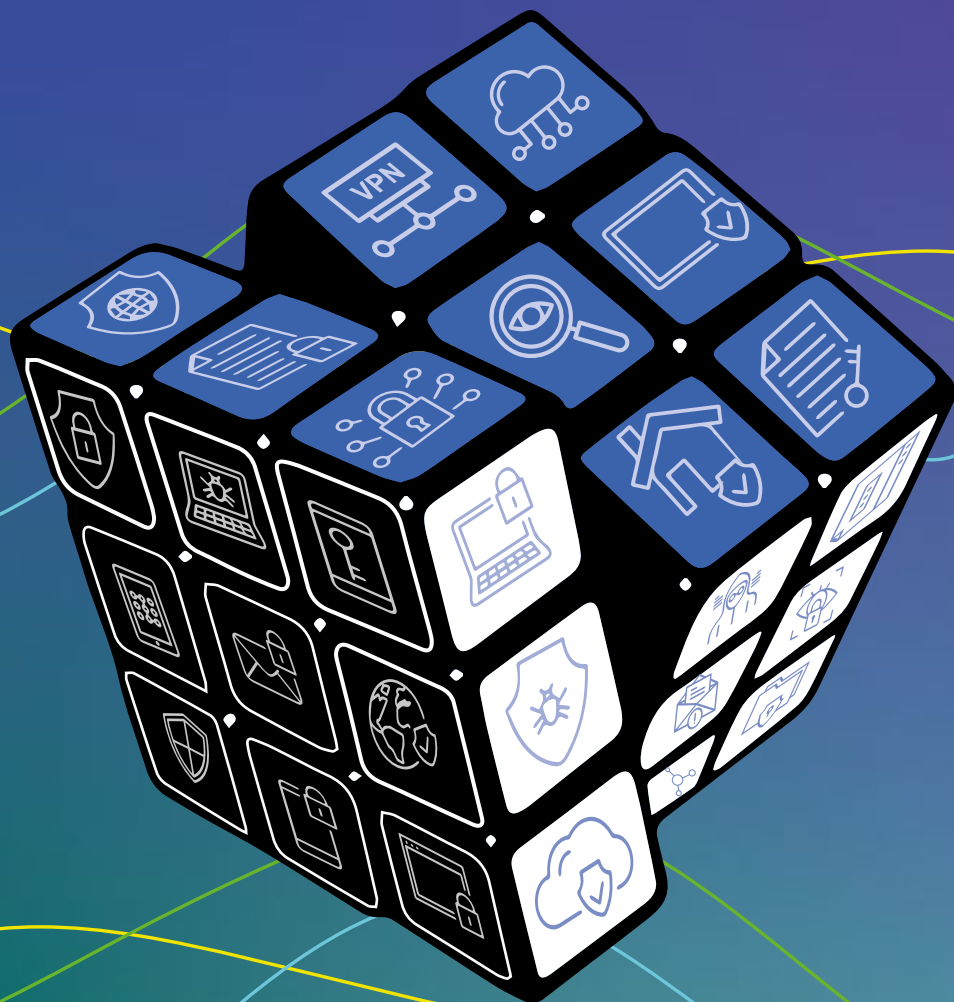




RIIGI INFOSÜSTEEMI AMET



KÜBER- TURVALISUSE AASTARAAMAT 2024



RIIGI INFOSÜSTEEMI AMET



Küberturvalisuse aastaraamat 2024

Sisukord

EESSÕNA

6

Surve kasvab

Küberrünnakud on muutunud sihitumaks ja olemuselt keerulisemaks, mis tähendab, et üha suurem on ka õnnestumistõenäosus. Peame õppima arvestama, et küberruumis toimuv mõjutab meid igal sammul, kirjutab Gert Auväär, RIA peadirektori asetäitja küberturvalisuse alal.

2023. AASTA ÜLEVAADE

8

Olukord küberruumis: ummistusrünnete aasta kordus

Ka eelmisel aastal jätsid kasvanud geopoliitilised pinged pitseri Eesti küberruumi. Novembripakases kajas Iisraeli ja Hamasi konflikt küberrünnetena Eesti katlamajades, kuid refräänina saatsid aastat taas teenusetõkestusründed, millest rõhuv enamik on seotud Venemaa täiemahulise sõjaga Ukraina vastu.

14

Sõda Ukraina küberruumis: mida näitas aasta 2023?

Ehkki Ukraina pinnal toimuv traditsiooniline sõjategevus saab põhjendatult rohkem tähelepanu, toimub selle taustal aktiivne ründe- ja kaitsetegevus ka küberruumis. Mida 2023. aasta selles osas tõi?

18

Võõrad andmed haigusloos

Möödunud aasta septembris avastas üks Raatuse perearstikeskuse patsient enda haigusloo kokkuvõttest võõrad kaebused ja diagnoosi. Ta oli üks ligi 600 patsiendist, kelle haigusluku sattusid tarkvaravea tõttu valed andmed.

20

Asper Biogene'i andmeleke – mis täpsemalt juhtus?

Detsembris sai avalikkus teada, et geneetilise testimisega tegeleva ettevõtte Asper Biogene süsteemidest laaditi ebaseaduslikult alla ligi 10 000 inimese isiku- ja terviseandmed ning ähvardati need avalikustada.

22

Lunarahanoõuded tabasid mitut suurt tootmisettevõtet

2023. aastal teavitati CERT-EE-d mitmest lunavararünnakust, mille ohvriks langesid Eesti mõistes suured, sadade töötajatega ettevõtted.



24

Kogemuslugu: rünnak, mis läks maksma miljeoneid

Mullu tabas lunavararünnak kaht Harjumaal tegutsevat metallitööstusettevõtet, kus töötab kokku ligi 400 inimest. Fimade omanikud räägivad avatult, mis ja miks juhtus, et aidata teistel sarnaseid ohte vältida.

26

Ummistusründed: mullu purunes senine rekord

Teenusetõkestusrünnete poolest oli möödunud aasta eelkäijale väärikas mantlipärija. Ei löödud ainult massiga, rünnakud muutusid ka paremini sihituks.

28

Pettusteaasta järelehuüe: kus mu raha on?

Kui ettevõtetele valmistasid eelmisel aastal peavalu ummistusründed, lunavara ja andmelekked, siis tavakasutajaid kimbutasid igast võimalikust kohast sisse trügivad pettused. Eelmisel aastal petsid kurjategijad Eesti inimestelt välja vähemalt 8,3 miljonit eurot.

32

Tavapärasest rohkem nullpäeva turvanõrkusi

Sarnaselt eelnevatega kihask

34

2023. aasta sündmused rahvusvahelises küberruumis

Geopoliitilised pinged, eelkõige Venemaa kestev agressioon Ukrainas ning oktoobris lahvatanud konflikt Iisraeli ja Hamasi vahel, peegeldusid ka rahvusvahelises küberruumis, kuid taustal käis tavapärane küberkuritegevus.

TURVALISEM KÜBERRUUM

38

RIA red team: „Tahame minna taristu lõhkumise kallale“

Riigi küberturvalisuse eest vastutava asutuse töötajalt on sellist soovi üllatav kuulda, aga just niisugune on RIA red team'i eesmärk: panna infosüsteemid tõsiselt proovile, et need oleksid pahahtlike ründajate eest paremini kaitstud.

42

IT-vaatlikult küberohtudele vastu

Küberohtude arengu ja kasvuga toimetulekuks on vaja, et kõik oleks varitsevatest ohtudest teadlikud ning oskaks küberruumis turvalisemalt käituda. Selleks viisime eelmisel aastal läbi kaks ennetuskampaaniat – ühe ettevõtetele, teise eraisikutele.

44

Kübertest tegi hoogsasti stardi

2023. aasta aprillist pakume tasuta küberturbealast õppeplatvormi Kübertest. Esimese aasta jooksul liitus sellega üle 200 asutuse ja ettevõtte ning koolituse ja testi läbis üle 15 000 inimese. Mis nende vastustest selgus?

46

Perearstide kübertervis jätab soovida

Sõeluuringu käigus selgus, et mitmete perearstide kübertervis pole kiita ning vajab kohe sekkumist. Infoturbe standardi rakendamine koostöös RIA järelevalvega aitab ennetada raskeid tagajärgi.

48

2023. aasta valimised tõid e-pöörde

Eelmisel aastal toimunud riigikogu valimised olid meie jaoks ajaloolised: sündis maailmarekord, sest esmakordselt oli e-hääle andnud rohkem kui pabersedeliga hääletanud.

50

Cyber4Dev: missioon täidetud

2023. aastal lõppes esimene globaalne Euroopa Liidu rahastatud küberturbealase arenguabi projekt Cyber Resilience for Development ehk Cyber4Dev. Selle raames panustasid kümned Eesti eksperdid 26 riigis turvalisema küberruumi loomisesse.



52

Küberpöörde toetus aitab kokku hoida

RIA pakub koostöös EAS-Kredexi ühendasutusega toetust väikestele ja keskmise suurusega ettevõtetele, et nad saaksid oma küberturvalisuse taset mõõta ja tõsta.

54

RIA kogemus: kuidas me E-ITSi rakendame

Eesti infoturbestandard ehk E-ITS on kohustuslik umbes 3500 organisatsioonile. RIA on üks neist. Oma avalike ülesannete ja ligikaudu 300 töötajaga tuli meil läbi töötada 6000 infoturbe-meedet.

56

Mida 2024. aastalt küberruumis oodata?

2023 tõi valusaid andmelekkeid, lunavararünnakuid ja pettuseid. Milliste ootustega vaatame 2024. aastat?

SURVE KASVAB

Küberrünnakud on muutunud sihitumaks ja olemuselt keerulisemaks, mis tähendab, et üha suurem on ka õnnestumistõenäosus.

Peame õppima arvestama, et küberruumis toimuv mõjutab meid igal sammul, kirjutab **Gert Auväärt**, RIA peadirektori asetäitja küberturvalisuse alal.

Venemaa täiemahuline agressioon Ukrainas on meile andnud võimaluse seada fookus täielikult laiapindsele riigikaitsele, sisejulgeolekule ja turvalistele digilahendustele, eesmärgiga hoida ühiskond toimimas ka kriisis. Pea kogu kriitiline taristu on Eestis seotud infosüsteemidega ja nende kaitsmine küberrünnete eest on riiklikult tähtis.

Aastatel 2013 ja 2015 ÜRO peaassambleel heaks kiidetud riikidevaheline kokkulepe, et teise riigi kriitilise infrastruktuuri ründamine on tabu, ei kehti Venemaa sõjategevuse näitel Ukrainas kahjuks enam ammu. Seekordse aasta-araamatu kaante vahelt leiab muu hulgas meie Ukraina kolleegidelt hea ülevaate väljakutsetest, millega küberruumis tuleb igapäevaselt toime tulla. Kübersektor moodustab tsiviiltaristu kaitsest olulise osa ning on hea meel tõdeda, et küberturvalisus on üle aastate taas tõusnud riigieelarve prioriteetide hulka.

UUS NIMI

Kui veel paar aastat tagasi töötas RIA küberturvalisuse teenistuses umbes 30 inimest, siis praegu-seks on meid juba üle saja ja ruumi kasvuks on veelgi. 2023. aasta märtsist alates kanname ka riikide kesksete küberasutuste rahvusvahelist tähist NCSC, mis tuleneb

inglisekeelsest nimetusest National Cyber Security Centre (e.k riiklik küberturvalisuse keskus).

NCSCd on riiklikud kompetentsikeskused, mis tegelevad avaliku sektori ja kriitilise taristu küberturvalisusega ning on võrgu- ja infosüsteemide turbe direktiivi (NIS) mõistes küberturvalisuse pädevad asutused ja kontaktpunktid. Lisaks meie pingutustele Eesti küberruumi parendamisel oli meil aasta jooksul väga palju kohtumisi ja arutelusid meie liitlaste ja partneritega üle ilma. Küberruumis sa ei toimetaks üksi ja suhteid ei hakata looma hetkel, mil kriis on käes, vaid suhtluskanalid peavad olema loodud, testitud ja pidevalt töös.

IDEOLOOGIAST KANTUD RÜNNAKUD

Lisaks Venemaa jätkuvalle agressioonile Ukrainas tõi 2023. aasta sõjalise konflikt ägenemise Iisraeli ja Hamasi vahel. Nägime, ja näeme kindlasti ka edaspidi, ideoloogilise häktivismi kasvu, mis väljendub ennekõike ummistusrünnakutes avaliku, aga ka finants-, transpordi- ja meediasektori vastu. Eestis tõi rekordi september, mil registreerisime 84 DDoS-rünnakut, mida võib seostada meie samumudega Ukraina toetamisel ja idanaabri meedias levinud libauudistega.



Foto: Rene Riisalu

Võrreldes möödunud aastaga on ideoloogiast kantud rünnakud muutunud oluliselt sihitumaks, mistõttu näeme ka mõjuga intsidentide kasvu. Valusa meeldetuletuse, et võid pihta saada sinust tuhandete kilomeetrite kaugusel toimuva konflikti mõjudega, tõi Iisraelis toodetud tööstusautomaatika seadmete vastu suunatud rünnak, mis häiris ka Eesti kohalike katlamajade ja pumbajaamade tööd.

Tuleb nentida, et küberrünnakud on muutunud meile mittesõbralike riikide ja rühmituste jaoks justkui üheks välispoliitiliseks tööriistaks eesmärgiga õõnestada meie turvatunnet. Sellega on vaja arvestada ning võtta juba eos konkreetseid samme nende riskide maandamiseks nii avalikus kui erasektoris.

Andmekaitse ja oma andmete kaitsmine on kindlasti valdkond, mis vajab meie jäagitut tähelepanu ja valvsust ka edaspidi.

Samal ajal tuleb rinda pista ka tavapärase küberkuritegevusega, mis muutub aina nutikamaks ja intensiivsemaks. Ettevõtteid üritatakse maha joosta ummistusrünnetega ning nende tööd halvata lunavaranoüetega. Aina enam kerivad esile just tarneahelarünnakud, kus lõppsihtmärgini jõudmiseks kasutatakse ära väiksemaid teenusepakkujaid. Eestis töid sellised ründed 2023. aastal ettevõtetele miljonitesse ulatuvad kahjud ning panid ohtu ka töötajatele palga maksmise.

KOOS SUUDAME

Oleme teinud pingsat tööd, et pakkuda ettevõtetele tuge küberturvalisuse juurutamisel – koostame selleks regulaarselt juhendeid, hoiausi ja ülevaateid. Kõik need on vabalt leitavad veebilehtedelt ria.ee ja itvaatlik.ee. Ka siit aastaraamatust leiab konkreetseid juhiseid, mida enda kaitseks ette võtta.

Seejuures ei piirdu meie tugi ainult nõuga. Koostöös EAS-Kredexi ühendasutusega pakume ettevõtetele rahalist tuge nii küberkerksuse mõõtmiseks kui ka tõstmiseks. RIA ei saa küberruumi kaitset üksi tagada, küll aga saame seda teha üheskoos.

Möödunud aastal seadsime järelevalves esmakordselt fookuse perearstide infoturbe olukorrale. Uudsuse tõttu algas protsess küll mõnetiste erimeelsustega, kuid aja edenedes kasvas arusaam küberturvalisuse vajalikkusest ja meiegi omalt poolt katsume võimalikult inimlikult selgitada, miks ja millist koostööd me ootame. Teeme pistelisi kontrole selle nimel, et Eesti infoturbestandardisse koondatud nõuded saaksid täidetud.

Aasta tõigi sektoris kaks väga ränka intsidenti. Tarkvaravea tõttu jõudsid riiklikku terviseandmete süsteemi mitmesaja inimese kohta väärad andmed ning geenitestidega tegelevast ettevõttest varastati 10 000 inimese kõige delikaatsemad andmed, mille osas on meil kõigil õigustatud ootus, et neid ükski asjasse mitte puutuv silm ei näeks.

Andmekaitse ja oma andmete kaitsmine on kindlasti valdkond, mis vajab meie jäagitut tähelepanu ja valvsust ka edaspidi. Summad, mis on Eesti inimestelt erinevate pettuste ja õngitsuste abil varastatud, küündivad isiku tasandil kümnetesse tuhandetesse ja koondina mitme miljoni. Kuigi statistika näitab, et Eesti inimeste küberteadlikkus on aasta-aastalt kasvanud, on skeemid, millega meid küberruumis õnge üritatakse tõmmata, peensusteni lihvitud.

Hea lugeja, mul on siiras heameel, et oled leidnud aja sirvida RIA aastaraamatut, milles oleme võtnud kokku möödunud aasta küberruumis nii Eestis kui laiemalt ning sammud, mida on RIA koostöös partneritega teinud, tagamaks meie turvalise eluviisi jätkumist. Loodan, et leiad siit inspiratsiooni ohutumaks küberkäitumiseks ja ehk ka enda tuleviku sidumiseks kübervaldkonnaga. ●



OLUKORD KÜBERRUUMIS: ummistus- rünnete aasta kordus

.....

Ka eelmisel aastal jätsid kasvanud geopoliitilised pinged pitseri Eesti küberruumi. Novembripakases kajas Iisraeli ja Hamasi konflikt küberrünnetena Eesti katlamajades, kuid refräänina saatsid aastat taas teenusetökestusründed, millest rõhuv enamik on seotud Venemaa täiemahulise sõjaga Ukraina vastu.

.....

Novembri lõpus, kui Eestisse olid jõudnud talvised külmakraadid, langes küberrünnaku ohvriks kaugkütteettevõte. Selle tagajärjel lõpetasid töö kaheksa katlamaja juhtseadmed. Katlamajad viidi üle käsijuhtimisele ja ohtu sooja tootmisele ega edastamisele ei tekkinud, kuid seadmed rikuti nii põhjalikult, et need tuli uute vastu vahetada.

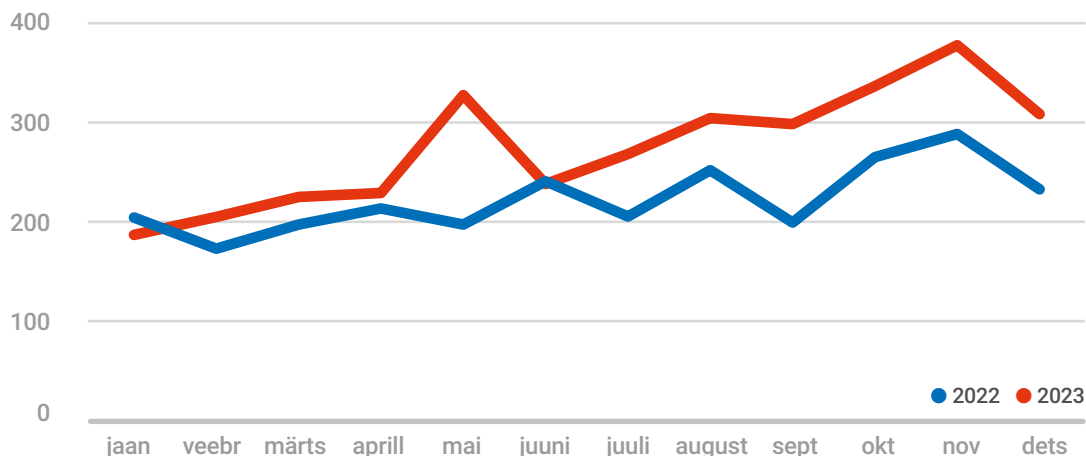
Sarnase ründe ohvriks langes veel vähemalt kaks Eesti ettevõtet, üks neist tegeleb veevarustusega, teine ehitussektoris.

Selle rünnakulaine sihtmärgiks polnud Eesti ettevõtted ega asutused, vaid Iisraelis toodetud tööstusautomaatika kontrollid (PLC-d), sõltumata nende asukohast. Samasuguse rünnaku said pihta näiteks ka USA vee-ettevõtted.

Ründajad väitsid end olevat Iraani taustaga rühmitus ning rünnak oli ajendatud Iisraeli ja Gaza vahel lahvatanud konfliktist. See on järjekordne näide, kuidas geopoliitiliste pingete ja tuhandete kilomeetrite kaugusel toimuvate sõjaliste konfliktide mõju võib jõuda küberrünnakute näol ka Eestisse.



Mõjuga intsidentide hulk kuude lõikes



UMMISTUSRÜNDED PÜSTITASID UUE REKORDI

Ukrainas alanud täiemahulise sõja üks suuremaid ja nähtavamaid kõrvalmõjusid Eesti küberruumis oli ummistusrünnete arvu neljakordistumine. Kui juba 2022 tundus selles osas tihe ja tempokas, siis eelmine aasta purustas varasema rekordi. Registreerisime 484 teenusetõkestusrünnet, mida on 60 protsenti rohkem kui tunamullu. Ainuüksi ühe kuu jooksul registreerisime rohkem ummistusründeid kui sõjaeelsel ajal terve aasta peale kokku.

Mõjuga rünnakuteks lugesime neist 139 ehk vähem kui kolmandiku. Enamasti piirdus kahju mõne veebilehe või muu teenuse lühiajalise katkestuse või tavapärasest aeglasema toimimisega, aga paraku oli erandeid. Kõige nähtavamad olid septembris nähtud rünnakud Elroni

Aasta jooksul muutusid rünnakud nutikamaks ja sihitumaks. Tehti rohkem eeltööd ja suunati oma energia sihtmärkidele, mille puhul oli mõju näha. Sageli toimusid rünnakud kahes laines. Esimene oli lühiajaline ja sellega prooviti sihtmärgi sitkust. Kui tervitusrünnak oli edukas ehk tekitas häireid või katkestusi, järgnes sellele jätkurünnak, mis kestis oluliselt kauem.

Sageli saatsid ummistusrünnakud meie otsuseid toetada Ukrainat või kehtestada Venemaa-le sanktsioone. Poliitiliselt ajendatud rünnakulaineid näeme ka sel aastal. Teenusetõkestusrünnetest kirjutame pikemalt lk 26.

IGA KATKESTUSE TAGA POLE RÜNNAK

Sageli pole teenuse katkemise taga rünnak, vaid inimlik eksitus või rike. 14. septembril katkes ligi tunniks ajaks umbes 25 000 kliendi jaoks kõneste ühe mobiilioperaatori võrgus. Sama operaatori numbritele läksid kõned läbi, aga teistesse võrkudesse mitte. Selle juhtumi põhjuseks polnud rünnak, vaid inimlik viga. Üks vale rida failis jättis kümned tuhanded inimesed kõnesideta.

Novembri alguses hakati ühes haiglas välja vahetama UPSi – see on puhvertoiteallikas, mille eesmärk on hoida seadmeid ja süsteeme voolukatkestuste korral töös. Selle käigus tekkis vooluvõrgus ülekoormus, mille tagajärjel lülitusid välja mitme elektrikilbi kaitsmed ja vool kadus ka UPS- pesadest. Välja lülitusid kõik seadmed (töö-

Ainuüksi ühe kuu jooksul registreerisime rohkem ummistusründeid kui sõjaeelsel ajal terve aasta peale kokku.

piletimüügisüsteeme haldava ettevõtte Ridango vastu. Nende tõttu katkes rongipiletite müük internetis ja rongides olevates terminalides ligi ööpäevaks.

jaamad, printerid jms), mis olid mõjutatud UPS-pesade külge ühendatud, töö lõpetasid võrguseadmed ning patsiendi jälgimisseadmete ja keskjälgimissüsteemi kuvarid. Vooluühendust taastus umbes tund pärast selle kadumist.

Samal kuul oli häireid ka ühe teise haigla töös. Sel korral tekkisid sidekatkestused (nii andmesides kui ka telefonühenduses) valguskaabli füüsilise kahjustuse tõttu. Haigla töötajatele tekitas see ebamugavust, aga patsientide ravi ei kannatanud. Probleemne kaabel vahetati uue vastu ja tavapärase sideühendus taastus.

Sellega lood haiglatest paraku ei piirdu. Juuni lõpus avastati ühes neist, et serverist on teadmata põhjusel kadunud suur hulk faile, mis puudutasid eelkõige administratiivtegevusi (palgaarvestus, e-postiteenus, toitlustus). Tervishoiuteenuse osutamine jätkus, kuid mõningate ebamugavustega. Õnneks olid haiglal olemas toimivad varukoopiad, millelt sai kõik andmed taastada.

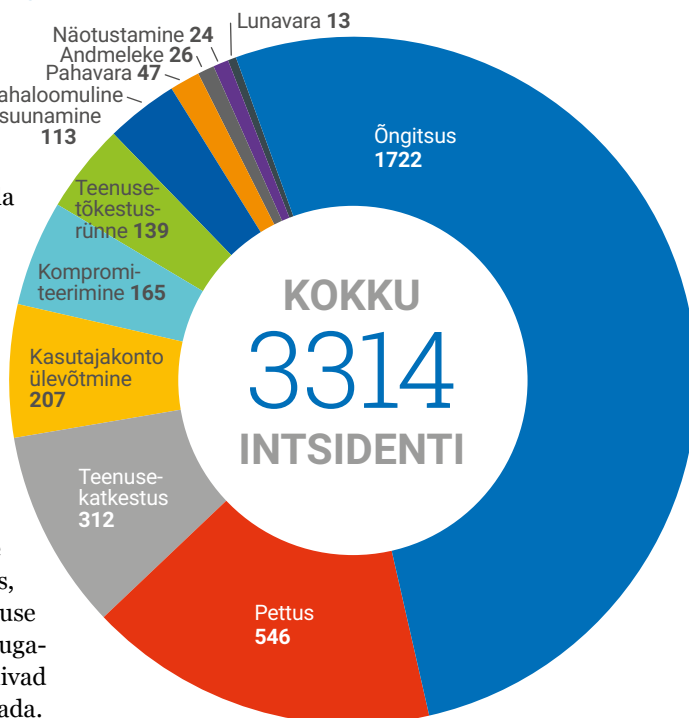
ANDMELEKKED

Mais selgus, et kurjategijad on ühe Eesti kõrgkooli süsteemidest kätte saanud selle tudengite ja vilistlaste andmed – nimed, kasutajanimed, e-posti aadressid, paroolid, IP-aadressid, passi-numbrid jm – ning pannud need müüki. Kuna andmete varastamiseks kasutati uuendamata tarkvaras olnud haavatavust, pakub see meile võimaluse korrata, et turvanõrkused tuleb paigata esimesel võimalusel, mitte lükata neid homse varna.

Märtsis saime teada, et sotsiaalkindlustusamet on kümne kuu jooksul avaldanud Ametlikes Teadaannetes dokumente, mis olid mõeldud asutusesiseseks kasutamiseks. Neis sisaldas detailne info laste ja nende vanemate kohta: vanemad, kes pole elatisraha maksnud; lapsed, kes on oma perekondadest eraldatud; lastele makstud toetused jmt. Inimliku eksituse tõttu oli avaldatud 103 sotsiaalkindlustusameti ettekirjutist, mis pidanuks olema võõraste silmade eest kaitstud.

Ent hullem oli veel ees. September tõi teadmise, et Medisofti Perearst3 tarkvaras, mida

Mõjuga intsidendid 2023. aastal



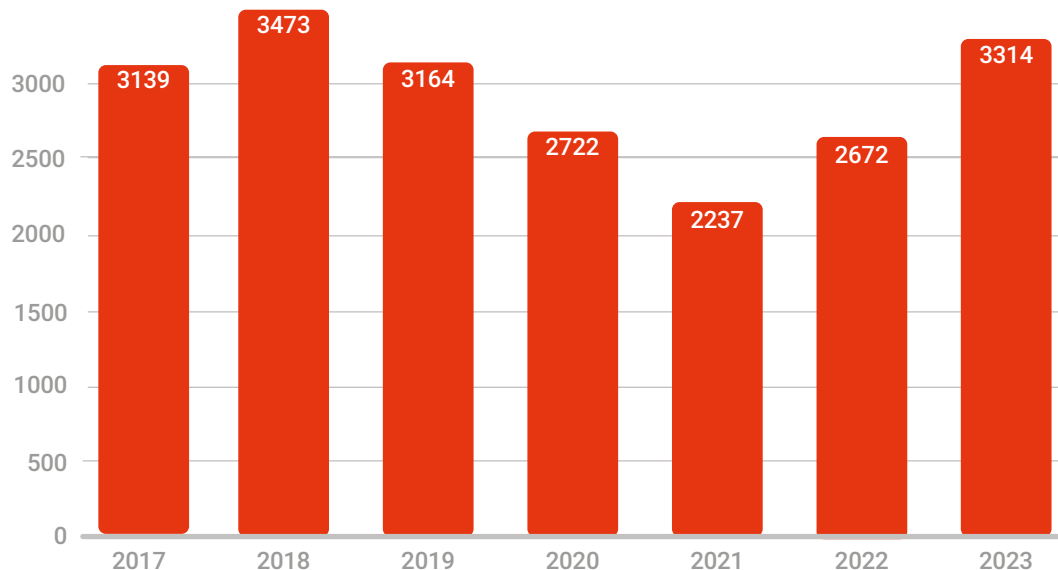
kasutab mitukümmend perearstikeskust patsientide kohta käiva info edastamiseks riiklikku tervise infosüsteemi, oli viga. Selle tõttu sattusid ligi 600 patsiendi haigusluku kellegi teise andmed. Üks probleem on siin andmete konfidentsiaalsuse kadu – patsiendi tervise kohta käivaid andmeid ei tohi näha asjasse mitte puutuvad silmad –, aga veel rängemaid tagajärgi võib kaasa tuua vale info sattumine haigusluku. Selle alusel panevad arstid diagnoose ja määravad ravi. Kui epikriisis olev info on vale, võib vale olla ka ravi. Terviseamet kutsus kiirabi ja erakorralise meditsiini osakondi Perearst3 tarkvara kasutavate perearstikeskuste andmetesse kriitiliselt suhtuma.

Probleeme põhjustanud tarkvaraviga pärines juba 2018. aastal kirjutatud koodist. Medisofti teavitati probleemidest andmete terviklikkusega eelmise aasta märtsis, aga siis pidas ettevõtte seda üksikjuhtumiks ega pööranud veale piisavalt tähelepanu. Selle juhtumi kohta loe pikemalt lk 18.

Leketeaastale pani punkti geneetilise testimisega tegeleva ettevõtte Asper Biogene süsteemi-



Mõjuga intsidentide hulk kasvas aastaga veerandi võrra



dest varastatud umbes 100 000 faili ligi 10 000 inimese isiku- ja terviseandmetega. Ründaja ähvardas need avalikustada, kui ettevõtte ei tasu nõutud summat.

Suuri andmelekkeid on olnud ka varem. Ühe valusama näitena võib tuua 2021. aastal aset leidnud dokumendifotode varguse isikut tõendavate dokumentide andmebaasist. See juhtum mõjutas ligi 300 000 inimest, kuid siis tabati süüdlane koos andmetega mõne päeva jooksul. Nüüd aga lekkisid terviseandmed, mis on dokumendifotodest oluliselt tundlikumad. Kuidas Asper Biogene'i vastu sooritatud rünne toimus ja mida sellest õppida, loe lk 20.

PETTUSTEL POLE OTSA EGA ÄÄRT

Eelmisel aastal tegid mõjuga intsidentidest suurima kasvu erinevad pettused. CERT-EE registreeris mullu 546 pettust, seda on ligi 2,5 korda rohkem kui aasta varem. Politsei- ja piirivalveameti andmetel peteti Eesti inimestelt välja vähemalt 8,3 miljonit eurot. Ainuüksi telefoni-pettustega suudeti ohvritelt välja meelitada kolm miljonit.

Pettuste amplituud on lai nagu Vaikne ookean. Mõni helistav pettur esitleb end politseinikuna, kes aitab ohvrit väidetava pettuse käest pääseda, kuid selle asemel tühjendab ise ta pangakonto. Teine mängib Facebookis huvilist, kes

soovib sealsel turuplatsil müüdavat kaupa osta, aga keelitab müüjat sisestama õngitsuslehele oma pangakaardi andmed või PIN-koodid. Kolmas kompromiteerib mõne ettevõtte e-posti konto ja saadab selle alt partneritele arveid, millel on muutunud arvelduskonto numbrit. Eelmisel aastal üritati ühe sellise skeemi käigus välja petta mitu miljonit eurot, kuid tänu teise osapoolle tähelepanelikkusele jäi petistel sel korral suurem palgapäev tulemata. Kuidas petturid töötavad ja kuidas vältida nende seatud lõksudesse langemist, loe lk 28.

LUNAVARA: VÄHEM RÜNNAKUID, ROHKEM KAHJU

Vaatamata sellele, et registreeritud lunavararünnakute hulk vähenes, oli nende põhjustatud kahju pigem tõusuteel. Kurjategijad teevad põhjaliku eeltööd, võtavad selleks aega ning sihivad Eesti kontekstis suhteliselt suuri ja edukaid ettevõtteid, kes on suutelised kopsakat lunaraha tasuma. Nägime ka seda, kuidas kurjategijad kasutasid IT- ja raamatupidamisteenuseid pakkuvaid ettevõtteid, et jõuda nende hoopis suuremate ja jõukamate klientideni ning istutada sinna andmeid krüpteeriv lunavara.

Selles aastaraamatus on harukordne lugu ühest eelmisel aastal toimunud lunavararünnakust, mis läks otsese kulu ja saamata jäänud

tuluna ohvrile maksma miljonitesse eurodesse ulatuva summa.

Erakordseks ei tee seda kaasnenud kahju, vaid asjaolu, et ettevõtja on valmis sellest avalikult ja avatult rääkima. Enamasti püütakse sellised ebaseadlikud kogemused maha vaikida või unustada, aga me julgustame neist siiski rääkima. See aitab teistel mõista, et laastavate tagajärgedega küberrünnak pole kauge ja abstraktne risk, mis realiseerub haruharva kuskil seitsme maa ja mere taga, vaid reaalne oht, mis võib homme su ettevõtte või asutuse rivist välja lüüa. Varukoopiate tegemine võib tekitada ettekujutuse, et sellega on risk maandatud, kuid paraku suudavad kurjategijad vahel ka need rikkuda. Lunavararünnakutest ja õpetlikust kogemusloost loe alates lk 22.

TURVANÕRKUSED KUI AVATUD USTE PÄEVAD

Möödunud aasta tõi tavapärasest suurema hulga nullpäeva haavatavusi. Need on tarkvaras olevad turvanõrkused, mille olemasolust pole tarkvaratootjal nende kuritarvitamise hetkel

Suhteliselt väikse vaevaga on võimalik oma küberturvet tõsta tasemeni, kus ründajad löövad käega ja otsivad kergemat saaki.

aimugi või pole neile avaldatud turvauuendust. Oktoobris teatas Cisco, et nende võrguseadmete veebileidest ohustab kriitiline turvanõrkus, mille abil on võimalik seade üle võtta. Kolm päeva pärast ametlikku pressiteadet oli Eestis üle võetud sadakond haavatavat seadet.

Nullpäeva turvanõrkused on kuum teema, aga selle varjus kipub ununema, et enamik ründajaid kuritarvitab haavatavusi, mis on ammu teada, tootja poolt tarkvara uue versiooniga parandatud, aga mõne süsteemi või teenuse haldaja pole seda paigaldanud. Sellega kuulutavad nad kõikidele maailma küberkurjategijatele välja avatud uste päevad. Mida kauem oodata, seda suuremaks kasvab tõenäosus, et mõni eba-

meeldiv külaline kutsele vastab ja kohale tuleb.

Näiteks kasutasid ründajad eelmisel aastal ära e-poe platvormis olnud turvanõrkust ja tungisid selle kaudu Eesti elektroonikatoodete müüja e-poodi. Tarkvaratootja avaldas turvauuenduse kuritarvitatud haavatavusele aasta varem, aga see paigaldati alles pärast edukat rünnakut. Loo olulisematest turvanõrkustest leiad lk 32.

ÕNGITSUSED TOIMIVAD ENDISELT

Kõikvõimalike õngitsuste hulk ja osakaal on jätkuvalt tõusulainel: kui 2022. aastal moodustasid need 45 protsenti, siis eelmisel aastal juba üle poole ehk 52 protsenti kõikidest mõjuga intsidendist.

Selles vallas pole petturitel vaja „tootearendusse“ liiga palju panustada, sest paraku toimivad vanad lahendused endiselt. RIA *red team*’i katsed näitavad, et õngitsuslehele läheb ligi kolmandik kirja saajatest ja 10–20 protsenti neist sisestab sinna ka küsitud andmed, näiteks oma konto salasõna.

Jätkuvalt jagunevad õngitsused laias laastus kaheks – kontoõngitsused (kasutajanimed ja salasõnad) ja pangaandmete õngitsused (krediitkaartide andmed, PIN-koodid). Viimaste puhul on kahju kiire tulema, paroolilekke tagajärjed võivad ilmnedu kuude või aastate pärast.

Endiselt levivad laialdaselt näiliselt mõne kullerifirma nimel saadetud õngitsuskirjad ja -sõnumid, mis paluvad paki kättesaamiseks tasuda mõne eurone summa. Kahjuks ei lase paljud ohvrid oma pangakaardiandmeid petturite loodud õngitsuslehele sisestades end häirida ka asjaolust, et nad polnud hiljuti ühestki e-poest midagi tellinud ega oodanud pakki.

GARANTIID POLE

Selles raamatus on palju nõuandeid ja soovitusi, kuidas end küberohtude eest kaitsta. Me ei saa anda garantiid, et nende järgija ei lange pettuse või küberründe ohvriks – sajaprotsendilist kaitset pole olemas. Küll aga teame, et suhteliselt väikse vaevaga on võimalik oma küberturvet tõsta tasemeni, kus ründajad löövad käega ja otsivad kergemat saaki. Ole IT-vaatlik! ●

SÕDA UKRAINA KÜBERRUUMIS: mida näitas aasta 2023?

.....

Ehkki Ukraina pinnal toimuv traditsiooniline sõjategevus saab põhjendatult rohkem tähelepanu, toimub selle taustal aktiivne ründe- ja kaitsetegevus ka küberruumis.

Mida 2023. aasta selles osas tõi?

.....

Maailm jälgib Ukraina sõda küberruumis pinge ja ebamugavustundega juba aastast 2015. Siis põhjustas küberrünnak Ukraina elektrivõrgu vastu südatalvise elektrikatkestuse ligi veerandile miljonile elanikule. Sama suure mõjuga ründed energiataristu vastu ei ole viimastel aastatel kordunud, ent olukord Ukraina küberruumis on kõike muud kui rahulik.

RÄNGIMA TAGAJÄRJEGA RÜNNAK

2023. aastal olid kõige rohkem rünnatud sektorid meedia ja telekommunikatsioon, keskvalitsusasutused ja kohalikud omavalitsused, kaitsevägi ja kaitsetööstus.

Aasta suurima mõjuga intsident toimus 12. detsembril, kui küberrünnak tabas Ukraina suurimat telekomiettevõtet Kyivstar. Hävitusliku ründe tagajärjel sai kahjustada Kyivstari infrastruktuur, mistõttu katkesid mitmeks päevaks nii kõnaside- kui ka internetiteenused

miljonitel inimestel üle kogu Ukraina. Lisaks sellele ei toiminud ka õhuhäire teavitused elanikkonnale. Ründe eest võttis vastutuse Vene sõjaväeluurega (GRU) seostatud tehniliselt võimekas küberrühmitus. Kyivstari tegevjuhi Oleksandr Komarovi sõnul kasutasid ründajad ettevõtte süsteemidesse tungimiseks ühe töötaja kompromiteeritud kontot, kuid juhtumi täpsemaid asjaolusid veel uuritakse.

Uue trendina kerkis esile kohtute ja teiste õiguskaitseasutuste ründamine. Peamiselt Vene riikliku taustaga küberrühmituste eesmärk oli saada kätte andmed kinni peetud sõdurite ja reetmises kahtlustatavate isikute kohta. Samuti soovisid ründajad saada ligipääsu materjalidele, mida Ukraina on kogunud Venemaa toime pandud sõjakuritegude kohta.

Rahvusvahelises meedias kajastati ka küberründeid Hollandis asuva rahvusvahelise kriminaalkohtu (ICC) vastu. Uurimise hõlbustamiseks avas ICC eelmisel aastal esinduse Kiievis



ning andis välja määruse Vladimir Putini vahistamiseks seoses Ukraina laste küüditamisega okupeeritud aladelt Venemaale. Oma küberkerksuse tõstmiseks ja taoliste rünnete edaspidiseks ära hoidmiseks küsis rahvusvaheline kohus abi ka RIA ekspertidelt.

KRIITILISE TARISTU KÜBERKAITSE ON PARANENUD

Jätkusid kriitilise infrastruktuuri vastu suunatud ründed, aga võrreldes varasemaga nende arv vähenes: kui 2022. aasta teises pooles said Ukraina küberasutused teateid 144 ründe kohta, siis 2023. aasta esimeses pooles oli neid 27. Ka ründed hävitusvaraga (ingl *wiper malware*) Ukraina taristu kahjustamiseks jäid pigem täemahulise kallale tungi esimesse aastasse (siiski kasutati suure tõenäosusega hävitusvara eelmainitud rünnakus Kyivstari vastu).

Ukrainas tegutseva küberturbe-ettevõtte Mandiant andmetel toimus üks märgiline intsi-

dent 2022. aasta sügisel, kui GRUGa seotud rühmitus Sandworm põhjustas küberrünnaku-ga elektrikatkestuse ühes Ukraina linnas. Elektriettevõtte süsteemid olid kompromiteeritud juba mõni kuu varem, ent küberrünnaku otsustav faas langes ajaliselt kokku Venemaa Föderatsiooni pealetungiga samas piirkonnas. Mandianti ekspertide hinnangul näitas see Sandwormi kasvavat tehnilist võimekust ohustada tööstuslikke SCADA süsteeme ning on näide kineetiliste ja küberoperatsioonide kombineerimisest. Tõenäoliselt näeme sama käekirja ka tulevaste konfliktide ajal.

Ukraina on viimasel aastal teinud märkimisväärsed jõupingutusi oma kriitilise taristu küberkaitse parandamiseks, seda nii tehniliste kaitsemeetmete kui ka strateegilise juhtimise poolest. 2023. aasta sügisel võeti Ukrainas vastu elutähtsa infrastruktuuri kaitse ning ohutuse ja stabiilsuse tagamise riiklik kava. See dokument määratleb kohustused ja ülesanded nii



elutähtsa infrastruktuuri ettevõtetele kui ka valdkondlikele riigiasutustele ning peaks soodustama avaliku ja erasektori koostööd.

KÜBERINTSIDENTIDE KOGUARV ON TÕUSNUD

Ehkki nende ridade kirjutamise ajaks pole terve aasta intsidentide arv veel teada, võime öelda, et kriitilise tähtsusega küberrünnete hulk 2023. aastal langes, kuid mõjuga intsidente oli siiski varasemast rohkem. Kui 2022. aasta teises pooles oli neid kuus keskmiselt 57, siis 2023. aasta esimeses pooles keskmiselt 128 (andmed pärinevad UKR SSSCIP ülevaatest Russias's Cyber Tactics H1 2023). Sarnast trendi näeme ka Eestis ja paljudes teistes riikides – sõltuvus digitaalsetest teenustest järjest süveneb, haavatavusi tuleb juurde ja ohupilt on viimastel aastatel muutunud halvemaks.

Ukraina andmed näitavad muu hulgas seda, et küberluure- ja muid militaarseid eesmärke täitvate operatsioonide ning poliitilise häktivismi

taustal kubiseb küberruum ka nii-öelda tavalisest küberintsidentidest. Pangatunnuseid ja kontoandmeid õngitsetakse ka ajal, kui riiki tabavad ründedroonid ja lennukipommid. Ettevõtetele saadetakse valearveid ning eraisikuid püütakse petta erinevaid toetusmeetmeid imiteerivate petuskeemide abil. Seejuures on just õngitsused, millega meelitatakse inimesi oma andmeid või kasutajatunnuseid libalehele sisetama, kujunenud üheks peamiseks ründeviisiks nii rahaliselt motiveeritud küberkurjategijatele kui ka eriteenistustega seotud rühmitustele.

Ehkki Ukraina pinnal toimuv traditsiooniline sõjategevus saab põhjendatult rohkem tähelepanu, on rünnakukatsed ja nende tõrjumine küberruumis selle konflikti igapäevane köögi-pool. Nagu eespool öeldud, oli edukate küberrünnete arv kõige tähtsama ehk kriitilise taristu vastu Ukrainas möödunud aastal väiksem kui 2022. aastal. Oma osa on siin ukrainlaste pikaajalisel kogemusel Vene küberrünnete vastu võitlemisel ning liitlaste ja erasektori toel

Ukraina kübeturbeekspert: küberrünnete arv Ukrainat toetavate riikide vastu võib suureneda

Kui vaenlane ei saavuta lahinguväljal piisavat edu, võivad sageneda destruktiivsed küberründed Ukraina kriitilise infrastruktuuri ja Ukrainat toetavate riikide vastu, ütleb intervjuus RIA aastaraamatule Ukraina riikliku julgeoleku- ja kaitsenõukogu küber- ja infoturbedirektoraadi tiimijuht **Serhii Prokopenko**.

Kuidas iseloomustaksite ohupilti 2023. aastal? Mis on muutunud võrreldes sellele eelnenud aastaga?

Ohupilt on muutunud mitmepalgelisemaks. Vene riikliku taustaga ohustajad on endiselt Ukraina jaoks oht number üks, aga oleme näinud mitmeid ründelaineid ka teiste riikide poolt, eelkõige küberluure eesmärgil. Kõik Ukraina küberasutused raporteerisid sel aastal intsidentide arvu kasvu (osalt tänu hoolsamale teavitamisele), ent



Serhii Prokopenko

kriitiliste intsidentide arv on võrreldes 2022. aastaga pigem vähenenud.

Venemaa arendab oma küberründevõimet nii taktika, tööriistade kui personali poolest eriteenistuste (FSB, GRU, SVR) vastavates osades. Samuti paraneb nii küber- kui hübriidoperatsioonide planeerimisvõime.

Vene APTsid (riikliku taustaga küberohustajaid – toim) iseloomustas 2023. aastal järgmine.

rakendatud aina uutel kaitsemeetmetel. Küllap on üheks põhjuseks ka vaenlase seni piiratud suutlikkus integreerida küberründeid vanaaegse robustse vallutussõja eesmärkide saavutamiseks.

LIIGA VARA, ET TEHA KAUGELEULATUVAID JÄRELDUSI

Samas ei saa 2023. aastal Ukraina küberruumis toimunust teha kaugeleulatuvaid järeldusi. Esi- teks on sellele domeenile iseloomulikult suur osa ründeid ja neid ettevalmistavaid tegevusi varjatud, mistõttu võivad olulised sündmused või asjaolud selguda kuid või isegi aastaid hiljem.

Teiseks on kübersõjas jõudude vahekor- datamatult väga muutlik, kuna iga uus päev võib tuua uudise kriitilisest haavatavusest mõnes teenuses või tarkvaras, mis just vaenla- sele trumbid kätte mängib. Ebakindlust ja ette- arvatust on palju, ent mõistagi püüavad riigid – ka Eesti – ukrainlaste kogemusest õppida nii palju kui võimalik. ●

- ❗ Rünatakse konkreetseid asutusi, mitte tervet sektorit.
- ❗ Paraneb võime koordineerida ründeid kineetiliste rünnetega.
- ❗ Küberoperatsioonide fookus ei ole ainult Ukrainal, vaid ka Ukraina liitlastel.
- ❗ Varem toime pandud rünnete käigus saadud infot ja andmeid analüüsitakse põhjalikult ning neid arvestatakse uute planeerimisel.
- ❗ Rünatakse valvekaameraid ja teisi asjade interneti seadmeid, eelkõige luureinfo eesmärgil.

Mida soovitate teistele riikidele? Kuidas kaitsta end küberruumis sellise vaenlase vastu, nagu on Venemaa?

Soovitan teadvustada ohtu, mida kujutavad endast Vene taustaga ettevõtted või ka sobiva taustaga töötajad. Varem või hiljem võivad Vene eriteenistused neid ära kasutada.

Parandada tasub CTI (*cyber threat intelligence*, küberohuteadmus) vahetamise efektiivsust. Sanktsioonidega tuleb piirata Vene tehnoloogia-

Käivitus Tallinna mehhanism Ukrainale küberabi andmiseks

20. detsembril 2023 käivitus Tallinna mehha- nism. See on Eesti ja liitlaste loodud süsteem võimendamaks doonorriikide kübertootust Ukrainale tsiviilvaldkonnas. Mehhanismi eesmärk on viia kokku Ukraina vajadused doonorite võimalustega, nii et abi oleks tõhusam ja võimaldaks Ukrainal end kübersfääris kaitsta.

Tallinna mehhanismi doonorriigid on Eesti, Madalmaad, Kanada, Poola, Prantsusmaa, Rootsi, Saksamaa, Taani, USA ja Suurbritan- nia. Vaatlejalikmed on NATO ja Euroopa Liit. Mehhanismil on Eesti koordinaator Kievis, Poola toetusüksus Varssavis ning Ukraina ja kõigi doonorite esindajatest koosnev koordinatsioonigrupp. Mehhanismi on kaasatud doonorriikide tehnoloogiasektori tippettevõtted.

sektori ligipääsu vajalikule tehnoloogiale ja neid sanktsioone ka päriselt rakendada.

Samuti soovitan jälgida andmelekkeid ja võimalusel piirata lekkinud andmete avalikusta- mist. Väga oluline on ka (vale)infooperatsioonide varajane tuvastamine ja takistamine.

Mida ennustate 2024. aastaks? Kas lisaks küberluurele suureneb destruktivsete rünnete oht?

Ründed kaitse- ja julgeolekusektori vastu kasva- vad. Infooperatsioonid muutuvad veel nutika- maks, sealhulgas tehisarv toel, ja neid viiakse läbi kõikide demokraatlike riikide vastu. Lekkinud isikuandmeid kasutatakse rünneteks sotsiaal- meedia kaudu, ummistusründed muutuvad veel võimsamaks, suureneb tarneahelarünnete oht.

Kui vaenlane ei saavuta lahinguväljal piisavat edu, võib juhtuda, et suurenevad destruktivsed küberründed Ukraina kriitilise infrastruktuuri vastu.

Küberrünnete arv Ukrainat toetavate riikide vastu võib samuti suureneda. ●



Võõrad andmed HAIGUSLOOS

Möödunud aasta septembris avastas üks Raatuse perearstikeskuse patsient enda haigusloo kokkuvõttest võõrad kaebused ja diagnoosi.

Ta oli üks ligi 600 patsiendist, kelle haiguslukku sattusid tarkvaravea tõttu valed andmed.

Kaugeltki mitte kõik intsidendid, mis võivad inimeste heaolu ja usaldust teenuste vastu mõjutada, pole tingitud kellegi pahatahtlikest plaanidest või soovist testida oma osavust mõne infosüsteemi kallal. Vahel võib suure mõjuga kriisi põhjustada vigane kood.

Enda haigusloost võõrad andmed leidnud patsient võttis ühendust perearstikeskusega ja keskus oma lepingupartneriga Medisoft. See ettevõtte pakub Perearst3 tarkvara, mille kaudu saadavad perearstid andmeid riiklikku tervise infosüsteemi, mida kasutatakse patsientide terviseandmete vahetamiseks ja vaatamiseks.

POTENTSIAALNE OHT ELULE JA TERVISELE

Vigastest terviseandmetest võib tekkida ränk potentsiaalne kahju. Nende alusel pannakse diagnoose ja määratakse ravi. Samuti on need aluseks hüvitiste ja toetuste määramisel, näiteks haiguslehe või puude raskusastme hindamise korral. Andmed inimese tervise kohta on tundlikud ja kriitilised, mistõttu ei tohi neid näha asjasse mitte puutuvad silmad.

Perearst3 tarkvara kasutab tervise infosüsteemi andmete edastamiseks 55 perearstikeskust, kellest 45 olid veast mõjutatud. Tervise infosüsteemi haldav Tervise ja Heaolu Infosüsteemide Keskus (TEHIK) piiras ligipääsu vigastele dokumentidele ja mitme päeva vältel oli häiritud ka kiirabide ja erakorralise meditsiini osakondade töö, sest terviseamet kutsus neid üles suhtuma Medisofti tarkvara kasutavate perearstikeskuste andmetesse kriitiliselt.

Kui algselt hinnati vigaseks 672 haiguslugu, siis lõplik hulk on 580. Andmed segunesid juhul, kui perearstil oli korraga lahti mitme patsiendi haiguslugu. Sassi võisid minna kaebused, diagnoosid ja ravi kokkuvõtted.

Esimest korda teavitati Medisofti andmete segunemisest juba möödunud aasta märtsis,

täielikult toimiv ja vigu haigusjuhtude kokkuvõtete edastamisel enam ei teki. Andmekaitse inspeksioon hindas juhtumi põhjuseks harva esineva ja raskesti leitava tarkavaravea ning lõpetas menetluse noomitusega. Vigastes epikriisides sisaldasid teise isiku terviseandmed valdavalt isikustamata kujul, mõnel üksikul juhul oli kirjas ka teise isiku tuvastamist võimaldavaid andmeid, näiteks nimi või isikukood.

Kas vigaste andmete alusel tehti ka raviotsuseid või hinnati abikõlblikkust, pole veel teada. TEHIK analüüsis vigaste andmete kasutust (nt töövoime määramine, kaitseväge teenistusse sobimine jms) ning edastas info vastavatesse asutustesse, et nad saaksid vajadusel eelnevalt tehtud otsuseid muuta.

KES VASTUTAB?

TEHIKul endal lepingulist suhet Medisoftiga tervise valdkonna infosüsteemide arenduseks ei ole. Lepingulises suhtes on Medisoftiga eraettevõtjatena tegutsevad perearstid, kellel on kohustus tagada terviseandmete kättesaadavus kogu tervishoiusüsteemis.

Äärmiselt kahetsusväärse juhtumi üheks laiemaks õppetunniks võib lugeda seda, et lepingutes tuleks võimalikult täpselt reguleerida nende eraettevõtete küberturvalisust puudutavad kohustused, kes pakuvad teenuseid avalikule sektorile või elutähtsate teenuste osutajatele, aga ei ole ise küberturvalisuse seaduse subjektid.

Vastutus hangitava teenuse turvalisuse eest on tellijal ja seda ka juhul, kus vastavat teenust või tarkvara pakkuvate ettevõtete ring on piiratud. Seetõttu tuleks lepingus lahti kirjutada ka teenusepakkujatele esitatavad nõuded ja kohustused, näiteks tegevused turvaintsidentide korral.

Riigi jaoks on aga mõttekoht, kas tulevikus oleks otstarbekas laiendada küberturvalisuse seaduse nõudeid ka neile ettevõtetele, kelle pakutavatest teenustest sõltuvad avalik sektor ja muud olulised teenuseosutajad. ●

Riigi jaoks on aga mõttekoht, kas tulevikus oleks otstarbekas laiendada küberturvalisuse seaduse nõudeid ka neile ettevõtetele, kelle pakutavatest teenustest sõltuvad avalik sektor ja muud olulised teenuseosutajad.

kuid siis pidas tarkvaraarendaja seda üksiku juhtumiks ega pööranud sellele piisavalt tähelepanu. Tegelikult pärines tarkvaraviga 2018. aastal kirjutatud koodist. Perearst3 käideldavust see viga ei mõjutanud, küll aga andmete terviklikkust ja konfidentsiaalsust.

Medisoft kõrvaldas vea tarkvarauuendusega ja kinnitab, et Perearst3 infosüsteem on nüüd

ASPER BIOGENE'i ANDMELEKE: mis täpsemalt juhtus?

Detsembris sai avalikkus teada, et geneetilise testimisega tegeleva ettevõtte Asper Biogene süsteemidest laaditi ebaseaduslikult alla ligi 10 000 inimese isiku- ja terviseandmed ning ähvardati need avalikustada.

Paraku pole andmelekked kaugeltki nii haruldased, kui me sooviks. Oleme neist kirjutanud ka varasemates aastaraamatutes, kuid millestki võrreldavast pole pidanud seni teada andma. Asper Biogene'i lekke teeb eriti ebameeldivaks asjaolu, et võõrastesse kättesse sattusid inimeste kõige tundlikumad andmed.

KUIDAS RÜNNE LÄBI VIIDI?

Nii nagu paljud teised ründed, sai seegi juhtum alguse kehvast küberhügieenist. Juba septembris proovisid ründajad ettevõtte serverite kallal erinevaid ründeviise ning leidsid päringu, millega said kätte edasise rünnaku jaoks vajalikud andmed. Nende abil sisenes ründaja Asper Biogene'i infosüsteemi ja hakkas sealt andmeid alla laadima.

Nädala jooksul laaditi andmebaasist alla ligikaudu 100 000 faili, milles on praegustel andmetel umbes 10 000 inimese isiku- ja terviseandmeid. Osa failidest sisaldas geneetiliste analüüside tulemusi, mida haiglad ja teised ter-

vishoiuteenuse osutajad ning eraisikud olid ettevõttelt tellinud. Failide seas on näiteks PDF-faile, milles on inimese nimi, isikukood ja analüüside vastused. Juhtumiga on seotud 42 haiglat ja tervishoiuteenuse osutajat, kellele Asper Biogene teenust osutas. Neist tuntumad on Ida-Tallinna keskhaigla ja Tartu Ülikooli kliinikum.

MAKSA VÕI AVALDAME ANDMED

Ettevõtte sai juhtunust teada alles siis, kui suurem kahju oli juba sünninud ja neile 11. novembril lunarahanõue esitati. Saadetud kirjas ähvardati kõik alla laaditud andmed avalikustada, kui ettevõtte ei maksa nõutud summat.

Ettevõtte käitus selles olukorras õigel viisil – ei maksnud lunarahanõuet, vaid võttis ühendust RIA, politsei ja andmekaitse inspektsiooniga. Samal ajal suleti kõigi süsteemide ligipääsud ja hakati kohe logisid uurima.

Selle käigus selgus, et kurjategijad käisid juba septembris Asper Biogene'i ukselinke lõgistamas. Edukas sisenemine ettevõtte süs-



teemidesse toimus 1. novembril ja 3.–10. novembrini laaditi failid alla. Ründajad varastasid ühtekokku 33 GB mahus erinevaid andmeid.

Juhtumi osas algatas politsei kriminaalmenetluse, andmekaitse inspeksioon järelevalvemenetluse ja väärtemenetluse. Juhtumi täpsemaid asjaolusid veel selgitatakse.

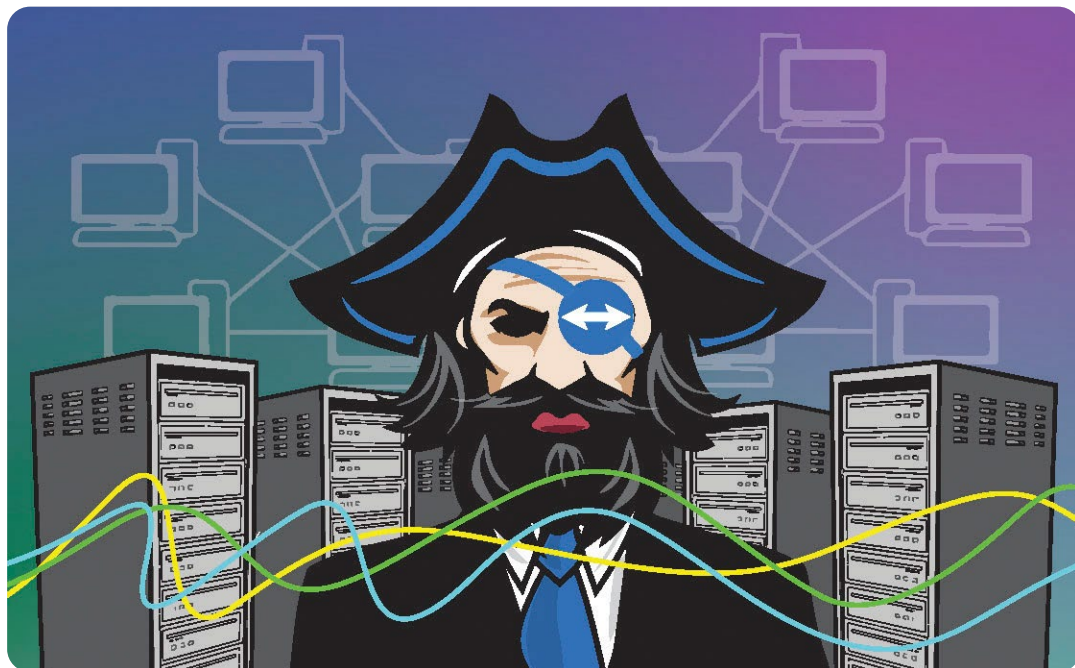
MIDA SAAB PAREMINI TEHA?

Toome mõned konkreetset soovitused, mida võiks niisuguste juhtumite vältimiseks järgida.

- ❖ Kasuta igal pool, kus võimalik, kaheastmelist autentimist. Paroolide lekkimine ei ava ründajale kiirteed ohvri süsteemidesse, kui lisaks kasutajanimele ja paroolile on vaja kasutada ka näiteks telefonile saadetavat ühekordset koodi.
- ❖ Kasuta erinevates keskkondades erinevaid parooli. Paroolide riskasutamisel on oht, et salasõna lekkimise korral saavad avalikuks nii isiklikud kui ka tööga seotud kontod.
- ❖ Tee avalikus võrgus kättesaadavaks ainult

vajalikud teenused. Kui kaughaldus on vajalik, tõsta seadmed tulemüüri taha ning kasuta kaheastmelise autentimisega kaitstud VPNi ehk virtuaalset privaativõrku.

- ❖ Kasuta viimast tarkvaraversiooni ning veendu, et kõik uuendused on paigaldatud. Tihtilugu toimuvad ründed just paikamata turvaaukude ehk uuendamata tarkvara kaudu.
- ❖ Varunda regulaarselt veebiserveri ja andmebaasi sisu välisesse asukohta. Toimiva varukoopia abil on võimalik küberintsidendi korral (nt pahavara paigaldamine) kiiremini töö taastada.
- ❖ Hoia delikaatseid isikuandmeid (sh terviseandmeid) krüpteeritud. Kui ründajal õnnestub krüpteeritud andmed varastada, ei saa ta neid avada.
- ❖ Vii läbi regulaarseid turvatestimisi. Turvatestimise käigus selgitatakse välja infosüsteemide puudused ning saadakse info selle kohta, mis vajab parandamist. ●



LUNARAHANÕUDED

tabasid mitut suurt tootmisettevõtet

2023. aastal teavitati CERT-EED mitmest lunavararünnakust, mille ohvriks langesid Eesti mõistes suured, sadade töötajatega ettevõtted.

Näiteks rünnati oktoobris üht Tallinna suuret ettevõtet, kus pahavaraga krüpteeriti kahes serveris olnud andmed. Rüündajad kasutasid lõppsihtmärgini jõudmiseks raamatupidamisfirmat, mille süsteemidesse tungiti kaugtöölaua protokoll (RDP) kaudu. Õnneks olid ettevõtte lukustatud andmetest värsked varukoopiad, tänu millele oli võimalik süsteemid taastada.

KOLM ÕPPETUNDI

Sellest juhtumist võib ammutada korraga lausa kolm õppetundi. Esiteks on Eestis ja ka mujal maailmas kasvav probleem tarneaahelarünnakud, mille käigus sageli kasutatakse IT- ja raamatupidamisteenuseid pakkuvaid ettevõtteid, et jõuda nende hoopis suuremate ja jõukamate klientideni. Seetõttu tasub ettevõtetel teenuste sisseostmisel tõsiselt analüüsida, kas partnerite

küberturbe olukord on ikka piisavalt hea ning millistele süsteemidele ja milliste õigustega on otstarbekas neid ligi lubada.

Samamoodi on levinud riskikoht nõrgalt kaitstud kaugtöölaud või VPN-võrk. Paraku näitavad CERT-EE monitooringuandmed, et Eestis leidub endiselt üle tuhande avalikult internetist kättesaadava kaugtöölauda, kuigi nende omanikke teavitatakse sellega kaasnevatest ohtudest sideettevõtete kaudu regulaarselt.

Ette on tulnud kurioosne lugu, kus IT-mees pani tööpäeva lõpus ajutiselt kaugtöölauda püsti, kavatsedes selle hommikul uuesti maha võtta, aga enne teda jõudsid kurjategijad kohale ja võtsid ettevõtte süsteemid maha. Häkkerid seiravad võrke pidevalt ja võivad nõrku kohti mõne tunniga ära kasutada.

Oktoobrikuine juhtum kinnitas taas kord töökindla ja muudest süsteemidest eraldatud

ei saaks süsteemi pääsedes kohe igale poole ligi. Näiteks tootmisseadmed peaksid asuma eraldatud võrgus, millele pääsevad ligi ainult kontrollitud isikud kontrollitud seadmetest. Kindlasti tuleks võrguliiklust ka monitoorida. Kui teenuseid hoitakse eraldi segmentides, peavad ründajad ringi liikudes rohkem „lärmi“ tegema. See aitab seirel sissetungijaid avastada.

ÄRA TOIDA KURJATEGIJAJAID

Juhul kui varundusest pole abi ja süsteeme tuleb hakata nullist üles ehitama, võib sellega kaasneda suur majanduslik kahju. Seetõttu on inimlikult mõistetu, miks osa rünnakuga pihta saanud ettevõtteid on otsustanud lunaraha maksmise kasuks. Teisalt tasub mees pidada, et see taastoodab kuritegevust, andes häkkerirühmitustele motiivi üha uusi rünnakuid korraldada. Samuti võidakse rünnaku käigus varas-

tatud andmed müüki paisata ja nende eest hiljem uuesti raha välja pressida või parandamata jäetud nõrku kohti jälle ära kasutada.

50 rahvusvahelise lunaravastase initsiatiiviga ühinenud riiki, nende seas Eesti, tegid 1. novembril 2023 ühisavalduse, millega nende

valitsusasutused lubavad edaspidi vältida lunaraha maksmist, näidates positiivset eeskuju.

Samuti rõhutati avalduses vajadust tõhustada koostööd erasektoriga. Sarnaselt enamiku maailma riikidega registreeritakse Eestis ainult väike osa lunavarajuhtumitest, mis raskendab võitlust küberkuritegevusega. Ettevõtjad on väljendanud kartust, et kui nad mõnd riigiasutust juhtunust teavitavad, võib sellega kaasneda karistus küberturbereeglite rikkumise eest või mainekahju juhtumi avalikuks tuleku tõttu.

RIA kinnitab, et ei karista kannatanuid, vaid aitab neid intsidendi lahendamisel, jagades oma oskusteavet ja võimalusel ka näiteks dekrüpteerimisvõtmeid. Juhtunu kohta info avaldamine jääb iga ettevõtte enda otsustada, kuid RIA peab seda väga kiiduväärseks – näo ja nimega kogemuslood panevad märksa paremini probleemi üle järele mõtlema kui anonüümsed hoiatused. ●

RIA kinnitab, et ei karista kannatanuid, vaid aitab neid intsidendi lahendamisel, jagades oma oskusteavet ja võimalusel ka näiteks dekrüpteerimisvõtmeid.

varunduse olulisust rünnaku tagajärgedega toimetulekul. Sarnaselt õnnestus oma infosüsteemid ja andmed kiiresti taastada ühel Lääne-Eesti tööstusettevõttel, mida lunavararünnak tabas detsembri lõpus. Nende puhul kasutati rünnakuks ära nõrka VPNi parooli.

Üle ega ümber ei saa me ka küberhügieenist, sest paljud lunavararünnakud algavad lihtsast õngitsusest, millega hõivatakse mõne töötaja kasutajakonto. Endiselt teevad ründajatele rõõmu seadmete vaikeparoolid, paikamata turvanõrkused ja vananenud tarkvara, mida tootjad enam ei toeta. Kui kasutada kaheastmelist autentimist ja automaatuendusi ning panna vabalt veebist ligipääsetavad teenused VPNi taha, kahaneb oht rünnaku ohvriks langeda märkimisväärselt.

Tootmisettevõtete jaoks on oluline vahend küberrünnakuga kaasnevate ohtude maandamiseks võrkude segmenteerimine, et kurjamid

RÜNNAK, mis läks maksma miljoneid

.....

Mullu tabas lunavararünnak kaht Harjumaal tegutsevat metallitööstusettevõtet, kus töötab kokku ligi 400 inimest. Firmade juhid räägivad avatult, mis ja miks juhtus, et aidata teistel sarnaseid ohte vältida.

.....

S amale äriperekonnale kuuluvad AS Estanc ja Tammer OÜ toodavad metallist aknaid, uksi ja mahuteid. Nende käive ulatub kokku 60 miljoni euron. Eelmise aasta alguses said mõlemad ettevõtted pihta lunaraharünnakuga, mille tagajärjel tootmine kuuks ajaks osaliselt peatus. Ettevõtete eestvedaja Mihkel Tammo sõnul jäi seetõttu saamata seitsmekohaline summa tulu, millele lisandus otsene kahju.

RÜNNAKU AVASTAMINE

Esimene märk, et midagi on valesti, ilmnes 1. veebruari varahommikul. Tammeri IT-juht Indrek Kink ärkas kell 6.20 telefonikõne peale, milles helistaja teatas, et IT-süsteemidele ei pääseta teadmata põhjusel ligi.

Teel kontorisse tegi Kink veel mitu kõnet ja kell 7.15 autoga Estanci parklasse jõudes oli selge, et tegemist on lunavararünnakuga. „Paraku olid ründajad selleks ajaks tõenäoliselt juba mõnda aega võrgus sees olnud, süsteeme kaardistanud ja plaane sepistanud,“ meenutab Kink. Tema sõnul ei saa öelda, et ettevõtete IT-süsteemid olid halvasti turvatud – ohtudest oldi teadlikud, kriisiplaanid olemas ja regulaarsete tagavarakoopiate süsteem paigas.

KAHE HALVA JUHUSE KOKKULANGEMINE

Nõrgaks kohaks osutus vana e-posti server, mille ülesanded olid tegelikult juba pilve kolitud. Pärast kolimist aga selgus, et serverit on siiski veel tarvis – see pandi ajutiselt taas tööle, kuid uuenduste haldamise süsteemi seda enam ei liidetud. Ajutine lahendus, nagu nendega pahatihti juhtub, jäi aga kasutusele plaanitud pikemaks ning paikamata Microsoft Exchange Serveri turvanõrkus ProxyLogon avas ründajatele pääsu sisevõrku.

Sealt edasi õppisid kurjategijad ettevõtete süsteeme vargsi tundma. Nad said aru, et neist tehakse sageli varukoopiaid, mistõttu polnud neil mõtet lihtsalt andmeid krüpteerida – ettevõtted oleksid saanud need võrdlemisi kerge vaevaga koopiast taastada.

„Paraku saime alles kuu pärast intsidenti teada, et koopiate tarkvaras oli avastatud nn nullpäeva turvaauk, millega pääseti ligi administraatorikontole. Seda kasutati nii lokaalsete kui ka pilves peidus olevate koopiate kompromiteerimiseks ja nende sisu lihtsalt kustutati,“ selgitas Kink. See andis kurjategijatele viimase puuduva pusletüki – ära võeti võimalus kasutada varukoopiaid – ja nad otsustasid rünnata.



VÕITLUS MITMEL RINDEL

Kui küberkriminaalid olid süsteemid halvanud ja lunarahanõude esitanud, peatus ühes ettevõttes kuuks ajaks tootmine peaaegu täielikult. Seisaku tagajärjed andsid tunda veel mitu kuud hiljemgi. „Tol hetkel oli seis kriitiline – meil oli vaja palgad maksta kahe ettevõtte peale rohkem kui 400 töötajale. Me tulime siiski toime,“ meenutab Mihkel Tammo. Kui äripoolel oli vaja tegeleda kahjude minimeerimisega, siis IT-tasandil pandi paika esiteks kolm võimalikku lahenduskäiku: taastada andmed vähemalt ühe varukoopia töölesaamisega, ehitada kogu andmearhitektuur nullist üles või sõlmida ründajatega võimalikult soodne kokkulepe.

Kohe esimestel päevade kaasati juhtumi lahendamisse küberturbeettevõtte CYBERS, samuti oldi pidevas suhtluses RIA intsidentide käsitlemise osakonnaga (CERT-EE).

Varukoopiate taastamisega nähti palju vaeva. Osa faile saadi kätte, kuid paraku olid need rikutud. Samal ajal tehti juba ettevalmistusi kõikide süsteemide nullist üles ehitamiseks. „18. veebruariks olime läbi katsetanud kõik mõeldavad lahendused ja tundus, et tuleb kurjategijate seljatamise osas käed üles tõsta,“ tõdes Kink.

Läbirääkimised kurjategijatega võttis enda peale CYBERSi tegevjuht Jürgen Erm: „Esialgu, kui veel teised võimalikud lahendused laual olid, mängisime rumalaid, et kurjategijatele mitte liiga palju infot anda. Samuti proovisime neilt saada mingitki tõestust või garantiid, et lunarahamakse tegemise järel saame andmed ka päriselt tagasi.“ Tammer OÜ juht Anti Tammo kinnitas, et otsus lunaraha maksta ei tulnud kergekäelselt: „Kaalusime läbi kõik muud variandid, meie IT-inimesed töötasid väsimatult erinevate lahenduskäikude kallal. Kuna lunarahanõue oli kordades väiksem, kui oleksid olnud kulud nullist ülesehitamisel, otsustas juhatus proovida.“

ÕPPETUNNID JA JULGUS RÄÄKIDA

Indrek Kingi hinnangul sai rünnak võimalikuks mitme halva sündmuse kokkulangemise tõttu: „Praeguseks oleme oma süsteeme täiendanud just turvaaspektist ja lisanud veel ühe, täielikult *offline* tagavarakoopia tegemise.“ Kuna reeglina ei soovita küberrünnakutest avalikult rääkida, kiidab Jürgen Erm ettevõtteid julguse eest: „See aitab ära hoida järgmisi võimalikke rünnakuid. Hetkel on valdav enesetsensuur, kardetakse mainekahju. Aga see näide on elav tõestus, et kahju rääkimisest ei teki – pigem vastupidi.“ ●

UMMISTUS- RÜNDED: mullu purunes senine rekord

.....

Teenusetõkestusrünnete poolest oli möödunud aasta eelkäijale väärikas mantlipärija. Ei löödud ainult massiga, rünnakud muutusid ka paremini sihituks.

.....

Mullu registreeris CERT-EE 484 ummistusrünnakut (DDoS-rünnakut), mida on 182 võrra rohkem kui 2022. aastal. Keskmiselt tehti iga kuu ligi 40 DDoS-rünnet ja enamasti oli ründeteravik suunatud avaliku sektori vastu. Ummistusrünnete eesmärgiks on valitud sihtmärgi üleujutamine suure hulga päringutega, et veebilehe, andmebaasi või muu teenuse tööd häirida. Osad eelmise aasta DDoS-rünnakutest olid väga intensiivsed. Näiteks tehti ühe elutähtsat teenust osutava ettevõtte vastu rünnaku ajal päringuid sellises mahus, mis täituks tavakorras mitme aasta jooksul.

ENAMIKUL RÜNNAKUTEL POLNUD MÕJU

Lõviosa Eesti suunal tehtud ummistusrünnetest ei põhjustanud olulist kahju ega pikki katkestusi olulistes teenustes, kuid oli ka ebameeldivaid erandeid. Näiteks sügisel nähtud rünnakute tõttu Elroni piletimüügisüsteeme haldava ettevõtte Ridango vastu katkes rongipiletite müük internetis ja rongides.

Kaheteistkümne kuu seast paistis kõige rohkem välja september, mil CERT-EE registreeris

84 DDoS-rünnakut. See on meie mõõtmisajaloo absoluutne rekord. Rahulikumal ajal registreerisime sama palju rünnakuid terve aasta jooksul.

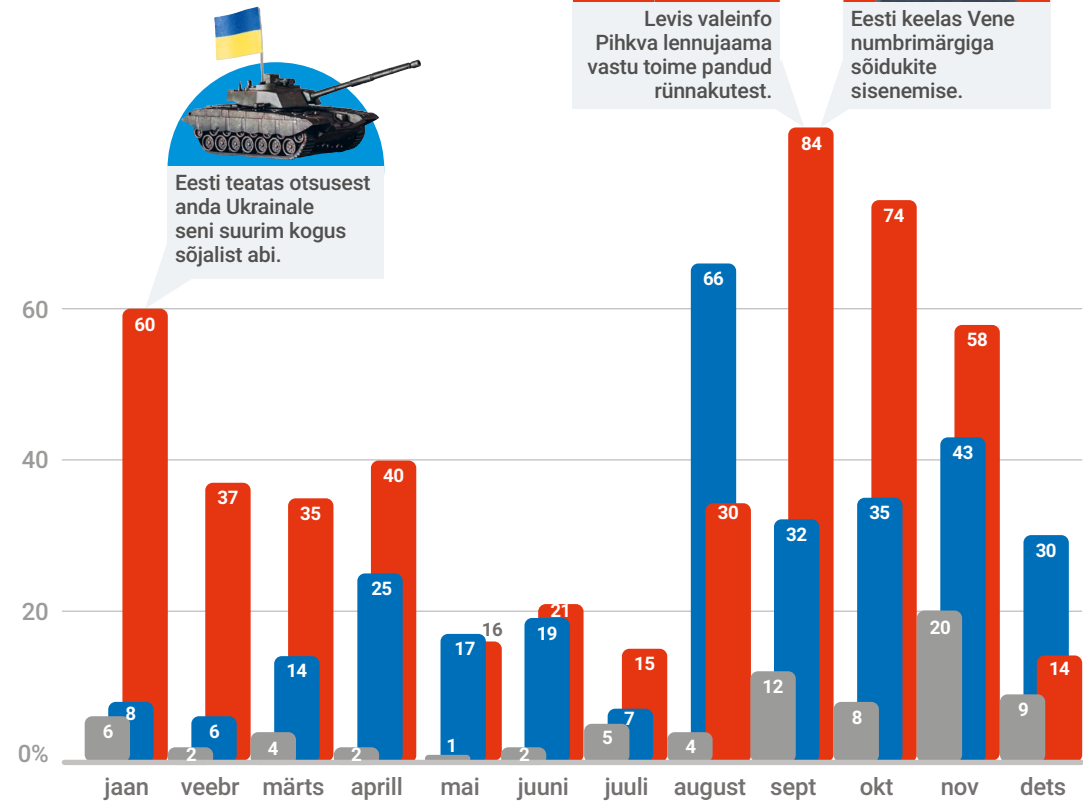
Mis selle rekordi tõi? Tõenäoliselt kaks sündmust. Esiteks levisid augusti viimastel päevadel idanaabri meedias kuuldused, nagu oleks Eesti süüdi Pihkva lennujaama vastu toime pandud rünnakutes. See libauudis tõi mõni päev hiljem DDoS-rünnakute laine Eesti veebilehtede vastu. Teiseks põhjuseks võis olla Eesti otsus keelata Venemaa numbrimärgiga sõidukite sisene mine Eestisse.

Poliitilistest sündmustest ja otsustest ajendatud DDoS-rünnakud on muutunud tavapäraseks nähtuseks ning tõenäoliselt jätkub see trend ka sel aastal.

RÜNNAKUD MUUTUSID SIHITUMAKS

Möödunud aasta tõi Eesti vastu suunatud DDoS-rünnakutes ka mõned muutused. 2022. aastal tehtud ummistusrünnakud olid pigem lihtsakoelised, samalaadsed ning kohati sihti nööri järjepidevusega veebilehti, mille tööd ei suudetud häirida. 2023. aastal nägime aga, et rünnakud muutusid sihitumaks, tehti rohkem

Kuus sama palju rünnakuid, kui muidu aastas



● 2021 ● 2022 ● 2023

eeltööd ja ründajad proovisid kõigest väest sihtmärke maha joosta.

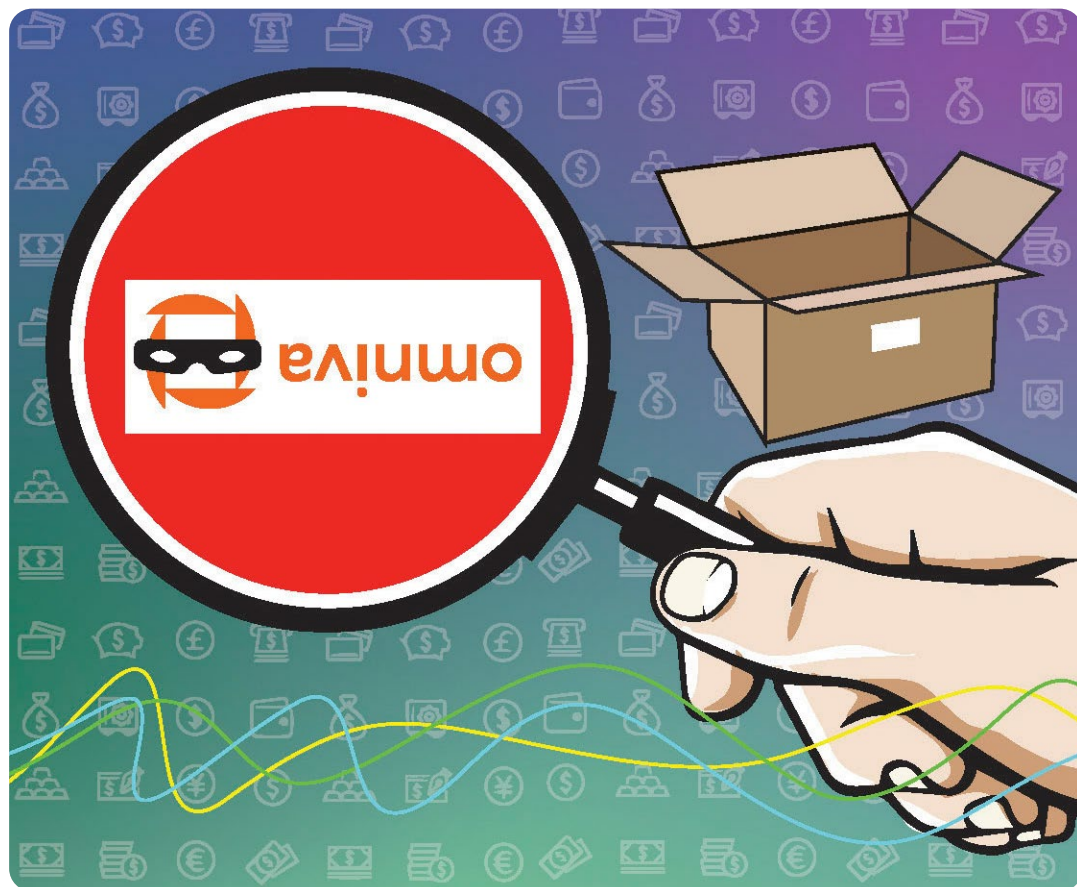
Enamasti kehtisid rünnakud lühikest aega ja sageli kasutati nende tegemiseks pilveteenust pakkuvate ettevõtete servereid. Lühiajaliste rünnetega testiti sihtmärgi vastupidavust. Kui sissejuhatav rünnak tekitas häireid või katkestusi, järgnes sellele juba oluliselt kauem kestnud jätkurünnak.

Lisaks eelnevale iseloomustasid möödunud aastat sagenenud rünnakud nimeserverite vastu. Nimeserverid viivad omavahel kokku õige IP-aadressi ja domeeninime, et kasutaja ei peaks näiteks RIA veebilehele jõudmiseks kirjutama sirviku aadressireale numbririda, vaid ria.ee. Tegu on omamoodi telefoniraamatuga – kui seda edukalt rünnata, mõjutab see korraga paljude veebiteenuste tööd. ●



Mida võib tuua 2024. aasta?

- Tõenäoliselt muutub DDoS-rünnakute tase paremaks, mistõttu võib mõjuga rünnakute hulk kasvada.
- Jätkub pilveteenust pakkuvate ettevõtete serverite kasutamine DDoS-rünnakuteks.
- Internetti lisanduvad IoT-seadmed võivad kasvatada DDoS-rünnakute intensiivsust. Tihti on sellised seadmed nõrgemate kaitsemeetmetega ja neid on kergem üle võtta. Kompromiteeritud seadmeid saab kasutada DDoS-rünnakute läbiviimiseks.
- Jätkuvad poliitilistest sündmustest ajendatud DDoS-rünnakud.



PETTUSTE AASTA JÄRELEHÜÜE: kus mu raha on!?

Kui ettevõtetele valmistasid eelmisel aastal peavalu ummistusründed, lunavara ja andmelekked, siis tavakasutajaid kimbutasid igast võimalikust kohast sisse trügivad pettused. Eelmisel aastal petsid kurjategijad Eesti inimestelt välja vähemalt 8,3 miljonit eurot.

Nagu meie digiühiskond, on ka küberkuritegevus viimaste aastakümnete jooksul tormiliselt arenenud. Ehkki esimene digitaalne pangarööv toimus juba 1995. aastal, oli küberkuritegevus veel selle sajandi alguseski suhteliselt uus ja harvaesinev nähtus. Sageli olid küberkurjategijateks noored, kes oma oskuste ja tehnoloogia abil hävitasid süsteeme või häirisid inimesi, kuid enamasti ei teinud nad seda eesmärgiga teenida rahalist kasu.

Olukord muutus, kui üha suurem osa pangandusest, kaubandusest ja suhtlusest kolis interneti. Sinna, kuhu liiguvad raha ja inimesed, seavad sammud ka kurjategijad. Mõne e-kanali kaudu toime pandud pettustest ehk e-pettusest on praeguseks saanud populaarseim küberkuritegevuse vorm, mille osakaal on ka Eestis järjest kasvanud.

PEENSUSTENI LIHVITUD MASINAVÄRK

E-pettused on üha keerukamad ja leidlikumad. Vanade ja toimivate mõjutusvahendite – hirm, ahnus ja suhtlemisvajadus – kõrval on kasutusel uued tehnoloogiad, näiteks tehisintellekt ja masinõpe. Tegu on organiseeritud kuritegevusega, mis on detailideni lihvitud. Suurtes kõnekeskustes töötavad sajad inimesed, kes lähtuvad petukõnesid tehes etteantud stsenaariumitest – potentsiaalse ohvri tõenäoliste vastuste ja reaktsioonide jaoks on valmis kirjutatud eraldi jutuliinid.

Tegu on omamoodi konveieriga: üks „spetsialist“ loob ohvriga usaldusliku suhte, teine tutvustab „investeeringusvõimalusi“, kolmas juhendab, kuhu andmed sisestada ja kuidas tehinguid teha. Kui tavapärasel konveieril panakse midagi kokku, siis selle liini mõte on lahutada ohver tema rahast.

Ühele meie poole pöördunud inimesele helistas vene keeles kõnelev isik, kes tutvustas end politsei- ja piirivalveameti töötajana. Võltspolitseinikul õnnestus kõnele vastanud inimest veenda, et pettur on tema nime alt teinud notariaalse volituse ning oma raha kaitsmiseks tuleb kiirelt tegutseda. Surve alla pandud ohver sisestas võltspolitseiniku palvel oma ID-kaardi PIN-koodid ning avastas järgmisel päeval, et tema nimel üri-

Kuidas PÄÄSEDA ärikirjapettusest?

- **Ole IT-vaatlik ja ära sisesta oma paroole kahtlastele lehtedele.** Enamik BEC-skeeme saab alguse kompromiteeritud meilikontost ja need omakorda mõnest paroolilekkest või õngitsuslehele sisestatud salasõnast. Samuti muudavad meilikonto haavatavaks liiga lihtsad või äraarvatavad paroolid.
- **Koolita kolleege,** et nad oleks teadlikud BEC-skeemidest ja muudest pettustest.
- **Kontrolli üle, kas teine osapool tahab tõesti pangarekvisiiti muuta.** Kui teine osapool soovib viimasel hetkel oma pangarekvisiiti muuta, tuleks enne tehingu sooritamist veenduda, et soovi avaldas tõesti äripartner, mitte temana esinev pettur. Vahel piisab kiirest telefonikõnest. Seejuures ei tasu helistada kirjas olevale telefoninumbriks, vaid otsida see ettevõtte ametlikult kodulehelt.
- **Rakenda meiliserverile turvameetmed.** Autentimisprotokollid nagu SPF, DKIM ja DMARC aitavad meilide võltsimist vältida. Lisaks tuleb rakendada kaheastmeline autentimine, kuna see vähendab oluliselt tõenäosust, et kurjategijad meilikontole ligi saavad.
- **Kontrolli saatja meiliaadressi ja muid ebakorrapärasusi.** Vahel registreerivad petturid domeeni, mille kirjapilt sarnaneb mõne tuntud ettevõtte omaga. Pealiskaudsel vaatlusel ei pruugi ühetäheline erinevus silma jääda.

tati pangast 5000 eurot laenu võtta. See ei õnnestunud, kuid paraku said petturid ohvri pangakontolt ligi 10 000 ja ta abikaasa omalt üle pooleteise tuhande euro. Ainuüksi telefonipettuste ohvreid oli politsei- ja piirivalveameti andmetel möödunud aastal 524 ja neile põhjustatud rahaline kahju kolm miljonit eurot.

Teine inimene sai näiliselt Omniva saadetud õngitsuskirja, milles paluti tarne eest tasuda. Kuna ta oli hiljuti e-poest kaupa tellinud ja vali-



nud selle kohaletoiemtamiseks Omniva teenuse, sisestaski ta petturite loodud õngitsuslehele oma pangakaardi andmed. See viga läks ohvrile maksma üle 10 000 euro.

Kolmas müüs Facebook Marketplace'i kaudu parfüümi. Temaga võttis ühendust potentsiaalne ostja, kes soovis kulleritarnet Elvasse. Ta saatis müüjale Omnivat matkiva õngitsuslehe ning palus müüjal sisestada sinna vajalikud andmed ja need PIN-koodiga kinnitada. Seda ohver ka tegi. Samal ajal logis pettur sisse tema ja tema ettevõtte pangakontole, kust varastas ligi 13 000 eurot.

ÄRIKIRJAPETTUSTEGA PÜÜTI VÄLJA PETTA MILJONEID EUROSID

BEC (*Business Email Compromise*) ehk ärikirjapettus on petuskeem, mille käigus kurjategija kompromiteerib mõne ettevõtte meilikonto, jälgib seal toimuvat kirjavahetust ning sobival hetkel sekkudes saadab sellelt välja arve, mis on äravahetamiseni sarnane õigega. Ainus erinevus on kontonumber.

Kui tavapärased e-pettused, nagu õngitsused ja petukõned, on enamasti tehtud juhuslikele tavakasutajate numbritele ja meiliaadressidele, siis BEC-skeemide puhul teevad petturid põhjalikku eeltööd ning sihivad konkreetseid ettevõtteid. Seetõttu on edukad BEC-skeemid rahalise kahju poolest palju laas-

tavamad kui tavapärased e-pettused.

Aasta lõpus üritati BEC-skeemiga ühelt ettevõttelt välja petta miljonitesse eurodesse ulatuv summa, kuid õnneks jäid kurjategijad sel korral saagita, sest tähelepanelik töötaja kontrollis koostööpartnerilt üle, kas nad on tõesti panka muutnud ja arve tuleb tasuda nüüd uuele kontole.

BEC-skeeme saab läbi viia kahel moel, sõltuvalt sellest, kas kompromiteeritud on ostja või müüja meilikonto. Kui kompromiteeritakse teenust või kaupa müüa plaaniva ettevõtte või eraisiku meilikonto, saadetakse kliendile arve, millel on valed pangarekvisiidid. Klient ei aima midagi halba, kuna arve tuleb ettevõtte ametlikult meiliaadressilt, ning kannab raha petturile. Sageli tuleb pettus välja mitu nädalat hiljem, kui ostja hakkab uurima, miks tellitud kaup pole kohale jõudnud. Ostja on enda meelest sel-

Edukad BEC-skeemid rahalise kahju poolest palju laastavamad kui tavapärased e-pettused.

le eest tasunud, aga raha ei läinud mitte müüja, vaid petturite kontole.

Kui aga petturitel õnnestub kompromiteerida meilikonto, mille omanik plaanib midagi osta, peavad nad tegutsema teisiti. Kõigepealt vaata-

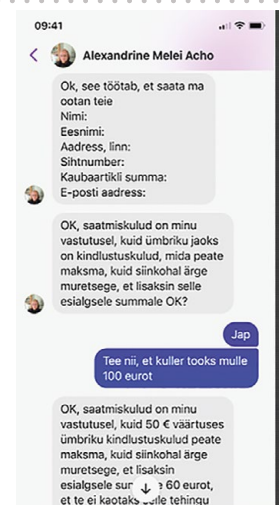
Facebook Marketplace'i pettuste anatoomia

Möödunud aastal sai CERT-EE kuus korda rohkem teateid õnnestunud Facebooki Marketplace'i pettuste kohta kui 2022. aastal.

Petturitel on nimekirjad, mis sisaldavad kümneid tuhandeid Eesti elanikele kuuluvaid meiliaadresse ja telefoni-numbreid. Nende alusel tehtud masspostituste – milles sageli jälgendatakse mõnd panka või kullerifirmat – edu sõltub lisaks õngitsuskirjade ja -lehtede kvaliteedile ka juhusest. Kui petturid saadavad välja õngitsuskirjad,

mis imiteerivad mõnd konkreetset panka või kullerifirmat, jõuab suur osa neist inimesteni, kes pole selle panga kliendid ega oota kullerifirmalt pakki. Piltlikult öeldes viskavad petturid potitäre spagette vastu seina lootuses, et mõned neist jäävad sinna püsima.

Facebook Marketplace'i kaudu toimuvad pettused on paremini sihitud. Seal otsivad kelmid inimesi, kes parasjagu midagi müüa üritavad ning võtavad nendega ühendust, väites, et soovivad pakutava ära osta. Seejärel



vad nad üle varasema kirjavahetuse isikuga, kellele meilikonto omanik plaanib raha kanda. Kasutades kirjavahetuses olevat informatsiooni (nt aadressaadi meilinimi, tehingu üksikasjad, summa jne), saadavad petturid teiselt meiliaadressilt kirja samale kompromiteeritud meilikasutajale, matkides ettevõtet, millele isik pidi raha kandma. Tihti peale muudavad petturid kompromiteeritud meilikonto reeglistikku nõnda, et tehingu teise osapoole kirjad ei jõuaks sinna kohale, vaid suunatakse petturite meilikasti.

KAKS EDUKAT PETTUSE TÜÜPI

Eelneva ilmestamiseks sobivad möödunud aastast kaks kurjategijate vaates edukat ärikirja-pettust.

1 Oktoobris sai sõidukite müügiga tegeleva ettevõtte töötaja Malle (nimi muudetud) kirja sõsarettevõtte raamatupidajalt, kes teatas, et Malle on meili teel palunud oma ettevõtte pangarekvisiite muuta. Malle taipas hetkega, et midagi on valesti, kuna sellist kirja polnud ta saatnud. Olukorda uurides avastas ta, et sõsarettevõtte on võõrale pangakontole saatnud juba ligi 40 000 eurot.

Kuna oma meilikontolt välja saadetud kirju läbi vaadates ei leidnud ta sealt midagi kahtlast, palus Malle raamatupidajal endale edastada meili, kus temana esinenud pettur palus pangarekvisiite muuta. Raamatupidaja tegi seda kahel korral, kuid kummalgi juhul ei jõudnud

kiri Malle postkasti. Selgus, et tema meilikonto oli kompromiteeritud juba tükk aega tagasi ning petturid olid selle alt pahaloomulise kirja saatnud kaks kuud enne pettuse avastamist. Petturid kustutasid saadetud kirjade kaustast pahaloomulise kirja ning muutsid meilikonto reeglistikke nii, et kompromiteerimist oleks raskem tuvastada.

2 Kalle (temagi nimi on muudetud) soovis osta autot ühelt Saksamaa ettevõttelt. Olles leidnud sobiva sõiduki, võttis ta ühendust autot müüva ettevõtte töötajaga ning pärast lühikest kirjavahetust jõudsid nad ostu-müügitehingus kokkuleppele. Kalle saatis ettevõtte esindajale oma kontaktid ning lepingu vormistamiseks vajalikud detailid. Mõni päev hiljem sai ta lepingu vastu, vormistas selle ning saatis ettevõttele tagasi. Vaid tund aega hiljem võttis inimene, kes esines sama ettevõtte esindajana, temaga ühendust ja saatis uue lepingu, kus olid muudetud pangarekvisiidid. Esialgu ei kahtlustanud Kalle pettust ning kandiski uuele pangakontole ligi 50 000 eurot. Kahtlus, et midagi on valesti, tekkis alles siis, kui ta sai ettevõttelt uue kirja, milles paluti lisaks 20 000 eurot, kuna Saksamaal olla käibemaksumäär tõusnud ja auto vabastamiseks on vaja lisaraha. Kalle võttis ühendust ettevõtte töötajatega, nüüd juba telefoni teel, ning kuulis, et mingit raha pole nad talt saanud. ●

Viada

<https://omniva.ee-inform.kaubavedu.com/cash40788071>

Ma olen juba maksnud tarne eest, te ei pea midagi maksma, palun võtke minuga ühendust, kui olete kõik kinnitanud ja kulleriga ühendust võtnud.

Peate järgima seda linki ja esitama oma aadressi, nime ja telefoninumbri ning raha kantakse teie kontole. Kui raha on üle kantud, võtab kuller teiega ühendust, et leppida kokku teile sobiv aeg ja kuupäev paki kättesaamiseks.

leiavad nad erinevaid ettekäandeid, miks hoopis müüja peab esimesena raha välja käima (nt kauba kohaletoimetamine või kindlustus). Nad lubavad, et maksavad pärast kõik kinni, aga esmalt peab müüja tellimuse ära vormistama.

Sageli küsivad petturid müüja nime, aadressi, telefoninumbrit jms. Küllap saab neidki andmeid edasi müüa ja järgmiste pettuste läbiviimisel ära kasutada, kuid eelkõige küsitakse neid käimasoleva vestluse usutavamaks muutmiseks. Tegelik

lõks on hoopis õngitsusleht, mille petturid ohvrile veebilingina saadavad. Petuleht jälgendab erinevaid kulleriteenuseid (Omniva, DPD, DHL vms).

Pahaaaimamatu ohver, kel on hea meel, et oma kaubast lõpuks lahti saab, sisestab küsitud andmed ja „kinnitab tehingu“ Smart-ID või mobiil-ID PIN-koodiga. Samal ajal kui kasutaja sisestab oma andmed õngitsuslehele, sisenevad petturid nende abil ohvri pangakontole ning võtavad sealt, mis võtta annab.

Tavapärasest rohkem NULLPÄEVA TURVANÕRKUSI

Sarnaselt eelnevatega kihas ka 2023. aasta erinevatest haavatavustest, kuid eriliseks tegi selle nullpäeva turvanõrkuste hulk ja nende avalikustamise sagedus.

Kevadel tabas üht e-poodi küberrünnak, mille tagajärjel võidi ligi pääseda klientide isikuandmetele. Ründajad kuritarvitasid e-poe tarkvaras olnud turvanõrkust, mille paranduse oli tootja avalikustanud rohkem kui aasta varem. Kuigi uuendamisega venitamise taga võib olla rida põhjuseid (hind, keerukus, veebilehe käideldavus jne), tasub teisele kaalukausile panna edukas rünnak ja selle tagajärjed. Need võivad olla pöördumatud.

AEGUNUD PISTIKPROGRAMMID AVAVAD TURVAUKSED

Eesti küberruumis näeme tihti veebilehti, mille uksed on pärani lahti. Möödunud aastal teavitas CERT-EE ligi 500 korral veebilehtede hal-



dureid turvanõrkustest, mis olid seotud konkreetsest mõne platvormi plugina ehk pistikprogrammiga. Leidsime ka veebilehti, mis olid aegunud pluginate tõttu juba üle võetud.

Mida rohkem pistikprogramme veebilehel kasutada, seda laiem on võimalik ründepind. Olukorra muudab keerulisemaks asjaolu,

et veebilehte jooksvat platvormi uuendamine ei pruugi automaatselt värskendada pistikprogramme, vaid selleks tuleb teha mõned lisasammud. Paraku jäävad need sammud sageli tegemata ning see avab ukse soovimatutel külalistele.

Kui ligipääs veebilehele on olemas, sõltub edasine ründaja eesmärkidest. Võimalik on lisada veebilehele pahavara, mis varastab külastajate andmeid (sh pangaandmeid), suunab nad petulehtedele jpm.

NULLPÄEVA TURVANÕRKUSTE AASTA

Möödunud aastat jäid meenutama nullpäeva turvanõrkused, eelkõige nende hulk ja avalikustamise sagedus. Nullpäeva haavatavus on nõrkus, millest tarkvara loojad pole selle ära kasutamise hetkel teadlikud või millele pole turvauuendust. Näiteks parandas Apple 2023. aastal 20 nullpäeva turvanõrkust ja Google Chrome'i veebibrauseris seitse. Vahel kasutavad seda tüüpi turvanõrkusi ära riiklikud ohustajad. Näiteks rünnati suvel Norra valitsusasutusi just ühe tarkvaraplatvormiga seotud nullpäeva turvanõrkuse abil.

Nullpäeva turvanõrkust kasutati 2023. aastal ka Eesti küberruumis. Nimelt teatas Cisco oktoobris, et nende võrguseadmete veebiliidest ohustab kriitiline turvanõrkus, mille abil on võimalik seade täielikult üle võtta. Ohustatud olid kõik võrguseadmed, mille veebiliides oli internetist avalikult kättesaadav. Kolm päeva pärast Cisco ametlikku pressiteadet oli Eestis üle võetud sadakond haavatavat seadet.

See näitas, kui kiiresti ründajad haavatavad seadmed tuvastavad ning need kompromiteerivad. Seadmete ülevõtmine ei pruugi olla enam päevade, vaid tundide küsimus. Teiseks tõestas see kaasus, kui suureks ohuks võib olla kõik, mis on internetist avalikult kättesaadav. On olukordi, kus otse internetti paisatud seade on vältimatu ja alternatiivseid lahendusi pole, kuid liiga palju nägime seadmeid, mis tegelikult poleks tohtinud avalikus internetis olla.

PUUGIPROGRAMM KOGUS HOOGU

Alates RIA *bug bounty* programmi loomisest 2022. aastal on meid teavitatud ligi 11 000 korral, neist 7859 jäi eelmisse aastasse. Üle poole teavitustest olid seotud XSS (*cross site scripting*) turvavigadega. XSS-rünnak tähendab piltlikult öeldes seda, pahalane riputab avalikule reklaamtahvile (veebilehele) kahjuliku sõnumi, mille tagajärjel jagavad seda näinud inimesed (veebilehe külastajad) temaga tundlikke andmeid või teevad muud pahalasele kasulikku.

Selleks, et XSS-vigu avastada, tuleks veebirakendusi regulaarselt testida. Samuti tuleks veenduda, et kasutusel pole aegunud tarkvara, mis võib XSS-vigu põhjustada. ●

9 SOOVITUST, kuidas end turvanõrkuste vastu kaitsta

1 Hoia operatsioonisüsteemi, rakendusi ja muud tarkvara ajakohasena.

Tarkvaravärskendused sisaldavad sageli parandusi turvaaukude jaoks, mis on avastatud pärast viimast värskendust. Automaatsete värskenduste lubamine tagab, et need ei jää paigaldamata.

2 Kasuta usaldusväärset ja uuendatud viirusetõrjetarkvara.

Sellised programmid suudavad tuvastada ja eemaldada pahavara, mis üritab turvaauke ära kasutada.

3 Ole e-kirjade, sõnumite ja veebisaitidega IT-vaatlik.

Andmepüügirünnakud püüavad välja petta tundlikku infot või meelitada pahavara alla laadima. Väldi meilides olevate kahtlaste linkide või manuste klõpsamist, eriti kui need on pärit tundmatutest allikatest.

4 Loo igale kontole tugev ja kordumatu parool.

See aitab vältida olukordi, kus ühe salasõna lekkimise korral on ründajatel võimalik ligi pääseda ka teiste kontodele, mis sama parooli kasutavad. Vajadusel kasuta paroolihoidlat.

5 Võimalusel kasuta mitmeastmelist autentimist (MFA).

Siis ei piisa konto kaaperdamiseks parooli lekkimisest.

6 Hoia end kursis turvaohutudega.

Selleks soovitame liituda CERT-EE uudiskirjaga ja lugeda RIA blogi, kust leiad iganädalased kokkuvõtted olulisematest turvanõrkustest.

7 Anna kasutatavale tarkvarale ja rakendustele ainult vajalikud load.

Õiguste piiramine võib vähendada ohtu, et pahatahtlik tarkvara pääseb ligi tundlikele andmetele.

8 Kaitse oma võrku.

Kasuta turvalist WiFi-ühendust ja kaalu täiendava turvalisuse tagamiseks VPNi (virtuaalne privaatvõrk) kasutamist.

9 Hari end ja lähedasi küberturvalisuse heade tavade osas.

Mida IT-vaatlikumad oleme, seda väiksem on tõenäosus, et langeme küberrünnete ohvriks. Kasulik materjale leiad itvaatlik.ee ja ria.ee.



2023. AASTA sündmused rahvusvahelises küberruumis

.....

Geopoliitilised pinged, eelkõige Venemaa kestev agressioon Ukrainas ning oktoobris lahvatanud konflikt Iisraeli ja Hamasi vahel, peegeldusid ka rahvusvahelises küberruumis, kuid taustal käis tavapärane küberkuritegevus.

.....



Kuidas APTd toimivad

APTd kasutavad oma ohvrite püüdmiseks sageli täpselt sihitud õngitsusi – huvi pakkuv inimene, näiteks ajakirjanik või diplomaat, saab pealtnäha tavalise meili koos manusega. Manuseks võib olla tööalane raport, asutuse eelarve, kutse mõnele koosviibimisele – peibutisena kasutatakse mis tahes teemat, millega sihtmärk arvatavalt iga päev kokku puutub ning mis seetõttu ei ärata kahtlust.

Kui riiklikud ohustajad ehk APTd on üldiselt tehniliselt võimekad, hästi ette valmistatud ja soovivad oma jälgi peita, siis häktivistid tegutsevad risti vastupidiselt. Nemad suhtlevad sageli erinevates sotsiaalmeedia-kanalites, õhutavad üksteist „karistusaktsioonidele” teiste riikide vastu ning hooplevad oma saavutustega veebilehtede või teenuste häirimisel.

Valitsuste heaks töötavad tehniliselt võimekad küberrühmitused, mida nimetatakse üldterminiga APT (ingl *Advanced Persistent Threats*), üritasid koguda strateegilist infot vastaste kohta ning mitmel juhul neid ka pahavaraga nakatada.

SIHIKUL UKRAINA RIIGIASUTUSED JA KRIITILINE TARISTU

Juulis avalikustas Ukraina CERT, et Vene eriteenistusega FSB seotud küberrühmitus **Gamaredon** ründas aktiivselt Ukraina riigiasutusi. Sihtmärkidele saadeti pahavara sisaldavaid faile, mis avamise korral asusid süsteemist andmeid varastama.

Nagu ka varasematel aastatel, ohustasid Vene taustaga rühmitused Ukraina kriitilist taristut, üritades tungida muu hulgas Ukraina elektriettevõtte võrku ja seal katkestusi põhjustada. Detsembris tabas ulatuslik küberrünnak Ukraina telekommunikatsiooniettevõtet **Kyivstar**, mille tõttu jäid miljonid inimesed üle Ukraina mitmeks päevaks kõneste- ja internetiteenuseta.

KÜBERRÜNNAKUTEGA RIIGIKASSAT TÄITMA

Küberründed kriitilise taristu vastu leidsid aset ka mujal, mitte ainult kriisikolletes. Novembris tabas küberrünnak Austraalia suurimat sadamate käitajat **DP World Australia**, mille kaudu liigub ligikaudu 40 protsenti Austraaliasse toodavast kaubast.

Ettevõtte teatel kompromiteeriti kriitilised süsteemid ning meretransport ja kaubalastide liikumine oli mitu päeva tõsiselt häiritud. Ehkki ründaja ei ole praeguse seisuga teada, viitavat rünnaku tehniline keerukus pigem riikliku taustaga ohustajale, mitte rahaliselt motiveeritud küberkurjategijatele.

Mõned riiklikud rühmitused keskendusid aga riigikassa täitmisele – Põhja-Korea rühmitust **Lazarus** seostatakse 2023. aastal mitmesse suurde krüptovahendusplatvormi (Eesti taustaga Atomic Wallet, CoinsPaid, Alphapoint) tungimisega. Küberturbefirma Recorded Future hinnangul on Lazarus varastanud viimase kuue aasta jooksul kolme miljardi dollari väärtuses krüptovarasid, millega on rahastatud riik-



likke projekte. Samuti süüdistab FBI Lazarust septembri alguses läbi viidud 41 miljoni dollari vargusega hasartmänguplatvormilt **stake.com**.

HÄKTIVISM VOHAS EDASI

2022. aastal tugevalt esile kerkinud ideoloogiline häktivism levis küberruumis ka 2023. aastal. Häktivistide peamine relv oli ikka ummistusrünne – ummistada püüti vastumeelsete riikide valitsusasutuste veebilehti, aga ka näiteks transpordi-, finants- ja meediasektorit.

Poliitiliselt motiveeritud häktivismi tüüpilise näitena võib tuua **Saksa veebilehete ummistamise** aasta alguses, kui Berliin oli heaks kiitnud otsuse saata Ukrainale tanke, või Leedu turismi- ja transpordiettevõtete kodulehete ummistamiskatsed Vilniuses 2023 suvel aset leidnud NATO tippkohtumise eel. Detsembris põhjustasid mitmel pool maailmas ärevust Iisraeli-vastased häktivistid, kes asusid ründama Iisraeli päritolu tööstusautomaatika seadmeid. Iirimaal Mayo maakonnas mõjutas selline tegevus kohalikku vee-ettevõtet, mistõttu jäi ligi paarsada inimest kaheks päevaks veevarustuseeta.

LUNAVARA KÜLVAS KAOST

Lunavararünded olid 2023. aastal levinud ja tulus kuritegevusliik, mille ärimudel pidevalt areneb. Erilise aktiivsusega paistis silma lunavararühmitus **Lockbit**.

Jaauanuaris ründas Lockbit Ühendkuningriigi postiettevõtet **Royal Mail**, mille tõttu hilines tuhandete piiriüleste saatetiste kohaletoometamine paari kuu võrra. Ettevõtte sai endale palju frustratsioon klientide ja oli sunnitud ründest ajendatuna tegema aasta jooksul infrastruktuuri ja protsesside parandusi rohkem kui kümne miljoni euro eest.

Oktoobris tungis sama rühmitus lennundusgigandi **Boeing** IT-süsteemidesse ning varastas seal 45 gigabaidi mahus andmeid, mille abil lunaraha välja pressida. Novembri alguses tabas Lockbitiga seostatud lunavararünnak Hiina suurimat kommertspanka ICBC.

Suurt ärikahju põhjustas läinud sügisel ka meelelahutus- ja hotellikontserni **MGM Resorts** vastu läbi viidud lunavararünnak, mille tõttu seiskunud tegevusest kaotas ettevõ-

tte hinnanguliselt üle saja miljoni dollari. Lisaks häirisid lunavararünded möödunud aastal mitmel korral USA erinevate linnade olulisi munit-sipaalteenuseid ning finantssüsteeme.

Lunavararühmitused tegutsevad üldiselt oportunistlikult, säästmata isegi tervishoiusektorit. Kohe läinud aasta alguses tabas lunavararünnak **Barcelona haiglat**, mille tõttu tuli edasi lükata 150 plaanilist operatsiooni ning tühistada 3000 arstivastuvõttu.

Jõululaupäeval sai üks Saksamaa haiglakett pihta lunavaraga, mille tõttu katkes kolmes haiglas erakorralise meditsiini osakonna töö ning patsiendid tuli niigi pingelisel pühadeajal ümber suunata. Rhysida-nimeline rühmitus ründas ühte haiglat Jordaania ning mainekat erahaiglat Ühendkuningriigis, varastades seejuures ka tundlikke meditsiiniandmeid, et ohvreid jõulisemalt survestada.

LEKKISID KÜMNETE MILJONITE INIMESTE ANDMED

Nii valitsused kui eraettevõtted olid möödunud aastal sunnitud mitmel korral teavitama suurtest andmeleketest. Näiteks jaauanuaris teatas globaalse haardega telekomiettevõtte **T-Mobile**, et nende andmebaasist on lekkinud 37 miljoni kliendi nimesid ja kontaktandmed.

Augustis teatas Ühendkuningriigi valimiskomisjon, et nende vastu pandi toime pikaajaline ja kompleksne küberrünnak. Häkkeritel õnnestus kätte saada valimisregistrite andmeid miljonite valijate kohta, sealhulgas nimesid, aadressid ja telefoninumbreid. Ehkki valimiskomisjoni kinnitusele ei mõjuta see kuidagi valimiste endi turvalisust, suurendab isikuandmete lekkimine suunatud õngitsuste ja identiteedivarguste ohtu.

Prantsuse tööamet teatas möödunud aasta augustis samuti suurest andmelekkest. Lekkisid ligi kümne miljoni töötaja nimesid ja sotsiaalkindlustusnumbrid, amet oli sunnitud informeerima oma riigi andmekaitseinspeksiooni. Kurjategijate jaoks oli ilmselt tegemist juhusliku saagiga, väidetavalt paisati andmebaas tumeveebis müüki vaid 900 dollari eest.

Küberrünnakute tagajärjel ei lekkinud delikaatseid meditsiiniandmed ainult Eestis, vaid ka mujal. Suvel rullus lahti skandaal Beverly

Hillsis tegutseva tunnustatud **ilukliiniku** ümber: kurjategijatel oli õnnestunud sisse murda kliiniku infosüsteemi ja varastada sealt patsientidega seotud infot. Kuna kliinik väljapressimisnõudele ei reageerinud, hakkasid kurjategijad postitama patsientide „enne“- ja „pärast“-fotosid ning nende ilulõikuste üksikasju, kusjuures kliiniku kliendid polnud andmevargusest isegi teadlikud.

TARNEAHELARÜNDED: ÜKS VIGA, TUHAT OHVRI

Juba aastaid on nii Eesti kui teiste riikide küberametid hoiatanud suureneva tarneahelarünnete ohu eest. 2023. aasta üks enim kajastatud tarneahelarünnak toimus failivahetuskeskonna **MoveIT** kaudu.

Üldiselt väga turvaliseks peetavas tarkvaras leidis nullpäeva turvanõrkus, mida asus varasuvel aktiivselt ära kasutama lunavararühmitus **Clop**. Kuna failivahetuskeskkonda kasutavad väga paljud organisatsioonid üle maailma, tõusis ohvrite arv kiiresti 1000 asutuse ja ettevõtte, millest enamik asub Ameerika Ühendriikides.

Samas sai ka eelmainitud Prantsuse tööametit tabanud andmeleke alguse just kliendihaldustarkvara pakkuva ettevõtte **Majorel** kaudu, kes oli paar kuud varem langenud MoveITi tarneahelaründe ohvriks. Majorelil on harukontor ka Eestis, kuid meile teadaolevalt Eesti kliente see rünne ei mõjutanud.

Märtsis kompromiteerisid väidetavalt Põhja-Korea taustaga häkkerid tarkvaraettevõtte **CX3** konverentskõnede rakenduse. Selle kasutajate seas on rahvusvahelisi ettevõtteid alates hotellikettidest kuni tervishoiuteenuse pakkujateni, mis kasutavad rakendust hääli- ja videokõnede jaoks. Seejuures õnnestus häkkeritel tarkvaraettevõtte süsteemidesse ligi pääseda teise tarkvaraettevõtte Trading Technologiesi kaudu, mille pahavaraga nakatud tarkvara üks CX3 töötaja kogemata alla laadis. Tegemist oli tarneahelaründega, mis viis järgmise tarneahelaründeni.

Ka Põhjamaades põhjustasid ründed teenusepakkuja kaudu täbaraid intsidente. Juulis teatas **Norra valitsus**, et 12 ministeeriumi on mõjutatud ulatuslikust küberrünnakust. Kõik

need ministeeriumid sõltusid ühest teenusepakkujast, kelle tarkvaras leidis turvanõrkus.

Augustis jäi mitusada ettevõtet Taanis ilma oma veebilehtedest, meiliteenustest ja muudest andmetest, mis olid usaldatud pilvepõhiste teenusepakkujate **CloudNordic** ja **AzeroCloud** hoolde – viimaseid tabas lunavararünnak ja andmeid taastada ei õnnestunud.

MÕNED EELISTAVAD VAIKIDA

Vaevalt leidub maailmas riiki, kes oleks 2023. aastal küberrünnetest täiesti puutumata jäänud. Erinev on aga see, kui palju riigid või ka ettevõtted nendest avalikult räägivad ja milliseid samme astuvad, et küberriske vähendada ning rahvusvahelist küberkuritegevust ohjata.

Mais teatas **USA valitsus** koos teiste Viie Silma (luureinfo jagamise ühendus, kuhu kuuluvad Austraalia, Suurbritannia, Kanada, Uus-Meremaa ja USA) riikidega, et ühisoperatsiooni tulemusel on kahjutuks tehtud Vene eriteenistuse FSB loodud ja juba 20 aastat kasutusel olnud küberluurepahavara **Snake**. Naiivne oleks arvata, et sellega Vene küberluure intensiivsus maailmas märgatavalt väheneb, küll aga näitab see Viie Silma riikide soovi ja võimet niisuguste ohtudega üheskoos ja tulemuslikult tegeleda.

Möödunud aasta sügisel kutsus USA oma lähimaid partnereid, sealhulgas Eestit, alustama strateegilist dialoogi seni vähem tähelepanu saanud kolmanda sektori küberturvalisuse suurendamiseks. Ehkki tulemustest rääkida on veel vara, võib ometi öelda, et nii poliitilise kui rahalise ressursi suunamine ühiskonna küberturvalisuse tõstmisesse on parem, kui hiljem kahjudega tegeleda.

Ja lõpetuseks – läinud aasta tõi halva uudise paljudele ametnikele, kes olid harjunud tööseadmest meelelahutuseks **TikToki** videoid vaatama. Veebruaris keelustati TikToki kasutamine Euroopa Liidu institutsioonide töötajate tööseadmetes. Riikide hulka, kes ei luba TikTokki valitsussektori tööseadmes kasutada, lisandusid eelmisel aastal ka näiteks Kanada, Austraalia, Belgia ja Norra. Eestis oli TikToki kasutamine tööseadmest paljudes valitsusasutustes keelatud juba varem, möödunud aastal laiendati seda piirangut kõikidele riigiasutuste keskselt hallatud mobiilseadmetele. ●

RIA *RED TEAM*: „Tahame minna taristu lõhkumise kallale“

.....

Riigi küberturvalisuse eest vastutava asutuse töötajalt on sellist soovi üllatav kuulda, aga just niisugune on RIA *red team*'i eesmärk: panna infosüsteemid tõsiselt proovile, et need oleksid pahatahtlike ründajate eest paremini kaitstud.

.....

RIA *red team* ehk punane tiim on nüüdseks tegutsenud natuke rohkem kui aasta. Eelkõige näevad nad end asutuste ja ettevõtete infoturbejuhtide partnerina nõrkade kohtade leidmisel, aga ka töötajate ja juhtkonna teadlikkuse tõstmisel.

Tiimi töös on läbi põimunud küberturvalisuse inimlik ja tehniline pool: saadetakse õngituskirju ning uuritakse veebilehtede ja -teenuste turvalisust, aga tegeletakse ka füüsilise läbistustestimisega ehk piltlikult öeldes käiakse asutuse ruumides luurel.

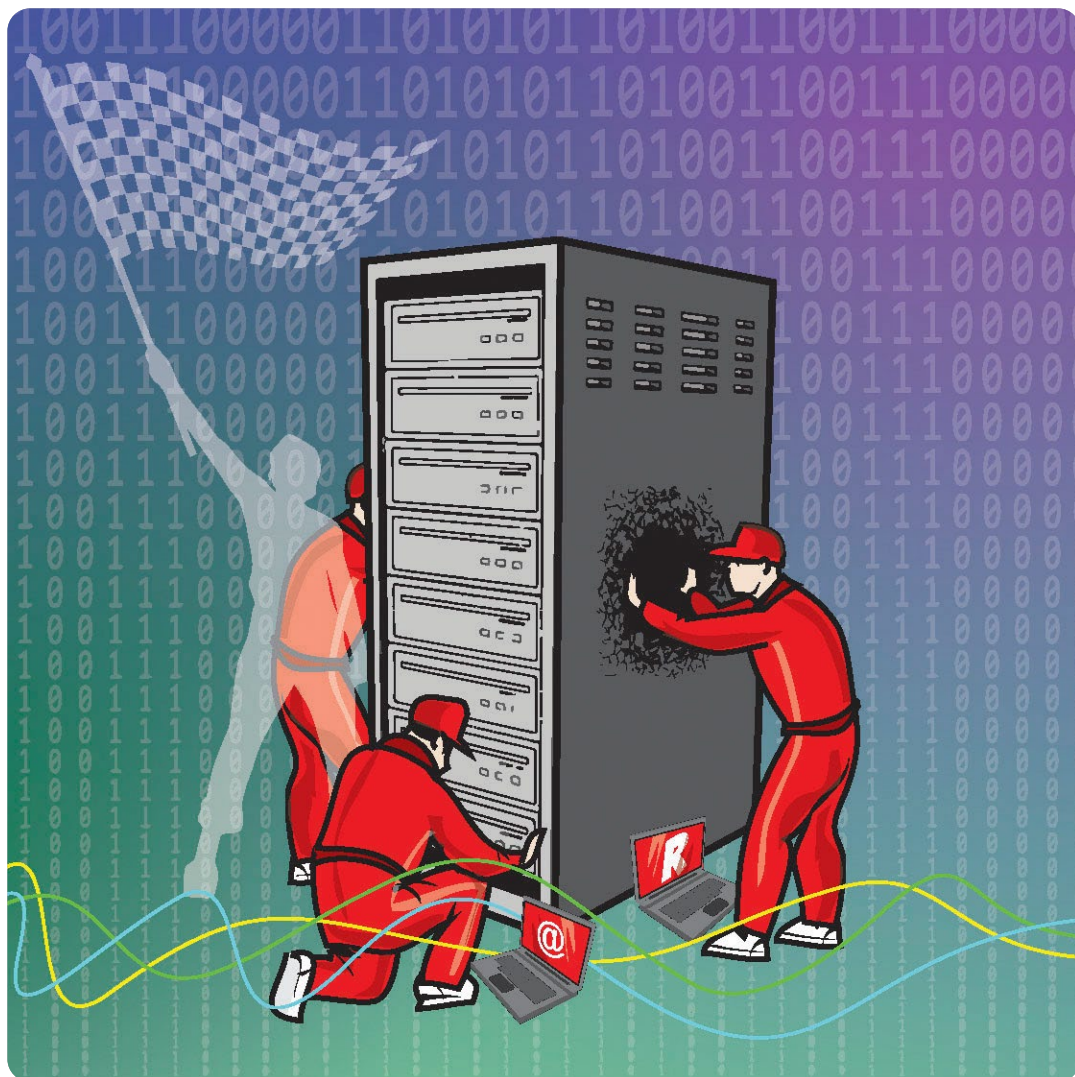
Edaspidi soovib *red team* proovile panna asutuste infosüsteemid, et näha, kuivõrd kerge on sinna sisse murda ja millist teavet on võimalik kätte saada. Igasuguse testimise puhul tuleb muidugi arvestada, et elutähtsa teenuse töö peab jätkuma ehk taristut ei tohi kahjustada.

MIKS JA KELLELE?

Punase tiimi tegevus hõlmab nii avalikku sektorit kui ka elutähtsaid ja olulisi teenuseid pakkuvaid eraettevõtteid. Koostööd on tehtud riigi-asutuste, haiglate, telekomide, energiaettevõtete ja teistega. Huvilisi on niivõrd palju, et vahepeal tekkis lausa järjekord.

Enamik klientidest on infoturbe küsimustes juba teatud küpsuse saavutanud ja lihtsamad probleemid on lahendatud. Seetõttu üritatakse rohkem raamidest väljapoole mõelda: kasutada IT-vahendeid näiteks eesmärgil, milleks need pole tegelikult mõeldud jne.

Mida konkreetsetes asutustes tehakse, selgub arutelu käigus infoturbejuhiga, kes otsib lahendust mingile küsimusele või probleemile. Kuivõrd teadlikud on tema asutuse töötajad küberturvalisusest? Kas keegi järgib ka päriselt turvanõu-



Tulemuse saavutamiseks on vaja leitud probleemid kõrvaldada.

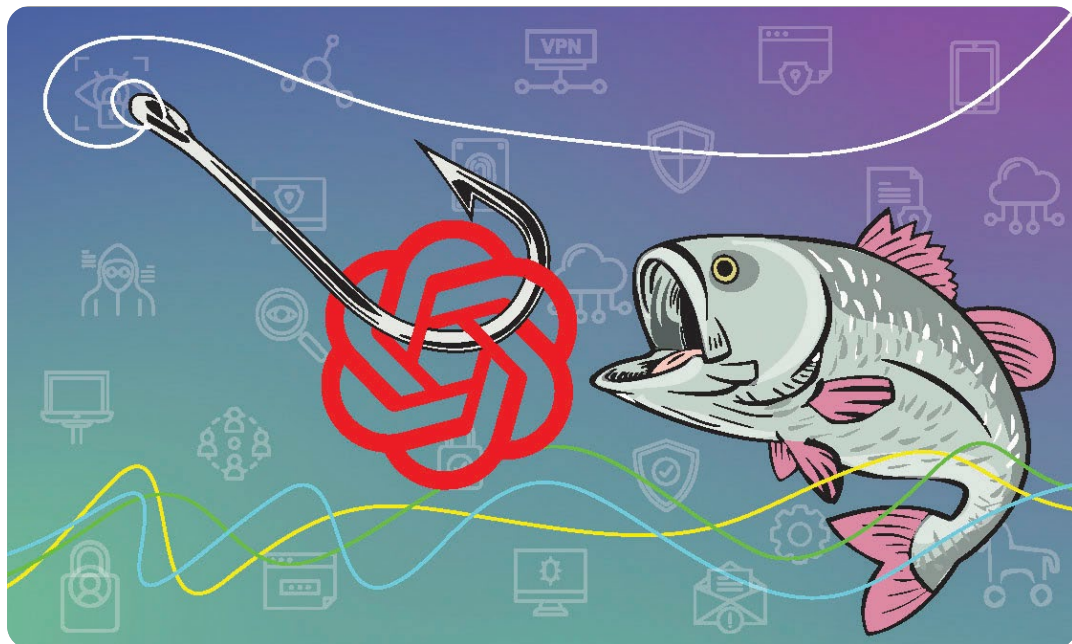
deid, mille ta on välja mõelnud? Kui turvalised on ettevõtte veebiteenused? Kuidas juhtkonnale infoturbe olulisust tõestada? Üks RIA eesmärke ongi n-ö targa tellija kasvatamine, et infoturbejuhid oskaks esitada õigeid küsimusi ka siis, kui nad tulevikus turvatestimist näiteks mõnelt eraettevõttelt sisse ostavad.

RIA *red team*’i teenuste eest tasub maksumaksja. Samas ei tähenda see, et tellija ei peaks ise panustama. Tulemuse saavutamiseks on vaja leitud probleemid kõrvaldada ning see nõuab enamasti investeerimist.

PIISAB, KUI ÕNGE LÄHEB ÜKS TÖÖTAJA

Punase tiimi tegemistest on kõige rohkem väljapoole paistnud õngitsuskirjad, mis jõudsid aasta jooksul postkasti rohkem kui 14 000 inimesele, kes töötavad mõnes riigiasutuses, kohalikus omavalitsuses või ettevõttes.





TEHISARU teeb punase tiimi elu lihtsamaks

Kiirelt areneva tehisintellekti võimalusi pole enda jaoks avastanud mitte ainult küberkurjapid, vaid ka küberruumi valvekoerad.

RIA red team on kasutanud ChatGPTd muu hulgas õngitsusideede leidmiseks. Näiteks tuli tehisaru välja stsenaariumiga, et asutuses on koostatud uus tööjaamade jälgimise poliitika, millega saab tutvuda veebilehel. Tehistaip sai kenasti hakkama ka poliitika kirjeldamisega – kui teksti süveneda, oli jutt ümmargune ja sisutühi, aga peale vaadates tundus nagu päris.

Samamoodi koostab tehismõistus vägagi veenvaid õngitsuskirju ja võimaldab genereerida õngitsuslehtede koodi. Eestikeelses tekstis leidub ainult üksikuid konarusi, mis meenutavad otsetõlget inglise keelest ja vajavad silumist.

Osa eksperte on hoiatanud, et tehisintellekti levik võib viia massilise automatiseerimise ja töökohtade kadumiseni, aga RIA punane tiim seda ei karda. Pigem võimaldab tehistaip turvatestimisel inimesi nürist tööst vabastada ja keskenduda asjadele, mis vajavad endiselt inimhõimust.

Õngitsus näeb enamasti välja nii, et inimene saab e-kirja, klikib lingile ja satub lehele, kuhu on võimalik jätta oma andmed: tavaliselt kasutajanimi ja salasõna. RIA kogemuste põhjal läheb õngitsuslehele keskeltläbi 30 protsenti kirja saajatest ja 10–20 protsenti sisestab ka oma andmed – kusjuures need tulemused on pärit asutustest ja ettevõtetest, kes on õngitsuste teemal varem selgitustööd teinud.

Ühe asutuse töötajatest loovutas oma andmed lausa 60 protsenti. Mõnes teises on see protsent olnud jällegi väga madal, aga „lahkeid“ inimesi leidub alati. Ja ühe töötaja andmetest täiesti piisab, et pääseda süsteemi sisse ning teha seal rohkelt kurja. Paljud Eestis viimastel aastatel toimunud tõsisemad küberkuriteod on saanud alguse just kasutajakonto hõivamisest.

Seetõttu kõlab õngitsuste peamine õppetund lihtsalt: kasuta kahetasandilist autentimist (2FA). Nii ei pääse kurjapid asutuse võrku, isegi kui neil on õnnestunud mõni kasutajanimi ja parool hankida. Samal põhjusel ei tohiks kaugtöölaud (RDP), siseveeb ja muud töötajatele mõeldud teenused olla vabalt internetist ligipääsetavad, vaid ainult läbi 2FAga kaitstud VPNi.

Õngitsused aitavad tõsta ohuteadlikkust. Kui muidu arvavad paljud, et nendega midagi sää-

rast ei juhtu, siis õngeminek paneb küberturbe teemade üle järele mõtlema. Selleks, et õngitsusest oleks küberhügieeni parandamisel päriselt kasu, peab järgnema selgitus – miks seda tehti ja kuidas inimene oleks pidanud pettuse läbi nägema – ning küberturbekoolitus. Muidu jääb toimunu paljudele töötajatele arusaamatuks ja nad võivad seda tajuda hoopis kiusamisena.

Õngitsused aitavad hinnata ka turvanõuete täitmist ja tööprotsesside toimimist: kas kahtlastest kirjadest antakse teada, kelle poole abi saamiseks pööratakse või kuidas administraatorid oma tööga hakkama saavad. Samas tuleb tellijal muidugi arvestada riskidega, mis õngitsusega kaasnevad: mitusada töötajat võib korraga kasutajatoele helistada, mõni lausa politseisse pöörduda.

Infoturbejuhil tasub õngitsuse tellimisel igal juhul põhjalikult järele mõelda, mis asutuses parajasti toimub. Kui sisekliima on halb, inimesed on rahulolematud, sest toimuvad näiteks suuremad ümberkorraldused või koondamised, ei maksa õngitsuskampaaniaga nende niigi kõrget stressitaset rohkem tõsta.

KÄIAKSE KA KONTORITES LUURAMAS

Veebilehtede ja -teenuste turvatestimisel kontrollib RIA *red team* neid kõigepealt automaatsete vahenditega, et tööjõudu mõistlikumalt kasutada, ja alles seejärel hakatakse „käsitsi“ vigu otsima. Isegi kui veebirakendust on pärast loomist juba testitud, tasub seda korrata, kui vahepeal on tehtud rohkelt muudatusi või on plaanis

Kõige kurvem on *red team*’ile see, kui nad leiavad vea, aga aasta hiljem on see endiselt parandamata.

mõni suurem uuendus. Muudatuste käigus võivad tekkida vead, mida varem polnud.

Füüsilise läbistustestimise käigus üritab punase tiimi liige oma tegelikke kavatsusi varjates asutuse ruumidesse imbuda ja sinna näi-

MIDA TEEB TÖÖTAJA, kui tal kästakse lekkinud salasõna vahetada?

RIA *red team*’i õngitsused paljastavad murettekitavaid seaduspärasusi inimeste küberkäitumises.

Ühe asutuse töötajatele saadeti õngitsuskiri, et nende salasõna on lekkinud ja paluti see uue vastu vahetada. Umbes 15 inimest sisestaski õngitsuslehele kohusetundlikult oma vana ja uue parooli – õngitsuse käigus salvestati selle pikkus ja kolm esimest märki. Andmete analüüsimisel selgus, et enamasti olid uue ja vana parooli algus ja pikkus sama ehk kui varem oli salasõna „Tallinn1“, siis uus oli ilmselt „Tallinn2“.

Ometi ütles juba õngitsuskiri, et salasõna on lekkinud, ja sel juhul tuleks parooli kindlasti oluliselt muuta. Kurjategijatele on salasõnade vahetamisel ainult kosmeetiliste muudatuste tegemine teada ja see pole suur takistus nende äraarvamisel.

teks luureseadme jätta. Vältimaks vahelejäämise korral tõsisemaid ebameeldivusi, võetakse igaks juhuks kaasa asutuse juhi allkirjaga luba.

Kutsumata külalise tellimisel tuleks infoturbejuhil läbi mõelda, mida ta sellega tõestada soovib. Kas juba see on oht, kui võõras pääseb uksest sisse, või ei juhtu midagi hullu, kui ta ei saa infosüsteemidele ligi? Üks võimalus ongi mõõta turvaeeskirjade täitmist. Näiteks kas valvetechnikuna esinev võõras pääseb asutuse ruumidesse, kas tema nimi pannakse kirja, antakse külalise kaart ja lubatakse ainult koos saatjaga ringi liikuda. Või kas laudadel olevad sülearvutid on lukus, nii et nendega on raskem kurja teha.

Igasugusel testimisel on mõte ainult siis, kui sellest tehakse vajalikud järeldused – korraldatakse koolitus, muudetakse asutuse turvapoliitikat jne. Kõige kurvem on *red team*’ile see, kui nad leiavad vea, aga aasta hiljem on see endiselt parandamata. ●



IT-VAATLIKULT

küberohtudele vastu

Küberohtude arengu ja kasvuga toimetulekuks on vaja, et kõik oleks varitsevatest ohtudest teadlikud ning oskaks küberruumis turvalisemalt käituda. Selleks viisime eelmisel aastal läbi kaks ennetuskampaniat – ühe ettevõtetele, teise eraisikutele.

Paljud ettevõtjad teavad küberruumis levivate ohtude kohta paraku üsna vähe, selgub nii RIA kui ka statistikaameti uuringutest. Pahatihti ei põhjusta küberrünnak kahju mitte ainult rünnaku ohvriks langenud ettevõttele, vaid ka selle klientidele ja äripartneritele. Sageli saab küberturbe tähtsus selgeks alles pärast seda, kui midagi tõsist on juba juhtunud.

JUHI IT-VAATLIKULT

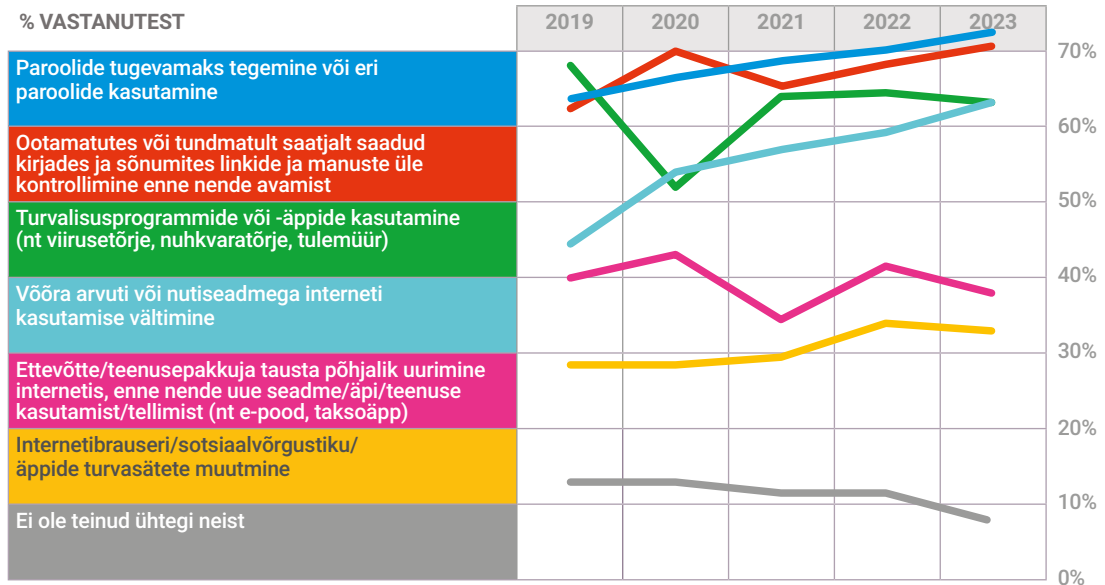
Oktoobris, küberturvalisuse kuul, andsime avapauku üleriiklikule „Juhi IT-vaatlikult“ kampaniale. Sellega juhtisime ettevõtjate ja juhtide tähelepanu levinumatele küberohtudele

ning selgitasime, kuidas end nende eest kaitsta. Kampania raames andsime välja ettevõtete küberturvalisuse uuendatud lühijuhendi, mis aitab väiksematel ettevõtetel teha esimesi ehk neid kõige tähtsamaid samme küberturvalisuse tagamisel.

„Juhi IT-vaatlikult“ kampania võtsid ettevõtjad vastu oodatust veelgi positiivsemalt. 81 protsenti sihtrühmast märkas kampaniat ja 91 protsenti neist tajus seda väga vajalikuna. Rõõm on tõdeda, et pärast kampania nägemist hakkas 43 protsenti sihtrühmast teema peale mõtlema või plaanis muuta oma äri küberturvalisemaks.

Tõstmaks ettevõtete teadlikkust küberturvalisusest, panime seljad kokku Eesti Infotehno-

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



loogia ja Telekommunikatsiooni Liiduga (ITL) ning korraldaskime eksperimendi korras heatahtlikud ründed kolmele ettevõttele, kes selleks soovi avaldasid. Nad teadsid, et nende süsteemid pannakse proovile, ent sellest hoolimata õnnestusid kõik rünnakud. Programmis osalenud ettevõtted said väärtuslikke õppetunde ja näpunäiteid oma kaitse tugevdamiseks ning jagasid saadud kogemusi ka avalikkusega, et tõsta ettevõtete teadlikkust laiemalt.

PANIME IT-VAATLIKKUSE PROOVILE

Suve hakul kutsusime kõiki üles testima oma IT-vaatlikkust, läbides praktilise küberkaitsekursuse ennetuslehel itvaatlik.ee. Lühikursusel selgitatakse kaasahaaravate õppevideote abil, kuidas ennast levinumate küberohtude eest kaitsta ning usinamad saavad oma teadmised proovile panna, läbides 12 küsimusega testi.

Paralleelselt kursuse väljakuulutamisega välitas üleriigiline küberteadlikkuse tõstmise kampania „Testi oma IT-vaatlikkust“. See viis laiem avalikkuseni põhilised ennetussõnumid küberhügieeni parandamiseks ning ärgitas mainitud küberkaitsekursust läbima.

Lisaks said kõik huvilised ennast küberruumis varitsevaga kurssi viia Kuku raadio eetris olnud saatesarja „Ohtlik klikk“ kuulates. Saatesarjas teavitati kuulajaid levinumatest pettustest, küberhügieeni olulisusest ja alaealiste käitumise

tumisest küberruumis. Lisaks rääkisid eksperdid tulevikutehnoloogiatest ja nendega kaasnevatest ohtudest, e-riigi võimekusest ning kübersõjast ja desinformatsiooni levikust. Saatesari „Ohtlik klikk“ sai kuulajatelt sooja vastuvõtu, iga osa kuulas otse või järelkuulamise võimalust kasutades enam kui 7000 inimest. Kes seda veel teinud pole, leiab saated levinumatest podcast'i-keskkondadest.

VIIS AASTAT ENNETUSTÖÖD

Juba viis aastat oleme statistikaameti kaasabil hoidnud silma peal Eesti elanike küberhügieenil. Viimase uuringu tulemused näitavad, et lausa 73 protsenti elanikest kasutab erinevaid tugevaid paroole ning 71 protsenti kontrollib ootamatud kirjad või lingid enne nende avamist üle. Eriti rõõmsaks teeb asjaolu, et neid, kes pole teinud midagi oma isikliku turvalisuse või privaatsuse tagamiseks, on vaid kaheksa protsenti elanikest. Veel aasta tagasi oli neid 11 protsenti.

Eesti elanike küberhügieeni tase on viie aastaga paranenud, kuid arenguruumi jagub. Andmed osutavad ka tõsiasjale, et paljud inimesed ei kasuta endiselt turvalisusprogramme, samuti muudab vaid kolmandik turvasätteid sotsiaalvõrgustikes või telefonirakendustes. Tänu kogutud statistikale saame veelgi paremini oma tegevusi planeerida ning keskenduda sihtgruppidele, kelle küberteadlikkus on madalam. ●

KÜBERTEST

tegi hoogsa stardi

2023. aasta aprillist pakume tasuta küberturbealast õppeplatvormi Kübertest. Esimese aasta jooksul liitus sellega üle 200 asutuse ja ettevõtte ning koolituse ja testi läbis üle 15 000 inimese.

Mis nende vastustest selgus?

Me kõik puutume iga päev kokku arvutite ja nutiseadmetega: näiteks e-kirju saates, erinevaid infosüsteeme kasutades, e-poest kaupa tellides, internetipangas makseid tehes jne. Kõigi nende tegevuste juures peaks meele olema küberturvalisuse baastõed ja Kübertest on hea võimalus need omandada või üle korrata.

Enamasti on küberintsidentide põhjuseks just teadmatus või inimlik eksimus. Teadlik arvutikasutaja on ka kindlasti eelisseisus nende ees, kes näevad esimest korda oma postkastis õngitsuskirja. Kuna Kübertesti puhul on tegemist e-kursusega, saab iga kasutaja selle läbida endale sobival ajal.

Kuigi Kübertest on suunatud eelkõige avalikule sektorile ning elutähtsa ja olulise teenuse osutajale, ootame liituma ka teisi soovijaid. Kübertesti kasutamine on kõigile tasuta.

LIITUNUD ON ÜLE 200 ASUTUSE JA ETTEVÕTTE

Esimese aasta jooksul liitus Kübertestiga enam kui 200 asutust ja ettevõtet. Nende hulgas on näiteks ministeeriumid ja nende hallatavad asutused, kohalikud omavalitsused, koolid, haiglad, perearstikeskused ja ettevõtted.

Aasta lõpu seisuga ehk üheksa kuuga oli

enam kui 15 000 inimest jõudnud oma teadmisi täiendada ja testida. Väga eeskujulikud on olnud näiteks siseministeeriumi ja kultuuriministeeriumi haldusala, kus pea kõik asutused on Kübertestiga liitunud ja selle edukalt kasutusele võtnud.

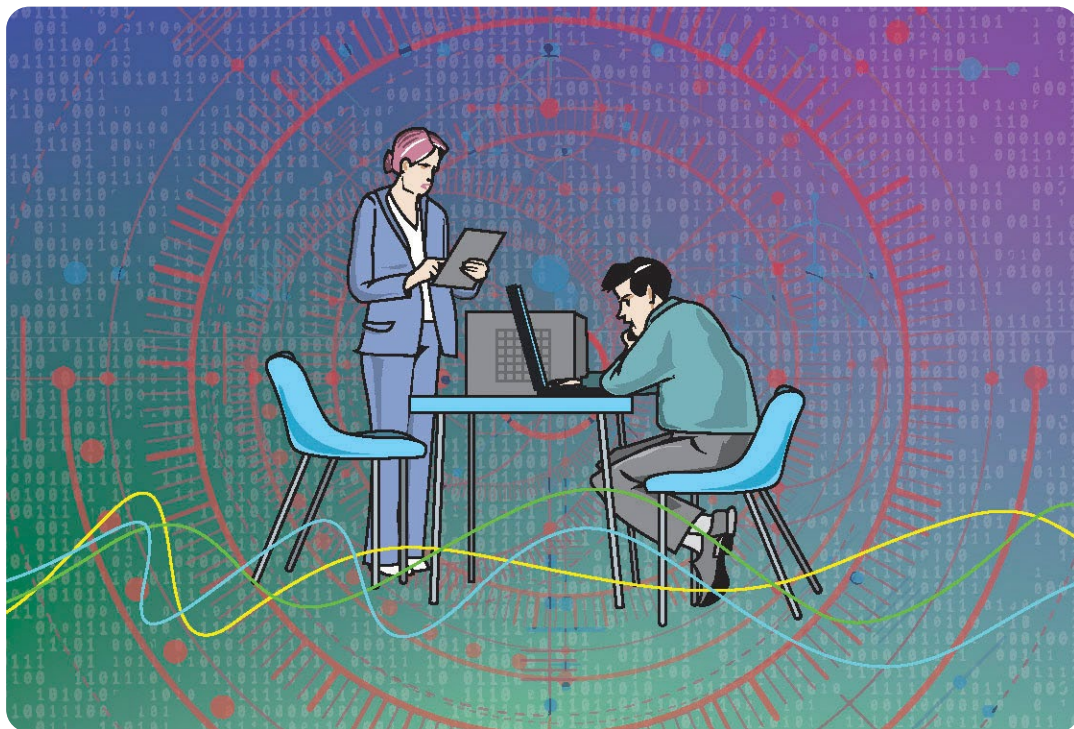
MIS TULEMUSTEST SELGUB?

Suurem osa Kübertesti kasutajatest teab hästi vajadusest kaitsta nutiseadmeid ja kaugtöö ohte – neil teemadel vastab enamik testi sooritajatest õigesti. Kui aga vaadata raskemaid küsimusi, siis need puudutavad õngitsuslehe äratundmist ja õiget tegutsemist. Kahjuks näeme seda trendi ka CERT-EE poolt registreeritud intsidentidest. Igal kuul on ligi pooled teavitused just õngitsuslehtede kohta ja paraku satuvad paljud Eesti inimesed õngitsuste ohvriks.

Teine murekoht on paroolide riskasutus – paljud vastanutest kasutavad sama salasõna nii tööarvutis kui ka eraelus. See ei ole hea praktika, sest parooli lekkimise korral satuvad ohtu nii isiklikud kui ka tööl kasutatavad kontod.

SEL AASTAL UUENDAME SISU

Selle aasta kevadel uuendame nii Kübertesti kursuse kui ka testi sisu. Uues versioonis saavad kaetud kõik olulisemad teemad: paroolid ja



kontode turvalisus, erinevad õngitsused ja petuskeemid, e-kirjade teel levivad ohud, WiFi-võrgu turvaline kasutamine ja seadistamine, mälupulkade ja muude andmekandjate kasutamine, turvaline kaugtöö, nutiseadmete kasutamine ja sotsiaalmeedias levivad ohud.

Lisaks on plaanis Kübertesti täiendada harravate õppevideotega, mis katavad kõik kursuse olulisemad teemad. Videotes räägime näiteks üle, kuidas levib pahavara, kuidas nutiseadmeid turvalisemalt kasutada ja mis täpsemalt on virtuaalne privaattvõrk ehk VPN. Uuenduse-na on võimalik aasta teises pooles kursust läbida lisaks eesti keelele ka inglise keeles.

RIA eesmärk on endiselt, et kõik avaliku sektori töötajad läbiks Kübertesti või mõne muu küberturbekoolituse vähemalt kord aastas.

KÜBERTEST ARVUDES (2023. a lõpu seisuga)

- Liitunud **205** asutust/ettevõtet
- Testi läbinud **15 160** inimest

RIA eesmärk on endiselt, et kõik avaliku sektori töötajad läbiks Kübertesti või mõne muu küberturbekoolituse vähemalt kord aastas. Soovitame ka kõigil teistel läbida regulaarselt küberturbealane koolitus. See aitab pöörata tähelepanu nii teada-tuntud petuskeemidele kui ka annab infot uute riskide kohta. Kübertesti läbides näeb koolitusel osaleja näiteid õngitsuskirjadest, -sõnumitest ja -lehtedest ning nii on tal neid kergem ära tunda.

Kui sul tekkis huvi Kübertestiga liitumise vastu või sel teemal mõni küsimus, siis kirjuta aadressil kybertest@kybertest.ee. Kübertesti kasutamise taotluse ja muu info leiad RIA veebilehelt. ●

PEREARSTIDE KÜBERTERVIS jätab soovida

Sõeluuringu käigus selgus, et mitmete perearstide kübertervis pole kiita ning vajab kohe sekkumist. Infoturbe standardi rakendamine koostöös RIA järelevalvega aitab ennetada raskeid tagajärgi.

P ea igal Eestis elaval inimesel, vähem või rohkem tervel, on oma perearst, kelle käsutusse on ta usaldanud oma terviseandmed. Seda tehes eeldame, et need andmed on õiged, kõrvaliste isikute poolt muutmatud, vajadusel kättesaadavad ja tagatud on andmete konfidentsiaalsus.

Kuna keegi meist ei taha, et tohtrile usaldatud delikaatsed terviseandmed lekiks või kaoks, sõltub perearsti usaldusvärsus lisaks meditsiinalastele teadmistele ja oskustele ka tema kübertervisest. Pahatihti pole viimasele piisavalt tähelepanu pööratud.

JÄRELEVALVE KUI SÕELUURING

Perearstide kübertervise kontroll, millega RIA järelevalveosakond möödunud aastal põhjalikumalt tegeles, polnud ajendatud ühestki intsidentist, kaebusest ega vihjest. Kuigi sõnast

„järelevalve“ võib jääda mulje, et tegeletakse tagantjärele tarkusega ning tagantjärele valvaga, on eesmärk probleeme ennetada. Samamoodi, nagu näiteks vähi sõeluuringuga. Piste- list kontrolli teeme selleks, et selgitada välja, kuivõrd hästi perearstikeskused küberturbe nõudeid täidavad. Kui järelevalve käigus avastame probleeme, juhime neile tähelepanu ja anname tähtajad puuduste kõrvaldamiseks.

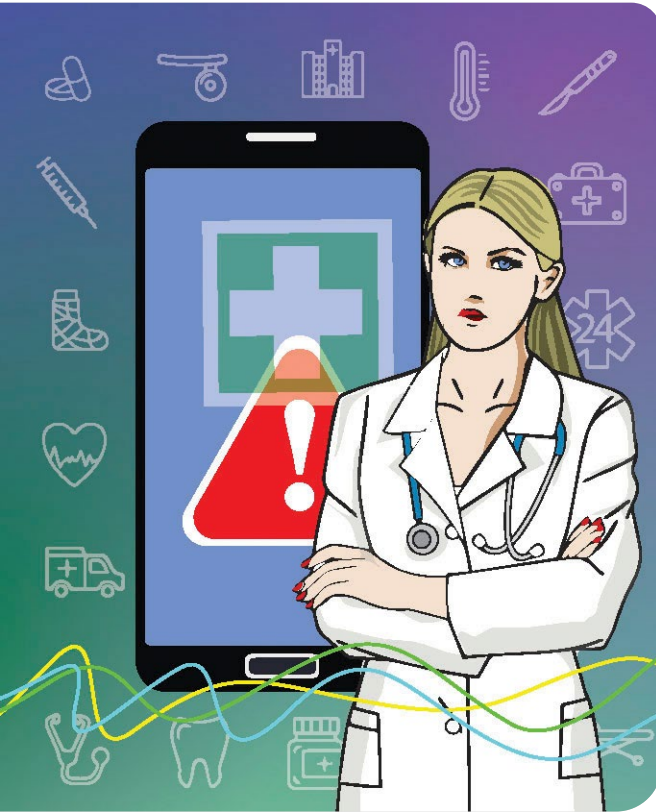
Küberintsidendid tervishoius ei pruugi olla seotud pahasoovliku välise sekkumisega. Tehniliste tõrgete tõttu on patsientide andmeid lihtsalt ära kustunud ning üks perearstikeskus oli pärast serveririket mõnda aega suletud. Selle juhtumi tagajärjed muutis raskemaks asjaolu, et keskus hoidis varukoopiaid samas serveris – ilmne eksimus hea tava vastu, mida varasem kontroll aidanuks vältida.

Andmelekke ebameeldiv tagajärg võib olla patsiendi privaatsuse rikkumine, andmete ter- vikkuse kadu võib viia vale diagnoosi ja ravini. See on sõna otseses mõttes oht elule ja tervisele.

Sisemistest põhjustest tulenevad vead kahva- tuvad siiski välise ees. Küberkurjategijad on Euroopa meditsiinisektori aktiivselt sihikule võtnud ning Euroopa infoturbeagentuuri (ENISA) andmetel kuulub tervishoiusektor sihitud rünnete ja registreeritud intsidentide arvu mõttes esikolmikusse. Eestis on rohkem

KOLM soovitus

- ❑ Iga perearst võiks läbida RIA Kübertesti.
- ❑ Perearstikeskusel võiks olla tugev IT-partner, kes toetab standardi rakendamisel.
- ❑ RIA soovitusi võiks järgida juba enne järelevalvet.



kõlapinda leidnud lunavararünnakute ohvriks langenud perearstikeskused.

TURVAVÖÖ JA TULEKUSTUTI

Ilmselt tekitaks igas patsiendis küsimusi, kui vaktsiinisüstile ei eelneks desinfitseerimist või kui operatsioonisaalis puuduksid personalil maskid. Sarnaselt tervisenõuetega on ka küberruumis vaja reegleid.

IT-süsteemide ohutusnõuded on koondatud Eesti infoturbestandardisse (E-ITS). See on justkui küberturbe kasutusjuhend, mille järgimisel peaks asutus olema enamiku küberohtude eest kaitstud. Perearstikeskustele on RIA teinud standardis eraldi profiili, kus on välja toodud nende tööks vajalikud nõuded ja ka juhised nende kasutamiseks turbehalduse rakendamiseks alustamiseks. Seda oleme perearstidele ka tutvustanud.

Reeglite kokkuleppimine ja tutvustamine on pikk protsess. Kui kord on jõutud niikaugele, et reeglid on paigas, on vältimatult vajalik ka nen-

Mõned on TERVEMAD

Kuus perearstikeskust – OÜ Aira Perearstikeskus, OÜ Tartu Raatuse Perearstikeskus, Karulaugu Tervisekeskus OÜ, OÜ Pirita Perearstikeskus, OÜ Järveotsa Perearstikeskus ja OÜ Pärnu Perearstid –, kus tegeleti nii tehniliste kui organisatoorsete infoturbe-meetmete rakendamisega aktiivselt ja piisavas ulatuses, läbisid järelevalvemenetluse puhaste paberitega. Kõigi nendega suheldes oli selgelt tunda, et juhtkond väärtustab infoturvet, sellega seotud riske on mõistnud ja adekvaatselt hinnatud. Samuti oli ühiseks jooneks pädev IT-partner, kes oli aidanud meetmeid välja valida ja juurutada.

MENETLUSED arvudes 2023. a lõpus

- Kontrollimisel on **41** perearstikeskust.
- Ettekirjutusi on täitmisel **12** keskusel.
- Uurimise ja otsustamise faasis on **21** keskus.
- Lõpetatud on **8** menetlust.

de jõustamine ja kontrollimine. Kui patsiendil on tuvastatud kõrge kolesterool ja määratud ravi koos dieediga, siis kutsutakse patsient reeglina järelkontrolli, mille vältimatu ja loogiline osa on kolesteroolitaseme mõõtmine.

RIA on korraldanud hulgaliselt tasuta E-ITSi koolitusi ning kaasamiseminare standardi rakendamise hõlbustamiseks. Samuti oleme teinud perearstidele kaks märgukirja lähenevast kohustusest, mille küberturvalisuse seadus neile paneb, ning korraldanud neile spetsiaalse infopäeva. Informeerisime perearste ka sellest, et hakkame nõuete täitmist kontrollima. Selgitasime perearstidele nende käes olevate terviseandmete tundlikkust ja väärtust, meditsiini-sektori suunas tehtavatest rünnakutest tulenevaid ohte ning neist tulenevat vajadust rakendada küberturbe meetmeid.

Pearstide selts on selgitustega rahule jäänud ning oma sõnul saanud nüüd paremini aru RIA tegevusest ja öelnud, et püüavad seda teadmist ka perearstide hulgas levitada. ●

2023. aasta valimised tõid E-PÖÖRDE

.....

Eelmisel aastal toimunud riigikogu valimised olid meie jaoks ajaloolised: sündis maailmarekord, sest esmakordselt oli e-hääle andnuid rohkem kui pabersedeliga hääletanuid.

.....

Aktiivsed ettevalmistused riigikogu valimisteks käisid RIAs terve aasta. Moel või teisel oli sellesse kaasatud sadakond ameti töötajat, lisaks partnerid väljastpoolt. Vastutasime valimiste infosüsteemi (VIS) arenduse ja töös hoidmise, e-hääletamise kogumislahenduse halduse, jaoskonnatöötajate arvutite haldamise ja kaitsmise ning valimiste küberturbe eest. Samuti pakkusime hääletajatele ja valimisjaoskondade töötajatele kliendituge tehnilistes küsimustes.

MAAILMAREKORD

Ühtekokku andis 27. veebruarist 5. märtsini kestnud valimisnädalal oma hääle 615 009 inimest. Võiks öelda, et sündis ka e-hääletamise maailmarekord (313 514 häält). Esimest korda 18 aasta jooksul oli e-hääle andnuid rohkem kui pabersedeliga hääletanuid. Meie jaoks on see usalduse märk.

Võrreldes neli aastat varem toimunud ehk eelmiste riigikogu valimistega oli sel korral kasutusel uus valimiste infosüsteem (VIS3), mis sai tuleristsed 2021. aasta kohalike omavalitsuste volikogude valimistel. Kasutusel oli sama süsteemi edasiarendatud versioon, mis

arvestab kõiki turvalise arenduse põhimõtteid ja muudab valimiste korraldajate, jaoskondade töötajate, kandidaatide ja hääletajate elu mugavamaks.

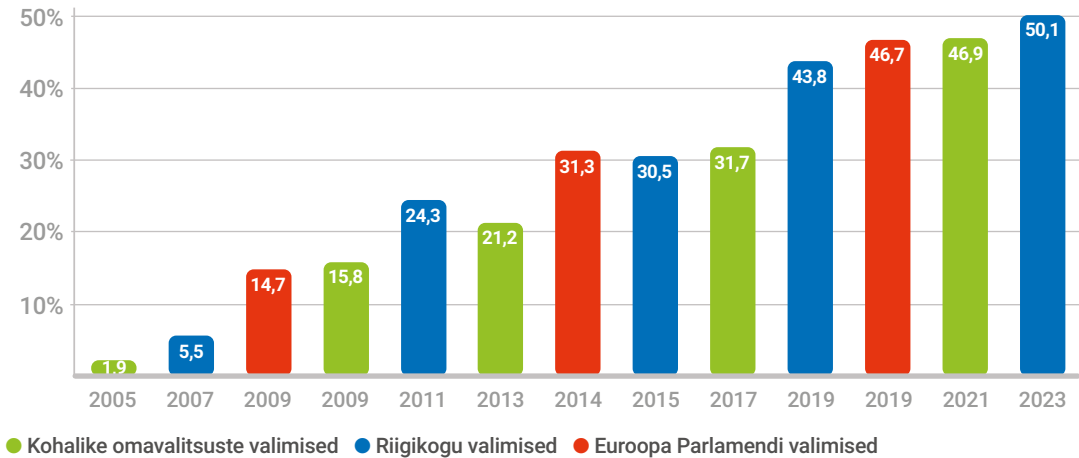
Elektroonilised valijanimekirjad võimaldavad jaoskonna töötajatel loobuda paberil joonlauaga järje pidamisest, kandidaadid saavad soovi korral oma kandidatuuri üles seada valimiste infosüsteemi kaudu ja hääletaja pole seotud enam ühe kindla valimisjaoskonnaga, vaid saab häält anda mistahes oma ringkonda kuulvas jaoskonnas.

Uuendusena oli 2023. aasta riigikogu valimiste valimisperiood pidev ehk e-hääletuse ja valimispäeva vahel polnud pausi. Samuti said e-hääletajad õiguse valimispäeval jaoskonnas pabersedeliga oma e-häält soovi korral muuta.

KÜBERRINDEL OLI VAIKNE

Valimistega seotud infosüsteemid toimisid tõrgeteta ja ka olukord küberrindel oli valimisnädalal suhteliselt vaikne – ühtegi rünnet valimiste süsteemide vastu ei tuvastatud. Küll tehti mõned katsed anda e-häält mitteametliku rakendusega ning üks katse autentida end Leedu ID-kaardiga, kuid need üritused ebaõnnestusid.

REKORD: üle poole valijatest andis hääle elektrooniliselt



Valimiste kuulsaima viperuse põhjustas hoopiski asjaolu, et valimisinädala esimesel päeval jõudsid valijate nimekirja viimased muudatused e-hääletamise süsteemi (EHS) väikse viivitusega. Seetõttu kuvas valijarakendus 57 inimesele, kelle elukohaandmed olid rahvastiku-registris hiljuti muutunud, vana valimisringkonda ja selle kandidaate. Vales ringkonnas hääletanutel paluti uuesti hääletada ja lõpuks tuli tühistada ainult kolm häält.

Valimiste korraldamise eest vastutavad vabariigi valimiskomisjon (VVK) ja riigi valimisteenistus (RVT). RIA roll tehnoloogiapartnerina on kasvanud alates 2019. aastast, mil võtsime koostöölepele alusel RVT-lt üle kohustuse arendada välja uus valimiste infosüsteem (VIS3). 2021. aastal muudeti valimistega seotud seadusi, mis pani süsteemile uusi kohustusi, muu hulgas tuli 2021. aastast kasutusele võtta elektroonilised valijanimekirjad, avaandmete funktsioon ning rahvahääletuse võimalus.

Niisiis nägi riik, et valimiste korraldamine võiks muutuda e-riigile omaselt efektiivsemaks ja vähem bürokratlikuks. Arenduse, majutuse, käitamise, analüüsi ja testimise (sealhulgas nii turvalisuse, kasutatavuse kui koormustestide) paremale planeerimisele ja protsessipõhisele korraldamisele aitab kaasa püsivama koostöövormi ja riskihaldusmudeli kokku leppimine. Samuti on praegu EHSi tööd ja roll jagatud kahe asutuse vahel.

Tehniline valmisolek m-valimisteks on olemas, aga sellest ei piisa

E-hääletamine on leidnud valijate poolehoidu, kuid e-hääletamise rakendus on kasutatav vaid arvutipõhiselt, kuigi inimesed kasutavad igapäevaselt aina enam mobiilseadmeid.

RIAs oleme loonud nutiseadmes elektroonilise hääletamise rakenduse prototüübi, mille abil on testitud hääle andmist, edastamist ja vastuvõtmist. Prototüüp toetab nii Android-kui ka iOS-seadmeid, samuti on arendatud nii m-ID kui ka Smart-ID tugi. Nutirakenduste juurde on arendamisel ka ID-kaardi NFC tugi, et luua tulevikus täiendav võimalus autentimiseks ja allkirjastamiseks. Rakenduse prototüübi on arendanud Cybernetica ASI teadurid, kes on arendanud ka e-hääletamise süsteemi. M-hääletuse kasutuselevõtt eeldab veel õiguslike ja korralduslike küsimuste lahendamist ning 2024. aasta europarlamenti valimistel saab e-häält anda ikkagi vaid arvutis või pabersedeliga.

EES OOTAVAD EUROOPA PARLAMENDI VALIMISED

Euroopa Parlamendi valimisinädal kestab 3.–9. juunini 2024. Ettevalmistused selleks on juba täies hoos. ●

CYBER4DEV: missioon täidetud

2023. aastal lõppes esimene globaalne Euroopa Liidu rahastatud küberturbealase arenguabi projekt Cyber Resilience for Development ehk Cyber4Dev. Selle raames panustasid kümned Eesti eksperdid 26 riigis turvalisema küberruumi loomisesse.

Projekti eesmärk oli koolitus- ja nõustamisprogrammide abil toetada Aafrika, Aasia, Ladina-Ameerika ja Kariibi piirkonna riikide küberturvalisuse tõstmist. RIA-le oli viis aastat väldanud Cyber4Dev esimene pääsuke rahvusvaheliste projektide elluviimisel. Konsortsiumipartnerite Suurbritannia ja Hollandi kõrval tõi just Eesti ja RIA projekti peamise sisulise küberekspertiisi. Kaasasime 60 Eesti kübereksperti nii RIA enda ridadest, mujalt riigisektorist, aga ka erasektorist. Ühtekokku täitsid nad 26 riigis üle 220 tööülesande.

Projektis osalemine meie jaoks kaugetes riikides tähendas ekspertidele tavarutiinist ja mugavustsoonist välja astumist. COVIDi-pan-



deemia ja erinevad ajavööndid tõi öised videosessioonid. Kui sai taas lennata, kulus maailma teise otsa jõudmiseks üle 24 tunni. Partnerivalitsusi tuli koolitada tölkide abil, trotsides elektrikatkestusi ja kohanedes kultuuriliste erinevustega.

VÕIMEARENDUS POLIITIKAST ÕPPUSTENI

Lähenesime sihtriikidele võimalikult terviklikult. Alustasime küberturvalisuse olukorra hindamisest ning lünkade ja koolitusvajaduse tuvastamisest. Seejärel koostasime kohapealse valitsuspartneriga koolitusplaani ning alustasime selle elluviimist. Keskendusime peamiselt kolmele valdkonnale.

AJAJAJOON

2017

UK, Eesti ja Hollandi konsortsium võidab projektikonkursi ELi esimese globaalse küberarenguabi projekti läbiviimiseks. Detsembris allkirjastatakse Cyber4Dev projektileping.

2018

MÄRTS: Projektimeeskonna esimene kohtumine ja Cyber4Dev ametlik algus.
SUVI: Esimesed Eesti eksperdid lähetati Sri Lankale, Mauritiusele, Botswanasse ja Ghanasse.

2019

JAANUAR: Botswana, Mauritiuse ja Sri Lanka CERTide visiit Eestisse.
AUGUST: Esimene kõrgetasemeline küberturvalisuse lauaõppus **Cyber Breeze** Mauritiusel.
DETSEMBER: Cyber4Dev'i sihtrühma kaasatakse Ladina-Ameerika ja Kariibi mere riigid. Nendega seotud tegevust hakkab juhtima RIA.

1 Seadusandlik nõustamine ja üldine küberteadlikkus. Eesti eksperdid osalesid Botswana, Ecuadori, Mauritiuse, Dominikaani Vabariigi, Costa Rica, Mosambiigi ja Kambodža küberstrateegiatega väljatöötamisel. Tötsime valitsuste teadlikkust küberohtudest, korraldades kõrgetasemelisi lauaõppusi. Viimasel kahel aastal panime rõhku ka üldisele küberhügieenile. Siin olid eeskujuks RIA loodud IT-vaatliku kampaaniad ja kübertest, mille tööme Cyber4Devi üle, kohandades neid vastavalt partnerriikide vajadustele. Näiteks Ecuadoris on RIA kübertesti analoogi järgi tehtud platvormi kasutanud üle 25 000 riigiametniku.

2 Töö küberintsi-dentide käsitlemise üksuste ehk CERTidega. Korraldasime CERTidele koolitusi alates tööprotsessidest kuni tehniliste tööriistade kasutamiseni. Üheksa riigi CERTid said Cyber4Devilt pikaajalist tuge ja parandasid selle abil oma võimekust. Eesti eksperdid panustasid Botswana, Mauritiuse, Sri Lanka ja Dominikaani Vabariigi CERTide ülesehitamisse.

3 Soodustasime regionaalset ja rahvusvahelist koostööd. Viisime läbi regionaalseid seminare ja konverentse, et tuua kokku projekti sihtriikide eksperdid. Eesmärk oli luua piirkonna ekspertide vahel suhtevõrgustik ja usaldus, mis päädiks operatiivse koostööga intsidentide lahendamisel.

PROJEKT TUTVUSTAS EESTI LAHENDUSI JA ETTEVÕTTEID

Eesti aktiivne panustamine küberarenguabi põllul kaugel Mauritiusel, Sri Lankal või Ecuadoris võib esmapilgul tunduda küsitav. Kuid aastatepikkuse töö käigus oleme aidanud kaasa Eesti ettevõtete ekspordivõimaluste leidmisele ning suurendanud Eesti tuntust küberturvalise digiühiskonna liidrina.

Eesti on inspiratsiooniks paljudele arenguteel olevatele riikidele, kuidas selgete poliitikate, otsuste ja tegevustega on võimalik riik 30 aastaga sisuliselt nullist üles ehitada.

Eesti on inspiratsiooniks paljudele arenguteel olevatele riikidele, kuidas selgete poliitikate, otsuste ja tegevustega on võimalik riik 30 aastaga sisuliselt nullist üles ehitada. 2007. aastal Eestit tabanud küberründed ja neist väljakasvanud edulugu on eeskujuks näiteks Costa Ricale, mida tabasid mullu laastavad küberründed ning mis loodab rahvusvahelise kogukonna toel sellest kriisist tugevamana väljuda.

Nüüdseks lõppenud Cyber4Devist on välja kasvanud ELi küberekspertide ja asutuste võrgustikku koondav EU CyberNeti projekt ja LAC4 küberkompetentsikeskus Dominikaani Vabariigis, mis veab ELi pingutusi Ladina-Ameerika ja Kariibi piirkonna kübervõimearenduses. ●

2020

DETSEMBER: Dominikaani Vabariigi CERT liitub Cyber4Devi abil rahvusvahelise CERTide koostöövõrgustikuga **FIRST**.

2021

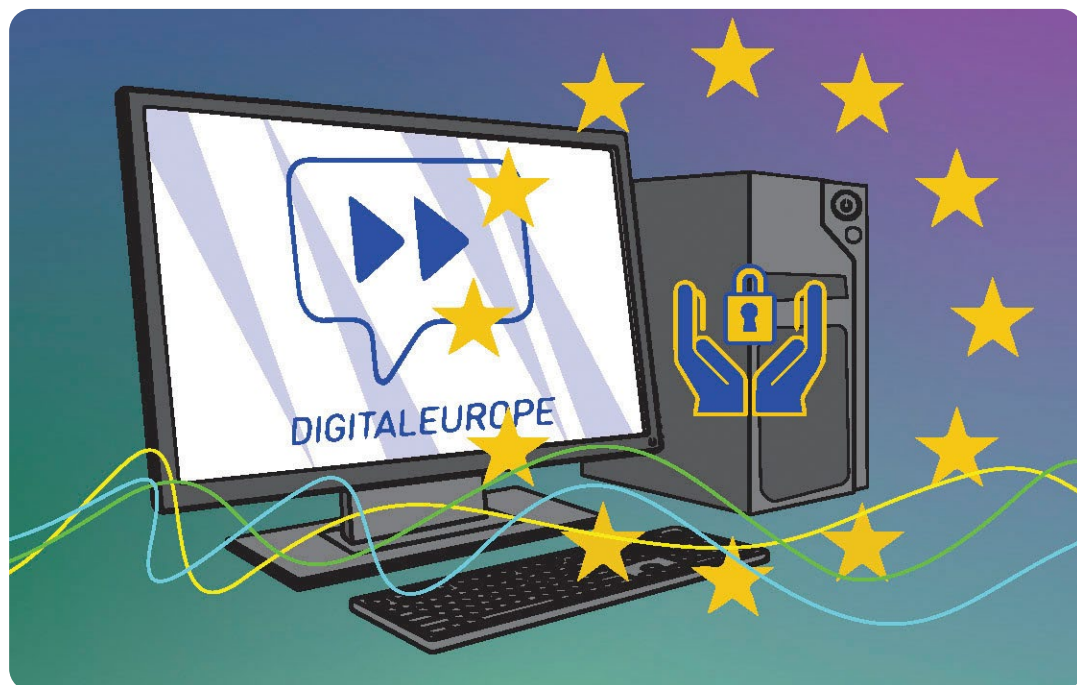
MAI: Cyber4Devi pikendatakse kahe aasta võrra. Esimene kõrgetasemeline küberturvalisuse lauaõppus **Cyber Llamas** Dominikaani Vabariigile. **SEPTEMBER:** Dominikaani Vabariigi valitsusasutuste õppevisiit Eestisse.

2022

JUUNI: Ecuadori esimene riiklik küberturvalisuse strateegia. **SUVI:** Mauritiuse, Sri Lanka ja Ecuadori valitsusasutuste õppevisiit Eestisse.

2023

MÄRTS: Esimene kõrgetasemeline küberturvalisuse lauaõppus **Tormenta Cibernética** Ecuadorile. **JUUNI:** Esimene kõrgetasemeline küberturvalisuse lauaõppus Seišellidele. Cyber4Devi aktiivsete koolitustegevuste lõpp. **OKTOOBER:** Cyber4Devi lõpukonverents Itaalias Firenzes.



KÜBERPÖÖRDE TOETUS aitab kokku hoida

RIA pakub koostöös EAS-Kredexi ühendasutusega toetust väikestele ja keskmise suurusega ettevõtetele, et nad saaksid oma küberturvalisuse taset mõõta ja tõsta.

Eesti on ettevõtluse digiteerimist toetanud juba aastaid ja selle käigus on jagatud miljoneid eurosid, kuid alles 2023. aasta kevadest avanes esimene küberturvalisuse tasemele pühendunud toetusvoor ettevõtjatele, kogusummaga 865 000 eurot.

ESMALT PAIKA TEEKAART...

Toetuse abil on ettevõtjatel võimalik tellida mõnelt küberturvalisuse teenusepakkujalt hinnang oma asutusele. Hinnang peab toetuma RIA kriitilise infrastruktuuri küberkaitse osakonna välja töötatud metoodikale ning selle tulemuse-na peab valmima teekaart: nõuanded, kuidas

ettevõtte saaks oma küberturvalisuse taset parandada näiteks järgmise aasta jooksul.

RIA välja töötatud ühtne metoodika on vajalik ühelt poolt selleks, et tagada teenuse kvaliteet. Teisalt annab see võimaluse ettevõtjatele võtta võrdlevaid pakkumisi sama taseme ja mahuga teenuse kohta. Kui me oma metoodika välja pakkusime, andis lausa 21 teenusepakkujat märku, et on valmis RIA metoodika alusel teenust pakkuma.

See on pannud küberturvalisuse teenusepakkujad uude konkurentsiolekorda, kus hinnad on mõnevõrra alla tulnud ja küberettevõtted peavad rohkem panustama oma müügitööle, referentsidele ja lisandväärtusele.

..JA SEEJÄREL TEGUTSEMA

Igal RIA metoodikat kasutanud ettevõttel on teenuse tulemusena teekaart, mille elluviimisele on tal samuti võimalik toetust küsida. Ehk et kui tööstusettevõtte tellib endale Küberpöörde teekaardi, on tal või-

RIA Küberpöörde toetust saab taotleda veel sel aastal, kuniks jagub Digital Europe'i fondi kaudu saadud raha.

malik saada kõigepealt toetust kuni 10 000 eurot, et oma küberturvalisust hinnata. Seejärel saab ta teekaardi elluviimiseks taotleda veel kuni 50 000 eurot toetust – mõnel juhul tähendab see võrkude segmenteerimist, mõnel juhul turvalistele pilveteenustele migreerimist, kolmandal puhul ehk hoopis töötajate koolitusprogrammi. Nii teekaardi tellimise kui tegevuste elluviimise faasis on ettevõttel 50-protsendiline omafinantseerimise määra.

RIA Küberpöörde toetust saab taotleda veel sel aastal, kuniks jagub Digital Europe'i fondi kaudu saadud raha. Seejärel saame taotluste ja teekaartide tulemuste pealt teha kokkuvõtteid ning otsustada, kuidas edasi liikuda. ●

RIA kasvatab ja hoiab küberturbe kogukonda

RIA täidab Euroopa küberkompetentsikeskuste juurde loodud koordineerimiskeskuste võrgustiku kohaliku rakukese (*national coordination center for Estonia* ehk NCC-EE) rolli, millel on sõsarasutused üle Euroopa. Need asutused igas Euroopa Liidu liikmesriigis edendavad kohalikku küberkogukonda – teaduse, tehnoloogia, turu ja järelkasvu tegevusi. Eesti NCC tegevuste hulka kuuluvad muu hulgas:

▀ **küberlaagrid tüdrukutele.** Kuna küberturbe valdkonnas süveneb tööjõupuudus, korraldame noortele küberturvalisuse suunitlusega laagreid, et valdkonna vastu huvi äratada. Et nii Eestis kui ka maailmas on see ala ka sooliselt tasakaalust väljas, keskendume Eestis just tüdrukute koolitamisele. 2023. aastal toimus kaks linnalaagrit koostöös Kaitseliidu egiidi all toimetavate Kodutütardega ning üks suurejooneline suvelaager, kus üle 70 tüdruku Eestist, Lätist, Tšehhist ja Itaaliast avastasid küberturvalisuse algtoodesid.

▀ **küberidude kiirendiprogramm.** RIA pani koostöös Tehnopol Startup Inkubaatoriga 2023. aasta sügisest tööle küberkiirendi programmi, kuhu pääsenud tiimid saavad oma idee arendamiseks tiptasemel nõu ja 48 000 eurot grantrahasust. Kiirendiprogrammi eesmärk on küberturvalisuse valdkonnas uute toodete ja iduettevõtete tekitamine – seeläbi jõuavad turule uued küberturvalisuse tooted ja teenused, mis loovad kasu ka teistele ettevõtetele. Kiirendis osalejate äriideed peavad vastama ühele kahest tingimusest: see peab olema kas tiptasemel küberturvalisuse lahendus erasektorile või uute tehnoloogiate (tehisintellekt, 5G, masinõpe jmt) küberturvalisusele keskenduv lahendus. Kiirendi kahe vooru vältel aidatakse oma tooteid või teenuseid arendada 15 iduettevõttel.

▀ **kohtumispaik CyberMeetUp.** 2023. aasta märtsist korraldame küberturvalisuse kogukonnale igakuiseid kohtumisõhtuid nimega RIA CyberMeetUp. Tegemist on lühikese programmi osaga, millele järgneb vabas vormis sotsialiseerumine. Oodatud on kõik, kes tunnevad end Eesti küberkogukonna liikmena. Programmiosa näeb ka otsepildis üle interneti ning kõik vastavad ülekanded on järelvaadatavad RIA Youtube'i lehel.

RIA KOGEMUS: kuidas me E-ITSi rakendame

.....

Eesti infoturbestandard ehk E-ITS on kohustuslik umbes 3500 organisatsioonile. RIA on üks neist. Oma avalike ülesannete ja ligikaudu 300 töötajaga tuli meil läbi töötada 6000 infoturbemeedet.

.....

E-ITS on loodud selleks, et tagada ühiskonna seisukohast oluliste organisatsioonide vastupanu küberohtudele. Selle parimad praktikad on taaskasutamiseks, et hoida teiste kogemusest õppides kokku infoturbe rakendamisele kuluvaid vahendeid ja aega.

Väiksematele asutustele, kelle senine kokkupuude infoturbenõuetega on olnud vähene, võib etalonturbe rakendamise süsteem tunduda esmapilgul hirmutav ja ülejõukäiv. Samas annab see võimaluse oma äriprotsessid läbi mõelda, sest küberriskid on äririskid.

ROHKEM VABADUST JA VASTUTUST

Võrreldes oma eelkäija ISKEga aitab E-ITS saavutada just asutuse äri vajadustega sobivat infoturbe taset. Organisatsiooni juhtkonnal on varasemast suurem vabadus – aga ka vastutus – otsustada, milliseid objekte ja protsesse on tarvis kaitsta.

Küsid endalt, mis on organisatsiooni eesmärk, miks see vajalik on ja mida selle eesmärgi täitmiseks teha tuleb, saab selgeks oma äriprotsessid. Võttes järgmiseks ette nõuded, mida eesmärgi täitmisel järgida tuleb, ja hinnates, milline kahju ja kellele tekib, kui neid nõudeid mitte täita, saab teada oma kaitsetarbe.

Selgitades detailselt välja varad ja vahendid, mis on ärieesmärgi saavutamiseks vajalikud, saab neile külge panna turvameetmed. Kui varad ja vahendid on sarnased paljudes teistes asutustes kasutusel olevatega, saab kasutada tüüpseid turvameetmeid. Spetsiifilisemate varade või suurema kaitsetarbe korral tuleb meetmed määrata riske analüüsides.

Kui meetmed määratud, saab ette pildi, millised neist on juba rakendatud ja millega veel vaja tegeleda ehk oma tegevused plaanida ning plaani rakendamist seirata. On loomulik, et kõike korraga ei saa ning ülesjäävaid riske tuleb juhtkonnal teadvustada ja aktsepteerida.

RIA KOGEMUS

RIAs võtsime E-ITSi rakendamise ette 2022. aasta kevadel kohe pärast määruse jõustumist. Vastuseid küsimustele, mis on RIA jaoks äriprotsess ja kuidas hakata kaitsetarvet määrama, hakkas otsima üheksast inimesest koosnev juhtgrupp.

RIAs on äriprotsessid teenusvaldkonna tasandil ja neid on kokku üle 50. Kuivõrd üksused vastutavad enamasti oma tehniliste lahenduste ja ka serverite haldamise eest ise, tuli kaitsetarvet määrama ja infoturbemeetmeid rakendama hakata just sel tasandil. Kaitsetarbe



määramise ülesanne oli kõigi jaoks uus ja nõudis juhendamist. Abiks olid ühiste koosolekute vormis tehtud näidised ja E-ITSi portaalist leitav kaitsetarbe määramise protokoll.

Kui teenusvaldkonnad said septembriks oma kaitsetarbed määratud, tuli lahendada rakendusplaani küsimus. Soovisime, et tekiksid selged seosed varade ja teenusvaldkondade vahel kuni selleni välja, et äriprotsessile tekiks id ainult neile rakenduvad infoturbemeetmed, mille rakendamist saaks mugavalt ja järjepidevalt jälgida. Otsuse tegime juba kasutusel oleva JIRA kasuks, et E-ITSi rakendamine oleks ühtlasi seotud igapäevase töö ja protsessidega. Selleks ajaks oli juhtgrupist tekkinud töögrupp, kuhu kuulus viis inimest, kes kõik pidid samal ajal ka muude tööülesannetega tegelema.

Ees ootas tõeliselt mahukas tööloik – JIRAsse tuli koondada seni eri keskkondades hallatud

varad. Keerukas oli ka algse andmestruktuuri paika saamine ja meeleheidet jagus, püüdes kõiki seoseid ning modelleerimisi õigesti toimima saada.

KAS SEE PÄRISELT TOIMIB?

2023. aasta alguses katsetasime struktuuri toomist X-tee teenusvaldkonna peal. Piloot vabahtlikega õnnestus ja andis kinnitust, et loodud seosed toimivad. Eesmärgiks sai võimalikult automaatse lahenduse loomine. Selleks oli vaja varade kogumiseks ja meetmepiletite loomiseks luua automaatikad. Esimesed neist löid RIA arhitektid ja teise tellisime väljastpoolt maja.

Kevadsuvel uuendasime ka teenuseportfelli ning vaatasime koos iga-aastase riskihaldusprotsessiga üle kaitsetarbed. Jätkutöid ja automaatikate arendusi jagus suvesse ning ka varade väljaselgitamise kaasasime kogu maja.

Järgnes juba käsitsi protsessipiletite loomine ja sügise teises pooles hakkasime katsetama automaatikaga. Praeguseks oleme olukorras, kus varade lisandumisel tekivad E-ITSi meetmepiletid JIRA rakendusplaanis automaatselt, sarnaselt toimub ka nende eemaldamine. Süsteem on elav ja jätkusuutlik.

ÜHISED RÕÖMUD JA MURED

Aastaga on toimunud muutus ka paljude kolleegide meelestatustes. Osakondade koostöös loodud tehnilisest lahendusest nähakse päriselt kasu – see hoiab oluliselt kokku osakondade aega E-ITSi rakendamisel ja teeb turvameetmete rakendamise jälgitavaks nii meeskondade kui ka asutuse tasandil. Ent sama väärtuslik on ka ühise eesmärgi nimel töötamisega kaasnenud osakondadevaheliste müüride langemine ning toote-, tugi- ja juhtimisüksuseid siduva töövoo loomine.

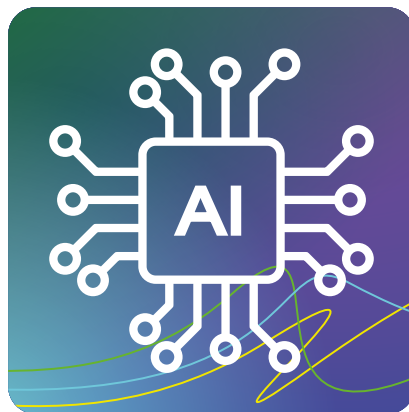
Pooletise aasta jooksul suhtlesime paljude teiste E-ITSi rakendajatega, et ühiselt rõõme ja muresid arutada. Oleme aja jooksul saanud häid mõtteid teistelt ning jaganud enda lahendust umbes 20 asutusega. Möödunud aastal jõudsime edukalt lõpule eelauditiga ning eesmärk on põhiauditiga lõpetada märtsis 2024. Valminud rakendusplaani oleme valmis ka edaspidi esitlema kõigile, kes soovivad meie kogemusest õppida. ●

Mida oodata 2024. AASTALT küberruumis?

TEHISINTELLEKT muudab mängu

Tehisintellekt on viimastel aastatel arenenud peadpöörivate sammudega. Selle abil juba koostatakse õngitsuskirju või -sõnumeid, millega petetakse välja raha või kasutajakontosid. Ent kaugel pole aeg, kus tehisintellekt muutub nii kurjategijate kui kurjade kavatsustega riikide käes võimsaks küberrelvaks, millega kutsuda esile suure mõjuga intsidente.

Õnneks on sel mündil ka helgem pool – nimelt saab tehisintellekti rakendada nutikate kaitselahenduste ülesehitamiseks, alustades selle kasutamisest riskiplaani koostamisel ning lõpetades näiteks süsteemide reaajas monitoorimisega. Igal juhul on lähiaastad siin vallas kiired ja põnevad.



Küberkerksus DEMOKRAATIA KAITSEL



Autoritaarsed riigid, näiteks meist ida pool, on aastaid üritanud Lääne demokraatiade avalikku arvamust desinformatsiooni levitamisega enda kasuks kallutada. Selline tegevus tavatseb intensiivistuda enne olulisi valimisi (USA presidendi-valimised, Saksamaa parlamendivalimised jne). 2024. aasta juunis valitakse kõigis 27 Euroopa Liidu liikmesriigis esindajaid Euroopa Parlamenti ja seega võib eeldada mõjutustegevuse intensiivistumist. Samal eesmärgil võidakse kasutada ebameeldivate

kandidaatide meili- või muudele kontodele sisse murdmist ja tundliku info lekitamist. Samuti ei saa välistada rünnakuid valimissüsteemide vastu.

Kuigi Eesti e-valimised on maailmas endiselt unikaalsed, kasutavad arenenud riigid valimiste läbiviimiseks ohtralt erinevaid IT-süsteeme. Seega peame nii meie Eestis kui meie liitlased teistes riikides olema valmis turvama valimisteks vajalikke süsteeme ning tõstma valimisjaoskondade personali ja kandidaatide IT-vaatlikkust.



KÜBER tõuseb juhtkonna tasandile

Mida aasta edasi, seda selgem on, et üheski arvestatavas ettevõttes või asutuses pole küberturvalisus ainult IT-spetsialisti või infoturbejuhi mure. See peab olema ka selgelt ja pidevalt juhtkonna tasemel seiratud risk, mis hooletusse jätmise korral võib väga valusalt hammustada nii mainekahju, saamata jäänud tulu või andmeleketest johtuvate trahvidena. Küberturvalisuse tagamiseks on vaja välja selgitada riskid, kujundada protsessid ning üles ehitada meeskonnad ja süsteemid. Kõik see nõuab muidugi raha, ent seda ei tohi käsitleda mitte kulu, vaid investeeringuna. Teenust väljastpoolt sisse ostes tuleb seda teha teadlikult, olles kindel, mida oma raha eest ikkagi saab. Ettevõtte, kes lähiajal nii käitub, ei leiuta küll jalg-ratast, aga aitab kindlustada oma tulevikku. Tähtis seegi.

Eesti IT-VAATLIKKUS paraneb

Alates 2019. aastast meie poolt statistikaametilt tellitud uuringute tulemused näitavad, et Eesti inimeste teadlikkus küberhügieenist on järjepidevalt tõusnud. Loodetavasti aitavad eelmisel aastal toimunud suurema mõjuga intsidendid – lisaks andmeleketele näiteks häired rongipiletite ostmisel või katlamajade töös – kaasa mõistmisele, et küberturvalisus on päriselt oluline, sest edukad ründed võivad segada harjumuspärast ja mugavat elu ning viia kurjategijate kätte kõige tundlikumad andmed. Teadlikkusest ei piisa, vaja on ka tegutseda – teha kiirelt vajalikke tarkvara-



uuendusi, paigata turvaauke ning jälgida muid RIA juhiseid küberriskide vältimiseks. Sageli on selleks vaja vaid üht-kaht näpuliigutust!

ANDMEKAITSE tuleb pildile

Küberrünnakule järgnenud andmeleke sisaldab suure tõenäosusega ka isikuandmete leket.

Varasemalt pole isikuandmete küsimus Eesti avalikkuses väga kuum olnud, kuid siingi raamatus käsitletud Asper Biogene'i juhtum – sh umbes 10 000 inimese terviseandmete varastamine kurjategijate poolt – muutis olukorda ning tõstis ühiskonna teadlikkust andmekaitse olulisusest. Muret oma andmete turvalisuse ja kasutamise pärast suurendas ka augustis avalikuks tulnud juhtum, milles küsiti rahvastikuregistrist välja tuhandete lastetute Eesti naiste andmed.

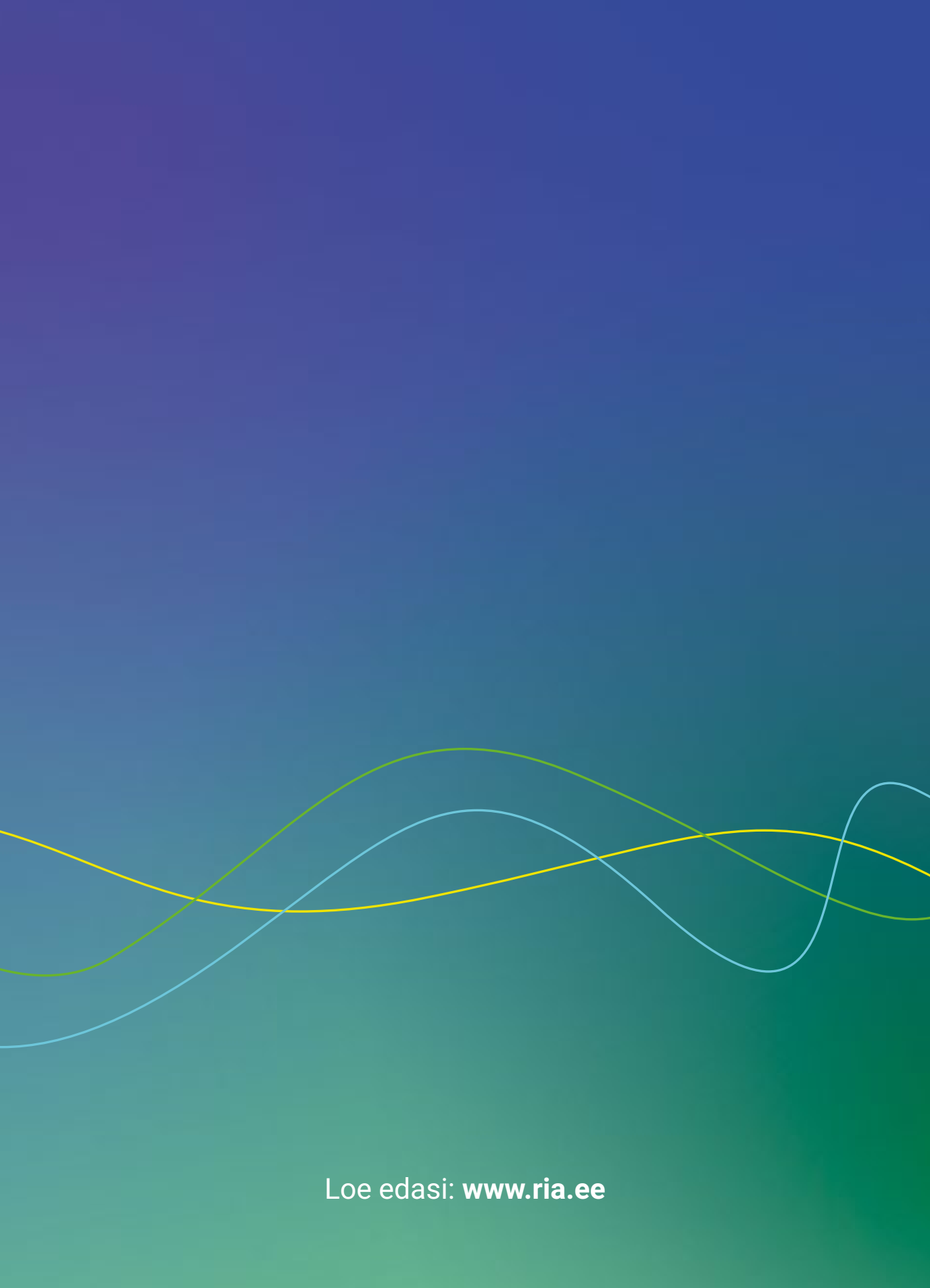
Ehkki Eestis pole seni tehtud GDPRi ehk isikuandmete kaitse



üldmääruse rikkumise eest suuri trahve, usume, et mainitud kaasuste jõudmine avalikkuse ette kasvatab asutuste ja ettevõtete soovi neile usaldatud isikuandmeid senisest paremini kaitsta.

Küberturvalisuse aastaraamat 2024

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



Loe edasi: www.ria.ee