebilehed olid küll kättesaadavad, ent kontole polnud võimalik sisse logida.

Ka päev enne Venemaa täiemahulise sõjalise rünnaku algust tabas Ukraina valitsusasutusi ja pankasid jõuline laine teenusetõkestusründeid. →

Seesugused ründed jätkusid aasta vältel: vahelduva eduga on maas olnud näiteks Ukraina valitsusasutuste, julgeolekuteenistuste ja mitmete ministeeriumite veebilehed.

HÄVITUSVARA LEVIK

Ukraina infosüsteemidest ja võrkudest on alates eelmise aasta algusest leitud mitut tüüpi hävituslikku pahavara. Tegu on andmete kustutamiseks ja seadmete kasutuskõlbmatuks muutmiseks mõeldud tööriistaga. Väidetavalt sai ühega neist pihta üks Ukraina piiripunkt, mistõttu pidi piiriületusi mõnda aega vormistama paberi ja pliiatsiga.

Hävitusvara saadeti Ukraina organisatsioonide poole nii enne kui ka pärast invasiooni algust, ent mõnel juhul ei piirdunud selle mõju ainult Ukrainaga. Nii oli küberründe piiriülest mõju lisaks Viasati KA-SAT satelliidi ründele näha ka ühe teise hävitusliku pahavara puhul, mida leidus lisaks sihtmärgile ühe Ukraina valitsusega koostööd tegeva ettevõtte Läti ja Leedu harukontorite võrgus.

KÜBERRÜNDED INFOOPERATSIOONIDES

Osa küberrünnete eesmärk polnud veebilehe või -teenuse töö häirimine, vaid valeinfo levitamine. Näiteks kompromiteeriti kohalike omavalitsuste veebilehed, kuhu postitati omavalitsuste nimel valeinfot, et Kiiev on langenud ja Moskvaga sõlmiti vaherahu.

Kompromiteeritud Ukraina uudisteportaalides (nt Ukraine 24) levitati süvavõltsitud ehk *deepfake* videot Ukraina presidendist Volodõmõr Zelenskõist.

SAADETI MASSILISELT ÕNGITSUSI

Mitmed küberohustajad sihtisid aasta vältel Ukraina inimesi ja organisatsioone õngituskirjadega. Sihtmärgiks olid nii valitsusasutused, relvajõud, MTÜd, õiguskaitseorganid kui meediatöötajad. Samuti õngitseti organisatsioone ja ametnikke teistes riikides ning rahvusvahelistes organisatsioonides, mis koordineerivad Ukrainale sõjalise või humanitaarabi andmist.

Tõenäoliselt oli rünnete peamine eesmärk saada kätte tundlikku infot, tekitada ligipääs süsteemidele ja liikuda juba kompromiteeritud organisatsioonide kaudu järgmiste sihtmärkideni. CERT-UA hoiatas õngitsuste eest ka tavainimesi, kelle kaudu üritati infooperatsioone läbi viia või kellegi teise nii-öelda kasulikuni jõuda.

Õngitsustes kasutati peibutusteemana ära sõda ja sellega seotut: näiteks viiteid maakaartidele, põgenikele või NATO kohtumistele.

Tõenäoliselt oli rünnete peamine eesmärk saada kätte tundlikku infot, tekitada ligipääs süsteemidele ja liikuda juba kompromiteeritud organisatsioonide kaudu järgmiste sihtmärkideni.

Sõja teemat kasutati õngitsuskampaaniates ka mitmete teiste riikide sihtmärkide puhul. Nii riiklike sidemetega küberrühmitused kui ka rahaliselt motiveeritud küberkurjategijad nägid selles soodsat võimalust suunata inimesi pahatahtlikke faile ja linke avama. Näiteks teatas Google, et Hiina küberrühmitus Mustang Panda olevat kasutanud sõda Ukrainas aktiivselt ära Euroopa organisatsioonidele saadetud õngitsustes. Kirjad sisaldasid pahavaraga nakatatud manust, näiteks nimega „Situation at the EU borders with Ukraine.zip“.

SÕDA TÕI HÄKTIVSIMILAINE

Käimasolevas sõjas valisid poole mitte ainult riigid, vaid ka mitmed ideoloogiliselt motiveeritud häkkerid ehk häktivistid. Vahetult pärast invasiooni kutsus Ukraina valitsus kõiki IT-oskustega vabatahtlikke üles liituma nn IT-armeega, et aidata kaitsta Ukraina kriitilist taristut ja tõrjuda Venemaa küberrühmituste ründeoperatsioone.

Lisaks kaitsele on Ukraina IT-armee läbi viinud teenusetõkestusründe, näotustamisi, aga

ka keerukamaid operatsioone Vene veebilehtede ja ettevõtete vastu. Näiteks olevat IT-armee sooritanud ummistusründeid Venemaa pankade, riigiasutuste ja meediaväljaannete vastu, aga häirinud ka näiteks sealsete kinode tööd ja löönud rivist välja Venemaa alkoholiarvestuse infosüsteemi, mistõttu tekkis ajutisi probleeme alkoholitarnetega.

Lisaks Ukraina IT-armeele aktiveerusid ukrainameelsed häktivistid mujal maailmas. Näiteks oli palju teateid Anonymouse rühmituse liikmete rünnetest Venemaa veebilehtede ja teenuste vastu ning hulgaliselt lekitatud andmeid, samuti olevat häktivistid muutnud Venemaa asutuste andmekogude, kaustade ja failide nimesid ukrainameelseks (nt Slava Ukraini, „putin stop this war“). Muu hulgas võeti sügisel sihikule Venemaa suurim taksoteenus Yandex: 1. septembril telliti Moskva taksod ühele aadressile ja tekitati nii kesklinnas suur ummik.

Ukrainameelne häktivism leidis koha ka tarkvaras. Nimelt hoiatas Venemaa suurim pank Sberbank venelasi venekriitilisteks muudetud tarkvarauuenduste eest. Selle all peetakse silmas avalikult kättesaadavaid programme, mille autorid on tarkvara moondanud nii, et see hakkas uuenduse järel kuvama näiteks sõjavastaseid ja ukrainameelseid sõnumeid.

UKRAINA SÕPRADEST SAID SIHTMÄRGID

Ent ka Venemaad toetavad häkkerid ei istunud käed rüpes – peatselt pärast täiemahulise sõja algust aktiveerusid mitmed Kremli-meelsete häktivistide rühmitused. Nende sihtmärgiks polnud ainult Ukraina, vaid ka paljud Ukrainat toetavad riigid, sealhulgas Eesti, Soome, Läti, Tšehhi, Rumeenia, Poola jt.

Ummistusrünnete sihtmärkide ring on riigiti laias laastus sama: ministeeriumid, riigiasutused, olulisemad e-teenused, transpordisektor, pangad ja meediaväljaanded. Sageli olid ummistusrünnete lained ajendatud sellest, kui riik on teinud mõne Ukrainat toetava poliitilise otsuse, näiteks kuulutanud Venemaa terrorismi toetavaks riigiks.

Tuleb arvestada võimalusega, et ühele või teisele riigile toetust või abi pakkudes võib abistaja ise küberrünnete sihtmärgiks sattuda. Senis-

ÄRA OSALE DDoS-RÜNNETES

Eelmise aasta veebruaris hakkasid sotsiaalmeedias, sealhulgas Eesti gruppides, levima üleskutseid toetada Ukrainat osalemisega teenusetõkestusrünnetes Vene propagandakanalite vastu. Olgu eesmärk kuitahes õilis, ei soovita RIA Eesti inimestel kaasa minna üleskutsetega osaleda küberrünnetes.

Kuigi võib tunduda, et lubades oma telefonis oleval rakendusel sooritada ummistavaid päringuid mõne Vene propagandalehe vastu, on hea võimalus midagi omalt poolt ukrainlaste heaks teha, kaasnevad sellega ohud. Seda tehes annab kasutaja oma seadme robotvõrgustiku käsutusse ja käitab tundmatut koodi – mõlemad tegevused on küberturvalisuse seisukohast lubamatud. Muu hulgas ei saa olla kindel, mis sihtmärgi pihta päringuid tehakse või kuhu ründerusikas järgmiseks suunatakse. Ukraina aitamiseks on paremaid viise.

te rünnete puhul olid sihtmärgid üldiselt eteaimatavad, ent edaspidi ei pruugi see nii olla.

UKRAINA TOIMEPIDEVUS ON MÄRKIMISVÄÄRNE

Küberturvalisuse mõttes on Ukraina kriitiliste teenuste toimepidevus olnud märkimisväärne, sest riigi digiteenused toimivad ja küberrünnete tõttu pole ka vesi ja elekter või muu vajalik kadunud. Neid katkestusi on põhjustanud peamiselt kineetiline sõjategevus.

Lisaks Ukraina enda võimetele on neile küberdomeenis appi läinud nii riigid kui ka mitmed globaalsed IT- ja küberturvalisuse ettevõtted. Ukraina julgeolekuteenistuse SSU teatel blokeeriti 2022. aastal edukalt üle 4500 küberrünnaku, mida olevat üle viie korra rohkem kui 2020. aastal, mil dokumenteeriti 800 küberrünnakut.

Üks edu saladusi on asjaolu, et küberründed Ukraina vastu ei saanud algust eelmisel aastal – sealsed organisatsioonid on küberrünnete sihtmärgiks olnud juba 2014. aastast. Varem saadud kogemused kulusid marjaks ära.

REKORDKOGUS teenusetõkestus-ründeid

2022. aastat Eesti küberruumis jäävad meenutama eelkõige igapäevaseks muutunud teenusetõkestusründed, mida tehti võrreldes 2021. aastaga neli korda rohkem. Miks tõusis ummistusrünnete arv nii palju, milline oli nende mõju ja mida neist õppida?

Teenusetõkestus- ehk DDoS-rünnete kasvu katalüsaatoriks oli Venemaa sõjategevuse laienemine Ukrainas 24. veebruaril. Siiani kestev sõda tõi kaasa massiivse küberaktivismi/häktivismi laine, mida pole varem nähtud.

Ideoloogiliselt motiveeritud häkkerid ehk häktivistid moodustasid palju grupeeringuid ning üritasid ummistusrünnetega ellu viia oma agendat: tavaliselt riigiasutuste diskrediteerimine, üldsuses hirmu ja/või ebamugavuse külvamine. Rünnati nii avaliku sektori asutusi kui ka riiklikult olulise tähtsusega ettevõtteid. Rünnakute edust (ka näilisest) anti hiljem kaasliikmetele teada suhtlusvõrgustikes.

Eesti asutused ja organisatsioonid ei jäänud häktivistide DDoS-rünnetest puutumata, kuid nende mõju oli marginaalne. DDoS-ründeid oli kahte liiki: ühed keskendusid otse veebilehtede ründamisele, teised sihtisid serverit, kus koduleht töötab, ning proovisid piltlikult öeldes internetikaabli ära ummistada.

LAINE LAINE JÄREL

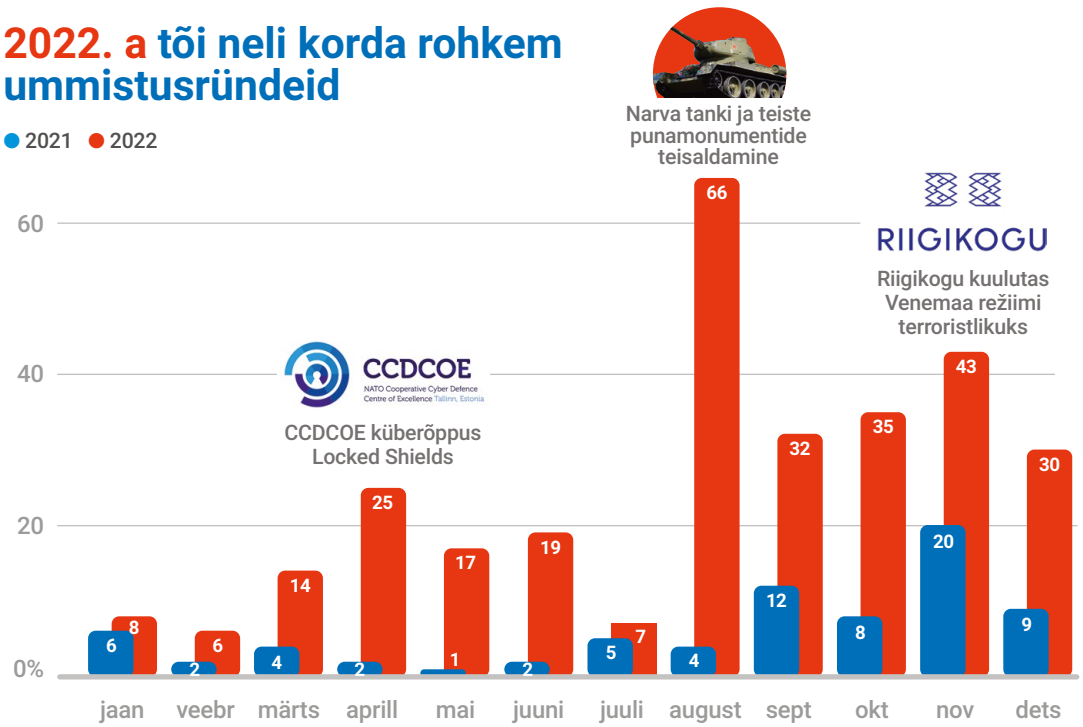
Esimene intensiivsem ummistusrünnete laine tabas Eestit aprillis – samal ajal, kui Tallinnas käis rahvusvaheline küberjulgeolekuõppus Locked Shields. Rünnati nii transpordiettevõtete kui ka riigiasutuste veebilehti. Ründajatel õnnestus mõni rünnaku alla sattunud veebileht muuta maksimaalselt kuni paariks tunniks kättesaamatuks, laiem mõju puudus.

> Eesti organisatsioonid ja asutused ei jäänud häktivistide DDoS-rünnetest puutumata, kuid nende mõju oli marginaalne.

Augustis tabas Eestit järgmine suurem DDoS-rünnakute laviin. Sel kuul tehti rekordilised 66 ummistusrünnet – üle 16 korra rohkem kui 2021. aasta samal ajal. Peamiselt sihiti avaliku sektori veebilehti, lisaks transpordi- ja finantssektorit. Ilmselt oli rünnakute suur hulk seotud Narva punamonumentide teisaldamisega. Enamikul rünnakutel polnud nähtavat mõju.

Pärast augustit rünnakute hulk stabiliseerus ja jäi igas kuus paarikümne juurde. Siiski nägi-

2022. a tõi neli korda rohkem ummistusründeid



me endiselt ka seda, et teatud poliitiliste otsuste või sõnavõttude järel algasid taas DDoS-rünnakud. Näiteks 18. oktoobril sattus riigikogu veebileht vahetult pärast Venemaa režiimi terroristlikuks kuulutamist ründelaviini alla.

MIKS POLNUD ENAMIKUL RÜNNAKUTEST MÕJU?

Lisarahastuse toel sai CERT-EE 2022. aastal rakendada täiendavaid kaitsemeetmeid, tänu millele ei toonud Eestit tabanud ummistusrünnete lained kaasa suuremaid teenusekatkestusi. See ei tähenda, et saame palmisaarele puhkama minna ja loota, et kaitsemeetmed tagavad DDoS-rünnakute eest kaitse nüüd ja igavesti. Teenusetõkestusrünnakud on siin, et jääda. Samuti võime suure kindlusega prognoosida, et ründajad püüavad leida viise neist mööda minna. Kui üks lähenemine ei toimi, proovivad nad uusi. Seetõttu peame olema alati valmis uut tüüpi DDoS-rünnakuid analüüsima, neid tõrjuma ning tegema järeldusi ja astuma nende mõju minimeerimiseks vajalikke samme. Mida kiiremini areneb tehnoloogia, seda mahukamaks muutuvad ründed, ning seda võimekamad peavad olema ka seadmed, mida ründajad püüavad üle koormata.

KUIDAS KAITSTA end ummistusrünnete eest?

- Veendu, et serverid kasutaksid uuendatud tarkvara.
- Võimalusel võta kasutusele täiendav DDoS-kaitse.
- Veendu, et serverid ja võrguseadmed oleksid piisavalt võimekad, sest aeg-ajalt tekitavad ka legitiimsed kasutajad suure koormuse võrguliikluses. Samuti võivad võrgu- või transpordikihi vastu suunatud ründed olla piisavalt väiksed, et nende tõrjumiseks mõeldud DDoS-kaitsed ei rakendu, kuid piisavalt mahukad, et võrguseadmed üle koormata.
- Analüüsi teenuste kitsaskohti ja proovi leida viise, mis võiksid need katki teha, sest ründajad otsivad samuti meetodeid, kuidas vähendada päringute hulka, kuid koormata lehte sellele vaatamata (nt andmebaasiotsinguid tehes).

E-PETTURITE PARADIIS

E-teenuste medali tumedamalt küljelt vaatavad vastu petturid ja nende ohvrid. Enamasti minnakse petukirjade ja õngitsuslehtede õnge, aga suuri kahjusid kanti ka krüptopettustega.

Koroonaviirus muutis maailma mitmel moel. Olude sunnil sai kodus töötamisest norm. Elu korraldati nii, et ühegi asja ostmiseks ei pidanud kodust lahkuma. Ja kui vahel pidigi välisukse avama, siis kulleriga kohtumiseks või lähima pakiautomaadini jalutamiseks. Iga kontakt inimesega võis olla ohtlik.

VILJAKAS PINNAS PETTUSTELE

Need arengud – inimkontaktide vähenemine ja e-teenuste suurem kasutamine – lõid viljaka pinnase netipetturitele. Paari klõpsuga kauba tellimine on mugav, kuid sellega kaasnevad ohud. Netikaubanduse kuldajal kasvas petturite kliendibaas, sest nüüd tellisid netist kaupa ka need, kes varem käisid poes.

Kodust tegid tööd inimesed, kes varem olid kontoris, kus nad said üle ukse kiireid asju üle küsida. Kui e-kirjade ja SMSide ehtsuse kontrollimine muutus natuke tülikamakas, jäeti see samm sagedamini vahele.

RIA-le anti 2022. aastal teada enam kui tuhandest õngitsuslehest. Need on veebilehed, mis on langenud kurjategijate kätte või on nende loodud. Just selliste saitide kaudu proovivad küberkelmid inimestelt välja meelitada nende andmeid, näiteks krediitkaardiandmeid või salasõnu. Jah, on libalehti, mis on väga kehvasti loodud, kuid suurem osa neist näeb välja piisavalt ehtsad, et kasutajaid eksitada.

PETTURID MATKIVAD PANKU JA KULLERIFIRMASID

Aasta jooksul saime hulgaliselt teateid libakirjadest ja sõnumitest, mis jäljendavad Eestis tegutsevaid kullerifirmasid. Peaasjalikult tehti järele Omniva, DPD ja DHLi e-kirju ning sõnumeid.

Teine grupp, kelle esindajana pätid proovisid esineda, on pangad. Saime iga kuu kümneid teateid kasutajatelt, kes said õngitsuskirja näiliselt SEB-lt, LHV-lt või Swedbankilt.

On ka neid petta saanuid, kellele läheneti Facebookis, kui nad seal parasjagu midagi

NÄITEID õnnestunud pettustest

- 4. juunil sai kasutaja SMSi, mis matkis SEB panka. Ta suunati õngitsuslehele, kus tal paluti Smart-ID kaudu ennast tuvastada. Pärast PIN2-koodi sisestamist kaotas kasutaja u 800 eurot.
- 13. detsembril sai inimene SMSi, mis matkis kullerifirmat DPD. Sõnum suunas kasutaja õngitsuslehele, kus küsiti tema pangakaardi andmeid. Ta kaotas 513 eurot.
- 4. detsembril sai kasutaja SMSi, mis matkis LHV panka. Kasutaja suunati õngitsuslehele, kus tal paluti sisse logida. Kuna ta mõtted olid mujal ja leht nägi veenev välja, sisestas kasutaja Smart-ID PIN2-koodi ning kaotas u 700 eurot.

müüsid. Nende kaasuste puhul esineb kelm huvilisena, kes soovib kaupa osta. Kui aga tehinguks läheb, toob pätt ettekäändeid ja põhjendusi, miks raha peaks välja käima hoopis kauba müüja – küll oli vaja tasuda transpordi, küll kindlustuse eest. Sellised huvilised tuleb pikema jututa pikalt saata.

Facebook Marketplace'i pettused pole ebatavalised ning nii ostjatel kui ka müüjatel tuleb olla tähelepanelik. Mullu kaotas üks Facebooki kasutaja paar tuhat eurot, kui soovis osta helitehnikat. Pettur esitas inimesele libaarved ja võltsitud pakisaadetise teavitused.

Sellised pettused käivad lainetena ja nende kvaliteet kõigub. Meie soovitus on alati kontrollida, kuhu oma andmeid sisestad. Kuklas tuleb hoida ka teadmist, et PIN2-koodi sisestamine võrdub allkirja andmisega ehk siis toimub juba midagi tõsisemat kui lihtsalt andmete kinnitamine või sisselogimine.

NETIPETTUSED ANNAVAD VALUSAID ÕPPETUNDE

Kadunud pole ka arve- ja palgakonto-pettused, millest oleme kirjutanud varasemates aastaraamatutes. Pettuseid viiakse ellu igal võimalikul moel: e-kirjade, Facebooki, Telegrami ja teiste sotsiaalmeediaplatvormide kaudu ning isegi arvutimängude abil.

RIA-le teatati 2022. aastal enam kui 150 finantspettusest. Kõige valutumad pettused põhjustasid vähem kui sada eurot maksvaid

→

õppetunde, kuid oli kuritegusid, millega ettevõtte esindajad kandsid pättidele kümneid tuhandeid eurosid.

2022. aasta alguses sai ühe Eesti suurfirma töötaja hästi koostatud õngitsuskirja, kus kelmid esinesid ettevõte tegevjuhina. Raamatupidaja kandis kelmidele enam kui 14 000 eurot. Märtsis kaotas Eesti töötusettevõte sarnase pettuse käigus rohkem kui 17 000 eurot. Juunis jäi järgmine ohver libaarvet tasudes ilma umbes 8000 eurost. Augustis kaotas Eesti ettevõte sarnase kelmuse tõttu 44 000 eurot. Novembris kaotas automüügiettevõte enam kui 70 000 eurot. Kurjategijad esinesid ettevõtte Skandinaavia partnerina ning saatsid Eesti ettevõttele libaarve. Tegelik makse tehti ühe Lõuna-Euroopa riigi panka.

Alati pole sääraste pettuste ohvrid Eesti ettevõtted või inimesed. Oktoobris pöördus RIA poole Leedu kodanik, kes kaotas 2500 eurot, kuna soovis osta Eesti libaettevõttena esinenud pättidelt pelleteid.

KRÜPTOPETTUSED

2022. aasta viimastel kuudel alustas Föderaalne Juurdlusbüroo ehk FBI menetlust kahe Eesti ja eestlastega seotud krüptofirma suhtes. Ligi kuu enne jõule pidasid politseinikud kinni kaks Eesti kodanikku, keda kahtlustatakse enam kui poole miljardi suuruse kahju tekitamises.

Detsembris alustati uurimist Eesti krüptovaluuta vahendusplatvormi 3Commas suhtes, et selgitada välja, kas platvorm on seotud miljoneid dollareid kahju põhjustanud häkkimisega. Sellega seoses on ka RIA poole pöördutud. Kasutajad on teada andnud vargustest, mille kahju jääb mõnekümne tuhande ja mõne miljoni dollari vahele.

Eelmise aasta oktoobris vahistas keskkriminaalpolitsei neli meest, keda kahtlustatakse investeerimiskelmuses, mille käigus esitasid nad valeandmeid, müüsid enda loodud *dagcoin*'i ja teenisid sellega kaheksa miljonit eurot.

RIA-le antakse enamasti teada eri krüptoplatvormidega seotud pettustest ning krüptoraha vargustest. Novembri alguses teatas kasutaja, et Metamaski keskkonna kaudu varastati temalt 4500 eurot. Kuu varem teavitas teine kasutaja, et tema Ledger Nano S krüptorahakotist varastati 50 000 dollari eest tokeneid.

MÄNGUMAAILMA PÄRISKAOTUSED

Internet pakub raha kaotamiseks muidki võimalusi. Üheks vahendiks, mille abil raha heausksetelt inimestelt petturiteni jõuab, on mängud, kus saab teha mikromakseid. Novembris saime kaks teadet pettustest, mis on seotud noorte seas populaarse „Fortnite'i" mänguga. Mängusiseste ostude sooritamiseks piisab telefoninumbrist ja sellele SMSi teel saabunud koodist. Võõras mängija küsis lapselt tema telefoninumbri. Lisaks sellele ütles ta ka kaasmängijale SMSiga saadetud koodi. Seeläbi sai paha-

ÜHE PETTUSE ANATOOMIA

2022. aasta jaanuari algus oli tallinlanna Johanna (nimi muudetud) jaoks põnev, kiire ja raske. Perre sündis tütar, kes tõi palju rõõmu, aga kes vajas arusaadavalt palju tähelepanu. Kogu elu tuli ümber korraldada ning lisaks kõigele muule tuli soetada pere kõige värskemale liikmele riideid ja muud.

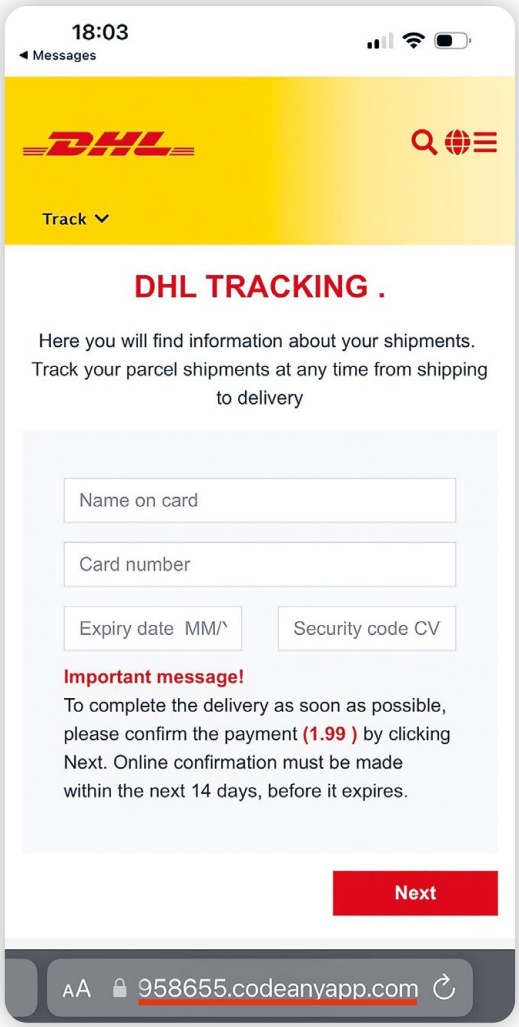
Oli tempokas aeg ning aja kokku hoidmiseks oli kõige mõistlikum tellida asju netist. Seda enam, et koroonaviirus polnud veel kuhugi kadunud. Niisiis ootaski Johanna pakke, millest üks pandi DHLiga teele välismaalt.

Ühel õhtul veidi pärast kella 20, kui laps oli just uinunud, sai Johanna sõnumi. „Teie pakk ootab kohaletoimetamist. Kinnitage makse (2,22 Eur) alloleva lingi all: bid.do/Estonia-Express." Selleks ajaks oli juba tavapärane, et telefoni laekus info eri pakkide kohta.

Johanna vajutas sõnumis olnud lingile ning avanes veebileht, mis nägi välja nagu DHLi koduleht. Seal nägi ta pakinumbrit, paki teekonda ja seda, et pakk on jõudnud Eesti piirile. „Kõik tundus ehtne. Korra oli mul küll kahtlus, et peaks pakinumbrit kontrollima, kuid jätsin selle tegema-

Ühe pettusekatse kaks osa

Inimene, kes polnud DHLi kaudu pakki tellinud, sai SMSi, milles olnud link viis õngitsuslehele. Seal paluti sisestada pangakaardi andmed. Vaata paremposse ekraanitõmmise URLi, mis viitab pettusele.



tahtlik mängija sooritada lapse kulul mängusiseseid oste 168 euro eest.

Sarnasest juhtumist „Fortnite'is" teatas ka teine lapsevanem. Kaks Eesti mängukaaslast veensid last jagama SMSiga saadetud koode. Nende abil sooritasid nad 225 euro eest oste. Kui pettus välja tuli, lõpetasid mängukaaslased ohvriga suhtluse. ●

ta. Oli veidi kahtlane, et pakk on tollis kinni ning pean selle kättesaamiseks 2 eurot maksma. Kahjuks ei pööranud ma punastele lipukestele piisavalt tähelepanu," ütleb Johanna.

Veebilehel „Edasi" nuppu vajutades jõudis ta kohani, kus saab maksta nn tollitasu. „Sisestasin pangakaardi andmed ning seejärel tuli ette Smart-ID kinnituskood. Mulle jäeti mulje, nagu peaksin Smart-ID kaudu veel midagi kinnitama," kirjeldab ta.

Tegelikult sooritasid kurjategijad samal ajal juba makset ning Smart-ID kontrollkood oli loodud kas kasutajas usalduse tekitamiseks või tema eksitamiseks. „Seni kuni ootasin Smart-ID vastust, tuli telefoni pangateade, et olen sooritanud makse. Nägin, et maha läks 745 eurot. Sain aru, mis juhtus," meenutab Johanna, kes helistas kohe kodupanka, kuid kuulis sealt, et tehtud makset ei saa enam tagasi pöörata. „Pangateller ohkas sügavalt," ütleb Johanna, „ilmselt polnud ma esimene, kes sellise pettuse ohvriks langes."

Seejärel pöördus ta veebikonstaablite poole, kes aitasid, kuidas oskasid, kuid ütlesid kohe alguses, et raha tagasisaamise tõenäosus on väga väike. Umbes neli kuud hiljem sai Johanna politseilt teate menetluse lõpetamise kohta. Selgus, et tema pangakaardiga tehti makse ühes Saudi Araabia elektroonikapoes. ●

LUNAVARA-RÜNNAKUD: arvuliselt vähem, kuid sama ohtlikud

Ehkki eelmisel aastal registreerisime vähem lunavararünnakuid ja enamikul ohvritel olid pantvangi võetud andmetest varukoopiad olemas, põhjustasid need Eesti ettevõtetele siiski olulist kahju ja ebamugavust.

Kui 2021. aastal registreerisime 30 Eesti ettevõtete, asutuste ja eraisikute vastu suunatud lunavararünnakut, siis eelmisel aastal 21. Ohvreid oli tootmisettevõtete seas, kaubanduses, majutuses, logistikas, energeetikas jm.

VARUNDAMINE EI PÄÄSTA KAHJUDEST

Isegi siis, kui ohvritel olid krüpteeritud andmetest varukoopiad olemas, häirisid lunavararünnakud oluliselt nende tegevust. Ühes ettevõttes seiskus rünnaku tõttu tootmisjuhtimise tarkvara, teises ei saanud kassasüsteemide lukustumise tõttu kliente teenindada, kolmandas katkesid sisemised tööprotsessid ja infovahetus – kui tuua vaid mõned näited.

Enamasti ei tea CERT-EE, kui suurt tasu ründajad andmete taastamiseks vajaliku võtme eest nõuavad. Esmases teates kutsuvad nad ohvrit ühendust võtma, et arutada summa üle, aga enamasti jääb see dialoog avamata. CERT-EE-le teadaolevalt ükski sihtmärk möödunud aastal lunavaranõuet ei tasunud ning kurjategijad jäid vähemalt Eestis tasust ilma.

MILLISEID LUNAVARARÜNNAKUID NÄGIME 2022. AASTAL?

Aasta algas nelja Eesti ettevõtte jaoks lunarahanõudega. Kahel juhul oli ettevõtte töö tugevalt häiritud, sest puudus ligipääs infosüsteemidele. Suures osas õnnestus ettevõtetel tänu tagavarakoopiatele oma tööprotsessid ja andmed siiski taastada, kuid ühel juhul hoiustati tagavarakoopiaid samas serveris, mis rünnaku käigus ära krüpteeriti. Siit ka soovitus hoida varundused eraldatud keskkonnas, et rünnaku korral ei krüpteeriks pahavara ka neid.

Juulis tabas Loki-nimeline lunavara ettevõtet, mis oli teinud oma IT-süsteemides muudatusi ja jätnud avalikult kättesaadavaks rohkem teenuseid kui olnuks turvaline. Ründajad kasutasid pakutud võimalust, tungisid virtuaalserverisse ja krüpteerisid selle sisu. Ettevõte eemaldas virtuaalserveri võrgust, taastas krüp-

teeritud andmed varukoopiast ja kurjategijad jäid palgapäevata.

VÄLK KAKS KORDA ÜHTE KOHTA EI LÖÖ?

2022. aastal suvel sai üks ettevõte lunavaraga pihta lausa kahel korral. Mõlemal puhul õnnestus andmed varukoopiatest taastada, kuid ettevõtte töö oli siiski rünnakutest tugevalt häiritud. Kuna server ei töötanud, ei toiminud ka sellest sõltuvad kliendihaldusprogrammid.

Rünnakud õnnestusid tõenäoliselt seetõttu, et ettevõtte võrguseadme haldusliidesed olid avalikult kättesaadavad ning ründaja suutis ühe kasutaja konto üle võtta.

Kurja JUUR

Enam kui pooltel juhtudel tungisid ründajad ohvri süsteemidesse kaugtöölaua protokolli (*Remote Desktop Protocol* ehk RDP) kaudu. 2022. aasta märtsis avaldasime ohuhinnangu, kus andsime juhtnööre kaugtöölaua protokolli turvamiseks.

1. Kasuta VPNi ehk privaatvõrku.
2. Luba ühendus vaid kindlatelt IP-aadressidelt.
3. Kasuta kaheastmelist autentimist.
4. Piira ebaõnnestunud autentimiskatsete hulka.
5. Uuenda tarkvara.
6. Kasuta turvalisi paroole ja uuenda neid regulaarselt.
7. Seadista ja jälgi logisid.
8. Seadista monitooring ja teavitused.

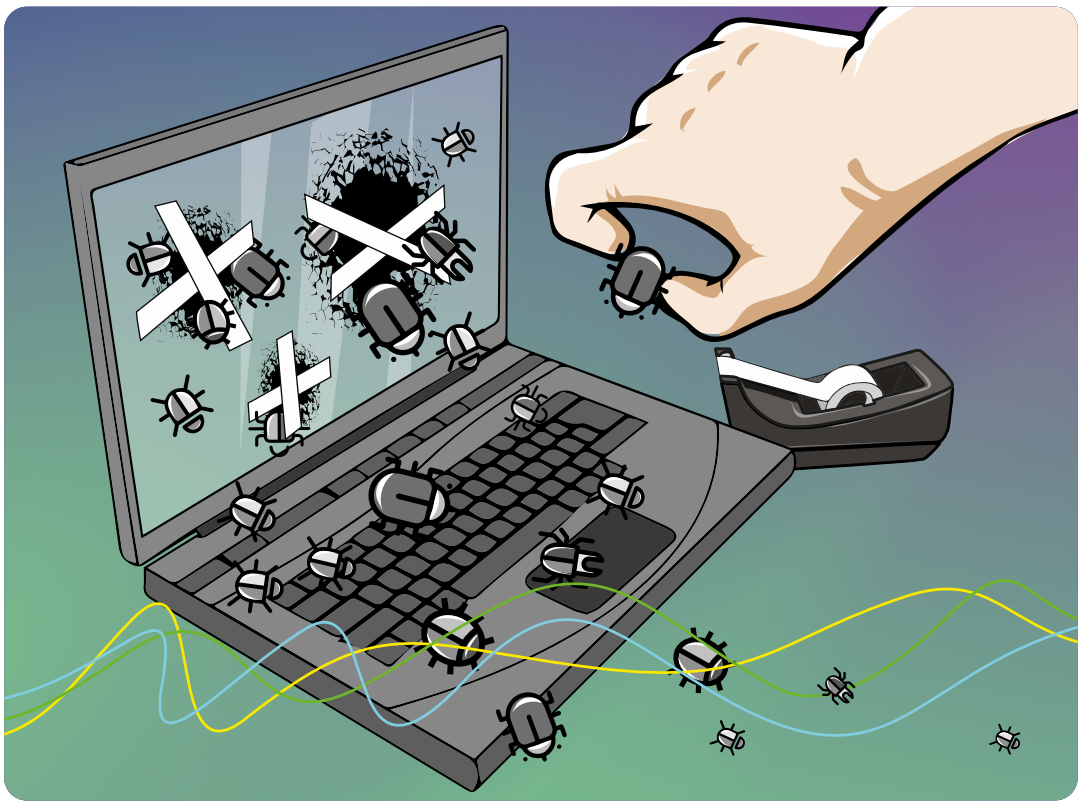
Samuti olid ettevõttes loodud paroolid liiga lühikesed ega sisaldanud piisavalt tähemärke või sümboleid. Selliste salasõnade murdmine on ründajale suhteliselt lihtne ning mitmed võimalikud näited eksisteerivad juba ründesõnastikes. Samuti polnud paroolidele kehtestatud aegumistähtaega. Pärast ligipääsu saamist krüpteeriti ettevõtte andmed Phobose-nimelise lunavaraga. Selline juhtum tuletab meelde, kui oluline on järgida küberhügieeni põhitõdesid.

Aasta teises pooles nägime võrdlemisi uue tulijana Royali-nimelist lunavara, mis tabas energiasektoris tegutsevat ettevõtet. Rünnaku käigus nakatusid nii ettevõtte tööjaamad kui ka serverid. Pahavara levik piirdus kontorivõrguga – tootmist ja lõpptarbijaid see ei mõjutanud.

Novembris ründasid kurjategijad Eesti ettevõtet, kes pakub teenuseid elutähtsa teenuse osutajatele. Tänu kiirele reageerimisele suudeti kõige mustem stsenaarium ära hoida ning ründaja ei jõudnud edasi ettevõtte koostööpartnerite süsteemidesse.

ÄRA MAKSA, VAID TEAVITA CERT-EEd

Paneme kõigile südamele, et lunavararünnaku korral ei tasu kurjategijatega koostööd teha. Lunaraha tasumine ei garanteeri andmete taastamist, küll aga annab see kurjategijatele indu juurde. Kui su ettevõte või asutus on lunavararünnaku ohvriks langenud, kirjuta **cert@cert.ee.**



Enam turvanõrkusi, VÄHEM MÕJU

Eelmisel aastal kasvas oluliselt turvanõrkuste tuvastamise, nende vastu võitlemise ja nendest teavitamise võimekus.

Esiteks algas 2022. aastal *bug bounty* programm. Selle kaudu anti CERT-EE-le Eesti organisatsioone ohustavatest haavatavustest senisest palju rohkem teada: kui 2021. aastal saatsime 1473 turvanõrkustega seotud teavitust, siis möödunud aastal 2634.

Teiseks rakendus riigivõrgu täiendav kaitsekiht, mis blokeeris sadu miljoneid rünnakukatseid. Sinna sisse loeme ka katsed leida turvanõrkusi ja neid ära kasutada.

Kolmandaks hakkas RIA alates septembrist avaldama regulaarseid ülevaateid nädala olulisematest turvanõrkustest, mis võivad mõjutada ka Eestit. Need avaldame iganädalaselt RIA blogis ja kodulehel.

Ehkki 2022. aasta ei pakkunud ründajatele sama palju kõlavaid turvanõrkusi kui 2021 (nt Log4Shell või Microsoft Exchange'i ProxyLogon ja ProxyShelli haavatavused), leiame möödunud aastast turvavigu, mille abil saanuks ründajad palju halba korda saata. Selliseid nõrkusi avastati näiteks Eestis laialdaselt kasutatavatest tarkvaradest nagu Magento, Confluence või Microsoft Exchange.

LIIGA AVATUD E-POED

Pärast koroonaperioodil tehtud rekordeid e-poodide kasutamine eestlaste seas 2022. aastal veidi langes, kuid oli siiski jätkuvalt populaarne. Veebruaris ja oktoobris avalikustati turvanõrkused Eestiski laialdaselt kasutatavas Magento e-kaubandusplatvormis. Need võimaldasid ründajatel Magento tarkvara kasutavad e-poed täielikult üle võtta ning paigaldada sinna näiteks pahavara või õngitsuslehe, mille abil e-poe klientide krediitkaardiandmeid varastada.

Kokku teavitas CERT-EE veebruaris ja oktoobris Magento turvanõrkustest mõjutatud veebilehtede omanikke või haldajaid 588 korral. Ühtegi konkreetset mõjuga intsidenti, mis just nende nõrkustega seotud oli, CERT-EE-le möödunud aastast teada pole.

LOG4J SUGULANE SPRING4SHELL

Aprillis avastati, et internetiavarustes liigub ringi uus ja esmapilgul kole haavatavus nimega **Spring4Shell**. Kas tagantjärele hinnates oli kartmiseks põhjust? Jah ja ei. Kõlava nimega haavatavus oli sarnaselt Log4Shelliga seotud Java programmeerimiskeele raamistikuga ja lubas ründajatel käivitada haavatavates süsteemides pahaloomulist koodi. Ohuks oli ka selle raamistiku suhteliselt laialdane kasutus erinevates rakendustes üle maailma. Seega oli loodud mitu eeldust tõsise mõjuga turvanõrkuseks.

RIA reageeris kohe ja hoiatas nii partnerasutusi kui ka avalikkust potentsiaalsetest mõjudest ning andis juhiseid, mida turvanõrkuse kõrvaldamiseks teha. Monitoorisime küberruumi ja kogusime infot rünnakukatsete kohta, kuid haavatavuse mõju jäi Eestis (ja ka maailmas) marginaalseks. RIA nägi, et seda küll püüti kuritarvitada, kuid ürituste hulk polnud kaugeltki võrreldav teiste turvanõrkuste ärakasutamiskatsetega.

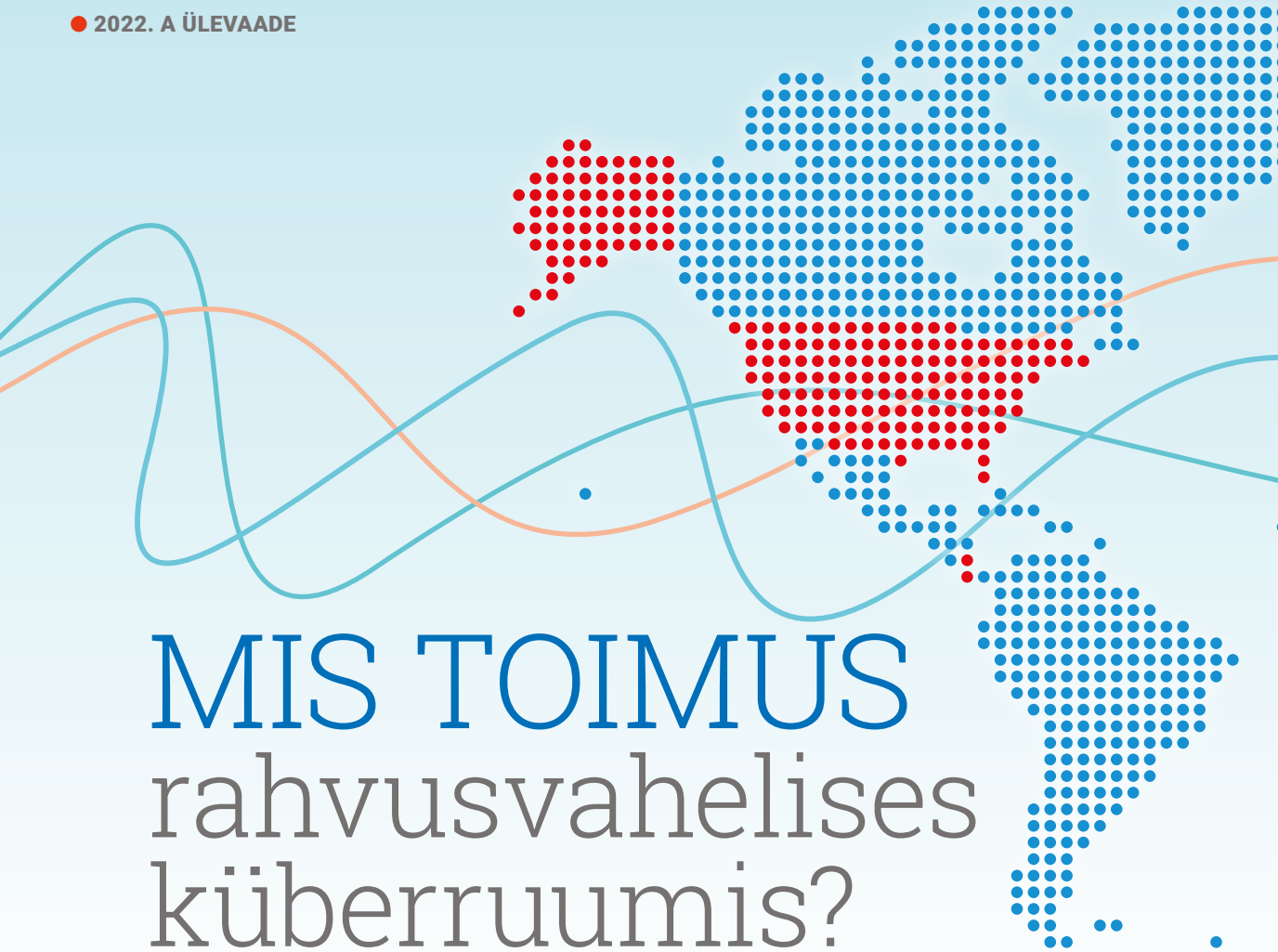
Tõenäoliselt ei jää Spring4Shell siiski unustuste hõlma, kuna uus robotvõrgustik Zerobot on turvanõrkuse enda arsenali võtnud.

VANA TUTTAV CONFLUENCE

Juunis teavitas Atlassian, et nende pakutavas siseveebitarkvaras Confluence on kriitiline haavatavus. Confluence'ist ei kuule RIA aastaraamatute lugeja esimest korda, sest ka 2021. aastal kirjutasime sama tarkvara mõjutanud kriitilisest haavatavusest. Kuna seda kasutatakse Eestis suhteliselt laialdaselt, on iga seda puudutav kriitiline haavatavus ka potentsiaalne sütikpomm siin tegutsevatele organisatsioonidele.

Turvanõrkust kasutati maailmas krüptoraha kaevandamiseks ja seda oli võimalik kuritarvitada tervete süsteemide ülevõtmiseks või lunavararünnakuteks. Eestit puudutas nõrkus õnneks minimaalselt. RIA-le teadaolevalt õnnestus ründajatel turvaviga ära kasutada vaid ühel juhul, kui rünnati edukalt üht finantsettevõtet. Selle intsidendi puhul õnnestus haavatav süsteem kompromiteerida kõigest paar tundi pärast nõrkuse avalikuks tulekut. Ehkki intsident möödus suuremate tagajärgedeta, ilmestab see, kui kiiresti tänapäeval haavatavaid süsteeme leitakse ja rünnatakse. ●

Selle intsidendi puhul õnnestus haavatav süsteem kompromiteerida kõigest paar tundi pärast nõrkuse avalikuks tulekut.



MIS TOIMUS rahvusvahelises küberruumis?

2022. aastal andsid rahvusvahelisele küberruumile tooni arengud seoses Venemaa invasiooniga Ukrainasse, ent oma tavapärast tegevust jätkasid küberkurjategijad ja riikide küberrühmitused ka mujal.

Suvel tabasid **Albaaniat** kaks mõjukat küberrünnete lainet. Juulis olid tundideks rivist väljas riigiasutuste veebilehed ja e-teenused. Septembris olid sihtmärgiks politsei arvutisüsteemid, mistõttu tuli välja lülitada ka sadamate, lennujaamade ja piiripunktide arvutisüsteemid. Albaania sõnul olid mõlema ründe taga Iraani riikliku taustaga häkkerid. Esimesed ründed Albaania pihta tulid vahetult enne konverentsi „World Summit of Free Iran“, mida seostati Albaanias paikneva Iraani opositsioonilise grupiga. Päev enne konverentsi plaanitud algust lükati see terroriohu tõttu edasi.

Küberrünnakute järel katkestas Albaania Iraaniga diplomaatilised suhted. NATO liitlased väljendasid Albaaniaga solidaarsust ja mõistsid hukka pahatahtlikud küberründed riigi kriitilise taristu pihta, solidaarsust väljendas ka Euroopa Liit.

Pretsedenditu küberrünnakuga sai suvel pihta ka Albaania naabri **Montenegro** digitaalne taristu. Riiki tabasid nii teenusetõkestusrünnakud (DDoS) kui ka lunavara, lüües rivist välja

paljud kriitilised teenused (sh transpordi- ja veeteenused), näiteks lülitati riigi elektrivõrk ümber manuaalsele režiimile. Kui esialgu teatasid Montenegro ametnikud, et rünnete taga on Vene eriteenistused, siis hiljem võttis vastutuse Cuba lunavara kasutav kuritegelik küberrühmitus. Cuba lunavararühmitus pole erinevate kübereekspertide sõnul seotud Kuubaga, vaid sellega toimetavad venekeelsed inimesed.

Märkimisväärne oli ka **Costa Rica** intsident, kus kuulutati riigi süsteeme ja teenuseid tabanud lunavararünnakute tõttu välja eriolukord. Rünnakute eest võttis vastutuse lunavararühmitus Conti, mis nõudis Costa Ricalt kümme miljonit dollarit dekrüpteerimisvõtme eest. Raha ei makstud, süsteeme üritati teisiti taastada, kuid ka veel kuu aega hiljem olid rahandusministeeriumi, maksu- ja tolliameti, sotsiaalkindlustusameti ning mitme teise asutuse teenused häiritud.

Riigi digiteenuste katkestused mõjutasid arusaadavalt ka erasektori tööd. Näiteks tolliametis oli impordi ja ekspordi deklareerimine rivist väljas ja piiridel vormistati dokumente käsitsi. See võttis tavapärasest märkimisväärselt rohkem aega ja toidukaubad riknesid pika ootamise tõttu. Riigis välja kuulutatud eriolukord andis valitsusele paremad hoovad kriisis tegutsemiseks.

KÜBERKURJATEGIJAD JAHTISID EUROOPA ETTEVÕTTEID JA ASUTUSI

Kuritegelikud küberrühmitused sihtisid möödunud aastal aktiivselt olulisi ettevõtteid, haiglaid, haridusasutusi, kohalikke omavalitsusi ja muid organisatsioone üle maailma. Üks aktiivsemaid oli **BlackCat**, mille lunavararünnakud tekitasid rahalist kahju ja ebamugavust mitmel pool **Euroopas**. Näiteks veebruari alguses võttis rühmitus vastutuse **Saksamaa** naftatoode-

→

te, kemikaalide ja gaasiterminalide ettevõtte Oiltanking ründamise eest. Ründe tõttu oli häiritud ettevõtte IT- ja laadimissüsteemide töö, pihta sai ka samasse gruppi kuuluv nafta ladustamise ja tarnega tegelev ettevõte Mabanaf. Ettevõtete teenuseid kasutab ka kütusefirma Shell, mis pidi tõrgete tõttu alternatiivsele tarneahelale ümber lülituma.

Sihtmärgiks oli ka avalik sektor, näiteks rünnati **Austria** Kärnteni liidumaa süsteeme. Avaliku info kohaselt oli rivist väljas liidumaa veebileht ja e-postisüsteem, lisaks ei saanud administratsioon väljastada passe ega liiklustrahve. Kurjategijad nõudsid dekrüpteerimisvõtme eest viis miljonit dollarit, ent liidumaa teatel seda ei makstud.

Ka teiste Euroopa riikide kohalikud omavalitsused sattusid küberkurjategijate ohvriks. Näiteks **Belgia** Antwerpeni linna süsteemid olid rivist väljas, sest linnale IT-teenust osutanud ettevõtet tabas lunavara. Häiritud olid linna teenused elanikele, koolidele, lasteaedadele ja politseile. Probleeme oli ka osa telefoniliinide ja e-postisüsteemiga. Teiste hulgas olid mõjutatud eakate hooldekodud, kus polnud võimalik kasutada tarkvara, mis aitab järge hoida, kes ja mis ravimit peaks saama. Nii pidid 18 hooldekodu appi võtma paberi ja pliiatsi.

LUNAVARA SUNDIS HAIGLAID PATSIENTE MUJALE SUUNAMA

Mitu **Prantsusmaa** haiglat sai möödunud aastal tunda küberrünnakute mõju. Augustis tabas lunavara tuhande voodikohaga haiglat Center Hospitalier Sud Francilien (CHSF), mille äritarkvara, salvestussüsteemid ja patsientide vastuvõtuga seotud infosüsteemid olid seetõttu rivist väljas. Erakorralise meditsiini ja radioloogiateenuseid vajanud patsiendid saadeti piirkonna teistesse haiglatesse. Tehnoloogilisest katkestusest olid mõjutatud ka operatsioonisaalid.

Paar kuud hiljem pidi teine Prantsuse haigla Versailles' küberrünnaku tõttu ära jätma operatsioone ja saatma patsiente teistesse haiglatesse. Rivist väljas olid nii haigla telefoniliinid, internet kui ka arvutisüsteemid. Intensiivravisse pidi kutsuma lisatööjõudu, sest ehkki seal olevad masinad töötasid, puudus neil võrguühendus ja seepärast pidi neid rohkem jälgima. Prantsuse terviseministri sõnul pidi küberrünnaku tõttu pea kogu haigla töö reorganiseerima. Kurjategijad nõudsid haiglalt süsteemide dekrüpteerimise eest lunaraha, ent seda ei makstud.

PROTESTID IRAANIS PANID HÄKTIVISTID TEGUTSEMA

Läänemeelsed häktivistid Anonymouse rühmitusest olid mullu poliitiliselt aktiivsed mitmel pool maailmas. Näiteks reaktsiooniks 22-aastase iraanlase Mahsa Amini surmale algatati operatsioon nimega OpIran. Iraani politsei arreteeris Amini hijabi väidetavalt valesti kandmise eest. Jaoskonnas ta suri, politsei väitel südamerikke tõttu. Juhtunu järel hakkasid paljud iraanlased võimude vastu meelt avaldama.

Anonymouse OpIrani kampaania käigus rünnati Iraani valitsuse veebilehti, sealhulgas Iraani luure ja politsei omi. Lisaks lekitasid häktivistid tundlikku infot, näiteks ametnike telefoninumbreid, e-kirju ja kaarte tundliku infoga.

Iraani aatomiagentuur teatas, et „võõra riigi heaks" töötavad häkkerid murdsid sisse nende filiaali võrku ja said ligipääsu e-postisüsteemile. Rünnaku eest võttis vastutuse vähetuntud häkkerirühmitus nimega Black Reward, kes nõudis Teheranilt „lunarahaks" poliitiliste vangide vabastamist. Oma sõnul lekitasid häkkerid 50 GB andmeid, sh sisemisi kirjavahetusi, lepingud ja Iraani Būshehri tuumajaama ehituskavandeid.

Protestide tõttu asus riigivõim võrguliiklust piirama. Reaktsioonina sellele hakkasid häktivistid Iraani meeleavaldajatele Telegramis, Signalis ja tumeveebis jagama tööriistu ja nõuandeid riigi kehtestatud internetitsensuurist pääsemiseks, sealhulgas pakuti proxy- ja VPN-servereid.

ANDMELEKKED PANID SEADUST MUUTMA

Möödunud aasta mõjus küberturvalisuse vaates äratuskellana **Austraaliale**. Nimelt teatas sügisel Austraalia suuruselt teine telekomiettevõte Optus, et küberründe tõttu on neilt varastatud ligi kümne miljoni kliendi andmed. Ettevõtte teatel lekkisid praeguste ja endiste klienti-

de andmed, sh nimed, sünnikuupäevad, koduaadressid, telefoninumbrid, e-posti aadressid, passi- ja juhiloanumbrid. Väidetav ründaja avaldas internetis näidised varastatud andmetest ja küsis ülejäänu lekitamata jätmise eest miljoni dollari väärtuses krüptoraha. Mõni päev hiljem avaldas häkker üle 10 000 inimese andmed, kuid ootamatu pöördena kustutas need peagi, loobus lunarahanõudest ning vabandas Optuse ees. Optus ei maksnud häkkerile, vaid tegi koostööd õiguskaitseorganitega.

Mõni nädal pärast Optuse leket teatas ka Austraalia tervisekindlustust pakkuv ettevõte Medibank, et hiljuti nende vastu korraldatud lunavararünnakus pääsesid häkkerid ligi kõigi, s.o 2,8 miljoni kliendi isiku- ja terviseandmetele. Kuna Medibank ei maksnud rühmitusele lunaraha, hakkasid kurjategijad varastatud tervise- ja isikuandmeid avalikustama. Austraalia politsei (AFP) teatel identifitseerisid nad koostöös Interpoliga häkkerid ja tegemist olnud Vene küberkurjategijatega.

Nende juhtumite ajendil hakkas Austraalia riigi küberturvalisus- ja andmekaitseseaduseid karmistama, näiteks tõusid märkimisväärselt trahvid ettevõtetele andmelekete eest.

EUROOPA KÜBERPOLIITIKA TEGI MITU EDUSAMMU

Möödunud aasta tõi Euroopa Liidu küberpoliitikas märkimisväärseid arenguid, mis mõjutavad lähiaastatel otseselt ka Eestit. Näiteks võtsid Euroopa Liidu liikmesriigid vastu uue võrgu- ja infoturbe direktiivi ehk nn küberturvalisuse direktiivi (lühend NIS 2.0). Uus direktiiv katab võrreldes praegu kehtivaga (nn NIS 1.0) rohkem sektoreid, mis on majanduse ja ühiskonna toimimise jaoks kriitilised ning peaksid oma küberturbesse panustama.

Lisandunud on näiteks jäätmekäitlus, posti- ja kulleriteenused, kosmosetööstus, keemiatööstus, elektriautode laadimispunktid, avalik sektor ja veel mitmed. Lisaks uutele nn kriitilistele sektoritele hakkavad NIS 2.0 direktiiviga selle kohuslastele kehtima senisest rangemad küberturvalisuse nõuded, suurenevad riikliku järelevalve hoovad, tõhustatakse rahvusvahelist koostööd ja palju muud.

Teine märkimisväärne areng Euroopa Liidu küberpoliitikas oli see, et alustati läbirääkimisi küberkerksuse õigusakti üle, mille mõjul peaksid tulevikus eurooplaste nutividinad turvalisemaks muutuma. Uue ettepaneku järgi peaksid kõik nii ELis toodetud kui ka siin müüdavad digitooted – tarkvara ja riistvara – vastama teatud kõrgetele küberturvalisuse nõuetele. See hõlmaks pea kõiki digitooteid, sh arvuteid, nutitelefone, nutikellasid, laste mänguasju jpm. ●

NOPPEID piiri tagant

- **Uber** langes küberrünnaku ohvriks. 18-aastane häkker pääses ligi Uberi sisesüsteemidele ja seal olevatele dokumentidele, sh turvanõrkuste raportitele. Ründaja olevat kasutanud Uberi Slacki keskkonda, et töötajatele ettevõtte häkkimisest teada anda.
- **Taani** suurim rongioperaator DSB pidi küberründe tõttu rongliikluse mõneks tunniks peatama. Rünne tabas DSB IT-teenusepakkujat Supeo, mis oli sunnitud oma serverid välja lülitama ja seetõttu ei saanud kasutada rongide juhtimiseks mõeldud tarkvara.
- **Saksa** ajalehe Heilbronn Stimme trükiversioon jäi neli päeva ilmumata, sest meediagrupi trükikoda tabas lunavararünnak. Väljaande IT-juhi sõnul päästis neid hullemast hea varundamisstrateegia, tänu millele õnnestus tootmiskriitilised süsteemid suhteliselt kiiresti taastada.
- **Hollandis** oli küberründe tõttu 120 hambaravipraksise töö päevadeks häiritud. Rünne tabas ettevõtet Colosseum Dental Benelux, millel on Belgias ja Hollandis kokku 130 haru.
- **USA** meediaettevõte News Corp langes küberrünnaku ohvriks, mille tulemusel said väidetavalt Hiina häkkerid ligi ajakirjanike ja teiste töötajate e-kirjadele ning Google Docsi materjalidele, sh artiklite mustanditele. Ettevõttele kuuluvad mitmed väljaanded, nt The Wall Street Journal ja New York Post.

TELIA: küberohud üha kasvavad

Küberohtude arv ja keerukus on üha kasvanud. Oma panuse on sellesse andnud nii epideemia-aastad kui ka poliitilised pinged ja sõda Ukrainas, kirjutab Telia turbevaldkonna juht **Aigar Käis.**

Mullusele aastale tagasi vaadates võime öelda, et targemaks said nii ründajad kui kaitsjad. Küberkuritegevus arenes jõudsalt edasi, kuid samas suutsime sellega ka järjest paremini toime tulla ning rünnakuid tõrjuda. Saime palju väärtuslikke õppetunde, mida aluseks võttes 2023. aastal oma klientide kaitsevõimet tugevdada.

Foto: Telia

Aigar Käis

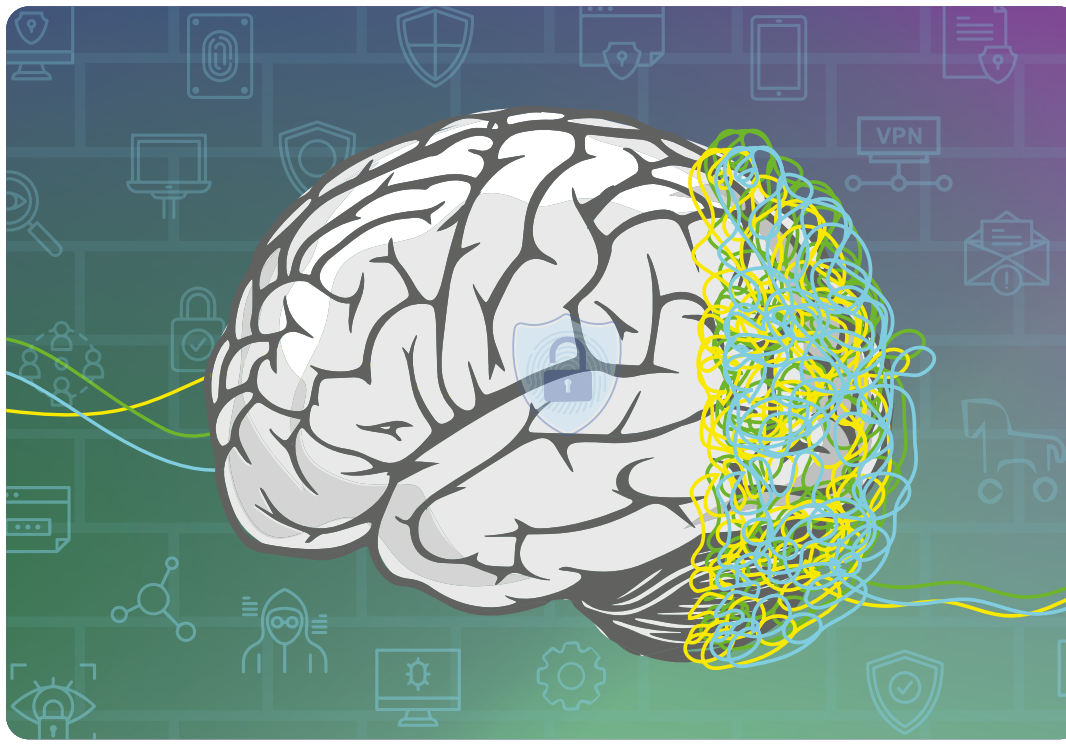
VÄIKEETTEVÕTTED ON KÜBERRUUMIS HAAVATAVAMAD

Ettevõtete vaates oli 2022. aasta üheks peamiseks märksõnaks teenusetõkestusrünnakute (DDoS) arvu oluline kasv. Sageli saatsid need rünnakud poliitilisi otsuseid ja samme. Näiteks Soome ja Rootsi otsus liituda NATOga tõi kaasa massiivse rünnakulaine nende riikide suunas, samamoodi kasvas küberkuritegevus vastusena otsustele teisaldada Narvast tank, lõpetada Vene telekanalite edastamine jpm.

Paraku näeme 2023. aastal sama trendi jätkumist – kurjategijad lihvivad ja mitmekesistavad oma tööriistakasti ning poliitiliselt ebastabiilne olukord ja sellega seotud sammud mõjutavad rünnakute intensiivsust ka edaspidi.

DDoS-rünnakud on enamasti sihitud suuremate riigi- ja eraettevõtete pihta, kelle teenuse halvamine tekitab kiire ja nähtava efekti. Lisaks nendele toimub ettevõtete suunal ka massiliselt automatiseeritud rünnakuid. Nende puhul ei lähtu kurjategijad ettevõtte suurusest – selliste rünnakute eesmärk on otsida turvaauke, mille kaudu saaks ettevõtte süsteemidesse siseneda.

Kuna suurte ettevõtete puhul on kaitsevõimekus sageli parem, on väikeettevõtted küberkurjategijate jaoks nii mõnigi kord lihtsam ja tulusam saak. Kui nn kalastamine õnnestub, järgneb enamasti pahavara paigaldamine ja lunarahanõue.



Selleks et kurjategijaid eemal hoida, tuleks hoolitseda kõigepealt selle eest, et ettevõtte võrk oleks kaitstud, ent oluline on kaitsta ka ettevõtte seadmeid. Kuna väga paljud töökohad pole enam paiksed ning tööd tehakse kontori turvalisest võrgust väljaspool, on kindlasti vaja arvutitesse ja nutiseadmetesse paigaldada ka kaasaegne viirusetõrje. Ning teadvustada, et hoolimata sellest, kui võimas turvalahendus kasutusel on, jääb ikkagi inimene nõrgimaks lüliks kogu ahelas. Teisisõnu: töötajate teadlikkuse kasvatamisel on küberriskide maandamises võtmeroll.

MENTAALSE TULEMÜÜRI TÄHTSUS

Ka eraisikuid ohustavate küberkuritegude ja -rünnakute foon on jätkuvalt kõrge. Siia nimistusse kuuluvad libakõned ehk nn kõnefarmid, samuti kõikvõimalikud kirjade ja sõnumite teel levitatavad petukampaaniad jpm.

Parim kaitse ja soovitus on ehitada endale mentaalne tulemüür – kasuks tulevad teadlikkuse kasvatamine, kriitiline meel, oskus eristada valet õigest ning „mõtle, enne kui tegutsed“ lähenemine. Seejuures tuleks hoolikas olla ka seadmete valikul. Eelistada tuleks tootjaid, kes panustavad oma seadmete turvalisusse, ning jälgida, et seadmel oleks toimiv regulaarne turvauuenduste tsükkel.

> Parim kaitse ja soovitus on ehitada endale mentaalne tulemüür.

Meid ümbritsev kübermaailm muutub üha keerukamaks. Peame aktiivselt tegelema teadlikkuse kasvatamisega nii ettevõtete kui eraisikute seas. Samuti on igal ettevõttel oluline leida endale kompetentne partner, kes aitab küberriskid välja selgitada ning luua ennetavaid ja paindlikke lahendusi, sest igal ettevõttel ja ka igal ründel on oma spetsiifika, mida tuleb arvesse võtta. Investeeringud küberturvalisusse tasuvad end kindlasti ära ning peavad eelolevatel aastatel aina kasvama.

Läbivalt küberturvaline EESTI

Selleks et luua läbivalt küberturvaline Eesti, mis peab vastu tehnoloogia arengutele ja võimalikele ohtudele, peame tegema koostööd, kirjutab majandus ja kommunikatsiooniministeeriumi riikliku küberturvalisuse juht / osakonna juhataja **Liisa Past**.

2023. aastal ei saa rääkida küberturvalisusest ilma 2022. aasta sündmusteta, millest määrav oli Venemaa Föderatsiooni täiemahuline invasioon Ukrainasse. Muutunud ohupilt nõudis kiiret reageerimist nii organisatsioonide infoturbe kui ka riigi julgeoleku osas. RIA panustas märkimisväärselt, et küberrünnakute mõju Eesti inimestele ja infosüsteemidele oleks minimaalne. Näiteks peatati massilised teenusetõkestusrünnakud suuresti enne, kui need saanuks kahju teha.


Foto: Kristi Sits

Liisa Past

2023 on loodetavasti kodu korrastamise aasta. Eelmisest saime kaasa õppetunnid, kuidas korraldada parimat võimalikku küberturvet ning kuidas ka kõige raskematel hetkedel suutis Ukraina oma infosüsteeme kaitsta ja e-teenused töös hoida. Riikliku küberturvalisuse korraldamisel küsime endilt, millisteks ohtudeks ja stsenaariumideks peame valmis olema ning kuidas kaitseme nende realiseerumise korral oma ühiskonda – inimesi, teenuseid, infosüsteeme ja kõike nende jaoks vajalikku.

Meie eesmärk on läbivalt küberturvaline Eesti, mis peab võimalikult hästi ja paindlikult vastu tehnoloogia arengutele ning võimalikele ohtudele. Sel aastal tahame kokku leppida ja vastu võtta riikliku küberturvalisuse strateegia aastateks 2023–2027, et sõidusuund enda kaitsmiseks oleks selge.

IGA RUUT LOEB

Ühiskonna küberturvalisus on nagu lapitekk, mis koosneb paljudest ruudukestest: asutuse või ettevõtte enda turbemeetmed, keskselt pakutavad kaitselahendused, nõuded ja normid, ohtudest teadlikud ja IT-vaatlikud lõppkasutajad. Eraldivõetuna ei taga ükski neist piisavat kaitset, aga koos moodustavad kilbi, millest läbitungimine on keeruline.

See lähenemine tähendab, et küberturvalise Eesti saavutamisel on vastutus kõigil IT- ja digiteenuste pakkujatel, neil, kes sellistest teenustest sõltuvad, ja riigil keskselt. Kogu-ühiskonna-lähenemine eeldab kõigi osapoolte panustamist.

Sealjuures on mitu asja mõistlik korraldada keskselt. .ee domeeni seire on koondunud RIAsse CERTi. Samuti on keskne infoturbestandard E-ITS ja mitmed teenused. RIA, RITi ja teiste IT-majade kesksetes teenustes on infoturbe osa sisse ehitatud ja neid pole võimalik pakkuda ega tellida selleta. Riigi IT arendusmudelis on läbivalt võtmeroll ka infoturbel.

Kuid iga teenusepakkuja peab oma teenuste ja süsteemide eest ise vastutama. Riskid peavad olema juhitud ning turvalisus osa teenuste ja süsteemide disainist. Turvalisus pole omaette eesmärk, vaid vahend. Selleta kaob usaldus ja usalduseta kaob teenus.

KINDEL EBAKINDLUS

Me ei tea, milline on meid ümbritsev tehnoloogia viie või kümne aasta pärast, aga panustame, et Eesti ühiskond oleks tulevikuarenguteks ja -ohtudeks valmis ning meie e-teenused ja keskkond püsiks turvalised. Muu hulgas tähendab see järjepidevat tööd pärandvarast vabanemiseks ja paindlikumatele IT-toimemudelitele üleminekut. Vaatame üle ka kehtivaid norme, et need toetaks nüüdisaegsete tehnoloogiate rakendamist ja küberturvalisema keskkonna loomist.

> Turvalisus pole omaette eesmärk, **vaid vahend.**

Riigi küberturvamise või ükskõik millise süsteemi infoturbe korraldamise eeldus on aga koostöö. Majandus- ja kommunikatsiooniministeeriumi riikliku küberturvalisuse meeskonna jaoks tähendab see ennekõike, et kõike eelkirjeldatut teeme koostöös ja koostöiselt, kaasates ja konsulteerides. Olenemata sellest, milliseks kujuneb 2023. aasta geopoliitikas ja tehnoloogia arengus, on Eesti inimesed küberohtude eest kõige paremini kaitstud koos. Seega palun olla avatud kutsetele tulla arutlema, kaasa mõtlema ja koos Eestit turvalisemaks tegema.

SIGA, KÄGU ja küberturvalisuse seadus

Küberturvalisus ja migratsioon on esmapilgul kauged kui siga ja kägu. Vene agressioon Ukrainas on aga toonud hulga ebameeldivaid õppetunde, mis sunnivad neid kahte riiklikes riskianalüüsides edaspidi ühte peatükki toppima, kirjutab Frontexi peadirektori asetäitja **Uku Särekanno**.

Rünnates elutähtsaid teenuseid ja e-ühiskonna toimepidevust, on eesmärgiks külvata segadust ning vähendada vastupanuvõimet. See on süsteemne osa nii ettevalmistavast kui ka toetavast tegevusest kineetilisele sõjapidamisele. Odav vahend, mille kasutamise saab mugavalt delegeerida kuritegelikele ühendustele, pestes ise avalikult käed vastutusest puhtaks. Rünnaku alla sattunud riik on sunnitud suurema kriisi korral kasutama meetmeid, mis tekitavad demokraatlikus õigusriigis teravat avalikku kriitikat.

Foto: Arno Mikkor

Uku Särekanno

MIS JUHTUS SEAL...

2021. aasta suvel hakkasid korraga sajad migrandid Valgevene kaudu ebaseaduslikult Leetu saabuma. Kehtestati eriolukord ning suve lõpuks oli Leetu saabunud üle 4000 sisserändaja. Kohalikud omavalitsused olid saabujate majutamisega tõsistes raskustes. Kõike sooviti ja prooviti teha kehtivate reeglite järgi. Neid on hulgi: alustades õigusest varjupaigale ja lõpetades nõuetega kinnipidamiskeskustele.

Polnud kahtlust, et Leedu-suunaline rändevoog oli korraldatud tahtlikult ja sedapuhku mitte üksnes inimkaubitsejate abil. Seda kinnitasid kriisi harjal rahvusvahelisse meediasse jõudnud Frontexi filmitud kaadrid, mis näitasid Valgevene ametnikke vedamas piirile kolmandate riikide kodanikke. Kogu ettevõtmine oli Lukašenka režiimi orkestreeritud julgeolekuoperatsioon.

Leedu tegi, mis suutis. Piir pandi kinni, selle valvet tugevdati ja juurdepääs rahvusvahelisele kaitsele jäi oluliselt piiratumaks. Vähem kui pooleteise kuuga võimendus kriis Poola suunal, eskaleerudes 2021. aasta detsembris.

... KORDUB SIIN

Paralleel küberturvalisusega on ilmne, kuna tegutsejate *modus operandi* on sarnane. Ei saa välistada, et ka tegijad ja niiditõmbajad ühtivad. Valgevene on seni olnud üks vähestest, kes on avalikult teatanud, et kasutab rännet poliitilise surve avaldamiseks. Jah, varasemalt on

sarnaseid avaldusi teinud ka teised diktaatorid, ent Leedu ja Poola vastu suunatud kampaania oli olemuselt midagi uut ja üsna toorest. Pole saladus, et kogu selle ürituse läbiviimiseks kasutati taas kombinatsiooni organiseeritud kuritegevuse ja julgeolekuasutuste koostööst.

Eesti vaates on vaid aja küsimus, mil Leedus ja Poolas nähtu kordub meil. Selleks tuleb valmis olla nii õiguslikus kui ka operatiivses vaates. Vene piiri valvab FSB. Asutus, mis on KGB järeltulija ja raporteerib otse presidendi administratsioonile. Kui paar tuhat sisserändajat ilmub Eesti rohelisele piirile, on tegemist julgeolekuoperatsiooniga, kui just põgenikeks pole sündmuste eskaleerudes venelased ise või ukrainlased. Sellise operatsiooni tõkestamine eeldab väga kiiret ja resoluutset tegutsemist, mis tähendab mitmete tavapäraste õiguste peatamist või piiramist.

Eesti on töötanud välja õigusliku raamistiku stsenaariumiks, kus rännet kasutatakse riigi vastu relvana. Sarnaselt Leeduga lähenetakse olukorrale julgeoleku vaatest, mis on suuresti meie endi ainupädevus. Eesti harjutab ka koostööd Frontexiga, mis on oluline just selleks, et kriisis reageerida ühiselt ja Euroopa lipu all. Viisil, et toimuv ei oleks Euroopa avalikkuse jaoks ainult meie, vaid kogu Euroopa probleem. Et suudetaks kiirelt toimetada tõendite, vastumeetmete ja hübriidrünnaku omistamisega.

KUIDAS SEOSTUB SEE KÜBERTURVALISUSEGA?

Sarnaselt rändega tuleks teha värske mõtteharjutus küberturvalisust puudutava seadusandluse teemal. Hinnata, kas viis aastat tagasi vastu võetud küberturvalisuse seadus on hübriidsõja kontekstis piisav, kas selles kirjeldatud meetmed ja RIA roll arvestavad uut julgeolekuolukorda.

Rände puhul on meil erimeetmed, siseturvalisuse asutuste operatiivvõimekus ja Frontexi tugi. Loodetavasti on ka Euroopa riikide selge arusaam, et välispiiril toimuv mõjutab vahetult kõiki, sest Schengenis sisepiire pole.

Sarnane on konstruktsioon ka küberturvalisuse puhul – erimeetmed, operatiivvõimekus ja ühise vastutuse ehitamine samameelsetega. Oluline, et me ei jääks kriisis üksi, omistaks kiirelt ja veenvalt, näitaks – sarnaselt Leedu rändekriisiga –, et ka küberründe korral on tegemist rünnakuga kogu Euroopa vastu.

Kirjutis väljendab autori isiklikke vaateid.

CERT-EE uued vahendid kaitsevad Eesti küberruumi

Eelmisel aastal astusime mitu olulist sammu Eesti küberruumi turvalisuse parandamiseks: riigivõrk sai täiendava kaitsekihi, rakendasime täiendavad meetmed ummistusrünnete vastu ja jälgime senisest aktiivsemalt tumeveebis toimuvat.

Juba aastaid kasutab suur osa Eesti avalikust sektorist – ministeeriumid, paljud allasutused ja kohalikud omavalitsused – riigivõrku, mis pakub kiiret ja turvalist andmesidet. Riigivõrgu juurde kuulub ka Eesti interneti sõlmpunkt (RTIX), mis võimaldab riigisisest andmeliiklust vahetada otse sideteenuse pakkujate vahel.

2022. aastal läbis RTIX uuenduskuuri ehk nüüdisajastati seadmed ja arhitektuur, mille tulemusel paranes andmevahetuse töökindlus ja kiirus. Ühtlasi vähenes võimalus pahatahtlikuks sekkumiseks Eesti-sisesesse internetiliiklusesse.

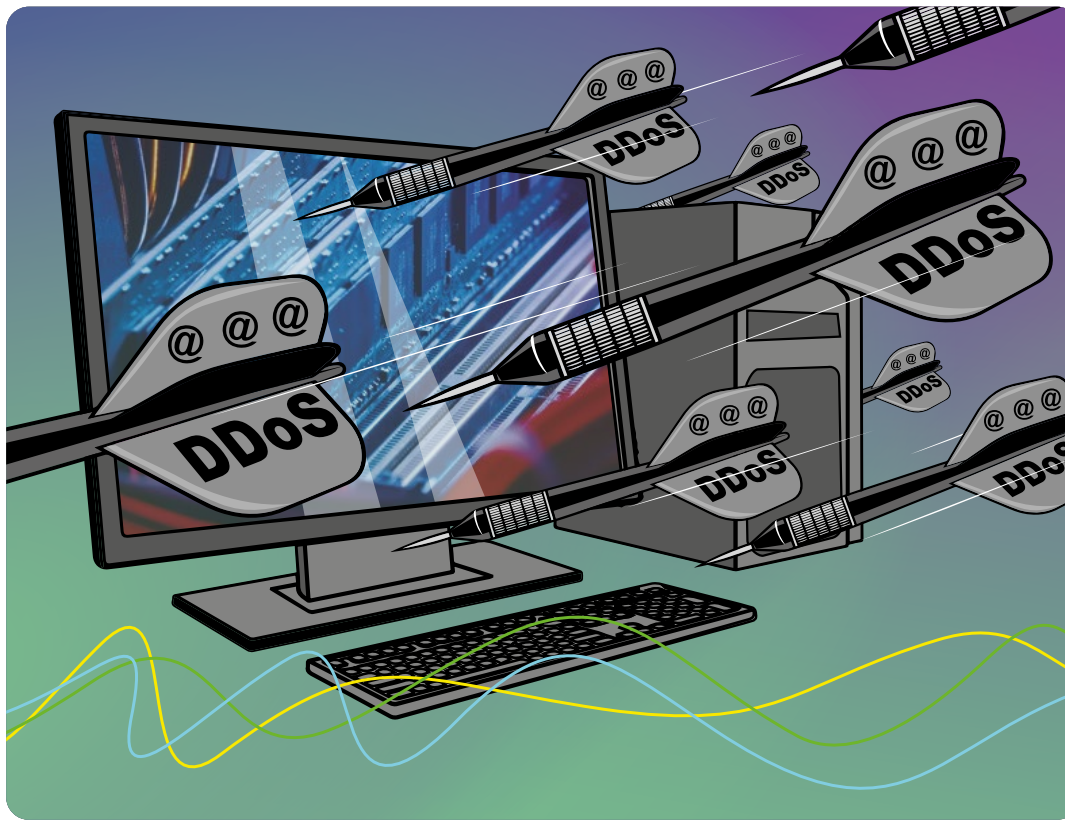
RIIGIVÕRK MUUTUS TURVALISEMAKS

Kuna riigivõrku haldab RIA, on CERT-EE-l võimalik tuvastada riigivõrgu suunas tehtavaid rünnakukatseid ning kõikvõimalikku pahavara, mida riigivõrgu klientidele üritatakse sokutada. 2022. aasta veebruaris rakendas RIA kõigile riigivõrgu kasutajatele veel täiendava turbekihi, mis pakub senisest tõhusamat kaitset rünnete eest, muutmata ühendust aeglasemaks.

Loodud turvafilter tuvastab võimalikud ohud ja tõkestab rünnakukatsed enne, kui need lõppkasutajani jõuavad – selliseid ära hoitud rünnakukatseid, tõkestatud ohte või nõrkuste kuritarvitamise üritusi on iga kuu miljoneid. Tavamaailma analoogiat kasutades on see justkui nähtamatu filter elutoa akna ees, mis takistab igapäevaselt loendamatu hulga tolmu, saaste ja haigustekitajate jõudmist tuppa ning hoolitseb seega kõigi majaelanike tervise eest.

UMMISTUSRÜNNETE VASTU LISAKAITSE

Oleme nii aastaraamatutes kui teistes kirjutistes varem tõdenud, et nii nagu paljudes teistes valdkondades, toimub ka küberruumis pidev võidujooks ründajate ja kaitsjate vahel. Nii nagu erasektor, peab ka riik siin olema paindlik ja ettenägelik ning möödunud aastal see mitmel korral ka õnnestus.



2022. aastal tabasid mitmeid Eesti inimeste jaoks olulisi või sümboolse tähtsusega veebilehti teenusetõkestusrünnete laviinid, eesmärgiga need ajutiselt käigust maha võtta. Nendest enamik ei avaldanud aga mingit nähtavat mõju, sest veebilehtede ja teenuste omanikud olid sellisteks rünneteks valmistunud ja võtnud CERT-EE vahendusel kasutusele täiendava kaitsekihi. Ummistusründeid tehakse erineval moel, mistõttu peab ka kaitse olema mitmekülgne.

Tahtmata lugejat tehniliste detailidega koormata, jääb üle vaid tõdeda, et ehkki Eesti oli teatud tüüpi DDoS-rünnete arvu ja intensiivsuse poolest möödunud aastal mitmel korral maailma tipus, pidas kaitse üldjuhul vastu ja ründajate pingutused olid asjatud.

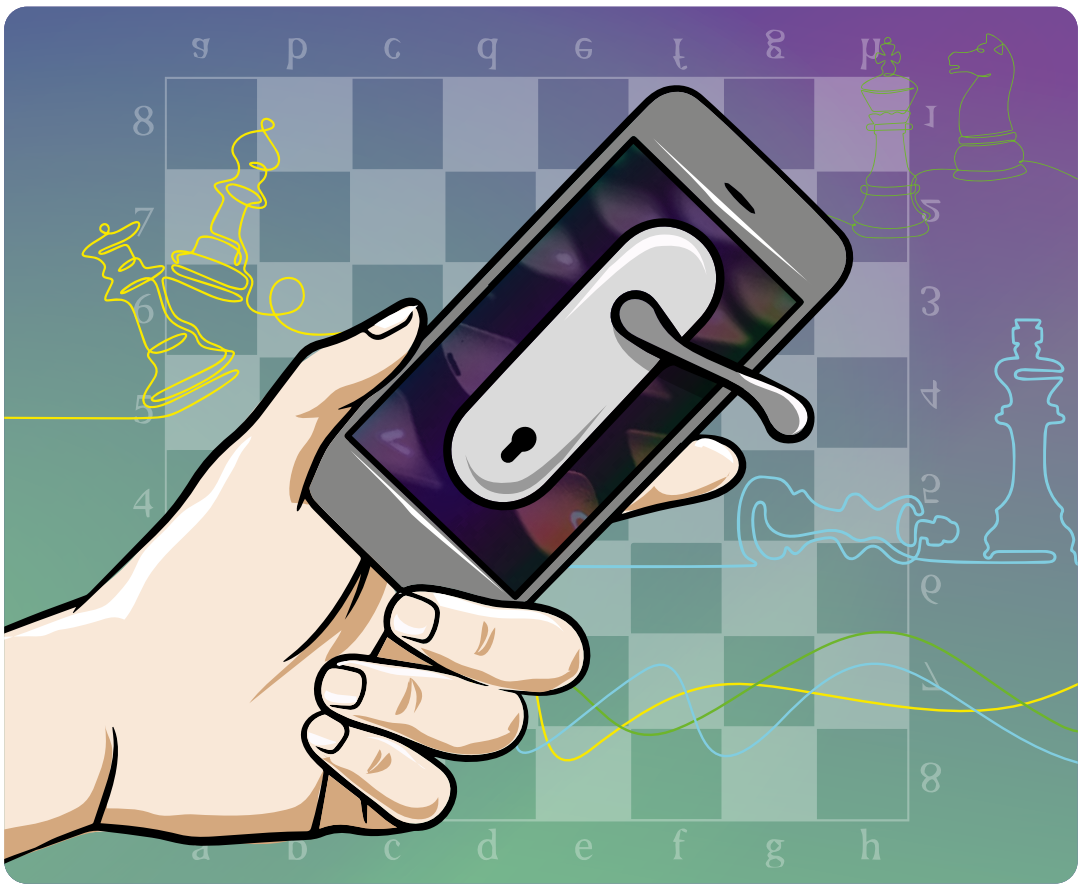
TUNNE OMA VASTAST

Tänapäevane küberturvalisus eeldab mitte ainult kaitsemüüride ehitamist, vaid kuigivõrd ka ründajate motivatsiooni, äriloogika ja neile kättesaadavate võimaluste tundmist. Mõistagi teeb RIA selles vallas koostööd eriteenistustega, ent ka meie enda vastavad võimed tegid lõppenud aastal läbi arenguhüppe.

> Ummistusründeid tehakse erineval moel, mistõttu peab ka kaitse olema mitmekülgne.

CERT-EE niinimetatud tagatoas töötavad inimesed, kes jälgivad tumeveebis toimuvat ning hoiavad end kursis ka häktivistide kogukonnas toimuvaga. Veelgi enam – CERT-EE koosseisus on nüüd lausa riiklikud häkkerid, kes aitavad RIA klientidel tuvastada ja parandada oma võrgus olevaid nõrkusi enne, kui seda teevad kurjategijad.

Kõlab intrigeerivalt? Kui jah, siis kirjuta **cert@cert.ee** ja uuri lähemalt.



RIA ukselinke lõgistades

RIA on teadaolevalt esimene Eesti riigiasutus, kes kutsub ise „küberpätte“ püsivalt oma ukselinke lõgistama.

Alates 2022. aasta kevadest on RIA-l püsiv lööktestimise ehk *continuous red teaming* (CRT) leping. See tähendab, et lepingupartner Clarified Security käib regulaarselt RIA ukselinke lõgistamas ja proovib RIA kaitsemüüridest läbi tungida.

Kasutades ehitusvaldkonna sõnavara, on klassikaline turvatestimine (*penetration testing*) võrreldav inspektori tegevusega, kes hindab, kas meie maja uksed ja aknad on turvalised, ning annab vajadusel nõu, kas ja kuhu on vaja panna lisalukke. Sama analoogiat kasutades

on lööktestimine võrreldav klassikalise kurjategija tegevusega. Teda ei huvita, et esimese korruse aknad ja uksed on turvaliselt lukustatud. Ta märkab teisel korrusel rõduakent, mille pererahvas on kas kogemata või teadlikult lahti jätnud, ning siirdub rõdu kaudu tubadesse väärtuslikku kraami otsima. Mida vaiksemalt, seda parem. Ehk kokkuvõtvalt: püsiva lööktestimise eesmärk on saada riskikohtadest tervikpilt ja see aitab meil omakorda RIAt paremini kaitsta.

Teadaolevalt on RIA Eesti esimene riigiasutus, kel on püsiva lööktestimise leping. CRT puhul eristatakse nelja meeskonda. *Red team* ehk punane meeskond otsib turvaauke ja -nõrkusi ning ründab. *Blue team* ehk sinine meeskond ennetab ja tõrjub rünnakuid. *Purple team* ehk huumoriga öeldes lavendlimeeskond on ründava ja kaitsva tiimi ühine meeskond, mis märkab reaalajas nõrkusi. *White team* ehk valge meeskond on sideohvitseri rollis ja lahendab n-ö jooksvaid probleeme.

ÜHISE KOOSTÖÖ FAAS

RIA ja Clarified Security on praegu ühise koostöö faasis ehk üritame koos ründajaga aru saada, kus on RIA haavatav. Me pole veel liikunud püsivasse ründeetappi, sest tahame olla kindlad, et meie küpsustase asutusena on selle vääriline.

Me pole veel liikunud püsivasse ründeetappi, sest tahame olla kindlad, et meie küpsustase asutusena on selle vääriline.

Laias laastus keskendub CRT konkreetsetele lõikudele, mis lepitakse omavahel eelnevalt kokku. Vastaspoolel on kindlad reeglid, mida nad järgivad. Toimetame sammhaaval eesmärgiga veenduda, et tegevused oleks seiratavad ja/või tõkestatud.

RIA ÕNGITSUS-kampaania

Seda, et piisab ainult ühest valest klikist ja vastane on sees, teab iga RIA töötaja une pealt. Sellepärast paneb RIA infoturbe osakond oma maja inimeste teadlikkuse tõstmisele suurt rõhku. 2022. aasta suvel korraldasid infoturve ja CERT-EE RIA töötajatele esimese suurema õngitsuskampaania, kus meelitati kolleege vajutama kahtlasel lingil.

Eesmärk polnud otsida patustajaid, vaid saada ülevaade, milline on hetkeolukord. On ebarealistlik oodata, et ükski inimene ei vajuta kunagi mitte ühelgi pahatahtlikul lingil, aga eesmärk on selliste klikkide arvu pideva ennetus- ja teavitustööga siiski vähendada.

Tavainimestele pakutavate RIA teenuste puhul lööktestimist ei kasutata. Avalike teenuste puhul rakendub klassikaline turvatestimine, mille käigus isikuandmeid ei töödelda.

Koostöö Clarified Securityga laabub hästi. Pole saladus, et CRT paneb RIA infoturbe meeskonna liikmete silmad särama, sest vastasmeeskond on tõeliselt tasemel ja paneb meie inimeste tehnilised teadmised proovile.

KROONIJUVEELIDE KAITSMINE

Senine püsiva turvatestimise kogemus on olnud väga õpetlik ja silmi avav. Loomulikult ei saa me detailidesse minna, aga on asju, mida saame nii sisu kui ka protsessi vaates teisiti teha, et oma kroonijuveele veelgi paremini kaitsta.

Soovitame ka teistel riigiasutustel kasutada CRT teenust ja vaadata üle asutuse seirevõimekus, sest Ukrainas toimuva sõja tõttu on olukord Eesti küberruumis üsna tuline. Lööktestimise teenuse pakkujaid on Eesti turul veel vähe, kuid mitu ettevõtet on seda võimekust lähiajal loomas.

ENNETUS-kampaaniatega küberturvalisema Eesti poole

2022. aastal viisime Eesti elanike küberhügieeni parandamiseks läbi kaks suuremat teavituskampaaniat. Suvel suunasime oma sõnumid vene keelt emakeelena kõnelevatele inimestele ja sügisel kutsusime IT-vaatlikumalt käituma kõiki eestimaalasi.

Eesti muust rahvusest elanike küberhügieen on keskmisest märkimisväärselt madalam ja küberturvalisuse parimate praktikate kasutus langeb vanusega. Neist järeldustest, mis põhinevad statistikaameti kogutud andmetel, lähtusime oma ennetuskampaaniate sõnumite ja sihtrühmade valikul.

RAADIOSARI „SISESTA PAROOL“

Suve hakul puhusime elu sisse venekeelsele raadiosaatele „Введи пароль“ („Sisesta parool“). Saatesarja kaudu teavitati kuulajaid küberruumis varitsevatest ohtudest ja murekohtadest, samuti isiklikust vastutusest küberintsidentide ennetamisel ja tagajärgedega tegelemisel. Raadio 4 eetris läbi suve väldanud küberturvalisuse saatesari osutus üle ootuste populaarseks. 13-osalise saatesarja iga episoodi kuulas eetris ligi 45 000 inimest.

Paralleelselt raadiosaatega käis venekeelsele elanikkonnale suunatud küberturvalisuse teavituskampaania, mis viis sihtrühmani põhilised ennetussõnumid ning ärgitas mainitud raadiosaadet kuulama. Küberturvalisuse kampaania saavutas oma tegevustega väga hea nähtavuse ja katvuse, jõudes rohkem kui 90 protsendini sihtrühmast.

OKTOOBRIS STARTIS KAMPAANIA „KONTROLLI ÜLE!“

Oktoobris, küberturvalisuse kuul, sai hoo sisse üleriigiline teavituskampaania „Kontrolli üle!“. See keskendus Eestis levinumatele petu- ja kuriteoskeemidele, mille tagajärjel jäävad ettevõtted ja inimesed ilma rahast, andmetest ja kontodest. Kampaaniaga kutsuti üles oma käitumist internetis teadlikumalt jälgima – näiteks kontrollima, millisele lingile klõpsad, kas kasutad tugevat parooli ja kuhu seda sisestad, kas oled veendunud, et sõbralt saadud e-kiri on just sõbra saadetud ning kas see, mida internetist alla laadid ja arvutisse paigaldad, on turvaline ja vajalik.

Ligi neli viiendikku eestlastest ja pool mitteeestlastest märkasid „Kontrolli üle!“ kampaa-

niat kas telepildis, raadioeetris, välireklaamil, ajalehes või digimeedias.

Kampaania järeluuringust selgus, et panime oma teavitustegevustega küberteemadele mõtlema iga teise eestimaalase, seejuures uuris 13 protsenti kampaania ajal täiendavalt lisainfot küberturvalisuse kohta ning kaheksa protsenti astus vähemalt ühe sammu, et enda või oma lähedaste turvalisust internetis suurendada.

Rõõmustav on, et kampaania peamisest sihtrühmast ehk 60–74-aastastest elanikest tegeles kampaania perioodil lausa veerand oma küberturvalisuse parandamisega.

Andmed kinnitavad: KÜBERHÜGIEEN paraneb

Igal kevadel uurib statistikaamet „Infotehnoloogia leibkonnas" küsitluse raames, milliste tegevustega tagavad inimesed oma turvalisust ja privaatsust internetis. Meie rõõmuks näitavad andmed elanike küberteadlikkuse jätkuvat kasvu.

2019. aastal väitis 64 protsenti statistikaameti küsitlusele vastanutest, et nad kasutavad miinimumnõuetest tugevamaid paroole või eri paroole eri kohtades. 2022. aastal oli samamoodi vastanuid juba 71 protsenti.

Teadlikkus on kasvanud ka ootamatute kirjade või sõnumite ning nendes sisalduvate linkide ja manuste osas. Kui 2019. aastal kontrollis tundmatult saatjalt saadud kirjades linke ja manuseid 62 protsenti vastanutest, siis 2022. aastal oli kontrollijate hulk tõusnud pea 68 protsendini.

Statistikaameti andmed annavad küll aimu küberhügieeni tasemest, ent ei selgita küberturvalise käitumise põhjuseid. Küberkäitumise paremaks mõistmiseks panime 2022. aastal seljad kokku uuringufirmaga Kantar Emor, kes uuris RIA palvel 16–24-aastaste ja 45–54-aastaste elanike küberkäitumist.

Ka selles uuringus osalenud inimesed tõid välja, et kaitsevad end eelkõige erinevate tugevate paroolide ja kaheastmelise autentimisega. Küll aga selgus, et inimesed ei pea küberrünnaku ohvriks langemist tõenäoliseks, sest usuvad end olevat piisavalt kriitilised ja küberohtudest teadlikud. Liigne enesekindlus võib aga pärssida ohutunnet, mille üle küberkurjategijad, keda tajutakse aina kavalamatena, oskavad vaid rõõmu tunda.

RIA-l valmib uus KÜBERTEST

Selleks et parandada avaliku sektori töötajate teadlikkust küberruumis varitsevatest ohtudest ja suunata neid turvalisemalt käituma, tegi RIA uue e-õppe keskkonna, kus saab oma teadmisi selles vallas täiendada ja kontrollida.

Kuigi vahel võib tunduda, et küberturvalisus on IT-inimeste pärusmaa, siis tegelikult algab see tavalise arvutikasutaja igapäevasest käitumisest: milliseid linke ja faile ta avab, mida arvutisse laadib, kuhu oma andmeid sisestab jne.

CERT-EE registreeritud intsidentidest kõige suurema osa moodustavad õngitsuslehed, mille eesmärk on saada heausklik kasutaja enda andmeid sisestama. Asutuse infoturbe eest vastutajad võivad anda endast parima, aga kui kõrvalkabinetis olev kolleeg sisestab oma parooli petturite üles seatud õngitsuslehele või avab kirjamanusesse pandud pahavara, ei pruugi sellest piisata.

KETI IGA LÜLI LOEB

Küberturvalisust on võimalik tagada ainult ohtudest teadlike inimeste abiga ja kõige lihtsam on ennetada neid intsidente, mida oskame ära tunda. Seepärast ongi vaja aeg-ajalt küberhügieeni baasteadmised üle korrata ja kontrollida oma teadmiste taset. Selleks on üks paremaid viise e-õppekoolitus, mille igaüks saab läbida endale sobival ajal ja tempos.

RIA pakkus alates 2017. aastast küberturvalisuse õppeplatvormi Digitest, mille läbisid tuhanded riigiametnikud. Alates 2023. aastast pakume enda loodud kübertesti, mis asub paljudele tuttaval Moodle'i platvormil. Uue kübertesti eesmärk on tõsta ja hoida asutuse töötajate küberturbeteadlikkust. Kübertesti saavad kasutada kõik senised Digitesti kasutajad ehk riigiasutused, kohalikud omavalitsused ja perearstikeskuste töötajad. Lisaks ootame uusi liitujaid avalikust sektorist.

ENNE KURSUS, SIIS TEST

Uus kübertest jaguneb kaheks. Esmalt palume kasutajal läbi töötada koolituse osa, mis katab tosinat olulisemat teemat. Neist paljude juurest leiab hoiatavaid näiteid päriselust, näiteks reaalseid õngitsuskirju ja pettuseid, mida on CERT-EE meeskonnale uurimiseks saadetud. Nende abil on võimalik kursuse läbijal olla paremini teadlik erinevatest pettustest ja pahavaraga kirjadest ning seesuguseid õngitsusi lihtsamini vältida.

Pärast kursuse läbimist tuleb sooritada test. Iga kasutaja saab kohe selle läbimise järel teada oma punktisumma ning tagasisidet õigete ja valede vastuste kohta.

Kursusel saab vastused küsimustele, kuidas luua turvaline parool, kuidas tunda ära õngitsuslehti ja -kirju, millised on levinumad petuskeemid, kuidas seadistada turvaliselt kodune WiFi-võrk, kuidas teha turvaliselt kaugtööd jmt.

ABIKS TAVAKASUTAJALE JA INFOTURBETIIMIDELE

Lisaks sellele, et töötajad saavad küberturbe teemal uusi teadmisi või varem kuuldut meelde tuletada, on kübertest kasulik töövahend ka asutuse infoturbe eest vastutavale inimesele. Testi tulemuste alusel saab asutuse infoturbejuhile selgemaks, millistes valdkondades ja küsimustes rohkem eksitakse ning mis teemad vajavad täiendavat koolitamist.

Kübertest ei asenda klassiruumi ja asutuse enda spetsiifilisi koolitusi, kuid on hea lisaabivahend infoturbekoolituste korraldamisel.

Kübertest ei asenda klassiruumi ja asutuse enda spetsiifilisi koolitusi, kuid on hea lisaabivahend infoturbekoolituste korraldamisel.

RIA eesmärk on, et kõik avaliku sektori töötajad läbiksid kübertesti või mõne muu küberturbekoolituse vähemalt kord aastas. See aitab meelde tuletada nii teada-tuntud petuskeemid kui ka annab infot uute riskide kohta.

DEMOKRAATIA ALUS on vabad valimised

2019. aasta riigikogu valimistel oli RIA roll märksa väiksem. Nüüd vastutame jätkuvalt e-hääletamise kogumislahenduse ja selle kaitsmise ning süsteemide majutamise eest, kuid lisandunud on valimiste infosüsteemi arendamine, töös hoidmine ja majutamine ning jaoskonnatöötajate rüperaalide kaitse.

Kõigel on oma eluiga, olgu selleks auto, sülearvuti või lihast ja luust inimene ise. Nõnda nägi seadus ette, et eelmine valimiste infosüsteem (VIS) tuli kohalike omavalitsuste volikogu valimisteks välja vahetada, et riik saaks kasutusele võtta elektroonilised valijate nimekirjad.

Seadusemuudatuste kõrval oli põhjuseid väljavahetamiseks veel: suurem turvalisus ja parem kasutajamugavus.

Praegune VIS tegi debüüdi 2021. aasta kohaliku omavalitsuse volikogu valimistel ning see vastab kõikidele praegustele turvalise arendamise põhimõtetele. 2023. aasta kevadistel valimistel kasutatakse sama süsteemi edasiarendatud versiooni. Infosüsteem on töövahend eeskätt valimisjaoskondade töötajatele ja teistele valimiste korraldajatele. Kuid mitte ainult.

Kandidaadid said soovi korral enda kandidatuuri üles seada valimiste infosüsteemi kaudu. Lisaks valijate ja kandidaatide nimekirjade haldamisele on süsteem vajalik paberhäälte lugemiseks jaoskondades, tulemuste protokollide koostamiseks, hääletustulemuste arvutamiseks ja tulemuste edastamiseks avalikkusele. Süsteemil on ka avalik kaardirakendus, mille abil leiab detailset infot hääletuspunktide kohta. Valimiste ajal avaldatakse kaart valimised.ee lehel.

Niisiis on süsteem paik, kuhu jõuavad kokku nii elektrooniliselt kui ka jaoskonnas paberil antud hääled ning sealt jõuavad tulemused nii valimised.ee kodulehele kui ka meediaportaalidesse. Meie ülesanne on ka kaitsta valimised.ee veebilehte ja valimistulemuste veebilehte rünnakute eest.

AUDITID, TURVA-, KOORMUS- JA KASUTAJATESTID

Valimiste turvalisus ja süsteemide töökindlus peavad olema tagatud parimal võimalikul moel. Nii valimiste infosüsteemi kui ka e-häälte kogumislahendust on korduvalt auditeeritud, turvatestitud ja turvalisemaks muudetud. 2022. aastal valmis VIS ISKE infoturbe ja valimiste protsesside audit, mis tõi välja vajaduse täpsustada eri asutuste rolle valimiste protsessis ning täiendada dokumentatsioone ja protseduure. Kriitilisi nõrkusi ja puudusi süsteemidel ei tuvastatud.

<table>
<tr><th colspan="7">RIIGIKOGU VALIMISED 2023</th></tr>
<tr><td>E
27.02</td><td>T
28.02</td><td>K
01.03</td><td>N
02.03</td><td>R
03.03</td><td>L
04.03</td><td>P
05.03</td></tr>
<tr><td colspan="6">EELHÄÄLETAMINE</td><td>VALIMISPÄEV</td></tr>
<tr><td colspan="4">Keskuste jaoskondades
hääletamine
kl 12.00—20.00</td><td colspan="2">Kõikides jaoskondades
hääletamine
kl 12.00—20.00</td><td rowspan="2">Kõikides
jaoskondades
hääletamine
kl 9.00—20.00</td></tr>
<tr><td colspan="6">ELEKTROONILINE HÄÄLETAMINE
E kl 9.00 kuni L kl 20.00</td></tr>
<tr><td colspan="3">Asukohas hääletamine kl 9.00—20.00</td><td colspan="4">Kodus hääletamine kl 9.00—20.00</td></tr>
</table>

Enne iga valimissündmust tehakse infosüsteemidele ka põhjalik turvatestimine, kus Eesti oma ala parimad eksperdid üritavad süsteeme katki teha või sisse murda. Seda tehakse piisavalt vara, et jõuaks enne valimisi kõik leiud ära parandada.

Me ei testi vaid turvalisust, aga ka seda, kuidas peavad süsteemid ja serverid vastu suurtele koormustele ning kui mugav on neid kasutada.

VALIMISTE TURVALISUSE TAGAMINE

Meil on vaja tervel valimisteperioodil teada, mis toimub valimiste infosüsteemi ja e-hääletuse süsteemiga. RIA küberintsidentide käsitlemise osakond CERT-EE seirab ööpäev läbi, kas meie serverite ja süsteemide vastu tuntakse ebatervet huvi.

Samamoodi seirame ja kaitseme valimisjaoskondade töötajate töövahendeid. Lisaks peavad kõik valimiskomisjoni liikmed läbima küberohtude moodulit sisaldava koolituse ja küberhügieenitesti, mis aitab meelde tuletada, millised ohud küberruumis eksisteerivad. Sarnaseid teste ja koolitusi korraldame ka kandidaatidele ja jaoskondade töötajatele.

2023. aastal on olukord Eesti küberruumis jätkuvalt rünnakuterohke ning enamasti saadetakse korda teenuste tööd häirivaid ummistusrünnakuid. Kuhugi pole ka kadunud pidev süsteemides nõrkuste otsimine, et nende kaudu süsteemi tungida.

Seda teadmist jagame ka erakondadele. RIA pakkus valimistel osalevatele erakondadele ja üksikkandidaatidele võimalust kontrollida neile kuuluvate digilahenduste turvalisust.

KES KEDA ehk valimiste rollijaotus

- **Riigi valimisteenistus** (RVT) tegeleb valimiste korraldamisega nii jaoskondades kui ka elektrooniliselt.
- **Vabariigi valimiskomisjon** (VVK) teeb järelevalvet. Tegeleb valimiskaebuste ja -rikkumiste ning valimiste usaldusväärsuse küsimustega.
- **Riigi infosüsteemi amet** haldab valimistega seotud infosüsteeme ja tagab valimiste küberturvalisuse.

MOODSAD AJAD

Lõpetuseks tuletame meelde, et 2023. aasta riigikogu valimiste valimisperiood on pidev ehk e-hääletuse ja valimispäeva vahel pole pausi. Samuti saab e-hääletaja valimispäeval ehk 5. märtsil oma e-häält veel muuta, hääletades jaoskonnas pabersedeliga. Kehtima jääb viimasena antud hääl.

Elektroonilise valijate nimekirja kasutusele võtmine tõi kaasa selle, et hääletaja pole seotud ühe kindla valimisjaoskonnaga. Ta saab häält anda mistahes oma ringkonda kuuluvas jaoskonnas.

JÄRELEVALVE: mitte karistada, vaid aidata

Umbes 13 protsenti RIA järelevalveosakonna algatatud menetlustest päädib ettekirjutustega. Üldjuhul kõrvaldatakse puudused kokkulepitud aja jooksul, kuid vahel harva tuleb ettevõttel või asutusel tasuda ka sunniraha.

Eelmisel aastal tegeles RIA järelevalveosakond 54 menetlusega. Vaatluse all olid peamiselt elutähtsa teenuse osutajad, sh vedelkütuse varustajad, elektri- ja gaasivarustajad, haiglad, autentimise ja digitaalallkirja sertifikaatide kehtivuskinnitusteenuse osutaja. Teistest olulistest teenusepakkujatest näiteks lennuvälja käitaja ja liikluse korraldaja, kauba- ja reisiveo ning sadamateenuse korraldajad.

KOLM LEVINUMAT PROBLEEMI

Kuigi meie järelevalveametnikele nõuete täitmise osas avanev pilt on kirju, saab üldistatult esile tuua kolm levinumat probleemi:

- puudub süsteemne lähenemine infoturbele ja IT riskihaldus,
- võrk pole loogilise ülesehitusega ja puudub selle kirjeldus,
- taakvara ning leige tähelepanu võrguseadmete turvanõrkuste tuvastamisele ja kõrvaldamisele, st tootjapoolse toeta tarkvara kasutamine ning paikamata haavatavused süsteemides.

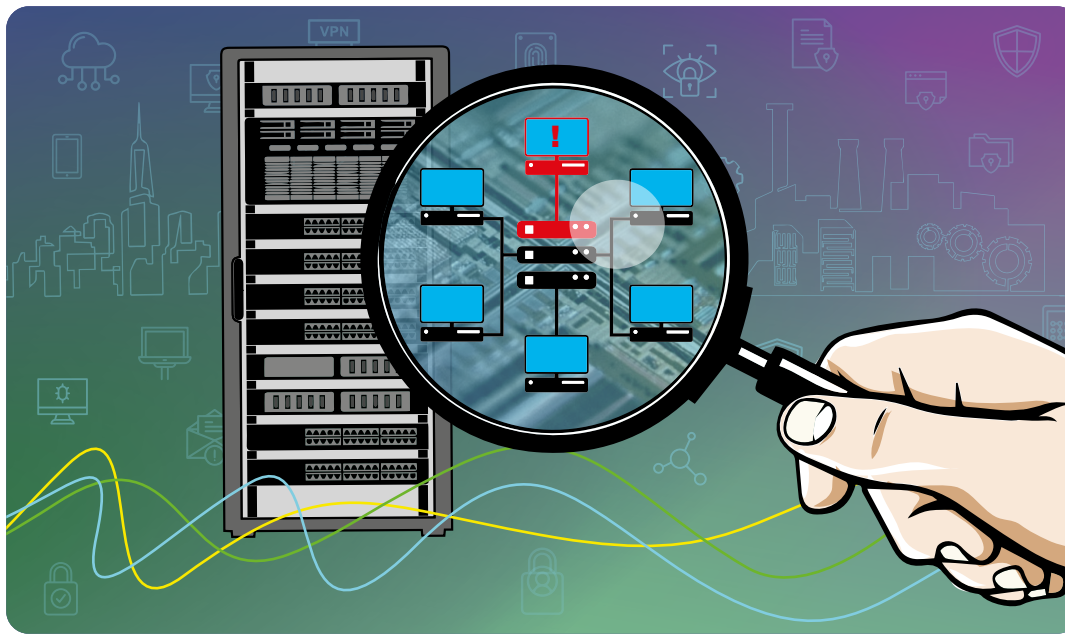
Umbes 13 protsenti nii planeeritud kontrollreididest kui ka mõne intsidendi tõttu alustatud menetlustest päädib ettekirjutustega, mis üldjuhul täidetakse kokkulepitud aja jooksul. Vahel harva jäävad väljatoodud puudused õigeks ajaks kõrvaldamata ning sel juhul tuleb ettevõttel või asutusel tasuda sunniraha.

Trahv ehk sunniraha määramine on viimane meede, et suunata juhtkonna tähelepanu infoturbe kitsaskohtadele ning survestada nendega tegelema. Selle maksmine aga ei päästa ettekirjutuste täitmisest – sunniraha võidakse määrata korduvalt, kuni ettekirjutuse täitmiseni. Lisaks võib küberturvalisuse nõuete täitmise eiramine tuua kaasa väärteomenetluse, mille karistusena saab RIA määrata isikule kuni 20 000 euro suuruse trahvi.

MENETLUSE EESMÄRK ON SUUREM TURVALISUS

2022. aastal tegi RIA 33 lõpetatud menetluse hulgas kuuele asutusele ettekirjutused. Sunniraha ükski asutus tasuma ei pidanud (üks selline juhtum oli 2021. aastal), samuti ei alustanud RIA ühtegi väärteomenetlust.

Sunniraha piirmääraks oli kuni 2021. aastani 9600 eurot, praeguseks on selle ülempiir kahekordne ehk ulatub 20 000 euroni. Reeglina on sunniraha maksmine tõhus meede, kuid üksikutel kordadel pole ühekordsest trahvist piisanud, mistõttu on pidanud menetlusalune tasuma riigile sunniraha mitmel korral.



Kui seaduse kohaselt kuuluvad RIA järelevalvatavate hulka u 2000 kas avalikke ülesandeid täitvat või/ja neile olulist teenust pakkuvat asutust ja ettevõtet (sh energia, side, transport, vesi, tervishoid jne), võivad aeg-ajalt osakonna huviorbiiti sattuda ka erasektori väiksemad ettevõtted, kes pakuvad teenust omavalitsustele. Näiteks tuli RIA järelevalveüksusel teha ettekirjutus ettevõttele, kes pakub IT-teenust paljudele omavalitsustele. Ettevõtte süsteemides ilmnesid turvanõrkused, mille kaudu tekkis võimalus pääseda ligi ettevõtte klientide süsteemidele, sh andmetele. RIA-le teadaolevalt pole nõrkusi ära kasutatud ning võimalikud riskid ei realiseerunud. Ettevõte kõrvaldas puudused, millele RIA ametnikud oma ettekirjutuses tähelepanu juhtisid.

SEL AASTAL FOOKUSES PEREARSTID

Sellel aastal on RIA eesmärk külastada perearste ja perearstikeskuseid, kuna nad peavad hakkama täitma 2018. aastal jõustunud küberturvalisuse seadusest tulenevaid nõudeid. Sealhulgas informeerima küberintsidendist RIAt ning tagama intsidendi lahendamise ja selle ennetamise meetmed, viima läbi riskianalüüsi ning rakendama teisi seadusest tulenevaid infoturbemeetmeid.

Millega tegeleb RIA järelevalveosakond?

RIA küberturvalisuse teenistuse järelevalveosakond kontrollib küberturvalisuse seaduse (KÜTS) nõuete täitmist, keskendudes võrgu- ja infosüsteemide turvameetmetele ning nende piisavusele. Järelevalve all on kõik KüTSi kohuslased ehk ligikaudu 2000 asutust ja ettevõtet, sealhulgas kõik avaliku sektori asutused, elutähtsa ja olulise teenuse pakkujad (perearstid, haiglad, elektri- ja veeteenuse pakkujad, side ja transport jne).

Lisaks lahendab osakond usaldusteenuse osutajate tegevusloa taotlusi, haldab Eesti usaldusnimekirja ning teeb järelevalvet teenusele kehtestatud nõuete täitmise üle.

Sedapuhku on järelevalve fookus ennetusel – arstide teadlikkuse tõstmine võimaluste ja kohustuste kohta. RIA plaanib korraldada perearstidele ka sellekohase infopäeva. 2023. aasta järelevalve kavas on kontrollida ka riigiasutusi, sh omavalitsusi.

Kaitstes kriitilist TARISTUT

Riik ei saa toimida, kui pole elektrit, kütet, arstiabi või teisi vajalikke teenuseid. Samamoodi on vaja kaitsta riiklikult olulisi andmeid ja andmebaase. RIA annab oma panuse, et Eesti kriitilise taristu ja riigi toimimiseks oluliste asutuste-ettevõtete süsteemid oleksid kaitstud.

RIA kriitilise infrastruktuuri küberkaitse osakond (KIKK) on ellu kutsutud selleks, et aidata riigi seisukohalt kõige tähtsamaid asutusi ja ettevõtteid. Teeme seda koolituste, testimiste ja õppustega. 2022. aastal viisime läbi kõrgetasemelisi harjutusi ja treeninguid nii ETOdele ja OTOdele kui ka riigi IT-majade töötajatele.

SÕNASTIK

- **ETO** – elutähtsa teenuse osutaja
- **OTO** – olulise teenuse osutaja
- **Küberreserv** – RIA ellukutsutud reserv, kuhu kuuluvad Eesti riigile IT-teenuseid pakkuvate riigiasutuste ja Kaitseliidu küberkaitseüksuse eksperdid
- **E-ITS** – Eesti infoturbestandard, mis vastab ISO27001 standardile
- **Riiklikud IT-majad** – **SMIT** ehk Siseministeeriumi Infotehnoloogia- ja Arenduskeskus, **TEHIK** ehk Tervise ja Heaolu Infosüsteemide Keskus, KeMit ehk Keskkonnaministeeriumi Infotehnoloogiakeskus, **RIT** ehk Riigi IT Keskus, **RMIT** ehk Rahandusministeeriumi Infotehnoloogiakeskus, **RIK** ehk Registrite ja Infosüsteemide Keskus ja **RIA** ehk Riigi Infosüsteemi Amet
- **CR14** – Eesti kaitseministeeriumi alla kuuluv sihtasutus, mille eesmärk on arendada kaitsevaldkonna küberjulgeoleku teadus- ja arendustegevust

AITAME VALMISTUDA HALVIMAKS

Sügisel toimusid üle maailma hinnatud ja nõutud digikriminalistikale (*forensics*) ning tööstusautomaatika turvalisusele keskendunud koolitused, millest igaüks kestis kuus päeva. Koolitusprogramm oli nii tihe, et appi tuli võtta ka laupäevad. Kursustel osalesid elutähtsa teenuse osutajate, IT-majade ja Kaitseliidu küberkaitseüksuse esindajad, kes said põhjaliku ülevaate, mida teha intsidendi korral, kuidas koguda ja säilitada andmeid ning viia läbi esmast analüüsi.

Automaatjuhtimissüsteeme kasutavate ETO-de töötajad olid tänulikud tööstusautomaatika turvalisuse tagamise kursuse eest. Seal näidati, kuidas süsteeme rünnatakse, mida organisatsioonid saavad nende kaitsmiseks teha ning kuidas tagada, et samal ajal oleks rahuldatud äripoole vajadused. Koolitus toimus spetsiaalsete tööstusautomaatika seadmetega. Igal osalejal oli laual hulk seadmeid ja oma keskkond, kus harjutusi läbi viia.

Kolmas seltskond sai ülevaate, kuidas oma infosüsteemide turvalisust korralikult auditeerida, neljas osales ISO standarditel põhinevatel küberturbe- ja toimepidevuse koolitustel. Kui kõik aasta teises pooles korraldatud koolituspäevad kokku lugeda, siis pakkusime rohkem kui 500 inimpäeva jagu maailmatasemel küberturbekoolitusi.

> Meie eesmärk on pakkuda võimalikult elutruid õppusi ja läbimänge.

Meie eesmärk on pakkuda võimalikult elutruid õppusi ja läbimänge. Üheks selliseks oli Powergrid, mille organiseerisime koos partnerasutusega CR14. Viiepäevasel õppusel pidid tehnikud seadistama, ründama ja kaitsma seadmeid, mida kasutatakse elektrivõrgu töös hoidmiseks. Sama põhimõttega tehnilisi koolitusi ja õppusi said ka haiglate, telekomide ja pankade töötajad.

TURVATESTIMINE AITAB HALVIMAT VÄLTIDA

Nii meie kui ka kriitilise taristu eest vastutavate organisatsioonide vahendid on piiratud. Igal aastal aitame turvatestida käputäit ettevõtteid. Rünnakuid simuleerides näeme meie ja asutus või ettevõte ise, kuhu tuleb raha, tehnoloogiat või töötunde investeerida, et hoida oma süsteemid ja seeläbi teenused töös.

Möödunud aastal aitasime turvatestida ja hinnata haigla, kaugkütte- ja lennundussektori ettevõtte IT-süsteemide vastupidavust, taasteplaane ja töökorraldust. Kuigi rünnak ise võib olla väga tehniline, sõltub selle lahendamine tihti organisatsiooni töökorraldustest ja sellest, kas on paika pandud, kuidas sääraseid olukordi lahendada. Raske on viga ja rünnakut tõrjuda, kui puuduvad logid ehk ülevaade, mida üldse süsteemides tehakse, ning plaan, mida ette võtta.

Maailmas ainulaadne KÜBERRESERV

RIA eestvedamisel sündis riiklik küberreserv, mis koondab enda alla pädevad IT-eksperdid, kes hakkavad lahendama suuri ja pikaajalise mõjuga küberintsidente. Idee luua säärane löögirühm sündis 2020. aastal ning 2022. aasta sügiseks oli küberreserv valmis.

Esimene õppus reservi liikmetele toimus Eesti suurimas haiglas, Põhja-Eesti regionaalhaiglas. Mängiti läbi stsenaarium, kus lunavararünnak lõi haigla süsteemid rivist välja ning need tuli võimalikult kiiresti nullist püsti saada, sest ohtu võisid sattuda inimeste elu ja tervis.

Reservi kuuluvad IT-majade ja teiste avaliku sektori IT-töötajad ning Kaitseliidu küberkaitseüksuse liikmed. Kui selleks tekib vajadus, on võimalik kaasata ka erasektori spetsialiste. Kogu küberreserv töötab vabatahtlikkuse alusel ning tehtud töö eest tasub eksperdi tööandja.

Praegu kuulub reservi umbes sadakond inimest. Meie eesmärk on kõiki liikmeid pidevalt koolitada ja treenida, et nad saaksid ise areneda ning neil oleks teadmisi ja oskusi, et riiki rünnaku korral aidata. Kuna reserv sündis alles 2022. aasta sügisel, pole praegu seda veel reaalsete intsidentide lahendamisse kaasatud, aga vaadates meie ümber toimuvat, siis ei pruugi olla kaugel aeg, kui peame nad päriselt appi paluma.

Kuidas kasvatada EESTI KÜBER-KOMPETENTSI?

RIA võtab sellest aastast senisest ambitsioonikama rolli Eesti küberkogukonna toetamisel. Eesmärk on anda oma panus, et küberturvalisuse teenuseid pakuks rohkem ettevõtteid, teadustööd jõuaksid teenusteks ja toodeteks, spetsialiste tuleks juurde ning kõigil oleks võimalik Euroopa küberökosüsteemi arengus kaasa rääkida.

Mullu jõustus määrus, millega loodi Euroopa küberpädevuskeskus ECCC ning riiklike koordinatsioonikeskuste (*national coordination center* ehk NCC) võrgustik. ECCC hakkab füüsiliselt paiknema Rumeenias Bukarestis ning selle põhiliseks väljundiks on Digital Europe'i ja Horizon Europe'i küberturvalisuse fondiraha strateegiline suunamine. Eesti riikliku koordineerimiskeskuse rolli hakkab täitma RIA, täpsemalt RIA küberturvalisuse teenistuse teaduse ja arenduse koordineerimisosakond.

PRAKTILISED VÄLJUNDID

Meie fookus on küberturvalisuse valdkonnas kompetentside kasvatamisel. Et oleks rohkem küberturvalisuse spetsialiste, on vaja sekkuda haridusvaldkonnas. Et küberturvalisuse teenuseid tarbitaks ja pakutaks rohkem, saame panustada toetuste ja iduettevõtete kiirendamisega. Et küberturvalisuse teadusvaldkond oleks paremini tarbijate vajadustega kooskõlas, tellime teadusasutustelt tulevikutehnoloogiate turvalisuse uuringuid ja ülevaateid.

Seda ei tee me üksinda. Eestis juba on mitu kogukonda, algatust ja foorumit, kus küberturvalisuse spetsialistid, valdkonnaliidrid, huvilised ja entusiastid käivad koos ja vahetavad mõtteid. RIA eesmärk on võimestada ja võimendada neid algatusi, mis on juba elujõulised, ning pakkuda laiapinnalist ülevaadet küberruumist, meil töötavate spetsialistide nägemust ning võimalusi kasutada ära RIA riigisiseste ja rahvusvaheliste kontaktide võrgustikke. Siin ei saa me läbi ilma Startup Estonia ja EASita, partneriks on meil ka Tallinna teaduspark Tehnopol, koostööd teeme AI ja robootika valdkonna Euroopa digitaalse innovatsioonikeskusega AIRE.

RÄÄGI KAASA

Küberturvalisuse toetuste, iduettevõtete, koolituste ja teadusülevaadete kõrval on oluline ära

märkida, et pikas perspektiivis peaks NCC-EE projekti kaudu olema küberturvalisuse kogukonna liikmetel (ettevõtetel, teadusasutustel ja muidugi ka eraisikutel) võimalik kaasa rääkida Euroopa küberturvalisuse arengus.

Olgu selleks ühiskondlikud trendid, teadusuuringute vajadused, investeeringute ja projektide suunad. Pikemas perspektiivis soovivad Euroopa Liidu institutsioonid toetada selle algatuse kaudu visiooni, kus Euroopa küberturvalisuse sektor saaks selgelt tugevamaks ja maailmas nähtavamaks.

NCC-EE projekti visioon

Eestis pakuvad küberturvalisuse teenuseid piisava tööjõuga, elujõulised ja teaduspõhiste tegevustega tulevikku vaatavad ettevõtted, kes panustavad nähtavalt sektori arengusse üle Euroopa ja kelle teenuste järele on tugev nõudlus nii Eestis kui ka ülejäänud maailmas.

Strateegilised tegevussuunad

Selleks et jõuda visioonis seatud eesmärgini,

1) **kasvatame küberturvalisuse sektori konkurentsivõimet.**
   - Levitame Eesti küberturvalisuse valdkonna teadus- ja arendustegevusest saadud teadmust nii Eestis kui ka koordinatsioonikeskuste võrgustiku vahendusel mujal Euroopas.
   - Toetame Eesti küberettevõtete osalemist rahvusvahelistes T&A projektides ja iduettevõtete loomist.
2) **edendame Eesti ühiskonna küberkerksust.**
   - Koostöös teiste ökosüsteemi osalejatega tõstame Eesti ettevõtete ja asutuste teadlikkust küberohtudest ja võimalustest, kuidas oma organisatsiooni paremini küberohtude eest kaitsta.
   - Viime ellu küberpöörde pilootprojekti: toetused ettevõtetele, kes tahavad oma asutuse küberturvalisuse taset suurendada.
3) **suurendame valdkonna järelkasvu ja spetsialistide hulka.**
   - Leiame kõigil vanuse- ja haridustasemetel võimalusi lisada küberturvalisuse õpiväljundeid olemasolevatesse õppekavadesse.
   - Töötame partneritega valdkonna populaarsuse tõstmise nimel ja toome naisi ja tüdrukuid valdkonda juurde.
4) **seirame ja toetame küberturvalisuse ökosüsteemi arengut Eestis.**
   - Koostöös küberkogukonna teiste liikmetega edendame teenusepakkujate, tarbijate, teadlaskonna ja teiste osapoolte omavahelist suhtlust, pakkudes selleks platvorme nii füüsiliselt (üritused-seminarid-konverentsid) kui ka virtuaalselt.
   - Eesti ja teiste liikmesriikide NCCde kogemuse pealt leiame võimalusi osaleda ise ja innustada kogukonda osalema Eesti ja Euroopa kübersektori arengut edendavates projektides.

E-ITS: miks ja kellele?

Jaanuarist jõustunud uus infoturbestandard (E-ITS) on väljakutse nii riigiasutustele kui ka ettevõtetele, kes peavad kolme aasta jooksul läbima auditi ning tõestama, et suudavad pakkuda teenust turvaliste süsteemide abil.

Uuenenud standard on mõeldud kasutamiseks laiemale sihtgrupile, kui seda oli 20 aastat kehtinud infoturbesüsteem ISKE. E-ITS kirjeldab meetmeid, mida järgides kasvab oluliselt organisatsiooni toimepidevus – tekib ülevaade protsessidest ja riskidest, paraneb nii küberrünnakute ennetamise kui ka tagajärgedega tegelemise võimekus.

KES SEDA RAKENDAMA PEAVAD?

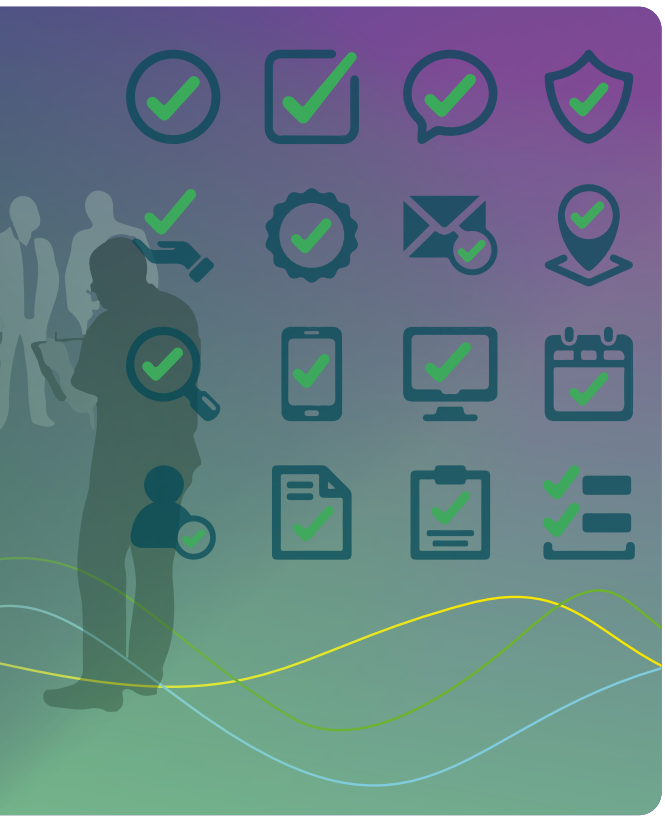
Töö uue standardiga algas 2019. aasta suvel. Alates 2021. aastast kuni selle aasta aprillini viib RIA läbi E-ITSi rakendamise pilootprojekte, kuhu kuulub üle 20 asutuse. Kolm piloodis osalenud asutust on rakendamisega n-ö finiši äärel ning ootavad auditeerimist.

Küberturvalisuse seaduse muudatuste tulemusel on standardi järgimise kohustus u 3500 organisatsioonil, sealhulgas kõigil avaliku sektori asutustel ja ühiskonna toimimiseks vajalike teenuste osutajatel. Hädaolukorra seaduse järgi on sellised teenused näiteks elektri, maagaasi ja vedelkütusega varustamine, riigitee sõidetavuse tagamine, telefoni- ja andmesideteenus, elektrooniline isikutuvastamine ja digitaalne allkirjastamine, esmaabi tervishoiuteenuses, makseteenus jms. Aga ka vähemalt 10 000 elanikuga kohaliku omavalitsuse veega varustamine ja kanalisatsiooni haldus.

Rakendamise kohustus on ka kõigil andmekogu vastutavatel või volitatud töötlejatel, riigi ja kohaliku omavalitsuse hallatavatel koolidel (v.a erakoolid) ning digitaalse teenuse pakkujatel juhul, kui ettevõttes töötab üle 50 inimese ja selle aastakäive on suurem kui kümme miljonit eurot. Tarkvaraarendajad peavad E-ITSi rakendama ulatuses, mida nõuab tellija.

PAINDLIK ÜLEMINEKUAEG

Standardi rakendamiseks ja auditeerimiseks on kuni kolm aastat. Esimeste toimingutega – E-ITSi rakendamise kontseptsioon ja ajaplaan – alustamise kohustus kehtib aga juba tänavu jaanuarist. Erasektori asutused, kes pole seni



ISKEt rakendanud, peavad suutma rakendamise alustamist tõendada alates 30. juunist 2023.

Avaliku sektori asutused, kes olid seni ISKE auditi kohuslased, peavad oma asutuse infoturbe rakendamist auditeerima enne ISKE auditi kehtivuse lõppu, kuid mitte hiljem kui kolm aastat pärast E-ITSi kehtestava määruse jõustumist, seega hiljemalt 2025. aasta detsembris. Kui ISKE auditeid oli asutuses mitu, tuleb arvestada kõige varem lõppeva auditi kehtivusajaga. Asutustel, kes seni polnud auditeerimiskohuslased, kuid nüüd on, tuleb audit läbi viia enne 2025. aasta detsembri lõppu (kuni kolme aasta jooksul pärast määruse jõustumist).

Kui seni võis auditite tellimise delegeerida IT-majadele, siis nüüd on turvameetmete rakendamise ja tõendamise kohustus asutusel endal. Asutuse kohustus on tagada teenuseand-ja infoturve vähemalt samal tasemel, mis vastaks asutuse enda kaitsetarbele.

E-ITSI rakendamise järelevalvet viib läbi RIA järelevalveosakond. Vaata ka eits.ria.ee.

Praktiku kogemus

Tartu linnavalitsuse infoturbejuht Martin Parv leiab, et E-ITSi rakendamine on vajalik, ent täis bürokraatiat.

Tartu linnavalitsuse teekond E-ITSini algas infoturbejuhi töökoha loomisega 2021. aasta lõpus. Linnavalitsus teadvustab IT olulisust ning on valmis valdkonna turvalisusse panustama.

Varasemast olid meil teenused kaardistatud ja varadest selge ülevaade olemas. Algne idee oli tekitada nimekiri meetmetest, mida tuleb konkreetsele varale rakendada, kuid see oleks muutnud rakendajate elu keeruliseks ja vara arvelevõtu aeganõudvaks.

Meetmed läbi töötades jõudsime järeldusele, et kõige mõistlikum on grupeerida need kokku vastavalt varagruppidele ning tekitada nendest dokumendid, mis sisaldavad E-ITSist tulenevaid ja ka muid vara turvamiseks vajalikke nõudeid ja toiminguid.

Lõime enda jaoks loogilised dokumendid, koondame nende sisse meetmed, mis on kirja pandud rakendajale arusaadavas keeles ja lingitud kõikide kasutatavate meetmetega, et meie süsteem vastaks E-ITSile. Nii on meetmete muudatuste puhul kerge jälgida, kus konkreetne meede asub ning kas uuendusega tuleb midagi muuta.

Meie plaan on teha rakendaja elu kergemaks ning selle asemel et ta peaks näiteks iga seadme kohta märkima rakendatuks suure hulga meetmeid, peab ta oma tegevustes jälgima tema seadme kohta käivat dokumenti ning käituma vastavalt sellele. Kui ta seda teeb, saab ta iga seadme kohta kinnitada vaid ühe korra, et meetmed on rakendatud, kuna ta võtab vara kasutusele vastavalt dokumendis toodule.

Peavalu valmistab bürokraatia, mis nõuab mõne korra, juhendi, eeskirja või regulatsiooni tegemist. Isegi kui need kokku koondada, on neid liiga palju, et iga asutus suudaks neid ise käsitööna teha. Puudu on meetmeid sisaldavad näidisdokumendid, kuhu oleks kogu nõutud bürokraatia kirja pandud, ja ühtne tööriist Eesti väiksele asutusele, mille abil saaks asutus hõlpsalt saavutada vähemalt põhiturbe.

Mida oodata 2023. AASTALT küberruumis?

OHUTASE tõuseb veelgi

Ründajate ja sihtmärkide ring laieneb. Viimaste seas on aina enam riigiasutusi ja ühiskonna jaoks kriitilisi teenuseid pakkuvaid ettevõtteid, näiteks vee-, energia- ja kütusesektor, telekommunikatsioonisettevõtted ja pangad. Nagu paljud teised valdkonnad, digiteerivad oma tööprotsesse ka elutähtsa teenuse pakkujad. See suurendab võimalust elu tõsiselt

häirivateks intsidentideks.

Küberohupilti mõjutavad arengud rahvusvahelistes suhetes ja julgeolekuolukorras. Eesti ja kogu läänemaailma jaoks tõstis küberohu taset märkimisväärselt 24. veebruaril 2022 alanud Venemaa täiemahuline kallaletung Ukrainale. Käimasolev sõda on näidanud, et lisaks küberrünnetele kineetilise sõjategevuse toetamiseks kasutatakse neid ka tööriistana reageerimaks ühe või teise riigi ebameeldivatele poliitilistele otsustele või tegevustele. Lisaks tuleb arvestada, et küberründed mõne teise riigi vastu võivad kanduda Eestisse.

Jätkub RIIKLIKE SIDEMETEGA RÜHMITUSTE tegevusulatuse kasv

Peamised riigid, kes küberrühmitusi enda huvides tegutsema suunavad, on hetkel väga pingelises olukorras. Venemaa pommitab jätkuvalt Ukrainat, Hiina on aina agressiivsem läänemaailma ja Taiwani suhtes, Iraan üritab maha suruda opositsiooni riigi sees. Küberrünnakud on neis valitsevatele režiimidele üks ja pigem mugav viis saavutada oma poliitilisi eesmärke või vähemalt meelsuse demonstreerimise vahend. Lihtsamate rünnakute – kodulehtede näotustamine ja teenusetõkestusrünnakud – kõrval on agressiivsete suurriikide kontrollitavate küberrühmituste (APT) arsenalis keerukamaid ja ohtlikumaid relvi: näiteks kriitilise taristu rivist välja viimine, küberspionaaž ja selle käigus saadud info valikuline lekitamine vastastele mainekahju tekitamiseks või konkreetselt Eesti puhul meile nii harjumuspärase e-riigi mõne põhikomponendi töö häirimine.

Ei tohi unustada, et vaenulike riikidega seotud tegelased peilivad regulaarselt Eesti

asutuste võrke ning avastatud haavatavused pannakse enda kasuks tööle. Mistõttu peab taas kord toonitama, et ükski riigiasutus, ettevõte ega tavakodanik ei tohi oma küberturvalisusse kergekäeliselt suhtuda.

KÜBER-KURITEGEVUS areneb edasi

Lunavarargründed on juba aastaid tähelepanu all kui üks kahjustavamaid küberkuritegevuse liike. Eesti küberruumis on registreeritud lunavarajuhtumite arv viimasel kahel aastal püsinud 20–30 ringis ning seni oleme puutumata jäänud ühiskonda tõsiselt häirivatest lunavararünnetest. Kuid oht, et Eestit tabab suure mõjuga lunavararünnak, on eelmainitud põhjustel kasvamas.

Samuti võib prognoosida, et järgnevate aastate jooksul muutuvad tehnoloogia – nt tehisintellekti – arenguga juba mitu aastat Eestiski probleeme tekitanud õngitsusrünnakud usutavamaks, sihitumaks ja seeläbi raskemini avastatavaks.

Lisaks e-postile levitatakse õngitsusi aina enam sotsiaalmeedia vahendusel, näiteks tööpakkumiste ja kuulutuste kaudu. Usutavuse tõstmiseks kasutatakse peibutusteemana ära aktuaalseid ja päevakajalisi teemasid, mis kõnetaks just sihtmärgiks valitud inimest. Seni on meid õngitsuste eest teatud määral kaitsnud keelebarjäär, kuid mida paremaks arenevad tõlkeprogrammid, seda keerulisemaks muutub libalehe või -kirja eristamine tõelisest.

TURVANÕRKUSTE osas tuleb aina valvsam olla

RIA eelmine aastaraamat nimetas 2021. aastat turvanõrkuste aastaks. Turvanõrkused ei kadunud kuhugi ka 2022. aasta vältel ning jäävad meiega nüüdki. 2023. aastal aeguvad mitmed populaarsed Microsofti tooted (Windows 7, Office 2012 jpt) ja sellest tulenevalt võivad pahatahtlikud osapooled seada fookuse just nende toodete häkkimisele.

Suure tõenäosusega ei pääse me ka kriitiliste tasemega turvanõrkustest. RIA hoiab erinevatel turvanõrkustel silma peal ja teavitab regulaarselt nendest nii erinevaid asutusi ja ettevõtteid kui ka avalikkust. Soovitame pidevalt jälgida RIA blogi ja sotsiaalmeediakanaleid.

Suur osa probleemist on jätkuvalt nn *anti-patcher*'id – turvajuhid või administraatorid, kes lubamatult venitavad oma asutustes kasutatavates tarkvarades avastatud haavatavuste paikamisega. Palume veel kord: reageerige RIA-lt tulnud ohuteavitustele ja paikamisjuhistele viivitamatult.

Eesti elanike KÜBERTEADLIKKUS paraneb pidevalt

Mitte kõik eesootav pole negatiivse alatooniga. Nagu võib lugeda seekordse aastaraamatu ennetustegevuste peatükis (lk 42), on Eesti elanike küberteadlikkus viimaste aastatega järjepidevalt kasvanud. Selle trendi kindlustamiseks kavatseb RIA edaspidigi jätkata ennetus- ja teavitustegevustega. Tänavu suvel läheb eetrisse järjekordne raadiosari, mis tutvustab kuulajatele küberruumis varitsevaid ohte ja enda kaitsmise nõkse. Aasta teises pooles avaldame RIA ennetusveebis itvaatlik.ee kübertesti, mille läbimise järel on iga külastaja peamiste kübertõdede võrra targem. Samuti suuname koos Eesti Infotehnoloogia ja Telekommunikatsiooni Liiduga (ITL) fookuse väikestele ja keskmise suurusega ettevõtetele, kellele meenutame enda küberruumis kaitsmise olulisust ja selle peamisi viise.

Küberturvalisuse aastaraamat 2023

Väljaandja: **Riigi Infosüsteemi Amet**
Pärnu mnt 139a, 11317 Tallinn
Kujundus: **Martin Mileiko** (Profimeedia OÜ)
Illustratsioonid: **Andres Varustin**
Trükk: **Ecoprint AS**

Loe edasi: **www.ria.ee**