

KÜBERTURVALISUSE AASTARAAMAT

2026



RIIGI INFOSÜSTEEMI AMET



Küberturvalisuse aastaraamat **2026**

SISUKORD

EESSÖNA

6

Usaldus, mis kannab

Ajal, mil ohud kasvavad ja sõltuvus digilahendustest süveneb, määrab meie vastupidavuse see, kui teadlikult suudame riske juhtida ja usaldust hoida, kirjutab **Gert Auväär**, RIA peadirektori asetäitja küberturvalisuse alal.



2025. AASTA ÜLEVAADE

8

Olukord küberruumis: pettuse aasta

Kaablitikked, teenusekatkestused ja ummistasründed – neid kõiki oli rohkem kui ootasime, aga eelkõige jäab 2025. aastat meenutama rekordarv pettuseid ning nende põhjustatud kahju.

14

Ummistasründed: Eesti võtsid sihikule uued rühmitused

Eesti võtsid sihikule Lähis-Ida, Põhja-Aafrika ja Kagu-Aasia riikidest pärinevad rühmitused.

16

Lunavara: uued ründed, vanad vead

Lunavararünnete arv ja nende põhjustatud kahju on maailmas kasvutrendis. Eestis on olukord pigem stabilne, kuid tõsiseid probleeme põhjustanud ründeid nägime ka siin.

18

Pettustelaviini kahju: 29 miljonit

Murenemise märke oli näha juba varem, kuid 2025. aastal varises kokku keelebarjaär, mis meid pettuse eest veidigi kaitseks.

22

Järjekordne rekordarv turvanõrkusi

Tõsiseid haavatavusi jagus võrguseadmetesse, tööstusautomaatikasse, operatsioonisüsteemidesse ja muudesse tarkvaradesse.

24

2025. aasta globaalses küberruumis

Lunavararünded räsisid tuntud brändide mainet, Põhja-Korea libatöötajad püüdsid imbuda rahvusvahelistesse tehnoloogiaettevõtetesse, ulatuslikud teenusekatkestused tõid esile kriitilisi sõltuvusi.

28

Sõda Ukraina küberruumis: kaitse pidas

2025 oli esimene aasta pärast Venemaa täiemahulise sissetungi algust, kus Ukrainas ei toimunud ühtegi väga suure ühiskondliku mõjuga küberrünnakut.

30

SSSCIP juht: rahuleping ei too rahu küberruumi

Ukraina side- ja teabekaitseteenistuse (SSSCIP) juht brigaadikindral **Oleksandr Poti** räägib, mis juhtus möödunud aastal Ukraina küberruumis ja mida oleks teistel sellest õppida.

32

Kübermenüü 2025: Pekingi part

Andmelekked võimaldavad meil heita pilgu Hiina ründavale küberökosüsteemile, mida iseloomustab erasektori ja riigi ulatuslik koostöö.

36

Vene karud küberruumis

Venemaa kasutab küberruumi sihipärase ja efektiivse tööriistana oma välis- ja julgeolekupoliitiliste eesmärkide toetamiseks.

TURVALISEM KÜBERRUUM

40

Ministeeriumi vaade: mis sai tehtud ja mis on plaanis?

Justiits- ja digiministeeriumi digitaristu ja küberturvalisuse asekantsler **Tõnu Grünberg** vaatab tagasi möödunud aasta arengutele riikliku küberturvalisuse vallas ja seab sihte 2026. aastaks.



42

20 aastat Eesti küberruumi kaitsel

20. sünnipäeva puhul vaatame tagasi CERT-EE sündmusterohkele ajaloole.

46

Alustas RIA juhtimiskeskus

1. juunil 2025 alustas RIA juhtimiskeskus, mille ülesanne on jälgida ja juhtida RIA teenuste tööd ning seirata Eesti küberruumis toimuvat.

48

Mida me ennetuse vallas tegime?

Eelmise aasta suurima ennetuskampaania suunasime ettevõtetele, et nad oskaks küberruumis varitsevaid ohte ära tunda ja end nende eest kaitsta.

50

Kuidas muuta avalikud teenused töökindlamaks

Eesti ühiskond toimib mugavatel avalikel teenustel, kuid nende taga peidab end sõltuvuste rägastik. RIA otsib ja parandab selle nörku lülsid, et teenused toimiksid ka siis, kui katkeb oluline sidekaabel või elektrühendus.

52

„Halvimal juhul jäädme päevadeks elektrita“

Need kurjakuulutavad sõnad kölasid Küberreservi öppusel, kus koostöös Eleringiga harjutati läbi, kuidas käituda, kui küberruunnaku tööttu satub ohtu kogu Eesti elektrivarustus.

54

Küberturvalisus kui organisatsiooni küpsuse peegel

Sageli räägitakse küberturvalisusest kui tehnilisest nähtusest, kuid see on vaid pool rehkendust.

56

Uus toetus küberturbeettevõtetele

RIA ja Ettevõtluse ja Innovatsiooni Sihtasutus (EIS) töötasid välja innovatsioonitoetuse küberturbeettevõtetele, et edendada selle valdkonna toote- ja teenusearendust.

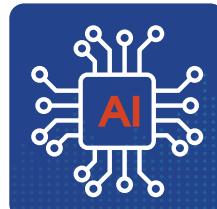
58

EU CyberNet laieneb itta

Euroopa Komisjon pikendas kolme aasta võrra RIA juhitavat ja ELi rahastatavat küberturvalisuse arenguabi projekti EU CyberNet. See toob uued partnerid ja võimaluse viia ELi abi Kagu-Aasia ning India ookeani piirkonda.

60

Mida oodata 2026. aastalt küberruumis?



USALDUS, MIS KANNAB

Ajal, mil ohud kasvavad ja sõltuvus digilahendustest süveneb, määrab meie vastupidavuse see, kui teadlikult suudame riske juhtida ja usaldust hoida – nii riigi, organisatsioonide kui ka inimeste tasandil, kirjutab **GERT AUVÄÄRT**, RIA peadirektori asetäitja küberturvalisuse alal.

Küberturvalisus on see, mis hoib argipäeva toimimas. See on taustajöud, mis kindlustab, et toas süttib valgus ja kraanist tuleb vesi, pangaülekanne jõuab kohale ja poes saab makstud. Enamasti me sellele ei mötgle – ja just nii peabki olema. Eesti digiriigi tugevus ei sünni pelgalt nutikatest teenustest, vaid nende vaiksest töökindlusest ka siis, kui küberruum on rahutu ja tehnoloogia ettearvamatu. See nähtamu toimepidevus on üks tänapäeva ühiskonna olulisemaid kokkuleppeid.

Möödunud aasta arengud näitasid selgelt, et küberjulgeolek ei ole ammu enam pelgalt IT-entusiastide kitsas pärusmaa. See on ühiskonna toimimise alus, mis puudutab korraga ettevõtlust, ava-

likke teenuseid, energiajulgeolekut ja inimeste igapäevast turvatunnet. Digiriigi toimimine on lahutamatult seotud küberruumi stabiilsusega ning iga tõrge või rünne võib avaldada mõju, mis ulatub kaugemale ühest süsteemist või teenusest.

OHUD, MIS EI KÜSI LUBA EGA AEGA

Küberohud kasvavad üle maailma ning muutuvad üha massilisemaks ja keerukamaks. Nullpäeva haavatavusi kasutatakse ära mõne tunniga, lunalvararünded põhjustavad nii otsest majanduslikku kahju kui ka usalduse murenemist ning riikliku taustaga ohustajad tegutsevad pika vaatega, otsides püsivat ligipääsu kriitilistesse süsteemidesse. Kõige selle kõrval muudab tehisaru areng ründed kiiremaks ja raskemini tuvastatavaks, mistöttu ei piisa üksnes reageerimisest – vaja on pidevat olukorrataju ja ennetavat valmisolekut.

Üha sagedamini puudutavad küberohud ka tavainimesi, kelle jaoks pettused tähendavad lisaks rahalisele kaotusele turvatunde kadumist. Möödunud aasta tõi selle eriti selgelt esile: Eesti inimesed kaotasid petturitele 29 miljonit eurot. Keelebarjääri kadumine ja osav sotsiaalne manipulatsioon on muutnud pettused massiliseks, eriti telefonikõnede kaudu, kus mängitakse kiiruse, hirmu ja näilise autoriteediga. See kinnitab, et digiriigi

Möödunud aasta arengud näitasid selgelt, et küberjulgeolek ei ole ammu enam pelgalt IT-entusiastide kitsas pärusmaa.



Gert Auväärts

turvalisus ei sõltu ainult tehnilistest lahendustest, vaid ka inimeste otsustest hetkedel, mil keegi püütab nende usaldust ära kasutada.

ENNUS ALGAB OTSUSTEST

Just sellises keskkonnas muutub keskseks küsimus, kuidas me ühiselt riske mõistame ja maandame. Suur osa küberintsidente on endiselt välditavad elementaarse küberhügieeni ja läbimöeldud juhtimisotsustele abil. Organisatsiooni kübervalisuse tase peegeldab otseselt selle kiupsust, vastutusvõimet ja valmisolekut ebamugavatele stseenariumitele ausalt otsa vaadata. Samas ei sünni kõik suure mõjuga digikatkestused pahatahtlikest rünnetest. 2025. aasta ulatuslikumad globalsed häired said alguse tehnilistest tõrgetest suurtes pilveteenustes, mõjutades korraga tuhandeid organisatsioone ja miljoneid kasutajaid. Need juhumid näitasid, kui sügavalt on meie igapäevalu ja majanduse toimimine seotud väheste, kuid kriitiliste globaalsete teenusepakkujatega.

Digiriigi tugevus ei avaldu ainult innovatsioonis, vaid võimes püsida toimivana ka siis, kui midagi läheb valesti. Ühtse vaate ja parema valmisoleku loomiseks on vaja tervikpilti. Oluline samm selles suunas oli RIA juhtimiskeskuse loomine, mis hakkab koondama ülevaadet Eesti

küberruumis toimuvast ja riigi jaoks kriitiliste teenuste seisust. Selline olukorrateadlikkus loob eelduse kiiremaks reageerimiseks, paremaks koostööks ja selgemaks juhtimiseks.

KÜBERRUUM EI TUNNE PIIRE

Kõiki neid teemasid seob üks läbiv põhimõte: kübervalisus on eeskätt juhtimise, vastutuse ja koostöö küsimus. Tehnoloogiad ja standardid on vältimatud, kuid neist üks ei piisa. Küps riik tunneb oma riske ja valmistub ka ebamugavateks stseenariumiteks.

Eesti kogemust ja kompetentsi vajatakse ja hinnatakse ka rahvusvaheliselt. Küberruumis ei ole piire ning nõrk lüli kusagil mujal võib kiiresti mõjutada ka meid. Rahvusvaheline koostöö, infojagamine ja ühised õppused on seetõttu oluline osa vastupanuvõime kasvatamisest.

Seda nähtamatut, kuid kriitilist vastupidavust kehastab köige selgemalt CERT-EE 20-aastane teekond. See on lugu järjepidevusest ja tööst, mis jäääb enamasti avalikkuse tähelepanuta, kuid mille tulemusel püsivad teenused töös, kriisid ennatakse ja usaldus säilib.

***Meie ühine eesmärk on,
et Eesti (digi)riik oleks
vastupidav. Et tuled
põleksid, vesi voolaks ja
digiteenused toimiksid.***

Meie ühine eesmärk on, et Eesti (digi)riik oleks vastupidav. Et tuled põleksid, vesi voolaks ja digiteenused toimiksid. Ning et usaldus – meie suurim ja sageli nähtamuim kapital – püsiks kindel. ●

Olukord küberruumis: **PETTUSTE AASTA**

Kaablitrikked, teenusekatkestused ja ummistusründed – neid kõiki oli rohkem kui ootasime, aga eelkõige jäab 2025. aastat meenutama rekordarv pettuseid ning nende põhjustatud kahju.

57-aastase mehega võttis ühendust end investeeringuisnõustajana esitlenud inimene. Nõustaja juhendamisel registreeris kannatanu end krüptoraha kauplemisplatvormil ning tegi sinna sissemakse 1300 eurot. Kelmide juhendamisel tegi kannatanu kuue kuu vältel enda ettevõtte kontodelt petuplatvormile ülekandeid kogusummas 504 400 eurot.

54-aastane naine tutvus Messengeris võõra mehega. Pärast paripäevast suhtlust viis mees teema investeeringisele ning soovitas kannatanul end registreerida investeeringisplatvormil. Kelmi-

de õhutamisel võttis kannatanu viie kuu vältel laene ning andis kelmidele sularaha ja kulda, et nad summa platvormile kannaks. Lisaks müüs kannatanu maha oma korteri ja andis saadud raha kullelile. Kelmusega tekitatud kahju on esialgsel hinnangul vähemalt 200 000 eurot.

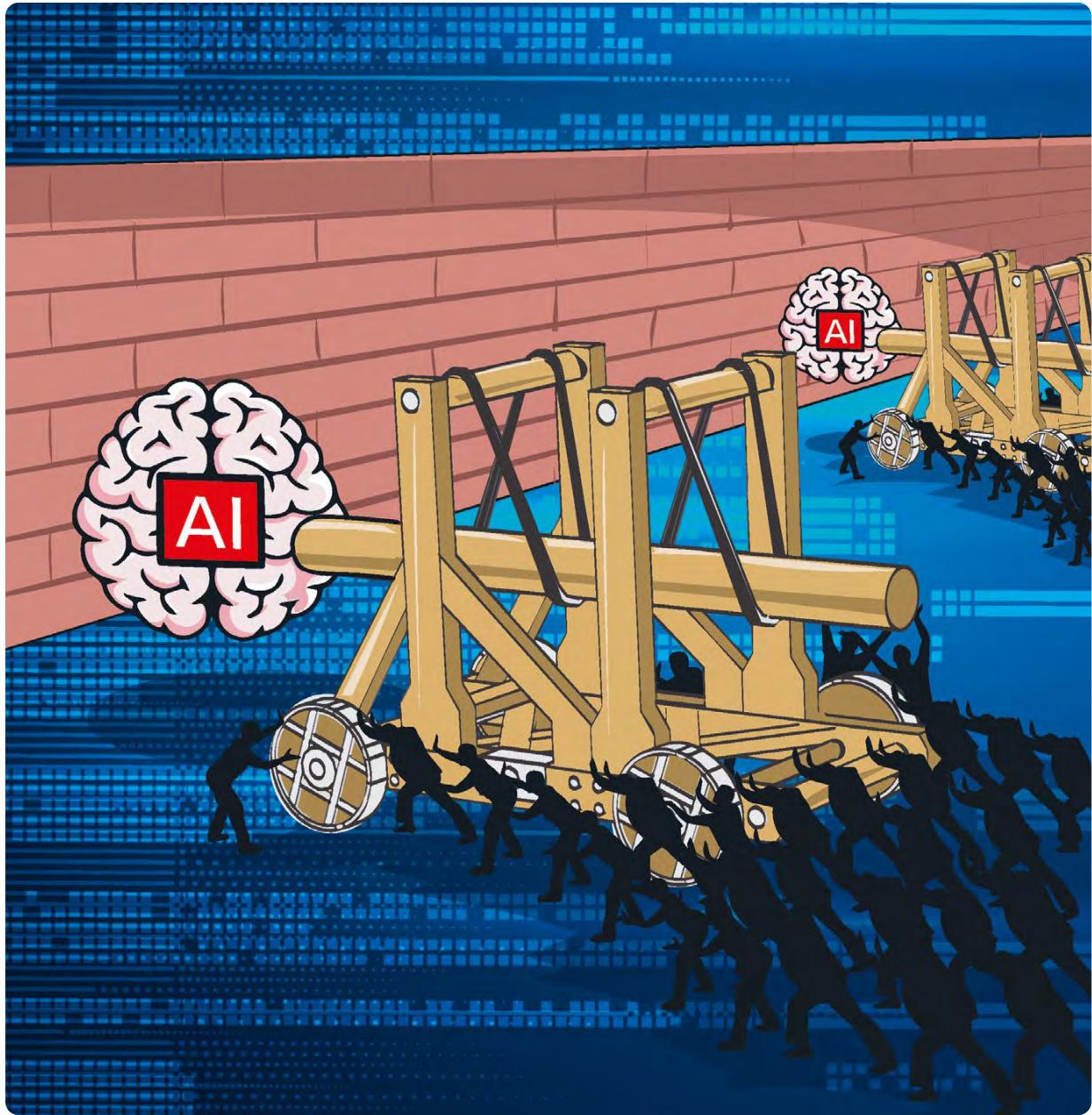
71-aastasele naisele helistasid näiliselt politsei ja panga nimel kelmid, kelle juhendamisel müüs kannatanu kaks talle kuulunud korterit. Korterite müügist saadud raha võttis kannatanu sularahas välja ja andis võõrastele. Kelmusega tekitatud kahju on esialgsel hinnangul 138 000 eurot.

JAANUAR ›

- Eestis tegutseva panga vastu toimusid teenusetõkestusründed, mille tõttu oli selle internetipanga töös lühiajalisi katkestusi.
- Levisid näiliselt maksu- ja tollimetri nimel saadetud petukirjad ja -sõnumid, milles väideti, et inimest ootab maksutagastus. Selleks suunati saajad skaneerima QR-koodi, mis viis õngitsuslehele.
- Sertifikaadi aegumise tõttu katkes automaatse piirkontrolli ehk ABC-värvate töö.

VEEBRUAR ›

- Kuu algul oli mobiil-ID töös törkeid Elisa ja kuu lõpus Telia võrgus.
- Häireid oli hädaabiteadete süsteemis. Seetõttu oli osale 112 könedele vastamise ooteaeg tavapärasest pikem.
- Eesti.ee rakenduse töö katkes rohkem kui ööpäevaks.



MÄRTS >

- ➥ Teenusetõkestusründed ühe panga nimeserverite suunal põhjustasid häireid selle internetipanga, mobiilirakenduse ja välkmaksete töös.
- ➥ Siseministeeriumi haldusalas oli häireid süsteemidesse sisselfogimisega, mh möjutas see PPA ja häirekeskuse süsteeme.
- ➥ Törkeid oli Smart-ID töös.

APRILL >

- ➥ Kuu algul oli suurem ummistusrünnete laine Eesti suunal. Rünnakud olid tehniliselt tavapärasest keerukamad, mistöttu oli osa veebilehtede töös lühiajalisi katkestusi.
- ➥ Levisid petuköned, kus petturid tutvustasid end tervisekassa töötajatena ja meelitasid sisestama Smart-ID PIN-koode.

LÕPUTU LAVIIN

Selliste nukrate kirjeldustega, mis politsei- ja piirivalveameti (PPA) ning RIA infovoost läbi käivad, võiks täita terve raamatut. Ainutiksi nende kolme juhtumi kahjustid kokku lüüs jõuame esimese miljoni lähistele. Kui liita kokku kõik 2025. aasta jooksul registreeritud kelmuskuritegude kahjud, vaatab vastu 29 miljonit eurot.

See summa on suurem kui kuurortlinna Haapsalu aastaelarve, selle eest saanuks ehitada uue riigigümnaasiumi või ostaa Elronile mõned rongid. ETV heategevussaate „Jõulutunnel“ käigus annetasime laste harvikhaiguste raviks alla 400 000 euro, petturitele aga kümneid miljoneid.

Kui varem päästis meid vähemalt osaliselt keeleruum, siis 2025. aastal varises see kaitsevall kokku.

Kui varem päästis meid vähemalt osaliselt keeleruum, siis 2025. aastal varises see kaitsevall kokku. Välismaistesse kõnekeskustesse, kust kelmid helistavad, on tööle jõudnud meie kaasmaaled. Ühe pettuse läbiviimisel osaleb tihti kaks-kolm sulaselget eesti keelt kõnelevat kelmi: esimene esitleb end näiteks tervisekassa töötajana, teine pangatöötajana ja kolmas politseinikuna.

Skeemid muutuvad – elektriarvesti vahetamine, erakordset tootlust lubav investeeringuskeem, kasutamata jäänud hüvitise või midagi muud –, aga tulemus on sama: kõne ajal PIN-kodee sisestades, pangakaardi andmeid ära andes või raha kahtlasel platvormile kandes jätab kannatanu oma säästudega hüvasti. Töenäosus seda raha tagasi saada on väga väike.

Seni on telefonipettuste taga luust ja lihast inimesed, kuid arvestades tempot, millega tehisaru eesti keelt õpib, võime võtta lahjemat mürki, et lähiaastatel hakkame saama kõnesid ka masinatelt. Vähemalt esialgu ei pruugi tehisaru olla sama veenev kui inimene, kuid kvantiteet aitab korvata kvaliteeti.

Tehisaru leiab juba mõnda aega raken-dust kõikvõimalike petukirjade, -sõnumite ja -lehtede loomisel. Siin on kvantiteeditöös olnud märgatav: peamiselt veebiboodideks ja investeeringusplatvormideks maskeerunud petulehti tuvastasime rohkem kui kunagi varem. Avastamise järel palume veebimajutajatel pahaloomulised lehed eemaldada, kuid sama hoogsalt tekib uusi.

Ehkki pettustekindlama Eesti loomisel on kõige tähtsamal kohal ohtudest teadlikud ja ettevaatlid inimesed, saame kelmide elu raskemaks teha ka tehniliste vahenditega. Telefonikasutajatele tuleb appi CERT-EE loodud rakendus Encrypted DNS, mis blokeerib ligipääsu meile teadaolevatele pahatahtlikele lehtedele, kus võib kaotada oma raha või andmed.

MAI >

- ➥ Ida-Tallinna keskhaigla IT-süsteemide hooldustööde käigus tekkis tõrge, mille tõttu ei saanud serverid vajalikele andmetele ligi. Haiglas kuulutati välja kriisiolukord: operatsioonid lükati edasi ning erakorralise meditsiini osakonda saabunud patsientid suunati teistesse haiglatesse. Võrkude töö taastati 2,5 tunni möödudes.

JUUNI >

- ➥ Hooldustööde käigus katkesid Tervise ja Heaolu Infosüsteemide Keskuse (TEHIK) välisühendused ja neist sõltuvad teenused: tervise infosüsteem, tervisekassa teenused (digiresept, kindlustatuse kontroll, töövõimetushüvitise), terviseportaal ja TEHIKu veebileht.
- ➥ Haldussüsteemi rikke tõttu tõrkusid paljud siseministeeriumi haldusala süsteemid. Seetõttu olid hädaabikõnedele vastamise ooteaeg ja järjekorrad piirpunktides tavapärasest pikemad. Katkes dokumentide väljastamine PPA esindustes ja Selverites.

SK ID Solutions tõi välja autentimisvahendi Smart-ID uuendatud versiooni Smart ID+. See pole võluvits köikide pettuse vastu, kuid osale telefonikelmustele, kus kasutajaid meelitatakse ja kiirustatakse sisestama PIN-koodi, peaks see pidurit tömbama.

Valvsust ei tasu kellelgi kaotada, sest kui üks võimalus kaob, hakkavad petturid otsima järgmisi. Naiivne oleks arvata, et nad neid ei leia.

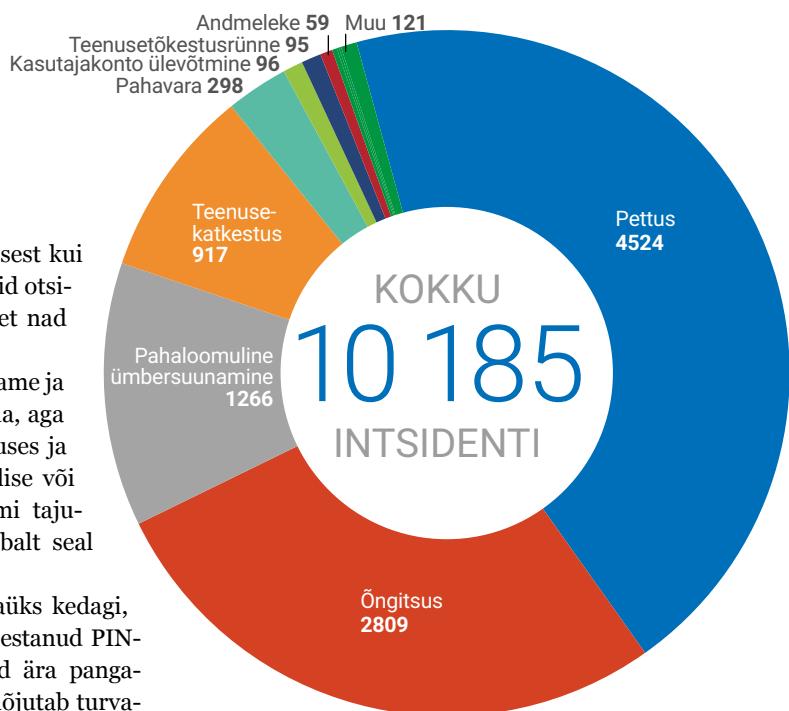
Miks me pettustest nii palju kirjutame ja räägime? 29 miljonit on suur summa, aga asi pole ainult rahas, vaid ka usalduses ja üldises turvatundes. See, kui turvalise või ebaturvalisena inimesed küberruumi tajuvad, sõltub suuresti sellest, kui vabalt seal kuritegevus vohab.

Kui mitte ise, siis küllap teab igaüks kedagi, kes on langenud pettuse ohvriks: sisestanud PIN-koodi, kui poleks pidanud; andnud ära panga-kaardi andmed või raha. Kõik see mõjutab turvatunnet, aga ka usaldust e-teenuste vastu laiemalt. Loe pettuse teemal pikemalt lk 18.

GEOPOLIITIKA KAJA ESTI KÜBERRUUMIS

See, et 2022. aastal alanud täiemahuline sõda Ukraina vastu mitmekordistas Eesti suunal tehut teenusetõkestusrünnete arvu, pole enam uudis – oleme sellest kirjutanud kolmes viimases

MÕJUGA INTSIDENDID 2025. AASTAL



aastaraamatus. Seekordne pole erand. 2025. aastal püstitas ummistusrünnete arv järjekordse rekordi, kuid suurt eduelamust me riindajatele ei pakkunud: selliste rünnete arv ja osakaal, millel oli mingi mõju (enamasti lühiajaline katkestus mõne veeblehe või -teenuse töös), oli teist aastat järjest languses.

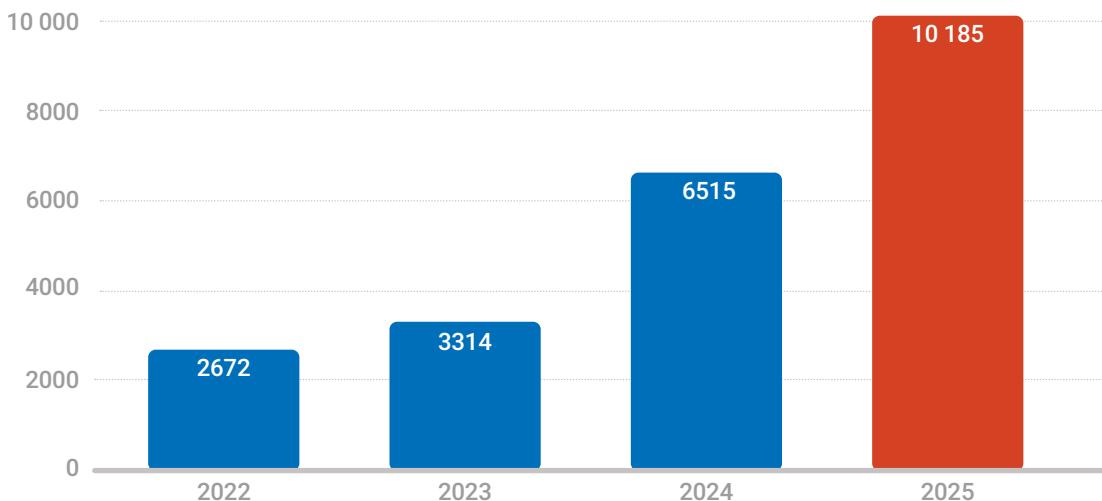
JUULI ➤

- ➥ Taas törkus hädaabiteadete menetlemise infosüsteem. Seepärast tehti häirekeskustes tööd paber ja pliatsiga, mis võttis tavapärasest rohkem aega ja tekitas könejärjekordi.
- ➥ Mitmel korral oli häireid mobiil-ID töös. Vähemalt kahel juhul oli nende põhjuseks teenusetõkestusrünne.
- ➥ Eesti äpis ei toiminud isikut töendavate dokumentide ega teiste teenuste päringud. Rakenduse kasutajate arvu hüppeline kasv tõi välja seadistusvea, mis väiksema koormuse korral ei avaldunud.

AUGUST ➤

- ➥ Sai teatavaks, et masinatööstusettevõte Hekotek kaotas petturitele üle miljoni euro. Suure kahjuga lõppenud sündmuste jada algas ettevõtte finantsjuhile tehtud petukönega, kus kelmid esitlesid end tervisekassa töötajana.
- ➥ Levisid Elisa ja Telia nimel saadetud petukirjad. Elisa nimel saadetud petukirjas väideti, et klient on teinud ülemakse ning tagasimakse tegemiseks on vaja kasutaja makseandmeid. Telia nimel saadetud kirjades aga väideti, et kliendil on viimane arve tasumata ja suunati petulingi kaudu makset tegema. ➤

MÕJJUGA INTSIDENTIDE HULK KASVAS POOLE VÖRRA



Siiski oli ka üllatusi. Kui varem olime populaarne sihtmärk kremlimeelsele häktivistidele, keda häiris meie toetus Ukrainale, siis eelmisel aastal võtsid Eesti sihikule ka palestiinameelsed rühmitused Lähis-Ida, Põhja-Aafrika ja Kagu-Aasia riikidest.

Nende silmapaistvamad etteasted toimusid aprillis ja mais. Need ründelained olid mahult suured ja keskmisest keerukamat: ründajad muutsid jooksvalt oma taktikat, eesmärgiga kaitsemeetmetest mööda minna.

Ummistusrünnetest, nende mõjust ja põhjustest, miks Eesti palestiinameelsele rühmitustele ette jäi, loe lk 14.

IGA INTSIDENDI TAGA POLE RÜNNAK

Kui ummistusrünnete tagajärvel oli mõne teenuse töös katkestusi või häireid 95 korral, siis muudel põhjustel ligi kümme korda rohkem. Enamasti polnud nende taga kellegi kuri käsi või salakaval plaan, vaid inimlik eksimus, seadistusviga, tarkvõi riistvara tõrge.

Eelmine aasta ei toonud kogu ühiskonda raputanud teenusekatkestusi, kuid väiksemaid ebamusgavusi jagus küllaga. Mais oli törkeid Elisa kõnesides, juunis said sama tunda osad Telia kliendid Lääne-Virumaal. Korduvalt oli häireid tervisekassa teenustes (digirest, kindlustatuse kontroll),

SEPTEMBER >

- ➥ Kahel korral katkes Elroni veebilehel rongipiletite müük. Mõlema katkestuse taga oli viga piletimüügisüsteemi haldava ettevõtte Ridango süsteemides.
- ➥ Törkeid oli Swedbanki (internetipank, äpp, kaardimaksed), Luminori (kaardimaksed) ja SEB (veebileht) teenustes.
- ➥ Levisid Omniva nimel saadetud õngitsussõnumid ja Telia nimel saadetud petukirjad.

OKTOOBER >

- ➥ Kohalike omavalitsuste volikogude valimised mõodusid küberruumis suhteliselt rahulikult. Valimistega seotud veebilehti tabasid teenustökestusründed, kuid mõju neil polnud.
- ➥ Törksid rahvastikuregistri teenused, mis omakorda häiris neist sõltuvate teenuste (hädaabiteadete menetlemine, isikut töendavad dokumendid jt) tööd.
- ➥ Levisid taas erinevad telefoni- ja internetipettused. Suur osa petukõnesid tehti Elektrilevi ja tervisekassa nimel, kus pakuti elektriarvesti vahetust või ravihüvitist.

mitmel korral seiskus automaatse piirikontrolli ehk ABC-värvate töö. Tõrkeid oli internetipankade, mobiil-ID ja Smart-ID töös. Mitmel korral ei saanud reisijad osta Elroni veeblehelt rongipiletid, sest piletimügisüsteemi haldava ettevõtte Ridango seadmed tõrkusid.

Küberturve peaks olema kihiline nagu Napoleon kook.

Kõige nähtavamad olid aga kaks teenusekatkestust, mille juured polnud Eestis, vaid USA-s. 18. novembril tabas rike globaalse haardega internetitaristu- ja turbeettevõtet Cloudflare, mille teenuseid kasutatakse laialdaselt ka Eestis. Paari tunni jooksul polnud kätesaadavad mitmed udisteportalid (Delfi, Eesti Ekspress, Õhtuleht), samuti olid häiritud LuxExpressi ja Elroni veebikeskkonna töö, mistõttu ei saanud sealtkaudu piletide osta.

Nii suure mõjuga rike ettevõttes, millest sõltub suur osa maailma internetist, on haruldane. Aga veel erakordsem on, et vähem kui kolm nädalat hiljem juhtus sama asi. Sel korral katkes Eestis paljude avaliku sektori veeblehtede töö, mh riigikogu, valitsuse ja politsei oma. Kasutada ei saanud Bolti veeblehte ega rakendust, riikliku autentimisteenuse TARA tõrked kestsid umbes paar-kümmend minutit.

Esimesel juhul põhjustas katkestuse andmebaasi uuendamise käigus tehtud apsakas, teisel

puhul tulemüüris tehtud muudatus, mis ei läinud päris nii, nagu plaanitud.

Aasta lõpp tõi meile aga taas mitu uudist probleemidest merekaablitega. 28. detsembril algasid rikked Eesti ja Roots'i vahelises Citic Telecomi andmesidekaablis, 30. detsembril Hiiumaa Mandri-Eestiga ühendavas Telia kaablis ning Hiiumaa ja Roots'i vahelises Arelioni kaablis. Aasta viimane päev tõi teateid kahe Eesti ja Soome vahelise merekaabli rikkest, üks neist kuulub Eli-sale, teine Arelionile. Mis kaablitega juhtus, selgitab välja uurimine, kuid olulisi teenusekatkestusi need juhtumid ei põhjustanud, sest andmeside suunati ümber teistesse kaablitesse.

Just sel moel peaks toimima kõik teenused ja meie küberkaitse. Kui üks ühendus või andmekeskus lõpetab rikke või ründe töttu töö, liigub teenuse osutamine kiirelt üle varulahendusele. Küberturve peaks olema kihiline nagu Napoleon kook. Kui esimene kiht ei suuda ründaja teed sulgeda ja petukirja saaja vajutab selles oleval lingil, siis tuleb appi teine ehk taustal töötav tarkvara, mis blokeerib ühenduse õngitsuslehega enne, kui kasutaja jõuab sinna oma andmed sisestada.

Kihiliist kaitset ja varulahenduste-rohkeid teenuseid! ●

Aasta lõpp tõi meile aga taas mitu uudist probleemidest merekaablitega.

NOVEMBER >

- ➥ Cloudflare'i rike põhjustas katkestusi paljudes riikides, sealhulgas Eestis – paar tundi olid kätesamatud Delfi, Eesti Ekspressi ja Õhtulehe uudisteportalid, samuti etv.ee ja vikerraadio.ee. Lisaks oli häiritud LuxExpressi ja Elroni veebikeskkondade töö, mistõttu ei saanud nende kaudu piletide osta, ja Enefiti koduleht.
- ➥ Tallinna ja Tartu veeblehtede vastu toimusid ummistusründed, mille töttu oli nende töös lühiajalisi katkestusi ja aeglust.

DETSEMBER

- ➥ Cloudflare'i süsteemid tõrkusid taas. Kätesaadavad polnud paljud avaliku sektori veeblehed, sh riigikogu, valitsuse ja politsei oma. Samuti katkes riikliku autentimisteenuse TARA ja Bolti rakenduste töö. Eestis kestsid tõrked umbes 20 minutit.
- ➥ Perearstikeskus teavitas, et on langenud lunavararünde ohvriks. Selle käigus krüpteeriti andmedkahes serveris ja ka varukoopiad. Krüpteeritud serveris olid patsienteide andmed, terviselood ja vastuvõtuajad, mistõttu halvas rünnak perearstikeskuse töö.
- ➥ Taas katkes rongipiletite müük Elroni veeblehel.

UMMISTUS- RÜNDDED: Eesti võtsid sihikule uued rühmitused

Kui 2022. aastast on paljude meie vastu suunatud teenusetõkestusrünnakute taga olnud Vene häktivistid, siis mullu võtsid Eesti sihikule ka Lähis-Ida, Põhja-Aafrika ja Kagu-Aasia riikidest pärinevad rühmitused.

Alustame halva uudisega. Eesti suunal tehtud ummistusrünnete (DDoS) arv kasvas ka 2025. aastal: registreerisime rekordilised 756 rünnet. Seda on üle kolmandiku võrra rohkem kui 2024. aastal ning peaegu sama palju kui aastatel 2022 ja 2023 kokku.

Hea uudis on see, et RIA DDoS-kaitse teenused ei jäänud ründajatele alla. Vaatamata järksult tõusnud ründeaktiivsuslele, on mõjuga rünnete hulk hoopis vähenedud. Kõikidest aasta jooksul regist-

reeritud ummistusrünnetest õnnestus sihitud teenustele mingit kahju (enamasti lühiajiline katkeskus või teenuse aeglus) tekitada veidi alla sajal rünnakul. Seega, mõjuga rünnakute osakaal moodustas vaid 12,5 protsendi. See on märkimisväärne areng vörreledes 2024. aastaga, mil ründajate vaatest oli edukas peaegu iga viies rünnak, või 2023. aastaga, kui mõjuga rünnete osakaal oli 27 protsendi.

Möödunud aasta oluliseks arenguks polnud ainult rünnakute mahu ja tehnilise keerukuse tõus, vaid ka ründajate ringi laienemine. Kui alates 2022. aastast on paljude Eesti vastu suunatud teenusetõkestusrünnete taga Vene häktivistide rühmitused, siis 2025. aasta algusest võtsid Eesti küberruumi sihikule ka Lähis-Ida, Põhja-Aafrika ja Kagu-Aasia riikidest pärinevad palestiinameelset rühmitused.

MIS ON DDoS?

Hajus teenusetõkestusrünne ehk DDoS on küberrünnak, mille eesmärk on muuta sihitud digitaalne teenus (nt veebileht, e-teenus, info-süsteem, võrguteenus jmt) kasutajatele kättesaamatuks. Ründaja tekibat sihtmärgi (serveri, võrguseadme või teenust vahendava süsteemi) suunas lühikese aja jooksul paljude erinevate seadmete pealt väga suure hulga pääringuid, mille tulemusel ei suuda teenus enam tavapäraselt liiklust teenindada ning muutub osaliselt või täielikult kättesaamatuks.

MIKS NEILE EESTI ETTE JÄI?

Olemuse ja tegutsemisviisi poolest sarnanevad palestiinameelsed häktivistid Vene omadega. Mõlema ründetegevus on loomult destruktiiivne ning suunatud riikide vastu, keda nad peavad ideoloogilisteks vaenlasteks. Tihti on nende rün-

UMMISTUSRÜNNETE HULK KASVAB, MÖJUGA RÜNNETE ARV VÄHENEAB



nakud sihitud kriitilise taristu vastu ning nende eesmärk on tekitada sihitud riikide elanikele võimalikult palju kahju ja ebamugavust.

Üldiselt piirdub häktivistide ründetegevus ummistusrünnete ja lihtsakooliste kompromiteerimiskatsetega. Need ei eelda ilmtingimata kõrget tehnilikst võimekust ega musta vööd kübervõtluses, kuid võivad külvata sihitud riikide elanikes hirmu või segadust ning tuua ründajatele kuulsust.

Kui Vene häktivistide peamiseks ideoloogiliseks sihtmärgiks on Ukraina ning teisejärgulisteks vaenlasteks Ukrainat toetavad riigid (peamiselt ELi ja NATO liikmesriigid), siis palestiinameelsete rühmituste keskseks vaenlaseks on Iisrael ning teisejärgulisteks sihtmärkideks riigid ja institutsioonid, keda nähakse Iisraeli toetajatena. Eesti sattus palestiinameelsete häktivistide fookusesse eelkõige seetõttu, et meid käsitletakse osana laiemast lääneriikide koalitsionist.

Lisaks mängib olulist rolli asjaolu, et Vene ja palestiinameelsed häktivistid teevald omavahel aktiivselt koostööd. Kuigi rühmituste peamised sihtmärgid on erinevad, kattuvad nende huvid ELi ja NATO liikmesriikide osas. Seetõttu liituvad palestiinameelsed häktivistid sageli Vene rühmituste algatatud Euroopa-suunaliste ründekampaaniatega ja nende sihtmärkideks saavad riigid, kel pole otsest seost Iisraeli ja Palestiina konfliktiga.

RÜNNAKUD EESTI VASTU

Palestiinameelsete häktivistide kõige märkimisväärsemad ründekampaaniad Eesti suunal toimu-

sid aprillis ja mais. Need olid 2025. aasta mahukaimad ja enim teenusekatkestusi põhjustanud ummistusründed.

Aprillis võttis Eesti küberruumi sihikule Alžeria päritolu palestiinameelne rühmitus, kes korraldas meie avaliku ja erasektori veebilehtede suunal kolm ulatuslikku ründekampaaniat. RIA tuvastas kolme ründelaine peale 44 teenusetõkestusrünnet ning neist 20-l õnnestus sihtmärgiks langenud veebilehtede töös ka katkestusi tekitada. Tegu oli suuremahuliste ja tehniliselt keskmisest keerukamate rünnetega: häktivistid kohandasid iga ründelaine järel oma taktikat, et kaitsemeetmetest mööda saada. Kolme tunni jooksul tegid häktivistid 15 rünnatud veebilehe suunas üle poolte miljardi päringu. 11 minuti jooksul tehti ühe veebilehe pihalt 84 miljonit ründepäringu – maht, mille täitmiseks kuluks tavaolukorras ligi 34 aastat.

Mais ründas Maroko rühmitus Eesti julgeolekuasutuste veebilehti. Kokku tuvastas RIA sellelt rühmituselt kümme rünnakut ning blokeeritud pahaloomuliste pärangute arv oli ligi 225 miljonit. Aprilli kampaaniaga võrreldes oli seda küll poolte vähem, kuid märkimisväärne oli, et need ligi vereand miljardit ründepäringu tehti vaid 39 minuti jooksul. See tähendab, et väiksemale ründepärinrete koguarvule vaatamata oli mai kampaania aprilli omast ligi kaks korda intensiivsem.

Suurtele ründemahtudele ja intensiivsusele vaatamata suutis RIA DDoS-kaitse suurema osa ründepäringetest blokeerida ja märgatavat möju rünnakutel polnud. ●



LUNAVARA: uued ründed, vanad vead

Lunavararünnete arv ja nende põhjustatud kahju on maailmas kasvutrendis.

Eestis on olukord pigem stabiilne, kuid tõsiseid probleeme põhjustanud ründeid nägime ka siin.

Selles, et mõne ettevõtte või asutuse veebi-leht koriks kätesaamatuks muutub, pole midagi erakordset. Sageli on põhjuseks mõni seadustusviga, aegunud sertifikaat või seadmerike, aga ühe meid teavitanud ettevõtte jaoks oli see esimene märk millestki tösisemast. Neid oli tabanud lunavararünnak.

KESINE TURVAPOLIITIKA

Töenäoliselt sai see juhtum alguse andmelekkes avalikuks tulnud firmajuhi paroolist, kuid see kasvas kogu ettevõtet hõlmavaks intsidentiks.

Rünnet soodustas mitu asjaolu. Juhi koduvõrk oli osa ettevõtte sisevõrgust ning tema isikliku arvuti töölauale oli salvestatud RDP-ühendus

ettevõtte serveritesse. Mugav, aga ohtlik.

Samuti sai saatuslikuks paroolipoliitika, sest töö- ja erakontode salasõnad olid ristkasutuses. Küllap olid ründajad tänulikud ka selle eest, et kõikides serverites kasutati sama parooli.

Lisaks firmajuhi isiklikule võrgusalvestile krüpteeriti ettevõtte serverite logid ja tagavarakoopiad, kuna need asusid samas võrgus. Õnneks sai ettevõte tegevust jätkata, sest ärikiitlisi protsesse rünnak ei halvanud, kuid süsteemi taastamine võttis nädalaid.

UUENDAMATA TARKVARA

Teise ettevõtte puhul, mis möödunud aastal lunavara ohvriks langes, tuvastasime põhjusena turvanõrkuse serveri tarkvaras. See haavatavus võimaldas käivitada pahatahtliku koodi, mille tulemuse na loodi uus kasutaja, et serveriga ühenduses olla. Kuigi vahepeal uuendati tarkvara turvalisele versioonile ja pahatahtlikud skriptid kustutati, säilis sissetungijate ligipääs serverile. Hiljem müüsidi nad selle edasi. Uued ründajad said kaughaldustarkvara abil süsteemi sisse, krüpteerisid andmed ning panid oma nõude ohvri töölauale.

Tänu varukoopiale oli võimalik server taastada ning ettevõtte tegevus jätkus.



KOLM KURJA JUURT

Kuigi iga juhtum on erinev, on lunavara-rünnakute vahel ka ühiseid jooni. Ründed ja hilisemad raskused süsteemide taastamisel on sageli põhjustatud järgmistest asiaoludest.

- ➥ **Kaugtöölaua rakendused** (RDP) on avalike IP-aadresside kaudu kogu internetile leitavad ja ligipääsetavad.
- ➥ **Nõrk paroolipoliitika.** Sageli kasutatakse paroole nagu Admin, Password123 ja qwerty, mille saab jõuründe teel kergelt ära arvata.
- ➥ **Varukoopiaid pole või asuvad need samas võrgus.** Kui ründaja krüpteerib ettevõtte serveri, saab ta sama teha varukoopiatega.

kokku paroolid ja kasutajaandmed, et päaseda ligi ka teistele süsteemidele.

Viimaks krüpteeriti serveris olnud andmed. Kuna kriitilised protsessid polnud mõjutatud, sai ettevõtte töö siiski jätkuda.

RÜNNAK HALVAS PEREARSTIKESKUSE TÖÖS

Aasta lõpus teavitas perearstikeskus, et on lange-nud lunavarariindegäa ohvriks. Selle käigus krüpteeriti varukoopiad ning andmed kahes serveris. Värskeim varukoopia, millele ründajad ligi ei päasenuud, oli 2021. aastast. Kuna ründajad suutsid lukku panna patsientide andmed, terviselood ja vastuvõtuajad, halvas see perearstikeskuse tegevuse.

Kuigi hüpotees, kuidas rünnak võimalikuks sai, on mitu, on tõenäolisim versioon endise töötaja konto, mida tema lahkumise järel ei suletud. Ründaja sai nii laialdaselt tegutseda, sest süsteemi kõikidel kasutajatel olid administraatori õigused. Spetsialistid suutsid taastada vaid osa krüpteeritud andmetest.

KUIDAS END KAITSTA?

Selleks, et vältida runde ohvriks sattumist ja minimeerida kahjustusi, kasuta unikaalseid salasõnu, võimalusel juuruta mitmeastmeline autentimine. Peida kaugtöölaua rakenduse ühendused avalikust võrgust ja isiklikest seadmetest. Vaata üle andmete varundamine. Uuenda regulaarselt seadmete tarkvara, et vältida turvanõrkuste ärakasutamist. Tutvu ettevõtte lühijuhendiga lehel itvaatlik.ee.

TEISTKORDNE JUHTUM

Ühel Eesti logistikaettevõttel oli esmane kokku-puude lunavarariindegäa paar aastat tagasi. Öeldakse, et välk kaks korda samasse kohta ei lõi, aga 2025. aastal sattusid nad taas samalaadse rünnaku ohvriks.

Ka ründe viis vastas tuttavale mustrile. Sisestung sai võimalikuks, sest kaugtöölaua rakendus (RDP) oli avalikult internetist leitav. Samuti oli kasutusel nõrk parool, mis murti jõuründera lahiti. Seejärel kasutasid ründajad tööriista, mis kogus



Pettustelaviini kahju: 29 MILJONIT

Murenemise märke oli näha juba varem, kuid 2025. aastal varises kokku keelebarjääär, mis meid pettuste eest veidigi kaitses.

Tulemus: Eesti inimesed kaotasid petturitele 29 miljonit eurot ehk kolm korda rohkem kui aasta varem.

Pettused olid pea terve aasta jooksul avalikkuse pilgu ees. Ajakirjandus avaldas sel teemal sadu lugusid, RIA, politsei- ja piirivalveamet, pangad ja mitmed teised organisatsioonid tegid kampaaniaid ja teavitustööd, kuidas ptureid ära tunda ja end nende eest kaitsta. Aga sellest hoolimata lahkusid petturid suurema saagiga kui kunagi varem. Ja meie registreeritud intsidentidest moodustavad suurima osa just pettused. Köige enam langevad pettuste ohvriks eraisikud, kuid kui vaadata üksikuid kahju summasid, siis suurima rahalise kahju tekitavad erinevad äripettused.

AINA USUTAVAMAD

Petturid muutuvad aina usutavamaks ja osavamaks. Kui varem võis pettuse ära tunda kas halva eesti keele, grammatikavigade või vene keele kasutamise järgi, siis neile abilistele enam toetuda ei saa. Praegu näeme pottuseid, mis tehakse korrektses eesti keeles ja heausksel ohvril on aina ras kem pottust ära tunda. Köige parem kaitse on olla teadlik hetkel levivatest petuskeemidest.

Nii nagu varasematel aastatel, levisid taas massiliselt erinevad postiteenuste pakkujate nimel saadetud öngitsussõnumid. Nende kõrval tegid aga hüppelise kasvu telefonipettused, mille ohvriks langesid nii eraisikud kui ka ettevõtete esindajad. Ettevõtete suunas tehtud pettused lõppevad sageli sadade tuhandete eurode kaotusega, mille tagasi saamise töönäosus on väike.

TELEFONIPETTUSED TEGID SUURE KASVU

Iga päev kaotavad eestimaalased telefonipettuste tõttu kümneid tuhandeid eurosid. Levib skeem, kus inimesele tehakse mitu järvistikust kõnet. Esimeses kiirustatakse teda tegutsema, näiteks pakutakse hüvitise tagastamist. Teises kõnes väidetakse, et eelmises kõnes tegutsesid kelmid ja nende tegevuse peatamiseks on vaja kohe panga siselogida, kinnitades seda Smart-ID või mobiil-ID PIN-koodide sisestamisega.

Sagedased on ka petukõned, milles väidetakse, et elektrimõõdik või -kilp on vaja uue vastu välja vahetada. Sellise skeemi ohvriks langes ka üks

mittetulundusühing. Esimene pettur, kes ohvrile helistas, esitles end elektrikilbi paigaldajana. Kuna köne vastu võtnud inimene ootaski oma ehitisele kilbi paigaldamist, leppis ta aja kokku. Köne lõpuks palus pettur kinnitada toiming Smart-ID abil ja ohver sisestaski PIN1. Sellele järgnesid kõned petturi telt, kes esitlesid end politseiniku ja pangatöötajana ning väitsid, et ohvri pangakontole on ebaseaduslikult sisenedut ja tehtud seal mitmeid toiminguid. Nende tagasipöörämiseks paluti korduvalt sisestada PIN1- ja PIN2-koode. Selle tagajärjel kandis ohver petturi tele endaga seotud MTÜ kontolt üle 120 000 euro.

Sarnast petuskeemi prooviti ka Äripäeva Lät projektjuhi peal. Esimeses könes paluti elektriarvesti vahetus kinnitada mobiil-ID koodi sisestamisega. Sellele järgnes köne näiliselt pangatöötajalt, kes väitis, et keegi võõras olevat proovinud pangakontole ligipääsu saada. Kolmas köne tuli libapolitseinikult WhatsAppi vahendusel, mida kasutati väidetavalts seetõttu, et seda on raskem pealt kuulata. Mingil hetkel hakkasid ohvrile kõned kaatlased tunduma ja ta helistas oma kliendihaldurile pangas ning sai teada, et tegemist oli pettusega.

MILJONIPETTUS, MIS VIIS KOHTUVAIDLUSENI

Augustis sai teatavaks, et masinatööstusettevõte Hekotek kaotas petturi tele üle miljoni euro. Sündmuste ahel algas ettevõtte finantsjuhile tehtud telefonikõnega, kus petturiid tutvustasid end tervisekassa töötajana. Selle käigus saadud info abil õnnestus petturiel luua finantsjuhi nimele uus Smart-ID konto. Järgmistes kõnedes etendati pangatöötaja ja politseiniku rolli ning selle tulemuse na pääsesid petturiid finantsjuhi arvutisse, kasutades selleks kaughaldusrakendust AnyDesk. Seal avasid nad pangarakenduse ja allkirjastasid maksed enda loodud Smart-ID kontoga. Kahe tunni jooksul tehti ettevõtte kontolt 52 väljamakset, mille kogusumma ulatus 1,6 miljoni eurooni. Osa sellest õnnestus tagasi saada, kuid kahjusumma ületab siiski miljoni piiri. Nüüd käib ettevõte oma endise finantsjuhiga kohut, kust oodatakse otsust, kes ja mil määral vastutab tekkinud kahju eest.

TEGEVJUHI PETUSKEEMID JA ARVEPETTUSED

Tegevjuhi petuskeem seisneb selles, et näiliselt saadetakse tegevjuhi nime alt kiri ettevõtte töötä-

KUIDAS TELEFONI- PETTUST ÄRA TUNDA JA SELLEST HOIDUDA?

- Petukõnedes on enamlevinud skeemid järgmised:
 - hoiatatakse kahtlaste tehingute eest pangakontol;
 - võetakse ühdust kasutamata hüvitise ajus;
 - küsitakse raha lähedasega juhtunud õnnnetuse lahendamiseks, näiteks haiglaarve tasumiseks;
 - pakutakse head investeerimisvõimalust.
- Kui sulle tehakse telefonikõne tundmatult välismaa suunakoodiga telefoninumbrit, siis ära vasta sellele, kui sa just ei oota sellist kõne.
- Ära jaga telefoni teel isiklikku infot ega sisesta seda veebilehtedele, kuhu könes suunatakse.
- Ära jaga ega sisesta oma PIN-koodi. Ükski pank ega riigiasutus ei küsi selliseid andmeid.
- Ära lase end meelitada alternatiivsesse suhtluskanalisesse, näiteks WhatsAppi.
- Kui palutakse seadmesse paigaldada mõni tarkvara (näiteks AnyDesk), siis katkestata kõne ja ära paigaldada tarkvara.
- Kui röhutakse kiirele tegutsemisele või hirmutatakse, siis võta aega ja aruta mõne usaldusväärse inimesega kõne sisu läbi.

jale (sageli finantsjuhile või raamatupidajale) palvega teha kiire ülekanne, mille tegelikuks kasu saajaks on pettur. Arvepettus aga on pettuseliik, mille puhul saadetakse organisatsioonile tema koostööpartneri nimel võltsarve.

Augustis õnnestus ühe ettevõtte töötaja meelitada kinkekaarti ostma. Pettur saatis kirja tegevjuhi nimel ja suunas edasise suhluse WhatsAppi. Seal jäeti töötajale mulje, et juht palub osta kinkekaarte. Töötaja tegi seda ja langes pettuse ohvriks, mille kogukulu oli umbes 550 eurot.

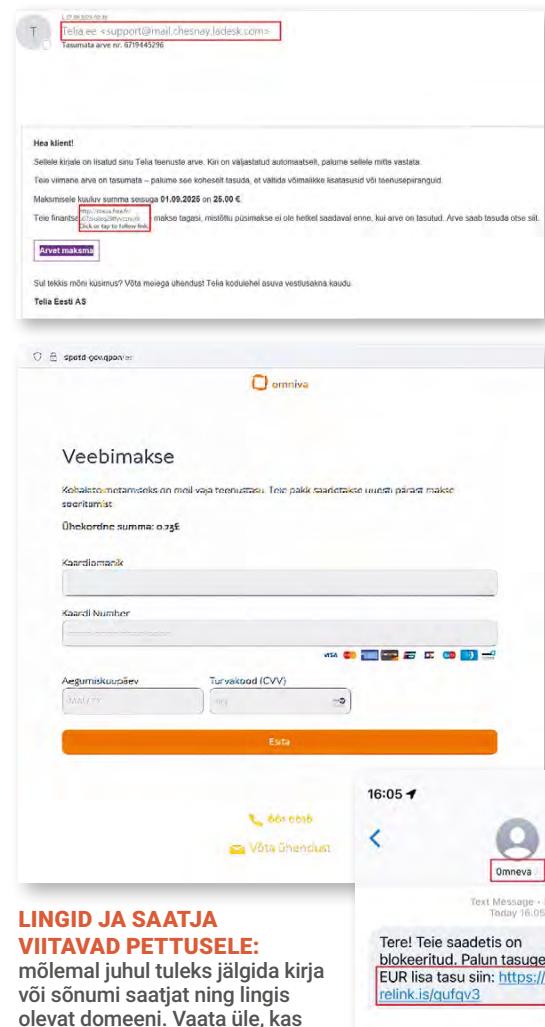
Novembris viisid petised läbi ka eduka arvepettuse. Ettevõte sai oma pikaaegselt tarnijalt e-kirja arvega, milles väideti, et pangakonto on muutu-

nud. Kuna ka varasemalt oli toimunud pangaandmete muudatusi, ei tekinud arve õigsuses kahtlust. Ettevõte tasus arve, mille suurusjärk oli 50 000 eurot. Hiljem selgus, et raha oli kantud petiste kontole ja seda enam tagasi ei saadud.

Novembris tuli avalikuks 2022. aastal läbivitud tegevjuhi petuskeem. Skeem õnnestus läbi viia mittetulundüsühingus Eesti Pärimusmuusika Keskus, mis organiseerib populaarset Viljandi folgfestivali. Raamatupidajale saadeti näiliselt tegevjuhi poolt kiri, milles uuriti pangakonto saldo kohta ja paluti teha ülekanne summas 28 000 eurot. Raamatupidaja andis nõusoleku ja tegi ülekanne. Järgmisel päeval saabus uus kiri, kus palutti teha järgmine ülekanne summas 19 500 eurot. Veel mõni päev hiljem tegi raamatupidaja kolmandagi makse summas 25 350 eurot. Kõik maksed läksid välismaa pankadesse ja kirja saatjaks tundus olevat keskuse juht. Kui pettus avastati, õnnestus üks makse tühistada ja kogukahjuks jäi üle 53 000 eurot.

KUIDAS VÄLTIDA ÄRIPETTUSTE OHVRIKS LANGEMIST?

- ➥ Kehesta oma organisatsioonis reeglid ja protseduurid maksete töötlemiseks. Näiteks võiks olla kehtestatud kahe silmapaari reegel, et iga tasumist ootav arve saaks kinnituse kahelt töötajalt.
- ➥ Koolita töötajaid erinevate küberohtude teemal. Näiteks tuleks regulaarselt meeلد teletada, kuidas õngitsuskirju ära tunda. Üks võimalus selleks on RIA Kübertest.
- ➥ Tee oma organisatsiooni e-posti aadresside võltsimine kurjategijatele võimalikult keeruliseks (seadista SPF, DKIM ja DMARC).
- ➥ Kaitse kodulehel kuvatavoid e-posti aadresse spämmirobotite eest või võimalusel ära avalda kõigi töötajate e-posti aadresse.
- ➥ Kahtluse korral helista tarnijale või koostööpartnerile ja küsi üle, kas tegemist on õige kirjaga. Helistada tuleks teadaolevale kontaktile, mitte võimalikus petukirjas olevale telefoninumbriile.



LINGID JA SAATJA

VIITAVAD PETTUSELE:

mõlemal juhul tuleks jälgida kirja või sõnumi saatjat ning lingis olevat domeeni. Vaata üle, kas see kuulub kirjas nimetatud teenusepakkujale. Lisaks tuletaame meeلد, et ükski asutus (pank, politsei, postifirma) ei küsi e-posti teel teie pangakaardi andmeid. See on kindel ohumärk, et tegemist on öngitsusega.

JÄTKUSID ERINEVAD ÖNGITSUSED

2025. aastal levisid nii Telia kui ka Elisa nimel saadetud petukirjad, milles väideti, et kliendil on kas tasumata arve või tehtud ülemakse. Mõlemal juhul oli kirjaga kaasas link, milles suunati kasutaja sisestama enda pangakaardi andmeid. Kirjad olid saadetud kahtlastelt e-posti aadressidelt, mis ei kuulu nimetatud teenusepakkujatele. Kumbki ettevõte ei saada niisuguseid kirju ega kõsi e-posti teel pangakaardi ega ka muid andmeid. Kogu arveldustega seotud infot saab näha ettevõtetise teenindusportaalil.

Kadunud pole ka varasematest aastatest tuttavad postiteenusepakkujate nimel tehtud õngitsused. Need levivad nii e-posti kui ka sõnumite teel. Kasutajale jäetakse mulje, et teda on ootamas pakk ja selle kättesaamiseks tuleb kas tasuda tollimaks või mõnel muul ettekäändel sisestada enda pangakaardi andmed. Selliste õngitsuste eesmärk on saada teada ohvri kaardiandmed ja nende abil võtta kontolt kõik, mis võimalik. Enamasti jäetakse mulje, et tuleb tasuda vaid paar eurot, kuid tegelik kahju on nii suur, kui kontojääk või limiit lubavad.

INVESTEERIMISPETTUSED: KAOTUS GARANTEERITUD

2025. aastal kaotasid Eesti inimesed erinevate investeeringispettustega läbi ligi 6 miljonit eurot. Ohvrile pakutakse pealtnäha väga head raha paitutamise võimalust, lubatakse madala riskiga või lausa riskivaba investeeringut ning garanteeritud ja kõrget tootlust.

***Kelmide juhendamisel
tegi kannatanu enda
ettevõtte kontodelt petu-
platvormile ülekandeid
kogusummas 504 400 eurot.***

Investeeringisvõimalusena võidakse pakkuda näiteks krüptoraha, aktsiaid või võlakirju, mida kurjategija esitleb kui uut toodet, tehnoloogiat või ärvõimalust. Ohvrile lähenetakse telefoni, e-kirja või sotsiaalmeedia vahendusel, kus suunatakse kasutaja mõnele pealtnäha legitiimsele veebilehele. Tänapäeval on petulehed väga tõetruud ja kasutajal ei teki kahtlust oma andmete sisestamisel.

Kõik ei ole kuld, mis hiilgab. Kahjuks kehtib siin tõdemus, et kui miski tundub liiga hea, et tõsi olla, on suure töenäosusega tegemist pettusega.

Petturid lähevad järjest nutikamaks. Näiteks levis möödunud aastal video Alar Karisest, kes kutsus inimesi üles investeeringima uuvel riiklikul

NÄITEID HALVASTI LÖPPENUD INVESTEERINGUTEST

- ➡ Internetis alanud suhtluse käigus meelitati 41-aastane naine tegema sissemakseid krüptoraha investeeringisplatvormile ning võtma selleks täiendavalt ka laenu. Kannatanu ei saanud platvormilt raha välja võtta ja temalt nõuti aina uute maksete teostamist. Tekitatud kahju on 9936 eurot.
- ➡ Suvel leidis 68-aastane naine internetist reklami investeeringisvõimaluse kohta ja jättis lehele oma kontaktid. Peatselt võttis temaga ühendust end investeeringismaaklerina tutvustanud inimene, kelle juhendamisel asus naine ülekandeid tegema. Tegemist oli libaplatvormiga, kust raha enam kätte ei saa ning väidetav finantsnõustaja pole enam tabatav. Kahju on ligi 15 000 eurot.
- ➡ 39-aastane mees nägi Facebookis investeeringisreklaami ja liitus WhatsAppis grupiga, kus selgitati platvormi toimimist ja loodi talle konto. Mees asus end maaklerina tutvustanud inimese vahendusel tegema ülekandeid ja andis oma arvutile kaugjuurdepääsu AnyDesk programmiga. Mees võttis ka mitu laenu, et rohkem investeerida. Tegemist oli libaplatvormiga ja raha ta seal enamat kätte ei saanud. Kahju on üle 28 000 euro.
- ➡ 57-aastase mehega võttis ühendust end investeeringisnõustajana esitlenud inimene. Nõustaja juhendamisel registreeris kannatanu end krüptoraha kauplemisplatvormil ning tegi sinna sissemakse 1300 eurot. Kelmide juhendamisel tegi kannatanu kuue kuu välitel enda ettevõtte kontodelt petuplatvormile ülekandeid kogusummas 504 400 eurot.



platvormil. Videos lubati kindlat sissetulekut 870 eurot nädalas. Tegemist oli loomulikult pettusega ja video näol tegemist süva-võltsinguga (*deep fake*). Petturid proovisid luua usaldusvärsust, kasutades ära Eesti presidendi autoriteeti. ●

Järjekordne REKORDARV turvanõrkusi

2025. aastal registreeriti üle 48 000 turvanõrkuse, mida on viiendiku võrra rohkem kui 2024. aastal. Tõsiseid haavatavusi jagus võrguseadmetesse, tööstusautomaatikasse, operatsioonisüsteemidesse ja muudesse tarkvaradesse.

Mullune aasta paistab silma paljude tõsistele nullpäeva turvanõrkustega, kus ründajad kompromiteerisid süsteeme juba enne turvanõrkuse avaldamist ja suutsid hoida ligipääse ka pärast haava-

tavuste paikamist. Võimalusel kasutavad nad ära ka turvanõrkusi, mis on siiani paikamata. Aina rohkem ja konkreetsemalt räägitakse riikliku taustaga grupeeritest, kes tegelevad kriitilise taristu süsteemides turvanõrkuste otsimise ja nende ärakasutamisega.

KUIDAS KAITSTA END TURVANÕRKUSTE ÄRAKASUTAMISE VASTU?

- ➥ Hoia köigi süsteemide operatsioonisüsteem või püsivara, rakendused jm tarkvara ajakohasena.
- ➥ Vaheta välja lõppenud tööeaga seadmed ja tarkvara, millele tootja enam turvauuendusi ei paku.
- ➥ Kaitse oma vörku ja administreerimisiideseid. Kasuta VPNi ja luba ligipääs seadmetele, eriti süsteemide haldusliidestele, vaid kindlatelt IP-aadressidelt.
- ➥ Seadista ja jälgvi oma süsteemi logisid ning paigalda monitooringurakendused, et märkaksid anomaliaid ja saaksid ründe korral kiirelt reageerida.

AASTA TURVANÕRKUS: REACT2SHELL

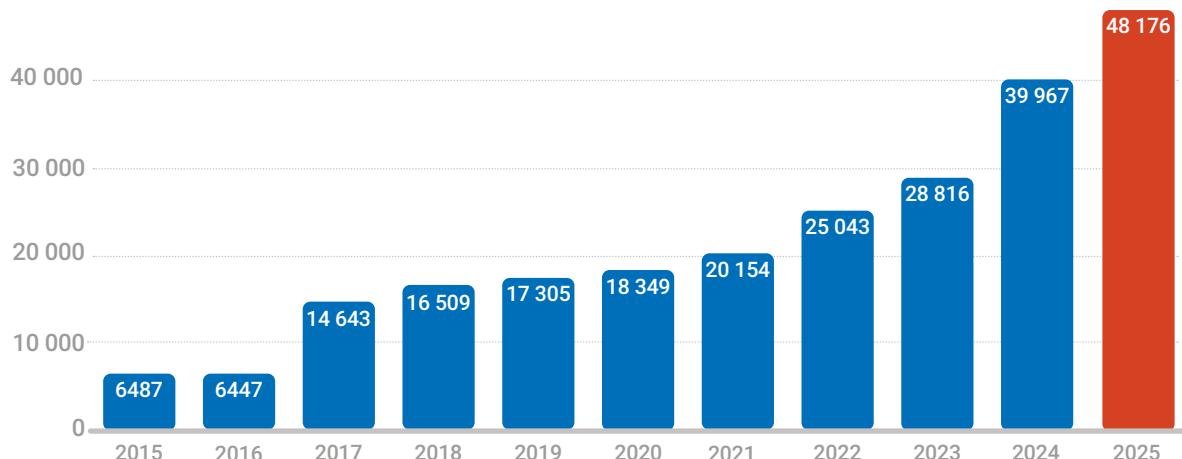
2025. aastal avastatud turvanõrkustest on kõige tõsisem ja laiema mõjuga detsembri alguses avatud haavatavus, mis sai hüüdnime React2Shell (CVE-2025-55182).

See on koodi kaugkäitust võimaldav turvanõrkus React Server Componentsi tarkvaras, mis võimaldab ründajal lihtsa vaevaga saada kontroll haavatavas serveris. Turvanõrkuse mõju on erakordsest suur, kuna React on laialt kasutuses veebiserverites, sh veebiteenustes, admin-paneelides ja rakendusliidestes ehk APIdes. Mitu rühmitust võtsid React2Shelli turvanõrkusega serverid sihikule vaid mõni tund pärast selle avalikustamist.

EESTIS OLID TULE ALL VÕRGUSEADMED

Eelmisel aastal avastati nullpäeva turvanõrkuseid mitmetes võrguseadmetes ja rünnati ka vanu paikamata haavatavusi. Soovimatut põnevust ja närikorral kihvitati.

REGISTREERITUD TURVANÕRKUSTE ARV 2015–2025



ALLIKAS: NVD.NIST.GOV/VULN

vipinget said nii FortiGate'i, Cisco kui ka Ivanti seadmete kasutajad.

Aasta algus töi uuvide, et kahe riigiasutuse Ivanti Connect Secure'i tarkvara kasutavad VPN-seadmed on kompromiteeritud. Töenäoliselt kasutasid ründajad ära nullpäeva turvanõrkuseid (CVE-2025-0282 ja CVE-2025-0283) ning kompromiteerisid seadmed veel enne turvauuenduste avaldamist. Aasta lõppes tödemusega, et Eestis on pihta saanud Cisco võrguseadmed, mis muutusid haavatavaks järjekordse nullpäeva turvanõrkuse (CVE-2025-20393) töltu.

Kevadel jagati ühe Eesti raamatukogu süsteemide kaudu pahvara. Intsidendi analüüs käigus selgus, et ründajad said süsteemi sisesse, kuna nii meiliserveri kui ka veebi sisuhaldustarkvara turvanõrkused olid paikamata ja toodete eluiga ammu lõppenud.

Kompromiteeriti mitmed WordPressi kasutavad veebilehed. Näiteks Laagri koolis algas õppa-aasta kooli kodulehe kompromiteerimisega: südaööl käivitati WordPressi aegunud tarkvara kaudu skript, mis keelas ligipääsu lehele. Avalehel kuvati sisselogimise aken, mis küsis kasutajanime ja parooli.

LUNAVARARÜNNAK PAIKAMATA TURVANÕRKUSE TÖTTU

Sügisel leidis ühe Eesti ettevõtte töötaja serveri krüpteerituna, ekraanil lunarahanõue. Analüüs

LOODI EUROOPA LIIDU TURVANÕRKUSTE KATALOOG

25. mail avaldati Euroopa Liidu turvanõrkuste kataloog European Union Vulnerability Database ehk EUVD, mida haldab Euroopa Liidu küberturvalisuse amet (ENISA). EUVD on eesmärk on koondada ELi vaatest oluline info turvanõrkuste, nende mõju, kuritarvitamiste ja leeendusmeetmete kohta.

2025. aastal sattus küsimärgi alla CVE (Common Vulnerabilities and Exposures) süsteemi turvanõrkuste andmebaaside (cve.org) ja USA riikliku standardi- ja tehnikaainstituudi (NIST) hallatava NVD (National Vulnerability Database) rahastus ning järgipidevus. Aasta lõpu seisuga CVE süsteemi turvanõrkuste andmebaasid toimivad, kuid vajadusel pakub EUVD neile alternatiivi.

tulemusena selgus, et kurjategijad olid saanud serverile ligipääsu, kasutades ära turvanõrkust, mis oli parandatud augustis 2024. Paraku jäi ettevõttel seda nõrkust parandav turvauuendus öigel ajal paigaldamata ning kevadel 2025 said ründajad ligipääsu süsteemile ja sügisel paigaldasid lunavara. ●

2025.

aasta globaalses küberruumis

Lunavararünded räsisid tuntud brändide mainet, Põhja-Korea libatöötajad püüdsid imbuda rahvusvahelistesse tehnoloogiaettevõtetesse, ulatuslikud teenusekatkestused töid esile kriitilisi sõltuvusi.

Lunavararünne on üks rängima mõjuga küberründeid. Sellega saab seisata suuri ettevõtteid ja haiglaid, sulgeda torujuhtmeid ning tekitada miljardites eurodes mõõdetavat kahju.

2025. aastal jätkus globaalne võitlus lunavararünnete mõju vähendamiseks ja nende taga olevate kuritegelike võrgustike paljastamiseks. Lunavararünnete arv maailmas on tõusuosal, aga kasumlikkus ründe kohta languses.

KOHUSTUS TEAVITADA LUNARAHHA MAKSMISEST

2025. aastal kehtestas Austraalia esimese riigina maailmas teatud sektoritele kohustuse raporteerida lunavararünnete puhul oma otsusest lunaraha maksta. Teavitamiskohustuse eesmärk on anda riigile parem ülevaade lunavararünnete ulatusest ja mõjust, ent küllap on selle taga ka lootus, et teavitamiskohustusega ettevõte pigem loobub lunaraha maksmisest.

Austraalia lähenemine on seni erandlik, kuid paljud riigid järgivad kirjutamata reeglit mitte maksta lunaraha avalikku sektorit tabanud rün-

nete puhul. Mitme küberturbeettevõtte raportitest nähtub, et ka eraettevõtted on järjest vähem altid kurjategijatega läbi rääkima ja lunaraha maksma. See näitab suuremat küpsust küberkriisidega toime tulemisel.

Lunavararünnete arv maailmas on aga tõusuosal. Kui sageli jääb nende mõju laiemale avalikkusele märkamatuks, siis mõõdunud septembris põhjustas lunavararünnak Collins Aerospace'i pardale registreerimise tarkvara vastu kaose mitmes suures Euroopa lennujaamas. Lennufirmad pidid hakkama reisijaid ja pagasit käsitsi registreerima, mis põhjustas pikki järjekordi ja jätkulendudest maha jäämist, kümneid lende tuli ka tühistada.

Septembris häiris lunavararünnak maailma üht suurimat joogitootjat Asahi, peakorteriga Jaapanis, mis toodab samanimelist õlut. Ründe kirjutas enda nimele Qilini lunavararühmitus, mis oli mõni kuu varem rünnanud ka Lõuna-Korea suurkontserni SK Group.

Ühendkuningriigis langesid mõõdunud aastal ohvriks mitmed mainekad kaupluseketid: Marks & Spencer, Harrods ja Co-op. Neist kandis suuri-



mat majanduslikku kahju, ligikaudu 300 miljonit naela, Marks & Spencer, mille veebimüük katkes mitmeks nädalaks. Prantsusmaal tabasid küber-ründed luksusbrände Cartier ja Dior.

Suure majandusliku ja maine-hoobi sai Ühendkuningriigi autotootja Jaguar Land Rover, mis oli sunnitud küberründe töttu peatama viieks nädalaks tootmisse paljudes tehastes kodu- ja välismaaling sattus raskustesse nii valmismasinate kui ka varuosade tarnimisel. Lisaks varastasid kurjategijad ettevõtete süsteemidest tundlikke andmeid.

Ründe omistas endale rühmitus Scattered Lapsus\$ Hunters, ent ettevõte ise ei ole selle toimepanijaid ega üksikasju avaldanud. Jaguar Land Roveri küberründe kahju Ühendkuningriigi majandusele hinnatakse suurusjärgus 1,9 miljardit naela, mis teeb sellest riigi ajaloo kõige kulukama küberründe.

JÄTKUSID TARNEAHELARÜNDDE

2025. aastal püsis trend kompromiteerida tarneahelaid ja olulisi teenusepakkujaid, mis laiendas oluliselt rünnete piiriülest mõju. Augustis õnnestus kurjategijatel rünnata USAs ja mujal laialt kasuta-

tavat kliendihi-dustarkvara Salesforce ja varastada sadade seda tarkvara kasutavate ettevõtete ja organisatsioonide tundlikke andmeid. Ohvrite hulgas on mitu rahvusvahelist suurettevõtet nagu Google, Toyota, FedEx, Qantas, Allianz Life jt.

Selliste rünnete puhul on tavoline, et kurjategijad kahmavad kokku nii palju andmeid kui võimalik ja asuvad siis nendega seotud ettevõtetelt üks-haaval lunaraha välja pressima. Rünne ei toimunud mitte Salesforce'i põhiplatvormi kaudu, vaid ära kasutati turvanörkust sellega integreeritud turundustöriistas Salesloft Drift. Ründajad otsivad pidevalt nörku lülisid suuremates süsteemides, mille haldamine, kaitsmine ja vastastikuste sõltuvuste mõistmine muutub ettevõtete ja asutuste jaoks järjest keerukamaks.

TEENUSEKATKESTUSED, MILLE MÖJU TUNDI ÜLE MAILMA

Selleks, et vallandada sadade organisatsioonide ja ettevõtete tööd halvav dominoefekt, pole alati ründajaid tarviski. 20. oktoobril olid üle tuhande ettevõtte digiteenused mitmel pool maailmas häiritud. See sai alguse Amazoni pilveteenuse →

(Amazon Web Services ehk AWS) Põhja-Virginias asuvast andmekeskusest ning intsidendi analüüsist selgub, et juurpõjhuseks oli tõrge nimeserverite haldussüsteemis.

Katkestus mõjutas kuni 14 tunni jooksul nii panku, lennuettevõtteid, meebleahutusplatvorme kui ka logistikaettevõtteid ja nende kaudu miljoneid inimesi. Katkestuse põhjustatud kahju hin-natakse miljarditesse dollaritesse. Ka mõned Eestis kasutatavad teenused, näiteks Signali sõnumirakendus, olid lühiajaliselt häiritud.

Kõigest kuu aega hiljem, 18. novembril, põhjustas mitmel pool maailmas frustratsiooni järgmine suure mõjuga teenusekatkestus. Tehnilise tõrke tõttu olid häiritud globaalse tehnoloogiaettevõtte Cloudflare võrguteenused ning see andis tunda ka Eestis. Paar tundi olid kätesamatud näiteks uudisteportalid Delfi, Eesti Ekspress ja Õhtuleht, samuti ei saanud inimesed mõnda aega Lux-Expressi ja Elroni veebikeskkonnast pileteid osta. Cloudflare'i blogipostitusest selgub, et tõrke põhjustas andmebaasi rutiinse uuendamise käigus tehtud apsakas, millega alguse saanud tehniline jada mõjutas suurt osa internetist.

Kolm nädalat hiljem, 5. detsembril, tabas ettevõtte teenuseid veel teinegi, seekord paarikümne-minutiline katkestus, mille põhjustas ettevõtte tehtud muudatus tulemüüris. See oli vajalik kaitsmaks kliente äsja avastatud kriitilise turvanõrkuse ärakasutamise eest, ent osa Cloudflare'i taristust ei tulnud sellega toime.

Juhtub ka parimatel, ent küllap pole me harjunud teadvustama oma igapäevaelu sõltuvust kesksetest globaalsestest teenusepakkujatest.

RIIKLIKUD RÜHMITUSED JA HÄKTIVISTID

Oleme varasemates aastaraamatutes kirjutanud, et maailma küberruumi mõjutavad geopoliitilised pinged ning mitmed riigid kasutavad körgetase-melisi häkkerirühmitusi oma strateegiliste eesmärkide saavutamiseks. See tegevus toimub üldjuhul varjatult ning rühmituste edu sõltub sellest, kui hästi suudavad nad oma jälgi peita ja kauaks võrgus märkamatuks jäädva.

Kui rünne siiski avastatakse, võib riinnatud riik pidada paremaks see enda teada jäätta või siis vastupidi, riunde avalikult omistada, sageli koos sanktsioonide ja muude õiguslike tagajärgedega. Aasta 2025 tõi mitu sellist uudist.

MITU RIIKLICKU RÜNNET OMISTATI VENEMAALE

Jaanuar	EL lisas kolm Vene sõjaväeluure üksuse 29155 liiget oma sanktsioneeritute nimekirja, põjhuseks Eesti vastu tehtud küberünded aastast 2020. Avalik omistamine Eesti poolt leidis aset juba varem, 2024 septembris.
Aprill	Prantsusmaa omistas Vene sõjaväeluurega seotud rühmitusele APT28 mitmed varasemad küberünded, sealhulgas 2017. aastal presidendi-valimiste eel Emmanuel Macroni kampaaniameeskonna e-kirjade varastamine ja lekitamine, ning infiltrerimiskatsed 2024. aasta Pariisi olümpiamängude korraldusega seotud organisatsioonidesse.
Mai	Tšehhi valitsus avalikustas, et on tuvastanud Hiina riikliku taustaga rühmituse APT31 seose Tšehhi välisministeeriumi vastu toime pandud küberünnetega. Ründed algasid 2022. aastal, mil Tšehhi oli Euroopa Liidu eesistujariik.
Detsember	Ühendkuningriigi valitsus seadis sanktsioonid kogu GRU-le ja nimeliselt kaheksale küberluure ohvitserile. Põjhuseks 2018. aastal Salisburys korraldatud mürgitamiskatse Vene topelttagendi Sergei Skripali vastu ja sellele eelnenud küberünded Skripali tütre Julia telefonile luure eesmärgil.
Detsember	Ühendkuningriigi valitsus pani küberünnete korraldamise ja toetamise eest Ühendkuningriigis ja teistes riikides sanktsioonide alla kaks Hiina tehnoloogiaettevõtet, mida tuntakse nimedega i-Soon ja Integrity Tech.

Kui enamikule riiklikele ohustajatele on nende avalik seostamine küberünnetega pigem nende tööd segav, siis ideoloogiliselt motiveeritud häktivistid naudivad tähelepanu. Nende eesmärk on tekitada ühiskonnas segadust, hirmu ja pahameelt ning oma riinnete tegelikku mõju üritatakse meedias võimendada. 2025. aastal jätkusid häktivistide ummistusründed nii valitsusveebide kui ka teiste oluliste sektorite vastu mitmes riigis, ent nende mõju oli üldjuhul väike.

Saavutamaks suuremat efekti ja tähelepanu, katsetasid mõned häktivistide rühmitused tööstuslike juhtimisseadmete manipuleerimisega. Augustis omistas Norra julgeolekuteenistus Venemaa toe-tavatele häkkeritele riunde Edela-Norras asuva, veevoolu reguleeriva paisu juhtimissüsteemide vastu, märkimisväärset kahju önneks ei sündinud.

29. oktoobril avaldas Kanada küberjulgeolekukeskus ohuhinnangu, milles kirjeldas häktivistide õnnestunud katseid manipuleerida regionaalse vee-ettevõtte surveleadmetega ning muuta temperatuuri- ja niiskusetaset ühes Kanada viljakuivatis.

Detsembri keskel avalikustas Taani luureteenistus, et 2024. aasta lõpus toimunud küberründe kohaliku vee-ettevõtte vastu viis läbi Vene häktivistide rühmitus, ründe töttu oli 50 majapidamist mitu tundi ilma veeta.

Detsembris hoiatas ka USA küberturbeagentuur (CISA), et venemeelsed häktivistid korraldavad oportunistlikke ründeid kriitilise taristu vastu USAs ja teistes riikides. Ehkki sääraste rünnete sagenemine teeb muret, on häktivistide rünnevõime seni siiski lihtsakoline ning tööstusseadmetele rakendatavad küberurbemeetmed aitavad tõsisemad ründed ära hoida.

TEHISARU RÜNDAJATE TEENISTUSES

Nii riikliku taustaga rühmitused kui ka küberjategijad rakendavad järjest rohkem tehisaru tööriistu oma teevuse tõhustamiseks ja laiendamiseks, paljude ründetüüpide puhul on suurenened sotsiaalse manipulatsiooni osatähtsus.

Kiiresti arenevad tehisaru tööriistad loovad uusi võimalusi kõigile, ent suurendavad ettearvamatust.

Põhja-Korea IT-töötajate pettusena tuntud skeem laiendas möödunud aastal oma haaret: tehisaruga loodud video- ja pildimaterjali ning völtsidentiteete abil üritasid globaalsetes ettevõtetes tööd leida sajad teesklejad. Skeem toimis ka vastupidi: Põhja-Korea ohustajad matkisid näiteks LinkedInis tööandjaid ja pöördusid teiste riikide arendajate poole fiktiiivsete tööpakkumistega. Koos proovitöö ettepanekuga sokutati neile aga paavara.

Põhja-Korea petuskeemi eesmärgid on erinevad: varastada tehnoloogiaettevõtete siseinfot, nakatada neid paavaraga ja selle abil hiljem raha välja pressida või lääne ettevõttesse tööle saada ja teenida tulu oma riigi hüvanguks.

ÄRA TOIDA KURJATEGIJAT

Küberkuritegevuse ärimudel on juba aastaid liikunud järjest suurema spetsialiseerituse poole. Ründe erinevaid etappe, alates sihtmärkide valimisest ja ligipääsu hankimisest kuni paavara paigaldamise ja lunarahaga nöudmiseni, saab osta teenusena (nn Ransomware as a Service ehk RaaS mudel). Et kuritegeliku äri kasumlikkust murda, püüavad valitsused vähendada lunarahaga maksmise tõenäosust.

2025 juulis mõisteti USAs üheksaks aastaks vangi skeemile kaasa aidanud ameeriklanna, kes aitas põhjakorealastel völtsidentiteedi abil USA ettevõtetes tööle saada.

Google'i analüüs kohaselt olid Põhja-Korea IT-töötajate fookuses möödunud aastal ka mitmed Euroopa kaitsetööstusettevõtted ning üks inimene kasutas vähemalt 12 erinevat völtsidentiteeti. Selle skeemiga on kokku puutunud ka mõnede Eestis tegutsevate rahvusvaheliste ettevõtete värabajad.

Nagu IT-töötajate värbamisega veel vähe muresid oleks, pole nüüd välisstatud võimalus, et laitmatu CV ja videointervjuul hea mulje jätnud kandidaadile kaugtöö võimalust pakkudes toetad tahtmatult hoopis Põhja-Korea tuumaprogrammi.

KÜBERRUUM MUUTUS ETTEARVAMATUMAKS

Kokuvõtlikult võib öelda, et 2025. aastal nägime globaalses küberruumis mitme varem kanda kinitanud trendi jätkumist: laiaulatuslikud ründed teenusepakkujate kaudu, tavaelu segavad lunavararünded koos andmevarguste ja väljapressimistega ning sotsiaalse manipulatsiooni kasutamine küberünnete hõlbustamiseks.

Paarist tehnilisest apsakast alguse saanud teenusekatkestused häirisid inimesi ühtmoodi nii Valgamaal kui ka Californias ja tuletasid meelde, et katkestusi ei õnnestu vältida isegi tipptegijatel.

Geopoliitiliselt pinevas maailmas toimetavad jätkuvalt riikliku taustaga küberohustajad, ent nii sihtmärgiks olevad riigid kui ka ohte analüüsivad ettevõtted on hakanud nende teevust aktiivselt avalikkuse ette tooma. Kiiresti arenevad tehisaru tööriistad loovad uusi võimalusi kõigile, ent suurendavad ettearvamatust. ●

Sõda Ukraina küberruumis: KAITSE PIDAS

Vaatamata sellele, et Ukraina oli eelmisel aastal riikliku taustaga ohustajate poolt enim rünnatud riik Euroopas, oli 2025 esimene aasta pärast Venemaa täiemahulise sissetungi algust, kus Ukrainas ei toimunud ühtegi väga suure ühiskondliku mõjuga küberrünnakut.

2025. aastat Ukraina küberruumis iseloomustasid jätkuvad ründed avaliku sektori ja kriitilise taristu vastu, millega vastaspool püüdis edendada oma agressioonisõja eesmärke ja murda ukrainlaste võitlusvaimu.

Microsofti 2025 Digital Defense Reporti andmetel on Ukraina riikliku taustaga ohustajate poolt kõige enam rünnatud riik Euroopas. Kui võtta arvesse ka tavapärane küberkuritegevus, oli Ukraina sama raporti andmetel viies riik maailmas küberrünnete intensiivsuse poolest.

Enam levinud küberintsidentide poolest aasta märkimisväärseid muutusi ei toonud: need on õngitsused, pahavara jagamine erinevatel eesmärkidel ja pahavaraga nakatumine, kontode ja infosüsteemide kompromiteerimine.

HUVI SIGNALI SÖNUMITE VASTU

Ründed ja ründekatsed küberruumis on osa Ukraina igapäevaelust ning nagu mujalgi maailmas, püüavad ohustajad kasu lõigata nii arenevast tehnoloogiast kui inimeste harjumustest. Veebruaris kirjutasid Google'i ohuanalüütikud, et on märgata Vene riikliku taustaga ohustajate kasva-

vat aktiivsust Signali sõnumirakenduse suhtes – püütakse saada ligi huvipakkuvate inimeste kontodele ning koguda sealta väärthuslikku luureinfot.

Paljudel juhtudel kasutati kompromiteerimiseks Signali pakutavat võimalust ühendada sama kontoga mitu erinevat seadet. Seadmete ühendamiseks peab kasutaja skaneerima QR-koodi, kui aga ründajal önnestus edukalt ette sööta enda tehutud QR-kood, sünkroniseeriti kogu sõnumivahetus edaspidi ka tema kontrolli all olevasse seadmesse. QR-koodile usutava konteksti loomiseks võltsiti Signali enda juhiseid või imiteeriti Ukraina kaitseväärsust.

Jaanipäeva paiku avalikustas Ukraina CERT teisegi ründelaine, kus sõnumirakenduste kaudu saadeti valitsusametnikele pahavara sisaldavaid dokumente. Selgi korral oli tegemist täpselt sihitud ja hoolikalt loodud konteksti kasutavate rünnetega.

TEHISARU RÜNDAJATE ARSENALIS

2025. aastat küberruumis iseloomustav trend mitmel pool maailmas oli tehisoru võimaluste kasutamine rünnete tõhustamiseks ning see avaldus ka Ukrainas. Ekspertide hinnangul kasutati



tehisaru tööriistu nii õngitsuste usutavamaks muutmisel kui ka pahavara koodi kirjutamisel. Tehisarule omast käekirja on leitud näiteks Wrecksteeli nime kandva pahavara koodist, mida kasutati rünnetes Ukraina valitsusasutuste ja kriitilise taristu vastu. Wrecksteeli ülesanne oli leida võrgust tundlikke faile ja saata neid ründajate kontrolli all olevasse serverisse.

Ukrainas ei toimunud mullu ühtegi väga suure ühiskondliku mõjuga küberrünnakut.

KARASTUNUD KAITSE

Aastatepikkune kogemus erineva taustaga ründajate huviobiidis ning Vene rühmituste jaoks teatud mõttes testpolügooniks olemine on Ukraina küberkaitsjaid karastanud ning riigi küberkerksust järk-järgult suurendanud. Aasta 2025 oli esimene aasta pärast Venemaa täiemahulise sisse-

RÜNDDED KRIITILISE TARISTU VASTU

Jätkusid ründded kriitilise taristu vastu. Märtsis tabas küberrünnak Ukraina riiklikku raudtee-ettevõtet Ukrzaliznõtsja, mille töötu katkes mõneks päevaks piletite müük veebist ja rakendusest. Suuremates raudteejaamades tekkisid pikad kassajärjekorrad, aga rongide liikumine ja graafikud mõjutatud ei olnud. Ukrzaliznõtsja on maailma suurimaid reisijate- ja kaubaveo ettevõtteid, millega on sõja ajal oluline roll ka inimeste evakueerimisel.

tungi algust, kus Ukrainas ei toimunud ühtegi väga suure ühiskondliku mõjuga küberrünnakut.

Olukord küberruumis on aga muutlik ja kuna tõsisemad ründded nõuavad enamasti ka pikemat, hästi varjatud ettevalmistusperioodi, ei saa selle edu pealt kaugele ulatuvaid järelusi teha. Eestil, nagu ka teistel riikidel, on põhjust Ukraina küberruumis toimuvat jälgida, sest läänevastase hüüriidsõja osana võib sarnaseid ründeviise ja -mustreid kohata ka mujal. ●

SSSCIP JUHT: rahuleping ei too rahu küberruumi

Ukraina side- ja teabekaitseteenistuse (SSSCIP) juht brigaadikindral **OLEKSANDR POTI** räägib, mis juhtus möödunud aastal Ukraina küberruumis ja mida oleks teistel sellest õppida.

Kuidas iseloomustate Ukraina-vastaseid küberründeid aastal 2025? Mis on muutunud võrreldes eelmise aastaga?

2025. aastal tähdasime, et vastase fookus nihkus küberluure poole, eriti kaitseväge ja kaitsetööstuse sektoris. Küberdomeenis on esile kerkinud uued ohud ja Venemaa värbab aktiivselt täiendavaid jõude rünnakuteks, kompenseerides tihti kvaliteedi piudumist kvantiteediga. Ainuüksi eelmise aasta jooksul hakkasime jälgima ligikaudu 20 uut küberohtude klastrit.

Täiendav tegur selles kiires arengus on tehisintellekti tehnoloogiate levik. Kui 2024. aastal kasutati neid peamiselt öngitsussõnumite loomiseks, siis 2025. aastal nägime mitte ainult tehisaru kaasabil loodud pahvara näiteid, vaid ka pahvara, mis kasutab pahatahtlike tegevuste läbivimiseks sisemisi tehisintellekti algoritme.

Häituslike rünnete arv pole samuti vähene nud. Samas on need muutunud vähem märgata vaks, kuna suur osa neist önnestus kahjutuks teha varases staadiumis. Seetõttu kajastati neid avalikkuses vähem.

Kas nägite möödunud aastal uusi taktikaid riikliku taustaga ohustajate poolt või uusi rühmitusi?
Nagu öeldud, hakkasime eelmisel aastal jälgima

ligikaudu 20 uut ohustajate klastrit. Samas pole kuskile kadunud ja arenevad edasi ka juba teada tuntud rühmitused, sealhulgas need, kes on riiklike taustaga. Kaitsemeetmete areng sunnib ründajaid oma lähenemist muutma, mis omakorda viib paremate kaitsemeetmeteni. See on pidev vastastikuse kohandumise tsükkeli.

Häkkerite küberarsenali lisandub pidevalt uusi pahavarasid, sealhulgas selliseid, mis kasutavad arenenud tehnoloogiaid. Üks näide siinkohal on pahvara LAMEHUG, mida kasutab Vene sõjaväeluurega seotud rühmitus UAC-0001 (tundud kui APT28).

Tänasel päeval ei levi pahvara mitte ainult manusega öngitsusmeilide kaudu, vaid see on sageli keerukas, sotsiaalset manipuleerimist kasutav mitmepäevane operatsioon. Samas kasutavad ründajad ka erinevaid turvanörkusi alternatiivse ründevektorina.

Üldiselt oli aastale 2025 iseloomulik, et häkkerrid aktiivselt arendasid ja kohandasid oma taktikaid, tehnikaid ja protseduure.

Detsembris 2024 kogesid ukrainlased küberünnet, mis mõjutas paljusid riiklike andmebaase. Inimesed ei saanud mõned nädalad müüa autosid, registreerida digitaalselt abieli ega pöörduda



Ukraina side- ja teabekaitseteenistuse (SSSCIP) juht brigaadikindral Oleksandr Poti.

kaebustega kohti poole. Kas teil on mõni õpikoht sellest rüdest, mida sooviksite Eestiga jagada?

Ka kõige arenenumad küber turbe meetmed ei anna sajaprotsendilist turvalisust – mistahes organisatsiooni võidakse rünnata mistahes ajal. Seetõttu on kriitiliselt tähtis valmistuda halvimaks võimalikuks stsenaariumiks. Isoleeritult ja toodangu keskkonnast lahus hoitavad varukoopiad on kiire ja kontrollitud taaste jaoks üliolulised.

Aastal 2025 õnnestus ukrainlastel ära hoida mitu rünnet kriitilise taristu vastu. Kas on mõni edulugu, mida saaksite jagada?

Tulemuslike küber rünnete osakaalu vähenemine on juba iseenesest edu näitaja. Keskendume efektivsuselise, eriti praktilise ohuinfo jagamisele reaalajas või sellele võimalikult lähdedal.

Näiteks veebruaris 2025 tuvastasime küber ründe, mille viis läbi rühmitus Sandworm. Peamise infiltreerumismetodina kasutati pahaloomulise manusega e-kirju. Seda kampaaniat analüüsides tuvastasime sarnase tegevuse rohkem kui 20 Ukraina logistikaettevõtte ja 25 automaatkontrolli

süsteemide arendaja vastu Ukrainas, aga ka teistes Euroopa riikides. Tänu sellele saime kiiresti reageerida ja rünnete õnnestumise ära hoida.

Selline infovahetus koos kohalike spetsialistide kõrge kvalifikatsiooni, kogemuse ja arusaamisega, kuidas sellistele signaalidele reageerida, võimaldab ründeid õigel ajal tuvastada ja kahjutuks teha.

Olme tänulikud kõigile, kes küberohtudealasesse infovahetusse panustavad ja oma teadmisi jagavad. Me mitte ainult ei võta infot vastu, vaid jagame seda kogukonnale ka tagasi koos oma tähelepanekute ja kogemustega – *sharing is caring*.

Kui alanud aasta peaks tooma Ukrainale relvarahu, siis mis võiks olla selle mõju küber ruumis? Kas küber ründed teie riigi vastu jätkuksid või suunaks Venemaa tähelepanu mujale?

Venemaa tegevust on võimatu ennustada. Muidugi loodame parimat, aga samal ajal valmistume mistahes stsenaariumiks. Juba enne täiemahulist sissetungi viis Venemaa läbi terroristlike küber ründeid Ukraina energiataristu vastu. Venemaa kasutab küber ruumi jätkuvalt hübiidrünneteks lääneriikide vastu, meie partnerite vastu ja kelle iganes vastu, kes neile parajasti huvi pakub. See tõttu, isegi kui mingi rahuleping alla kirjutatakse, on ebatõenäoline, et küber ründed lakkaks. Nende intensiivsus võib väheneda, aga ära need ei kao.

Väljastpoolt vaadates tundub, et viimane töeliselt hävitluslik küber rünnak Ukrainas oli Kyivstar vastu detsembris 2023. Mis puudutab sõda Ukraina küber ruumis, kas usute, et halvim on möödas?

Me oleme üle elanud rohkem kui ühe hävitlusliku küber ründe: Kyivstar detsembris 2023, riiklikud andmebaasid detsembris 2024, Ukraina raudtee infosüsteemid märtsis 2025. Meie pidavalte arenev küber kaitse on arvatavasti põhjus, miks detsember 2025 oli suhteliselt vaikne. Kas see tähendab, et halvim on seljataga? Seda ma ei arva, sest vaenlane viib pidavalte küber ründeid ellu. Mõned neist on edukad, mõned vähem edukad. Teeme kõik, mis meie võimuses, et halvimat ära hoida, aga kui see peaks juhtuma, oleme valmis. ●

Kübermenüü 2025: PEKINGI PART

Lääneriigid omistavad aina rohkem küberründeid Hiinale ja peavad seda riiki enda jaoks suurimaks küberohuks. Andmelekked võimaldavad meil heita pilgu Hiina ründavale küberökosüsteemile, mida iseloomustab erasektori ja riigi ulatuslik koostöö.

Eelmises RIA küberturvalisuse aastaraamatus kirjutasime, et Hiina Rahvavabariigi küberrühmitused on ilmselt kõige võimekamat ja keerulisimaid küberoperatsioone läbi viivad läänevastased jõud maailmas. 2025. aastal nägime sama trendi tugevnemist ehk Hiina kübertegevuste haarde ja ulatuse suurenemist – alates globaalsetest luure- ja ründekampaaniatest ning lõpetades enda eelpositiioneerimisega lääne kriitilisse taristusse.

Hiina tegevusi kübersfääris iseloomustab väga kõrge tehniline võimekus, kiire (sh nullpäeva) turvanõrkuste äarakasutamine, operatsioonide globaalne ulatus ning Hiina riiklike ambitsioonide toetamine.

MAGUSHAPU KANA

2025. aastal omistati Hiina riiklikele ründajatele ehk APTdele kümneid küberründeid. Peamiselt sihtisid nad valitsusasutusi, telekommunikatsiooniettevõtteid ja (kaitse)tööstusettevõtteid, kuid puutumata ei jäanud ka muude valdkondade ettevõtted.

Peamine eesmärk on saada ligipääs tundlikele andmetele, et lõigata nende abil nii majanduslikku, poliitilist kui ka sõjalist kasu. Näiteks jaanuaris teatas Taiwan, et Hiina rünnakud Taiwani vastu on kahekordistunud – eeskõige tabasid need valitsusasutusi ja telekommunikatsioonifirmasid. Mais

kuulutas Suurbritannia küberturvalisuse amet, et Hiinat loetakse nende rahvuslikule küberturvalisusele peamiseks ohuks, sest Hiina rühmitused ründasid nii valitsusasutusi, kriitilist taristut kui ka parlamentiliikmeid. Ka Eesti välisministeerium mõistis need rünnakud hukka. Ameerika rahvusliku luure direktori hinnangul on Hiina Ameerikale kõige aktiivsem ja pikaajalisem küberohut.

Tshehhi Vabariik omistas mais esmakordselt rünnaku Hiina rühmitusele APT31, kes sihtis kampaaniaga Tsahhi välisministeeriumi. Prantsusmaa küberturvalisuse amet avaldas raporti ründekampaaniast Houken, millega sihti Prantsusmaa valitussektorit ja eraettevõtteid. Need on ainult mõned näited ilmestamaks, kui ulatuslikud on Hiina riigi toetatud küberrünnakute kampaaniad.

Jätkusid ka teated eelpositioneerimisest, näiteks avastas USA küberväejuhatuse, et Hiina pahvara on mitme Ladina-Ameerika riigi võrkudes. Eelpositioneerimine kui mõiste sai laiemat tähelepanu 2024. aastal, kui Ameerika võimud süüditasid Hiina küberrühmitusi, et nad on tunginud erinevatesse võrkudesse. Kahtlustatakse, et eesmärgiks on eelkõige ennast positsioneerida, et sobival hetkel halvata kriitilist taristut ning häirida sellega riigi ja selle elanike igapäevast toimetulekut. 2024. aastal palju kajastust saanud Salt Typhooni kampaania, mis sihtis telekommunikatsioonisektorit, ei raugenud, vaid vastupidi, suure-



nes – esialgu tuvastatud kaheksa ettevõtte asemel on nüüd ohvreid üle 600 ettevõtte 80 riigist.

Samuti on Hiina jätkuvalt suurim nullpäeva turvanõrkuste ärakasutaja. Näiteks kasutasid Hiina küberühmitused aktiivselt ära turvanõrkusi märtsis Ivanti VPN-seadmetes, aprillis SAP NetWeaveris, mais Ivanti Endpoint Manageris, juulis Microsofti SharePointi tarkvaras. Microsofti SharePointi turvanõrkust kasutati ära rohkem kui 400 asutuse ründamiseks üle maailma, sh ka Ameerika Ühendriikide valitsusasutustes.

HIINA SÖÖGIPULGAD EHK 筷子

Hiina küberühmituste *modus operandi* ehk toimetamise viis on päaseda võrkudesse ja jäädä seal võimalikult pikaks ajaks peidetuks. Tihtilugu üritatakse liikuda ühest süsteemist teise, kasutades ära asjaolu, et seadmed või süsteemid juba eelnevalt usaldavad üksteist. Näiteks 2025. aastal vaadeldud Hiina küberünnakutest pea 75 protsendi olid pahavaravabad, mis tähindab, et sissepääsuks kasutati kas turvanõrkuseid või varastatud sisselogimistunnuseid. Seda tehnikat kutsutakse Living Off The →

Land, mis teeb sissetungikatsed raske-
mini märgatavaks.

Teise trendina jätkub ääreseadmete ja pilveplatvormide nõrkuste ärakasutamine. Sellele juhtis tähelepanu ka mitmekümne luure- ja küber turvalisuse asutuse avalik teadaanne, mille USA koos liitlastega septembris avaldas.

Euroopa küber turvalisuse amet (ENISA) toob oma aastaaruandes välja, et aina rohkem kuritarvitatakse ka erinevaid IoT-seadmeid, sh ruutereid. Hiina rühmitus Flax Typhoon kasutas ära Quad7 robotvõrgustikku, mis koosnes tuhandetest TP-Linki ruuteritest Euroopas. Teiseks näiteks on robotvõrgustik BADBOX 2.0. Google'i andmetel oli sellesse liidetud üle kümne miljoni nakatumud koduseadme, mille kaudu said küber kurjategijad viia läbi pahatahtlike tegevusi. Ka Eesti ei jäanud puutumata – tipp hetkel oli meil üle 7000 nakatumud seadme. Paljudesse seadmetesse oli paigaldatud pahavara juba enne selle müümist või saadi pahavara oma seadmesse, kui Androidi rakendusi laeti alla mitteametlikust kohast. Enamik sellistest seadmetest tuleb Hiinast.

Iseloomulikuks jooneks on see, et Hiina rühmitused jagavad omavahel tööriisti. Tihtilugu teeb

Aina rohkem kuritarvitatakse IoT-seadmeid, sh ruutereid. Hiina rühmitus Flax Typhoon kasutas ära Quad7 robotvõrgustikku, mis koosnes tuhandetest TP-Linki ruuteritest Euroopas.

see konkreetse tööriista omistamise konkreetsele toimijale raskeks. Seetõttu on ka paljud omistamised viimasel ajal keskendunud rohkem mitte ühe rühmituse tuvastamisele, vaid pigem tuuakse esile Hiina firmasid, mis aitavad kaasa küber rünnakute läbiviimisele.

TOIDUPLEKID SÄRGIESISEL

Novembris lekkis Hiina tarkvara firmast Knowsec üle 12 000 salastatud dokumendi, mis näitasid, kuidas firmal õnnestus kompromiteerida rohkem kui 80 sihtmärki üle maailma. Lekked paljastasid, et neil on pahavara ja troojalased kõikidele suur-

TASUTA LÕUNAID POLE OLEMAS

Ameerika Ühendriikide ja Hiina vahel käib tehnoloogiline võidujooks, mille väljapaistvamaks osaks on Al-tehnoloogia. 2025. aasta algul üllatas Hiina firma DeepSeek avalikkust oma uue keelemudeliga, mille loomine oli väidetavalт kordades odavam kui lääne analoogide arendamine. Küll aga ei jäanud see võimekuselt alla tolleaegsetele lääne keelemudelitele. Ameerika Ühendriikides kirjeldati DeepSeeki avalikustamist kui „Sputniku hetke“ tehisaru valdkonnas, sest möisteti, et Hiina võib tehisaru arendamises mitte ainult järele jõuda, vaid ette minna.

DeepSeeki keelemudelite kasutamise potentsiaalsed plussid on lihtsad – tegemist on võimsa, küllalt avatud, odava ja kiire mudeliga, mida saab kasutada eri rakendustes, teenustes ja ettevõtetes laiemalt. DeepSeeki enda kasutajatingimustes on kirjas, et nad

koguvad andmeid, kasutavad neid mudeli treenimiseks ja jagavad ka teiste teenusepakkujatega. Hiina seaduste kohaselt peavad nad jagama kõiki andmeid ka Hiina valitsus- ja luureasutustega. DeepSeeki keelemudelid ka tsenseerivad teemasid, mis on ebamugavat Hiina Kommunistliku Partei jaoks, nagu näiteks Tiananmeni väljakу veresaun 1989. aasta suvel.

See kõik ei tähenda, et Hiina rakendusi peaks igal pool ja alati vältima. Oluline on meeles pidada, et tasuta lõunaid pole olemas. Valitsusasutustes ja teistes olulistes ettevõtetes soovitab RIA mitte kasutada Hiina firma DeepSeek rakendusi tööseadmetes. Samuti ei peaks sinna sisestama tundlikku informatsiooni. Iga kasutaja peaks enda jaoks põhjalikult läbi mõtlema, millist infot nad soovivad tehnoloogiaettevõtetega jagada.

tele operatsioonisüsteemidele – Windows, Linux, MacOS, iOS ja Android.

Teine leke sisaldas Salt Typhooni rühmituse liikmete isikuandmeid ja tehingute infot. Kolmas kirjeldas, kuidas Hiina eksportib teistesse riikidesse oma internetimudelit, mis võimaldab kodanike massjälgimist. Neljas leke paljastas, kuidas Hiina firmad viivad tehisaru abiga läbi infooperatsioone poliitilisel väljal.

Need lekked näitavad, et Hiina riik kasutab pahatahtlike küberoperatsioonide läbiviimiseks erafirmade abi. Samaaegselt annab see riigile võimaluse taandada end rünnakutest, sest läbivija on ju erafirma, mitte riiklik asutus.

HIINA TOIT EESTIS

2025. aastal oli ka Eesti Hiina kübergevuste huviorbiidis. Oluline on mõista, et kui kuskil maailmas avaldatakse mõni turvanõrkus, mida kasutatakse aktiivselt ära, siis suure töenäosusega on huvatavaid seadmeid ka Eestis ja on vaid aja küsimus, millal mõni pahatahtlike kavatsustega rühmitus need avastab. RIA-le teadaolevalt on nii mitutki turvanõrkust, mida aktiivselt kasutavad ära Hiina küberrühmitused, proovitud kasutada ka Eestis ning nii mõnelgi korral on see õnnestunud.

Tuletame meelete, et turvanõrkuste kiire paikamine ning küberhügieeni järgimine aitavad ennetada märkimisväärse osa küberohitudest. Samuti matkitakse Eesti ettevõtteid Hiina küberkurjategijate loodud SMS-õngitsuskampaaniates ning oleme olnud sihtmärgiks ka Hiina riiklike ründajate õngitsuskirjadele.

„KUI PALJUD KORJAVAD HALGE, TÕUSEB LEEK KÖRGEKS“*

Aina rohkem lääneriike nimetavad üha häalekamalt Hiinat küberohuks ja omistavad sellele küber-rünnakuid. Tehakse ühisavaldisi (Tšehhi, Suurbritannia, Prantsusmaa, USA ja teised) ning kirjeldatakse detailiselt Hiina häkkerite taktikaid. Peab valmistuma selleks, et Hiina küberündajad hakkavad aina rohkem kasutama ka tehisaru abi, et leida kiiremini turvanõrkuseid ja neid ära kasutada.

Mida saame Hiinast pärít küberohu vastu teha? Paigata üha kiiremini turvanõrkuseid, jälgida oma võrkudes toimuvat, edendada riigisisest ja rahvusvahelist koostööd. ●

* Hiina vanasõna

12 AASTAT HIINA RIIKLIKKE KÜBERRÜHMITSU

Veebruaris 2013 avaldas küberbefirma Mandiant raporti, mis raputas kübermaailma. Selles kirjeldati salajast Hiina häkkerirühmitust, mis oli arvukate luureoperatsioonide taga. Rühmitus sai nimeks APT1 (*advanced persistent threat* – arenenud püsiv oht ehk riiklik ründaja) ning see seoti Hiina Rahvavabastusarmeega üksusega 61398.

Raport kirjeldas, kuidas rühmitus varastas rohkem kui 20 riigis ligi 150 asutuselt sadu terabaite andmeid. Lisaks toodi selles nimeliselt välja rünnakute taga olnud isikud. See oli esmakordne taoline omistamine, mille järel hakkasid lääneriigid ja ettevõtted avalikult palju rohkem rääkima küberohitudest. See oli ka üks peamistest teemadest, mida arutasid omavahel Ameerika ja Hiina juhid 2015. aastal. Suurriigid leppisid kokku, et nad ei vii enam läbi intellektuaalomandi varguseid küberfääris ning selle pakti nimeks sai Obama-Xi küberkokkulepe. Kahjuks on ajalugu töestanud, et see lepe kaua ei pidanud.

Järgneva 12 aasta jooksul avastati kümneid Hiina riiklike häkkerirühmitusi. Analüütikute arvamusel on Hiinas kõige rohkem riiklikult toetatud küberrühmitusi. Kuigi täpset arvu on raske öelda, arvatakse, et neid on vähemalt 60. Teiste suurte läänevastaste küberjöudude – näiteks Venemaa, Iraan ja Põhja-Korea – rühmitusi kokku on teadaolevalt alla 30.

Hiina kultuuris on tavapärasne mõõta aega 12-aastaste tsüklitega. 2025. aastal ehk 12 aastat pärast esimese APT raporti avaldamist lisandus Hiina riiklike häkkerirühmituste nimekirja uus tegija – Phantom Taurus. Kui APT1-taolised rühmitused olid laia haardega ja üritasid koguda võimalikult palju andmeid, siis uuemate rühmituste eriprärs on täpsemalt sihitud ründed, eesmärgiga jäada võimalikult pikaks ajaks asutuse või ettevõtte võrgus varjatuks. Phantom Taurus kasutab uudseid tööriistu, mida pole eelnevalt Hiina rühmituste puhul täheldatud. Märkimisväärne on seogi, et Phantom Taurus tegutses kaks ja pool aastat nii, et keegi neid ei märganud.

VENE KARUD küberruumis

Venemaa kasutab küberruumi sihipärase ja efektiivse tööriistana oma välis- ja julgeolekupoliitiliste eesmärkide toetamiseks. Idanaabri arsenalis on küberluure, destruktiovsed ründeoperatsioonid ja infooperatsioonid.

Sellise ulatusliku ja koordineeritud küberluuretegevuse praktiliseks elluviimiseks kasutab Venemaa režiim muu hulgas riikliku taustaga küberühmitusi, mida rahvusvaheliselt kutsutakse APTdeks (*advanced persistent threat*). Need suudavad läbi viia keerukaid ja sihitud küberoperatsioone, mille eesmärk on muu hulgas luureinfo kogumine, kompromiteeritud infosüsteemides püsiva ligipääsu hoidmine ning ka häirivate või destruktiovsete rünnete elluviimine.

Need rühmitused tegutsevad Venemaa eriteenistustesse ja sõjaliste struktuuride huvides ning täidavad luure- ja ettevalmistusülesandeid nii rahuajal kui ka täiemahuliste sõjaliste konfliktide taustal.

Vene APT-rühmituste tegevus ei piirdu Ukraina vastu suunatud küberoperatsioonidega, vaid on sihitud ka nende riikide vastu, kes toetavad Ukrainat poliitiliselt, majanduslikult või sõjaliselt. Euroopa Liidu (EL) ja NATO liikmesriigid on jää nud Vene APT-rühmituste püsivateks sihtmärkideks, kusjuures rünnete eesmärgiks on olnud nii tundliku teabe kogumine kui ka võimalike edasiste mõjutus- või ründeoperatsioonide ettevalmistamine.

VEEL ÜKS KARU: LAUNDRYBEAR

Lisaks varem tuntud ja laialdaselt kajastatud Vene APT-rühmitustele (näiteks CozyBear ja FancyBear), mis on juba aastaid sihtinud ELi ja NATO liikmesriike, kerkis 2025. aastal esile uus, seni teadmata Vene rühmitus. Küberturbekogukondades sai see nimeks **LaundryBear** (Microsofti järgi Void Blizzard).

Hollandi julgeoleku- ja luureteenistustesse (AIVD ja MIVD) hinnangul on suure töenäosusega tege mist Venemaa riigi sponsoreeritava rühmitusega, kelle tegevus on alates 2024. aastast keskendunud peamiselt lääneriikide vastu suunatud küberrünnakutele. Eelkõige on LaundryBeari fookuses ELi ja NATO liikmesriikide valitsusasutused, kaitseorganisatsionid, välisministeeriumid, kaitsetööstusettevõtted ning muud asutused, mis on seotud Ukraina toetamisega.

LaundryBeari küberrünnakute iseloom ja sihtmärkide valik viitavad eelkõige luuretegevusele, mitte häirivatele või destruktiovsetele küberoperatsioonidele. Rühmituse tegevuse peamiseks eesmärgiks on tundliku teabe kogumine, sealhulgas e-kirjavahetuse, kontaktandmete ja muude organisatsioonisest andmete varastamine, mis võimaldab Vene eriteenistustel saada paremat ülevaadet lääneriikide poliitilistest, sõjalistest ja kaitsealastest kavatsustest.

Tehnilisest vaatenurgast ei iseloomusta LaundryBeari tegevust uute või eriti keerukate rünnevekto ride kasutamine. Vastupidi, rühmitus tugineb pigem suhteliselt lihtsakoelistele, kuid tõhusatele meetoditele, nagu varastatud kasutajakonto-andmete kuritarvitamine, paroolide pihustamine (*password spraying*), autentimisküpssite (*session cookies*) ja pilvepõhiste e-posti keskkondade (eelkõige Microsoft Exchange Online'i) kuritarvitamine.

Sageli hangitakse vajalikud autentimisandmed kolmandate osapoolte kaudu, kasutades tumeveebi turuplatvormidel müüdavaid, nuhkvaraga kogutud andmeid. Sellist lähenemist illustreerib näiteks



2024. aastal Hollandi politsei vastu toime pandud rünne, mille käigus sai LaundryBear ligipääsu ühe töötaja kasutajakontole, kasutades varastatud sisselogimisessiooni. Selle kaudu koguti organisatsiooni kesksetest süsteemidest töölaseid kontaktandmeid ja muud teavet, mida saab kasutada edasiste sihitud rünnete ettevalmistamiseks.

Sihtmärgiks võib sattuda iga töötaja asutustes, mille vastu ründaja huvi tunneb, sõltumata tema ametikohast või ligipääsu ulatusest.

See juhtum näitab taas, et sihtmärgiks võib sattuda iga töötaja asutustes, mille vastu ründaja huvi tunneb, sõltumata tema ametikohast või ligipääsu ulatusest. Samal ajal tuleb silmas pidada, et suurem osa sääristest rünnakuteest on kergesti ennetatavad elementaarsete küberhügieeni põhimõtete (mitmeastmeline autentimine, tugev paroolihaldus ja kasutajate teadlikkuse tõstmine) järgimise abil.

VENOMOUS BEAR JA COZYBEAR LUURASID DIPLOMAATIDE JÄRELE

Diplomaatilised sihtmärgid on Venemaa riikliku küberluure jaoks strateegiliselt tähtsad juba aastaid ning 2025. aasta ei toonud ses osas muutust. Välisministeeriumid, saatkonnad ja muud diplomaatilised esindused kujutavad endast Venemaa jaoks kõrge väärtsusega luureobjekte, kuna nende kaudu on võimalik koguda varajast infot poliitiliste seisukohtade, otsustusprotsesside, liitlassuhete ning Ukraina-teemaliste arutelude kohta. 2025. aastal paistsid selles vallas silma kaks pikaajalise tegevuslooga APT-rühmitust: APT29 ehk **Cozy-Bear** ja **Venomous Bear** (tuntud ka kui Turla).

APT29, keda seostatakse Venemaa välisluureteenistusega (SVR), jätkas 2025. aastal sihitud õngitsuskampaaniatega Euroopa diplomaatiliste asutuste töötajate vastu. Rünnete aluseks oli usaldusväärne ja kontekstipõhine peibutuslugu, mille

raames esineti välisministeeriumite või muude sarnaste institutsioonide nimel ning edastati e-kirja teel näiliselt ametlike kutseid ja teateid, näiteks diplomaatiliste ürituste või kohtumistega seoses.

Need kutsed sisaldasid pahaloomulisi linke või manuseid ning kui sihtmärk ei olnud piisavalt ettevaatlik ja nendele vajutas, andis see ründajatele ligipääsu tema tööarvutile ja e-posti kontole. Selle kaudu sai APT29 jälgida ohvri suhtlust, koguda dokumente ning kasutada kompromiteeritud kontot edasiste sihitud luurerünnete ettevalmistamiseks.

Venomous Bear, keda peetakse Venemaa üheks pikaajalisemaks ja tehniliselt võimekamaks APT-rühmituseks ning keda seostatakse Venemaa föderaalse julgeolekuteenistusega (FSB), jätkas 2025. aastal diplomaatiliste sihtmärkide vastu suunatud tegevust teistsuguse lähenemisega. Kui APT29 tugines eesköögi petukirjadele, mis olid suunatud välismaal asuvatele ELi diplomaatidele, siis Venomous Bear keskendus hoopis diplomaatilistele esindustele ja töötajatele, kes viibisid Venemaa territooriumil ning kasutasid sealset side- ja võrgutaristut.

See võimaldas Venomous Bearil suunata diplomaatide veebiliiklust nn vahepeatusse (*adversary-in-the-middle*), kus kasutajale kuvati näiline sertifikaadiviga või turvateade. Selle lahendamiseks paluti ohvril alla laadida ja paigaldada vastav tarkvarakomponent, mille abil said ründajad ligipääsu seadmele ning võimaluse jälgida diplomaatilist suhtlust.

SAMMUD AUTONOOMSE PAHAVARA SUUNAS

Viimastel aastatel toimunud tehisaru ja suurte keelemudelite hoogne areng on loonud uusi võimalusi igapäevaste tööülesannete automatiserimiseks ja tõhustamiseks, kuid samal ajal on need tehnoloogiad leidnud laialdast rakendust ka küberkuritegives.

Näiteks on need võimaldanud automatiseerida ja kiirendada küberrünnakute ettevalmistavaid etappe, nagu petusõnumite koostamine, sihtmärkide profileerimine ning ründestsenaariumite kohandamine vastavalt kontekstile ja sihtmärgile.

Vene riikliku taustaga ohustajate seas on üks silmapaistvamaid selliste võimaluste kasutajaid APT28 ehk FancyBear. Tegu on Vene sõjaväeluure-

VENE LUURETEENISTUSTEGA SEOTUD APT-RÜHMIDUSED

	FANCYBEAR / APT28	COZYBEAR / APT29	VENOMOUS BEAR / Turla	LAUNDRYBEAR / Void Blizzard
Sihtmärgid	Riigiasutused, kaitsetööstus, tehnoloogia- ja logistikaettevõtted, kriitiline taristu ning NATO ja ELiga seotud rahvusvahelised institutsioonid.	Pearmiselt ELi ja USA valitsusasutused, valitsusväilised organisatsioonid (NGO), energiasektor, välis- ja julgeoleku-politikaga seotud institutsioonid ning tehnoloogia- ja pilveteenuste pakkujad.	Ida-Euroopa ja Kagu-Aasia valitsusasutused, sh välisministeeriumid, diplomaatilised esindused ning julgeolekuasutused Euroopas ja Euraasias, samuti rahvusvahelised organisatsioonid ja teadusasutused.	NATO liikmesriikide valitsusasutused, telekomiettevõtted, tervishoiusektor, kaitsetööstus ning meedia- ja transpordisektor.
Seotud luureteenistus				
Rünnakud	Viimastel aastatel viis läbi mitmeid luurekampaaniaid Ukraina toetamisega seotud lääneriikide logistika- ja transpordiettevõtete vastu.	Jätkas Euroopa diplomaatiliste asutustest vastu suunatud luurekampaaniatega, kasutades pahavara sisaldauid peibutuskirju.	Möödunud aastal viis läbi luurekampaaniaid Euroopa diplomaatiliste välisteenistustest vastu.	Viimati seostati Hollandi politsei vastu suunatud küberluure-üksustega, mille käigus sai rühmitus volitamata ligipääsu organisatsiooni-sisestele kontaktandmetele.

ga seotud rühmitusega, kes kasutas 2025. aastal küberünnakutes oma kodukootud pahavara, mis sai küberurbekogukonnas nimeks **LAMEHUG**.

Mitme uurija hinnangul on tegemist esimese avalikult dokumenteeritud pahavaraga, mis kasutab ründeoperatsiooni käigus otseselt suurt keelemudelit (LLM). Nimelt rakendab LAMEHUG rünnaku käigus suurt keelemudelit selleks, et geneereerida konkreetseid pahaloomulisi süsteemikäskke ja skripte, mida pahavara nakatunud süsteemis seejärel täidab. Need käsud on möeldud muu hulgas nakatunud seadme süsteemiinfo kogumiseks, kasutajafailide otsimiseks ning seejärel kogutud andmete koondamiseks ja ründajale edastamiseks. See tähendab, et erinevalt tavaliisest pahavarast ei pöhine LAMEHUG staatilisel koodil, vaid võib ründeoperatsiooni käigus esineda erine-

vates vormides ja variatsioonides. Nõnda jätab see pahavara vähem korduvaid mustreid ja raskendab selle tuvastamist traditsiooniliste viirustörje- ja signatuuripõhistele kaitselahendustele poolt.

LAMEHUG pole küll veel otseselt iseseisvalt otsuseid langetav tehisarupõhine pahavara, vaid pigem näide sellest, kuidas ründajad kasutavad keelemudeleid olemasolevate ründetaktikate paindlikumaks ja kiiremaks rakendamiseks. Kuid tasub silmas pidada, et need on alles esimesed sammud. Töenäoliselt näeme lähiaastatel senisest autonoomsemaid pahavarasid, mis suudavad iseseisvalt kohandada oma käitumist vastavalt kompromiteeritud süsteemile ja kaitsemeetmetele. Selline areng tähendaks kvalitatiivset hüpet pahavara arengus ning paneks proovile senised tuvastus- ja kaitselahendused. ●

MINISTEERIUMI VAADE: mis tehtud ja mis teoksil?

Justiits- ja digiministeeriumi digitaristu ja küber turvalisuse asekantsler
TÖNU GRÜNBERG vaatab tagasi möödunud aasta arengutele riikliku
küberturvalisuse vallas ja seab sihte 2026. aastaks.

2025. aasta oli küberjulgeoleku arendamisel murranguline. Ministeeriumi vaatest keskendusime sellele, et Eesti digiriik püsiks usaldusväärne, toimepidev ja kooskõlas kiiresti arenava Euroopa Liidu õigusruumiga. Fookuses olid nii strateegilised raamistikud kui ka praktilised sammud, mis aitavad turvanõudeid paremini mõista ja neid kasutusele võtta.

ESMASED TURVAMEETMED VÄIKSEMALE

Üks märgilisemaid samme oli esmatest turvameetmetest koosneva raamistikku loomine väike- ja mikroettevõtjatele. E-ITS on sisuliselt tugev ja terviklik raamistik, mis loob selged põhimõtted küber turvalisuse juhtimiseks ning sobib eelkõige suurematele organisatsioonidele, kellel on vajalik võimekus turvanõuetega süsteemeks hindamiseks ja rakendamiseks. Väiksemate organisatsioonide jaoks on olukord aga teistsugune. Neil puudub sageli nii erialane kompetents kui ka jääb puudu inimestest ja ajast, et keerukates nõuetes iseseisvalt orienteeruda

ning hinnata, millest alustada või millised meetmed on nende jaoks kõige olulisemad.

Väikesed ja mikroorganisatsioonid vajavad eelkõige selgeid, praktilisi ja üheselt mõistetavaid juhiseid ehk konkreetset arusaama, mida nad peavad tegema, et oma küber turvalisuse taset mõistlikult ja jõukohaselt tagada.

Just sellest vajadusest lähtuvalt töötasime välja esmased turvameetmed, mis aitavad keskenduda olulisele, vähendada halduskoormust ning parandada realselt turvalisust. Selle lähenemise praktilist väärust kinnitas ka perearstide poolt antud aasta teo tunnustus.

UEENES KÜBERTURVALISUSE SEADUS

Teiseks oluliseks versta postiks on küber turvalisuse seaduse muudatus, mis jõustus 2026. aasta alguses ja millega võeti üle Euroopa Liidu küber turvalisuse (NIS2) direktiiv. Meie töö ei lõppe seaduse vastuvõtmisega, vaid ees seisab seotud rakendusmääriste jõustamine ning mitmete ettepanekute täiendav läbivaatamine koos sidusrühmadega.



Justiits- ja digiministeeriumi digitaristu ja küberturvalisuse asekantsler Tõnu Grünberg.

Ülereguleerimise vältimiseks hindasime iga sätte puhul, kas see vastab direktiivi miinimumnõuetele või läheb neist kaugemale. Selleks kasutusime lihtsat, kuid visuaalselt mõjusat analüüsni, mis aitas kiiresti eristada kohustuslikke nõudeid, varasemaid õiguskorrast tulenevaid erisusi ning tuvastada võimalikke ülereguleerimise, kinnirkirjutamise või rikkumiste ohte.

See lähenemine andis otsustajatele ja huvigruppidele selge ülevaate, millistes kohtades püsime Euroopa Liidu raamides ja kus teeme teadlikke poliitilisi valikuid. Sellist praktikat võiks Euroopa Liidu direktiivide ülevõtmisel ja õigusloomes ka edaspidi rakendada. See suurendab läbipaistvust, õigusselgust ja usaldust kogu protsessi vastu.

VALMISTUME KVANTARVUTITE TULEKUKS

Olulise arengusuunana jälgisime kvantarvutite tehnoloogilist arengut, mis võib muuta praegused krüptolahendused ebaturvaliseks ning mõjutada andmete ja teenuste kaitset. 2025. aastal alustasime postkvant-krüptograafia teekaardi koostamist. See annab selge suuna, kuidas valmistuda

krüptograafiliste algoritmide vahetuseks olukorras, kus kvantarvutite areng muudab senised lahendused ebapiisavaks. Fookus pole kiirustamisel, vaid teadlikul ja ajastatud üleminekul, mis arvestab tehnoloogilisi sõltuvusi, prioriteete ja organisatsioonide valmisolekut.

LIIGUME JÄRGMISESSE ARENGUFAASI

Vaates tulevikku, on meie eesmärk liikuda kasutajakesksema ja toimivama süsteemi ning intsidente ennetavate seadmete suunas. Küberturvalisus peab olema osa ärist ja iga imimese igapäevaelust. See tähendab, et turvanõuded peavad muutuma inimsõbralikumaks, nii et nende mõistmine ja rakendamine oleks lihtne, arusaadav ja teostatav ka väiksemates organisatsioonides või tehnoloogia kasutajatele, kes pole spetsialistid.

Olulise uue võimena on kavas arendada riiklikku küberjuhtimiskeskust, mis parandab riigiliste olukorrateadlikkust, reageerimisvõimet ja koostööd küberintsidentide ennetamisel ja lahendamisel.

Liigume sihikindlalt digiriigi järgmisse arengufaasi, kus rõhk pole üksnes nõuetel ja tehnoloogial, vaid ka arusaadavusel, koostööl ja usaldusel.

Õigusloome poolelt ootab meid 2026. aastal ees otsekohalduvate Euroopa Liidu küberkerksuse määrase (CRA) ja küberturvalisuse määrase (CSA) ülevõtmine miinimummahus. Meie eesmärk on täita nõuded mõistlikult, proporsionaalselt ja liigse halduskoormuseta, tagades samal ajal turvalisemad digitaalsed tooted turul.

Kokkuvõttes liigume sihikindlalt digiriigi järgmisse arengufaasi, kus rõhk pole üksnes nõuetel ja tehnoloogial, vaid ka arusaadavusel, koostööl ja usaldusel. ●



20 AASTAT

Eesti küberruumi kaitsel

1. jaanuaril 2026 tähistas **CERT-EE** oma 20. sünnipäeva.
Sel puhul vaatame intsidentide käsitlemise osakonna sündmusterohkele
ajaloole tagasi, et minna targemana edasi.

CERT-EE (Computer Emergency Response Team; eesti kintsidentide käsitlemise üksus) moodustab Eesti digiriigi ühe olulisema kaitseliini. Enamasti tegutseb see meeskond nähtamatult, sest nad ei otsi tähelepanu, vaid lahendusi. Nende töö edukust mõõdetakse selle järgi, kui harva tuleb avalikkust teavitada kriitilistest küberintsidentidest.

KAHEKESI KÜBERSÖJAS

2000. aastatel kolis üha enam teenuseid internetti, internetikasutus kasvas, ründevektorid laienesid. Kuigi häkkerid, pahavara ja andmepüük polnud toona veel Eestis igapäevased märksõnad, seisid pangad silmitsi juba esimeste küberünnakutega ja erinevad intsidentid panid aluse arutelule, kuidas tagada üha digitaalsema infoühiskonna turvalisus.

2005. aastal sai tollase Riigi Infosüsteemide Arenduskeskuse infoturbejuht Toomas Viira ülesandeks luua visioon Eesti CERTi jaoks ning selgitada üksuse vajalikkust nii ministeeriumiametnikele kui ka poliitikutele. Ajal, mil Eesti digiriik oli juba hoogsalt kujunemas, kuid küberturvalisus paljude jaoks veel uus ja abstraktne valdkond, sai Viira mitu kuud vastata küsimustele, mis on küberintsident ja miks sellega riigi tasemel tegelema peab. Õnneks mõisteti üsna ruttu, et Eesti ei saa endale lubada olukorda, kus digilahendused on küll uuenduslikud, aga kaitsmata. Pärast kuudepiikkust selgitustööd saabus positiivne otsus.

CERT-EE alustas tööd 1. jaanuaril 2006. „Juba tollal oli näha esimesi algelises vormis õngitsuspettusi ja viiruseid. Enim rünnati pankasid ja nende kliente, aga küberünnakute alla sattusid ka mitmed teised asutused,“ kirjeldab Viira tollal küberruumis toimunut. Kuigi algus oli kõike muud kui mugav – ehitada tuli tööprotsessid ja tekitada usaldus –, tõdeb Viira, et raskustest hoolimata sai CERT loodud õigel hetkel, veidi enne 2007. aasta küberünnakuid.

Üksuse esimene juht Hillar Aarelaid sai karmid tuleristsed: pärast pronkssõduri eemaldamist algas maailma esimene internetisõda, mis halvas Eesti veebilehed ja -teenused. Selle tõrjumist koordineeris CERT-EE, kus töötas toona vaid kaks inimest: Aarelaid ja Tarmo Randel. Randel, kellega sai hiljem üksuse juht, tödes CERT-EE 2007. aasta kokuvõttes, et too kevad tõi Eesti maailmakaardile ja sündmuste negatiivsest ise-

MIS ON CERT?

Riigi infosüsteemi ameti intsidentide käsitlemise osakond CERT-EE jälgib Eesti küberruumi, tegeleb avaliku sektori ennetava kaitsega ning tuvastab Eesti arvutivõrkudes toimuvaid küberintsidente. Intsidenti korral aitab CERT-EE uurida selle põhjust ning nõustab lahendamist.

CERT-EE on Euroopa info- ja võrguturbeameti (ENISA) küberurbemeeskondade võrgustiku CSIRTS Network liige.

loomust hoolimata oli nende efekt positiivne. Avalikkuse jaoks oli see esimene kord, mil küberintsident muutus rahvusliku julgeoleku küsimuseks ning paljud ettevõtted ja riigid hakkasid oma taristut tõsiselt analüüsima ja kaitsmma.

PÖÖRASED 2010NDAD

2010ndatel kasvas CERT-EE töö maht plahvatuslikult. Kui 2013. aastal oli töölaual umbes 300 intsidenti, siis neli aastat hiljem kümme korda rohkem. Aastail 2014–2018 üksust juhtinud Klaid Mägi võrdleb toonast tiimi *start-up’iga*: „Meeskonda kuulusid entusiastid, kes tegid suuri asju parasjagu käes olevate vahenditega põlve otsas.“

2015 mõisteti, et kella kaheksast viieni süsteemiga pole võimalik operatiivselt intsidente lahendada, mistõttu seati sisse ööpäevaringne valve, palgati juurde spetsialiste ning sama aasta suvest jälgis meeskond Eesti küberruumis toimuvat 24/7.

„Tänu ööpäevaringsele kiirele reageerimisele avanes võimalus hoiata üldsusst suuremate õngitsus- ja pahavarakampaaniate eest, teavitada majutusteenuse pakkujaid ning kodulehtede omanikke probleemsetest veeblehtedest ning anda operatiivsemal infot turvanõrkuste kohta, mis ohustasid suurt hulka kasutajaid,“ kirjeldab Mägi.

Seejärel pandi alus CERT-EE igapäevasele uudiskirjale, mille eesmärk on tänaseni kajastada operatiivselt küberruumis toimuvat. Praegu tellib uudiskirja juba ligi 2200 huvilist.

VALMIS JUUBELIRÜNNETEKS

2017. aastal saavutas Eesti CERT esimest korda SIM3 (Security Incident Management Maturity Model) sertifikaadi ehk kõrgeima rahvusvahelise CERTide standardi, mille saamiseks hinnatakse dokumenteeritust, töökorraldust, infovahetust,



valmidust koostööks, juhtumite käsitlemise efektivsust ja professionaalsust jms, mis tagavad parema intsidentide lahendamise võimekuse ja küber turvalisuse tagamise. CERT-EE oli maailmas viies, kes selle tasemini joudis.

Samal aastal valmistutti kümme aastat tagasi toimunud küber rünnakute aastapäevaks, eeldades potentsiaalseid kordusrünnakuid Venemaa poolt. „Meil oli arvamus, et naaberriik võib nii-öelda juubeli puhul midagi korraldada ning olime valmis. Õnneks „juubeliründeid“ ei tulnud, küll aga tõi aasta meile kaks teist tuntuks saanud rünnet – WannaCry ja NotPetya –, mis mõlemad olid üle maailma väga suure mõjuga,“ meenutab Mägi. Ja nagu sellest poleks veel piisanud, järgnes sama aasta suve lõpus ID-kaardi kriis, mis puudutas ligi 750 000 inimest. Seega jagus väljakutseid ühe aasta peale enam kui küll.

Sündmuste keerises muutus meeskonna tehniline analüüs aina sügavamaks ja automatiseritud tuvastussüsteemid tugevamaks. CERT-EE eksperdid olid sageli avalikkuse ees nii televisioonis, raadios kui ka sotsiaalmeedias, rõhutades küber turbe olulisust.

Suurte rahvusvaheliste küber rünnakute lahendamiseks panid CERT-EE liikmed aluse rahvusvahelisele Mattermosti kanalile (suhtlusplatvorm, mis võimaldab turvalist ja kontrollitud kommunikatsiooni), kuhu esimest korda koondati kokku

huvitatud osapooled erinevate Euroopa Liidu riikide CERTidest. Selles tänaseni toimivas kanalis mõtteid vahetades asuti ühiselt lahendama WannaCry kriisi.

OHUPILT HAKKAB MUUTUMA

Kuigi 2019. aastal polnud küberohud enam kellelegi uudiseks, kasvas rünnakute sagedus, automatiseritus ja sihitus Eesti suunal. Samal aastal sogenesid hüppeliselt Smart-IDga seotud öngitus- ja petuskeemid. Sai selgeks, et pelgast teavitamisest enam ei piisa ning CERT muutis oma lähenemist. „Soovitusi on lihtne anda. Aga kui asutus ei jõua neid ellu viia, on mõistlikum pakkuda lahendust teenusena,“ kirjeldab tollal üksust juhtinud Tõnu Tammer. CERTi portfellil lisandusid praktilised ja skaleeruvad teenused, mis aitavad ohtusid ennetada ka siis, kui asutusel endal napiib selleks võimekust. Näiteks arendati küberohtude filtreerimiseks nimeserveri- ehk DNS-põhine lahendus, mis peatab pahtahtliku tegevuse enne, kui ühendus tildse tekib.

Paralleelselt sisuliste arendustega tehti olulisi samme ka Eesti internetitaristu tugevdamisel. Uuendati riiklik internetisõlm, mis võimaldab sideoperaatoritel vahetada liiklust tõhusamalt ja hoida Eesti-sisene internetiliiklus riigi sees. See suurendas nii toimepidevust kui ka vastupidavust rünnetele.

RÜNDAJATE KULUD ÜLES JA TULUD ALLA

2022. aasta tõi uue nähtuse: veebilingid, mille avamine pani kasutaja brauseri automaatselt osalema teenusetõkestusrünnakutes. „Oli vaja vaid link avada ja tehniliselt mittepädev imimene sai enese teadmata ründes osaleda,“ kirjeldab Tammer. Vastuseks võeti kasutusele Cloudflare'i teenus, pakkudes üheskoos Eestis veelgi tugevamat kaitset. Eesmärk oli viia kurjategijate kulud võimalikult üles ja tulud alla. „Mida rohkem suudame erinevate tehniliste meetmetega seda saavutada, seda vähem on Neil huvi Eestit rünnata,“ selgitab Tammer.

Alustati koostööd turvalahenduste pakkujatega, jagades nendega valideeritud ohuteavet. See võimaldas küberohkte kiiremini nn mustadesse nimekirjadesse lisada, vähendades ründajate võimalusi. Ühe suure tootja tagasiside põhjal moodustas CERT-EE jagatud info märkimisväärse osa nende esmatest ohuteadmistest.

ME EI RAHULDU EILSE TASEMEGA

Kahe kümnendiga on CERT-EE kasvanud usaldusväärseks ja arrestatavaks tegijaks, kes kaitseb Eesti digitaalset ökosüsteemi – tavainimesest kuni riigi kriitilise taristuni. Infoturbevõimekus on riigis kasvanud, kuid mida rohkem on tugevaid ja iseseisvaid meeskondi, seda olulisem on keskne koordineerija. Kübergastupidavus ei sünni üksikutest tegijatest, vaid hästi juhitud koostööst. „Kui CERT-EE on 20 aastaga midagi töestanud, siis seda, et Eesti digiriik püsib seetõttu, et me ei rahuldu eelse tasemega,“ ütleb CERT-EE juht Taavi Kupper. Meeskond jätkab samasuguse vastutuse, sisemise põlemise ja eesmärgiga, et Eesti digiriik oleks usaldusväärne mitte ainult täna, vaid ka homme.

CERT-EE arengule tagasi vaadates ütleb Tammer, et CERT-EE on aastate jooksul muutunud proaktiivsemaks: „See on meeskond, kes hoiab küberruumi toimivana ja vähendab riske – sageli nii, et keegi ei pane seda tähelegi.“

See on ka küberkaitse paradoks: mida paremini on töö tehtud, seda nähtamatum see on. Kui inimesed ei pea mõtlema teenuste ebastabilse või katkestuste peale, tähendab see, et CERT-EE on teinud oma tööd hästi.

IGA PÄEV JA KOGU AEG

Tulenevalt geopolitiilistest sündmustest meie ümber, kasvas järgnevatel aastatel CERTi töömaht märgatavalt. 2023. aastast meeskonda juhtinud Veikko Raasuke kirjeldab selle tööd igapäevase võitlusena. „Meid rünnatakse iga päev, proovitakse süsteemidesse siseneda või ummistusrünnakutega midagi maha joosta. CERT-EE ülesanne on sellele vastu seista kogu aeg – nädala-vahetuse, öösiti, koolivaheagadel, riigipühadel, jõuludel. Ehk ajal, mil enamik meist on pere keskis, teevad kübervalvurid tööd, et ülejäänud riik saaks rahus sülti süüa,“ räägib Raasuke.

„Ajal, mil enamik meist on pere keskis, teevad kübervalvurid tööd, et ülejäänud riik saaks rahus sülti süüa.“

2024. aasta 9. märtsil toimus Eesti küberajaloo suurima mahuga ummistusrünne avaliku sektori veebilehtede vastu: veidi enam kui nelja tunni jooksul tehti ligi kolm miljardit pahaloomulist päringut. CERT oli ja on endiselt kaitsmises edukas: rünnakutel on harva mõju. Kui on, siis on see lühiajaline.

Nii nagu CERT arendab pidevalt kaitsetaktikaid, tegeleb ka vastane oma tööriistade arendamisega ning ründetaktikate muutmisega. Raasukese sõnul katsid töölaua peamiselt ummistusrünnakud, aga ka erinevad õngitsused. Näiteks kasutasid kurjategijad osavalt ära suurüritust, mille raames külasta-

sid Eestit paljude riikide kõrged ametnikud. Üritusel osalejatele saadeti justkui korraldaja poolt väga gi usutava välimusega õngitsuskiri.

Kui varasematel aastatel läks CERT-EE-finantspettuse lehe sulgemiseks seitse kuni kümme tööpäeva, siis koostöös politsei- ja piirivalveameti, pangaliidu ja pankadega suudeti see aeg viia alla ühe tunni.

Naljaga nimetas tiim perioodi oktoobrist jaanuarini „jõulurahuks“, mil peamiselt logistikaettevõtete nimel tehtavate pettuse hulk kasvas kümneid kordi. Kuid 2024. aasta jaanuaris vaibumist enam ei tulnud. Petturid läksid aina aktiivsemas ning enam ei kasutatud ära ainult logistikaettevõtteid, vaid ka kõikvoimalikke muid firmasid ja riigiasutusi. „Seejuures on petturitele suureks abiks olnud ka AI areng, mis aitab neil hõlpsasti toota usutavat eestikeelset sisu,“ ütleb Raasuke.

VAADE TULEVIKKU

Suunates pilgu minevikust tulevikku, seisavad CERT-EE ees üha suuremad väljakutsed. Küberturvalisus pole enam üksikute organisatsioonide mure, vaid globaalne küsimus. Pildil on täiesti uued ohud, näiteks tehisintellekti abil teostatud rünnakud, kvantarvutite pakutavad võimalused või 5G-võrgu potentsiaalsed haavatavused.

Praegu üksust juhiv Taavi Kupper sõnab, et Eestis on infosüsteemide ja e-teenuste turvalisuse tase kõrge, kuid keskkond muutub pidevalt. „Uued ohud nõuavad järjepidevat kohanemist. Järgnevatel aastatel tuleb CERT-EE-i üha enam panustada rahvusvahelise koostöö ja partnerluste tugevdamisse, sest küberturvalisus on globaalses mastaabis kollektiivne ülesanne,“ ütleb Kupper ja lisab, et meeskond on valmis seisma silmitsi uute ja muutuvate ohtudega.

Tulevik tähendab ühtlasi proaktiivsemat ja andmepõhisemat lähenemist. „Kui praegu räägitakse küberintsidentide ja rünnakute tõkestamisest, siis edaspidi tuleb CERT-EE-i kanda üha suuremat rolli andmepõhisest analüütikas ja ennetavas tegevuses. Tänu uutele tehnoloogiatele, nagu masinõpe ja tehesisintellekt, on võimalik palju kiiremini analüüsida süsteemide käitumist ja tuvastada ka kõige keerukamaid ning varjatumaid rünnakumustreid. Üks on siiski kindel: CERT-EE on olnud ja on ka edaspidi üks Eesti küberturvalisuse tugsiambaid,“ kinnitab Kupper. ●

Alustas RIA JUHTIMIS- KESKUS

1. juunil 2025 alustas RIA juhtimiskeskus, mille ülesanne on jälgida ja juhtida RIA teenuste tööd ning seirata Eesti küberruumi toimuvat. Juhtimiskeskusel on reaalajas pilt digitaristust ja seal reageeritakse kohe, kui miski hakkab tõrkuma.

Eesti digiriik toimib suuresti tänu sellele, et kriitilised teenused töötavad ööpäev läbi ja katkestusteta. Olgu selleks isiku tuvastus, riiklikud portaalid või taustal toimiv taristu – need köök peavad olema kättesaadavad ka siis, kui enamik meist ööund magab.

Selleks loodi 1. juunil 2025 RIA juhtimiskeskus, mille ülesanne on jälgida ja juhtida RIA teenuste ning Eesti küberruumi toimimist. Juhtimiskeskusest võib mõelda kui RIA „südamest ja närvisüsteemist“. Kohast, kus on reaalajas pilt kogu digitaristust ja kus reageeritakse kohe, kui miski hakkab tõrkuma. Juhtimiskeskus tugineb neljale omavahel seotud sambale.

SEIRE

Seire on juhtimiskeskuse tuumik. Seiretiim tuvas tab ja registreerib ööpäev ringi küberintsidente, teeb esmase mõjuhinnangu ning koordineerib edasisi tegevusi.

Lisaks tehnilisele valvele kogutakse ja koondatakse teavet ka laiemalt. Näiteks koostab seire igal hommikul ülevaate, mis annab huvilistele pildi Eesti küberruumi viimase ööpäeva jooksul juhtunust ning olulisematest küberbeudistest mujalt maailmast.

Lisaks jälgib seiretiim RIA enda teenuseid ja füüsilise turbe häireid, et köök süsteemid toimiksid katkestusteta.

TEENUSTE JÄLGITAVUS

Juhtimiskeskus tagab, et RIA teenuste seisund oleks reaalajas nähtav. Vajalik ülevaade aga ei teki iseenesest: selle taga on tööriistad, mis koondavad eri allikatest infot, ning kompetents, mis aitab kogutud teavet mõtestada ja kasutada.

Juhtimiskeskuse pakutavad lahendused on paindlikud ja skaleeritavad. Neid saab vajadusel laiendada ja kohandada nii väiksemate kui ka suuremate süsteemide jaoks. Lisaks võimaldab avatud ja läbipaistev lähenemine hoida kulud kontrolli all, välvides dubleerimist ja kallite erilahenduste loomist.

Selle tulemusena saadakse kiiremini aru, kus probleem peitub, reageerida sellele täpsemalt ning vähendada katkestuste mõju nii asutustele kui ka lõppkasutajatele.

KLIENDIKOGEMUS JA TEENINDUS

Juhtimiskeskuse üks rollidest on suhelda partnerite ja kasutajatega. Kliendikogemuse tiimi põhifunktsioon on lahendada kasutajate pöördumisi, uurida klientide vajadusi ja ootusi, koguda tagasisidet ning viia läbi uuringuid, mis aitavad teenuseid arendada või muresid lahendada.

Olenemata kliendist või partnerist peaks RIA poole pöörduja tajuma, et organisatsioon räägib temaga sama keelt. Mis veelgi olulisem – pöördumine või mure peab saama võimalikult kiiresti



lahendatud. Juhtimiskeskus koondab pöördumised ühte kohta ning hoiab suhluse selge ja sujuva.

JUHTIMISRAAMISTIKE JA PROTSESSIDE ARENDUS

Lisaks operatiivsele tööle kujundab juhtimiskeskus ka seda, kuidas toimib teenuseportfelli haldus, IT haldusprotesside kujundamine ning ühte juhtimismudeliarendamine. See aitab tagada, et kõik teenused on üheselt mõistetavad, vastutused ja rollid on paigas ning tegevused toetavad nii strateegilisi sihte kui ka igapäevast tööt.

MIS SAAB EDASI?

Mõistmaks intsidentide laiemat mõju avalikele teenustele ja loomaks olukorrateadlikkust, on riigil vaja kokku tuua tervikpilt. Selleks on RIAs olemas tugev vundament, milleni oleme jõudnud aastatepikkuse eeltööga.

2026. aastal loome lahendused, mille abil saavad riigi digiteenuste omanikud saata teenuste kättesaadavuse ja tõrgete info oma monitooringusüsteemidest automaatselt RIA-le, kus sellest tekib kõlkehõlmav ülevaade. Lahenduste loomisel peame tähtsaks, et asutuste jaoks oleks pardaletulek võimalikult lihtne.

HEAL LAPSEL MITU NIME

RIAt võib selles rollis nimetada kui küberjuhtimiskeskus või GovSOC (Government Security Operations Centre), ent olulisem on sisu. Tekkiv olukorrateadlikkus võimaldab avalikul sektoril paremini juhtida ja koordineerida suure mõjuga küberintsi-

JUHTIMISKESKUSE NELI SAMMAST

- ➥ Seire: tuvastame ja registreerime küberintidenti ööpäev ringi.
- ➥ Jälgitavus: tagame, et RIA teenuste seisund oleks reaalajas nähtav.
- ➥ Kliendikogemus: lahendame kasutajate pöördumisi ja uurime klientide vajadusi.
- ➥ Juhtimisraamistike arendus: paneme paika, kuidas teenused kliendini jõuavad, kuidas neid töös hoida ja arendada.

dentide lahendamist. Samuti saavad teenuste omanikud olla kindlad, et keegi hoiab nende kriitilistel teenustel silma peal 24 tundi ööpäevas.

Siiski tuleb meeles pidada, et RIA ei asenda teiste asutuste monitooringut, vaid toob tervikpildi ühte kohta kokku. Ka edaspidi vastutab iga asutus oma teenuste käideldavuse, terviklikkuse ja konfidentsiaalsuse eest ise.

MIKS SEDA VAJA ON?

RIA juhtimiskeskus loodi selleks, et Eesti digiriik toimiks katkestusteta ja oleks valmis reageerima nii tehnilistele tõrgetele kui ka küberohtudele. Ühes keskuses on koos seire, teenindus, kliendi-suhted ja juhtimisprotsessid. Need loovad terviku, mis aitab digiriigil olla tugevam, kindlam ja läbi-paistvam. Tänu sellele on Eesti küberruum ja riigi digiteenused kaitstud, juhitud ja usaldusväärased. Igal päeval. Igal ööl. ●

Mida me ENN ETUSE vallas tegime?

Elmise aasta suurima ennetuskampaania suunasime ettevõtetele, et nad oskaks küberruumis varitsevaid ohte ära tunda ja end nende eest kaitsta. Jätkasime õpitubadega vanemaealistele ja jagasime õpilastele küber turvalisuse tööraamatuid.

EKKI arvuliselt on eraisikute vastu suunatud küberrünnakuid rohkem, on keskmised kahjusummad suuremad nende pettuse ja rünnete korral, mille ohvriks on mõni ettevõte.

Möödunud aasta mahukaima küber turvalisuse ennetuskampaania suunasimegi väikestele ja keskmise suurusega ettevõtetele. Selle eesmärk oli tõsta ettevõtete juhtide teadlikkust, et küber turvalisus on ettevõtte ellujäämise küsimus ning et selle eest vastutab tegevjuht. Tema otsustab, kuhu läheb ettevõtte ressurss, milline on ettevõtte kultuur ning kas töötajad on küberohtude teemal koolitatud.

BEC-SKEEMID JA LUNAVARA

RIA andmetel kannavad Eesti ettevõtted suurimat kahju erinevate ärikirjapettuste ehk BEC-skeemide ja lunavararünnakute töltu. Kampaania raames juhtisime nendele ohtudele tähelepanu ja andsime näpunäiteid, kuidas ohvriks langemist vältida. Avaldasime sel teemal artikleid, käisime rääkimas raadios ja levitasime RIA loodud ettevõtte küber turvalisuse uuendatud lühijuhendit.

Kampaania osutus edukaks: järeluuringust selgus, et üle poole kampaaniat märganud sihtrühmast hakkas teema kohta rohkem uurima või plaanis muuta oma ettevõtet küber turvalisemaks.



OLE IT-VAATLIK

Eriallikate • Ettevõtlate • Küberkaits Kätirasus • Stated ja videoo ▲ Levinud pettused ja riimakud ▲

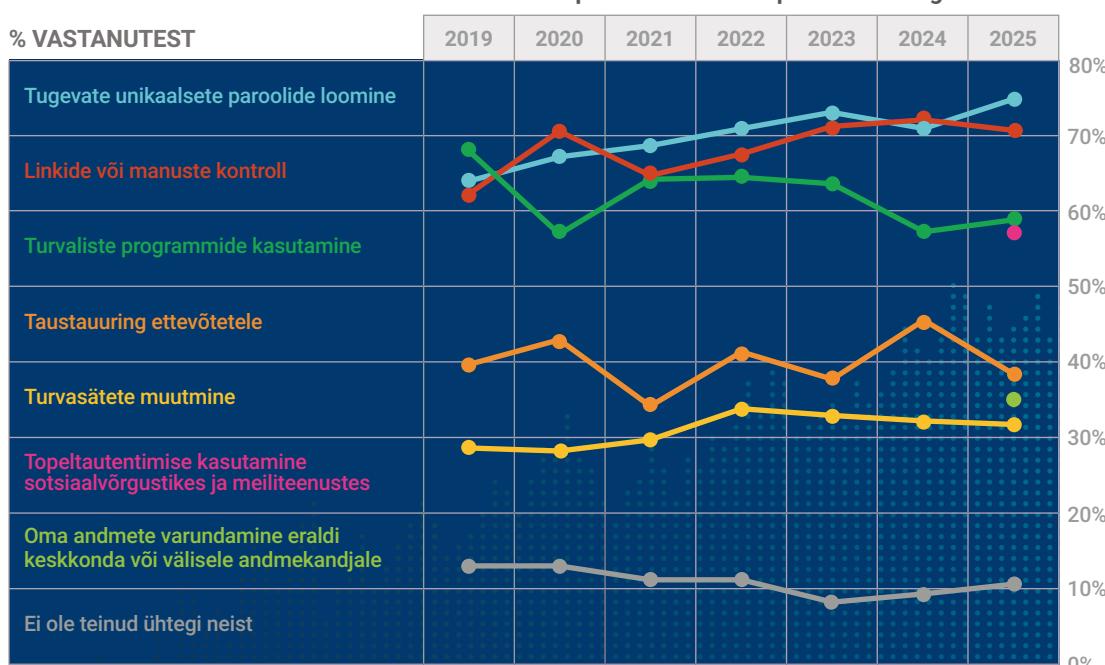
SINU PIN. SINU PRIVAATSUS.

Öpia ärä turmida olukordi, kus keegi üritab su PIN-kodele välja petta.

Pettused Levinud pettused

Tulevate pettuseid ei oleksid peatasamist vältida. Uueandme pettuse nimetus on jooksvalt, mit et vold seda aegajalt üle vastamas kilia. Jälgi operatörivõtet infot ka RIA Facebooki lehel!

Levinud

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


Allikas: statistikaamet

Ettevõtte küberturvalisuse juhendi ja selle, milles on Eesti ettevõteid ohustavad petuskeemid ja rünnakud, leiad RIA ennetuslehelt itvaatlik.ee.

TÄHELEPANU PETTUSTEL

Lõppenud aasta töö petukõnede kasvu. Seepärast korraldasime aasta lõpus kampaania, mis juhtis tähelepanu sellele, kuidas ära tunda olukordi, kus üritatakse välja petta PIN-kode. Sellest, kuidas petukõnesid tehakse, millised on ohumärgid ja millal peaks kindlasti kõne katkestama, saab lugeda samuti lehelt itvaatlik.ee, kuhu lisame jooksvalt infot levinumate petuskeemide kohta.

ÕPITOAD VANEMAEALISTELE JA UUS KÜBERTEST

Kuna ennetuses on oluline roll järjepidevusel, jätkasime mitmete varasemate tegevustega ka 2025. aastal. Jätkusid küberturvalisuse töötoad vanemaalistele. Eri maakondade kesk- ja linnaraamatukogudes toimus 15 küberturvalisuse töötuba, milles osales kokku ligi paarsada inimest. Töötoad olid osalejatele tasuta ning lisaks said koolitatud koju kaasa võtta küberhügieeni põhitödedega brošüüri.

Aprillis sai kätesaadavaks juba hästi tundud Kübertesti uus versioon, mille võttis kasutusele enam kui 426 asutust ja ettevõtet. Nende hulgas on

NUMBRITE KEELES

Juba seitsmendat aastat hoiame statistikaamet abi silma peal Eesti elanike küberteadlikkusel. 2025. aasta uuringu tulemused näitavad, et Eesti elanikud pööravad küberturvalisusele jätkuvalt tähelepanu, kuid praktika on valdkonniti ebaühiline. Kõige aktiivsemalt panustatakse paroolide tugevdamisse ja ootamatute sõnumite sisukontrolli, mis viibab et inimesed möistavad hästi levinumaid riske. Samas viitavad madalamad näitajad turvasätete kohandamisel, taustauuringute tegemisel ja regulaarse varundamise juures, et tehnilisemad või aeganöuvamad tegevused kipuvad tagaplaanile jäma ning vajavad jätkuvalt rohkem teadlikkust ja harjumuste kujundamist.

näiteks riigiasutused, kohalikud omavalitsused, koolid, haiglad, perearstikeskused ning ka ettevõtted. Aasta lõpu seisuga on ligi 32 000 inimest jõudnud oma teadmisi täiendada ja testida.

Jätkasime ka nooremale kooliastmele mõeldud küberturvalisuse tööraamatute levitamisega. Sel sügisel jõudis koolidesse üle 12 000 eksemplari materjale, mis õpetavad lastele internetis ohult toimetama. ●

Kuidas muuta AVALIKUD TEENUSED töökindlamaks

Eesti ühiskond toimib mugavatel avalikel teenustel, kuid nende taga peidab end sõltuvuste rägastik. RIA otsib ja parandab selle nõrku lülisid, et teenused toimiksid ka siis, kui katkeb oluline sidekaabel või elektrühendus.

Politseiniku töö avaliku korra tagamisel, arsti ligipääs patsiendi terviseandmetele raviotsuste tegemiseks, väljastatud retseptide vaatamine riiklikus mobiiliraken-duses, dokumendi digiallkirjastamine – need kõik on avalikud teenused. Ühiskondlik ootus ja vajadus on, et olulisimad neist toimiksid ööpäev läbi, seitse päeva nädalas, 365 päeva aastas. Katkegu kaablid või sadagu pussnuge.

TÄHTSATEST TÄHTSAMAD

Olulisimate teenuste all mõistame eeskätt neid, mille toimimisest võib sõltuda kellegi elu, tervis, avalik kord, riigi olukorrateadlikkus ja sellest lähtuvalt ka julgeolek. Samavõrra olulised on teenused, mis hoiavad töös majanduse vereringet.

Avalike teenuste toimimine on osa meie iga-päevalust. Digitaliseerituse tase on jõudnud saja protsendini ja asjaajamine veebis muutunud normiks. Teisisi tundub ebamugav, vahel isegi võimatu. Selle märkamatu mugavuse varjus peidab ennast sõltuvuste rägastik, mille najal toimib kogu Eesti ühiskond. Sõltuvused hõlmavad endas nii riigi kui ka erasektori digitaalset taristut.

Merealuste kaablite katkemised on asjakohased

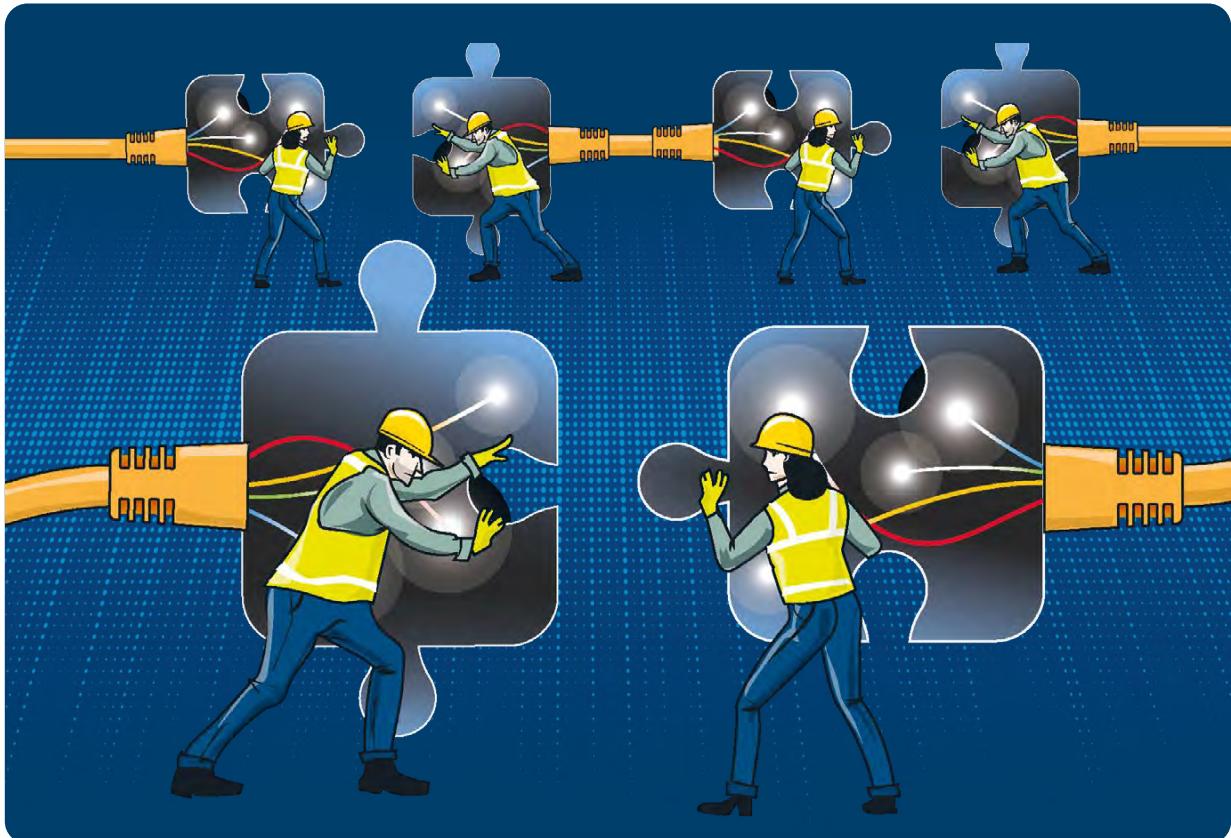
näited intsidentidest, mis panevad meid tegutsema selle nimel, et ühiskond saaks keerulistes oludes ootuspäraselt toimida.

ÜKS AHEL, SADA LÜLI

Olukorra illustreerimiseks tasub mõelda lihtsustatud ahela peale, mis tuleb läbi käia, et mõni teenus muutuks inimese jaoks veebis kasutatavaks. Arendaja teeb valmis teenuse pakkumiseks vajaliku koodi; seejärel kasutab ta internetiühendust, et loodud kood serveris paigaldada ja käivitada. Andmekeskuses, kus server asub, tuleb tagada vajalik elekter, andmeside, jahutus ja füüsiline turvalisus. Teenuse kasutajal on vaja internetiühendust kodus või nutitelefonis.

Kõige selle toimimiseks peab hulk tehnilisi komponente laitmatult toimima. Mida detailsemaltoodud näidet kirjeldada, seda rohkem neid komponente ilmneb.

Teenuste töökindlus tõuseb, kui igale komponendile, mis selle pakkumise ahelas on, luuakse varulahendus. Näiteks elektrivarustuse katkemisel lülitub andmekeskus generaatoritele, sidekaabli katkemise puhuks on olulistes kohtades ühendused mitmekordsed, serverite ja neis töötan-



vate tarkvaraade tõrge teenuseks pakutakse teenuseid üheaegselt mitmest andmekeskusest.

RIA TEENUSED KUI VUNDAMENT

Paljud avalikud teenused sõltuvad RIA pakutavatest kesksetest teenustest. Sellest vastutusest lähtuvalt panustasime 2025. aastal oluliselt oma teenuste töökindluse töstmisesse ning jätkame vajalike tegevustega ka lähiastatel.

See tähdab nii asutusesissele kui ka välistele sõltuvustele varulahenduste loomist või sõltuvuste kõrvaldamist. Füüsilise taristu puhul on märksõnaks dubleerimine, vajadusel mitmekordne. Tarkvaraliste teenuste töökindluse töstmisel vähendame sõltuvust füüsilisest taristust ja selle pakkujatest. Sealjuures ei saa ega tohi me teha järeleandmisi lahenduste küber turvalisuse tagamisel.

Roomat ei ehitatud ühe päevaga, samamoodi ei saa töökindlust tösta hoogtööna – tuleb teha valikuid, määradata prioriteedid. Selle käigus saame hinnata, mida peame riigiasutusena tingimata ise ehitama ja töös hoidma ning mida on mõistlik täisteenusena lasta ära teha kellelegi teisel – avalikust või erasektorist.

Avalike teenuste töökindluse töstmisega ei pea tegelema mitte ainult RIA, vaid kogu avalik sektor. Kui edukad selles riigina oleme, sõltub koostööst ja valmidusest muuta seniseid tehnoloogilisi valikuid ja lahendusi.

Avalike teenuste töökindluse töstmisega ei pea tegelema mitte ainult RIA, vaid kogu avalik sektor.

VALMISTUME HALBADEKS ÜLLATUSTEKS

Heade üllatustega toimetulek ei vaja eeltööd, ent halbadega saame kõige paremini hakkama, kui oleme nendeks läbimöeldult valmistunud. Pingutused teenuste töökindluse parandamiseks ei tähenda, et prognoosime meie harjumuspärist mugavust halvavate intsidentide arvu kasvu. Küll aga peame olema selleks valmistunud. ●



„Halvimal juhul jääme päevadeks **ELEKTRITA”**

Need kurjakuulutavad sõnad kõlasid Küberreservi õppusel, kus koostöös Eleringiga harjutati läbi, kuidas käituda, kui küberrünnaku tõttu satub ohtu kogu Eesti elektrivarustus.

Eesti elektrisüsteemi tähtsus on raske ülehninnata. Selle toimimisest sõltub, kas meie kodud on soojad ja valgustatud, kas kraanist tuleb vett ja ruuterist internet, kas poest saab piima ja tanklast kütust.

Digitaalne juhtimine, kaugjälgimine ja automatiseerimine on muutnud energiasüsteemi tõhusamaks, kuid sellegi mündil on teine külg: energia-

julegeoleku tagamiseks peame toime tulema ka seda möjutavate küberohtudega.

AASTA SUURIM KÜBERÕPPUS

2025. aastal korraldas RIA koostöös Eleringiga Küberreservi kompleksõppuse, mille käigus harjutati, kuidas tagada Eesti energiasüsteemi toimimine ulatusliku küberintsidendi korral.

Õppuse stsenaariumi kohaselt tekkis reaalne, kuid algfaasis veel realiseerumata oht Eesti elektri põhivõrgu juhtimiskeskuste toimepidevusele. Sel-lise olukorra halvim võimalik areng on elektrisüsteemi ulatuslik kustumine ehk *blackout*.

Õppuse kesksed küsimused olid, kuidas tuvastada ja maandada oht olukorras, kus on tekkinud kahtlus, et ettevõtte IT-süsteemidesse tunginud ründaja võib põhivõrgu juhtimissüsteeme dis-tantsilt mõjutada, ning kuidas tagada elektrisüsteemi juhtimine äärmuslikes tingimustes.

Õppus, milles võttis osa ligi 200 eksperti pea kümnest organisatsioonist, sidus küberjulgeoleku, elektri varustuskindluse ja kriisijuhtimise tervikuks. Selle käigus anti osalejatele realistik vaade, kuidas võib küberintsident häirida elektrisüsteemi ning millised on riigi ja elutähtsate teenuste osutajate võimalused sellise olukorra lahendamiseks.

JUHTIMINE JA OTSUSTAMINE KRIISIOLUKORRAS

Kompleksõppuse oluline osa oli juhtimise ja otsustamise harjutamine. Küberintsidentid energiasüsteemis nõuavad piiratud info tingimustes kiireid ja kaalutletud otsuseid, millel võivad olla kaugeluletuvalud tagajärjed.

Õppus kinnitas, et meil on vaja hoida ja arendada võimekust taastada elektrisüsteem ka olukorras, kus digitaalsed juhtimissüsteemid on ajutiselt häiritud.

Õppuse käigus seati osalejad silmitsi dilem-madega, kus tuli tasakaalustada süsteemi turvalisuse ja elektrivarustuse katkemise riskid. Reageerimine toimus reaalajas ning eeldas tihedat koostööd

MIS ON KÜBERRESERV?

Küberreserv on RIA hallatav ja arendatav üleriigiline ekspertide võrgustik, mille eesmärk on toetada riiki ja elutähtsate teenuste osutajaid suure mõjuga küberintsidentide korral. Küber-reservi kuulub üle saja eksperti üle Eesti – nii avalikust kui ka erasektorist –, kelle teadmisi ja oskusi saab kasutada olukordades, kus tava-pärasest ressurssidest ei piisa.

Küberreservi kasutamine eeldab head koordi-neerimist, selgeid juhtimisahelaid ning ühist arusaama olukorras. Just nende aspektide harjutamiseks korraldab RIA igal aastal kom-pleksöppusi, kus lahendatakse küberintsidentist tulenevat hädaolukorda või selle ohtu ja testitakse koostööd nii tehnilisel kui ka strateegilisel tasandil.

Eleringi, RIA, teiste riigiasutuste (ministeeriumid, riigikantselei jt) ning Küberreservi eksperti-de vahel.

VARUSTUSKINDLUS SÖLTUB KA KÜBEROHTUDEST

Õppus kinnitas, et varustuskindlus pole üksnes füüsилiste rikete või tootmisvõimsuste küsimus. Küberohud võivad mõjutada süsteemi juhtimist ka siis, kui füüsiline taristu on terviklik ja tootmi-ne vastab tarbimisele. Seetõttu on oluline, et ener-giasüsteemi planeerimisel ja arendamisel arvesta-takse süsteemselt ka küberriskidega ning nende mõjuga sage-duse hoidmisele, reservide kasutami-sele ja taastamisprotsessidele.

Õppus kinnitas, et meil on vaja hoida ja arenda da võimekust taastada elektrisüsteem ka olukorras, kus digitaalsed juhtimissüsteemid on ajutiselt häiritud. See tähdab nii tehnilisi lahendusi kui ka vajalike teadmiste ja oskustega inimesi, kel on selged rollid ja vastutus.

Küberreservi õppus näitas, et küberjulgeolek ja energiajulgeolek on omavahel tihedalt põimunud. Suure mõjuga küberintsidenti lahendamine eel-dab valmisolekut tegutseda ebakindlas ja muutuvas olukorras, teha otsuseid puuduliku info tingi-mustes ning hoida toimivat koostööd erinevate organisa-tsionide vahel. Koos on kindlam. ●

KÜBER-TURVALISUS kui organisatsiooni küpsuse peegel

Sageli räägitakse küberturvalisusest kui tehnilisest nähtusest – kas tulemür on, logisid kogutakse ja riskianalüüs tehtud. See kõik on oluline, kuid järelevalve vaatenurgast jääb pinnapealseks. Praktika näitab järjekindalt, et küberturvalisus on otseses seoses organisatsiooni üldise küpsustasemega.

Küberturvalisus pole tehniline, vaid juhtimise küsimus. Seal, kus juhtkond mõistab infoturvet kui organisatsiooni toimimise loomulikku osa, on ka küberturvalisuse tase parem. Kus infoturvet nähakse mõttetu kohustuse, paratamatu tüütuse või välise vaenlase, pole põhjust oodata sisulist paranemist.

Kui juhtkond ei võta vastutust, ei tee otsuseid, ei eralda vahendeid ega oska põhimõtteid selgida, siis ei jõuta ka tulemuseni. See kehtib ühtemoodi nii avalikus kui ka erasektoris, nii suurtes kui ka väikestes organisatsioonides. Dokumentatsioon võib olla laitmatu, poliitikad korrektselt vormistatud ja auditiks vajalik kaust kenasti komplekteeritud, kuid tegemist on näilise infoturbega, mis annab ainult näilise turvatunde. Kehvemal juhul hammustab see peagi valusalt mõne intsidendi näol.

KÜBERTURVALISUS POLE KALLIS KAST RIULIS

Kuuleme sageli, et küberturbe jaoks pole raha. Arvatakse, et küberturvalisus tähendab kalleid vilkuvate tulukestega kaste serveriruumis või pilve-

teenuseid, mille nimed kõlavad muljetavalda vält. Kuid küsimus pole rahas, vaid tahtes ja suutlikkuses asju läbi mõelda ja kokkuleppeid järgida. Varade kirjapanek, vastutuste määratlemine, ligipääsude mõistlik haldamine, varundamise distsipliin ja muudatuste juhtimine on tegevused, mille rahaline kulu on sageli väike.

Endiselt kohtame arusaama, et järelevalve või auditi käigus kontrollitakse eelkõige dokumentide olemasolu. Dokumendid pole vajalikud järelevalve, vaid organisatsiooni enda jaoks, kirjeldamaks, kuidas peaks protsessid toimima.

Järelevalve huvi ei ole paber, vaid protsesside toimivus. Dokumente on vaja täpselt nii palju, kui need aitavad kirjeldada ja toetada reaalseid tegevusi. Küps organisatsioon kasutab dokumente töövahendina. Ebaküps toodab neid järelevalve või auditi rahustamiseks.

STANDARD EI PÄÄSTA, KUI MÖISTMINE PUUDUB

Praktikas ei ole sisulist vahet, kas organisatsioon lähtub E-ITSist, ISO27001st või muust raamistikust, sest probleemid ei teki reeglinä sellest, et



meedet ei osata rakendada, vaid palju varem. Sageli komistatakse juba varade mõistmise faasis: ei teata, mis varad organisatsioonil on, kui olulised need on. Sealt edasi: miks ja kui kiivalt peaks neid kaitsma ning kes peaks otsused tegema.

Kontrollide käigus selgub sageli, et süsteeme käsitletakse võrdselt, riskianalüüs on kõik riskid keskmised ning meetmed rakendatud pigem üldise kontrollnimekirja kui teadliku valiku alusel. Alles pärast tösisest intsidenti mõistetakse, et mõni seni tagaplaanil olnud süsteem oli tegelikult ärikuuiline.

Riskihaldus on siin hea lakkuspaber. Kui ei tehta vahet riskil ja ohul, kui riske käsitletakse formaalse tabeli, mitte otsustusvahendina, on ka infoturbemeetmed juhuslikud ja ala- või üle-dimensioneeritud. Ebaküpses organisatsioonis on riskianalüüs sõimusõna.

VASTUTUST EI SAA SISSE OSTA

Väiksemate organisatsioonide puhul on koostöö, ühishanded ja kesksete teenuste kasutamine sage li mõistlik ja välimatu. Need võimaldavad teha rohkem ja tõhusamalt.

Paraku tuleb järelevalves ette olukordi, kus organisatsioon eeldab ekslikult, et näiteks pilve- või turvateenuse kasutamine vabastab sisulisest vastutusest infoturbe eest. Küsimusele riskide hindamise või teenusepakkuja üle järelevalve tegemise kohta viidatakse lepingule või teenuse mainele.

Tegelikkuses täidab teenusepakkija lepingut, kuid ei tee strateegilisi otsuseid organisatsiooni eest. Küps organisatsioon mõistab, et ka teenuse sisestmisel jääb vastutus enda kanda.

ALUSTA ENDAST

Küberturvalisuse tase on otsene peegeldus organisatsiooni küpsusest: juhtimiskultuurist, vastutusvõimest, protsesside mõtestatusest ja valmisoolekust teha otsuseid.

Küps organisatsioon mõistab, mida ta teeb, miks ta seda teeb ja kes vastutab.

Kui organisatsioon soovib parandada oma küberturvalisuse olukorda, ei tasu alustada uue standardi või järgmisse tehnilise lahenduse otsimisest. Alustada tuleb iseendast. Küps organisatsioon mõistab, mida ta teeb, miks ta seda teeb ja kes vastutab. Ebaküps tegeleb sümpтомite, mitte põhjustega. Küberturvalisuses joonistub see vahe välja halastamatult.

Vastutus jääb alati organisatsioonile endale. Kui see põhimõte pole selge, hakkavad probleemid kiiresti kuhjuma. ●

UUS TOETUS küberturbe- ettevõtetele

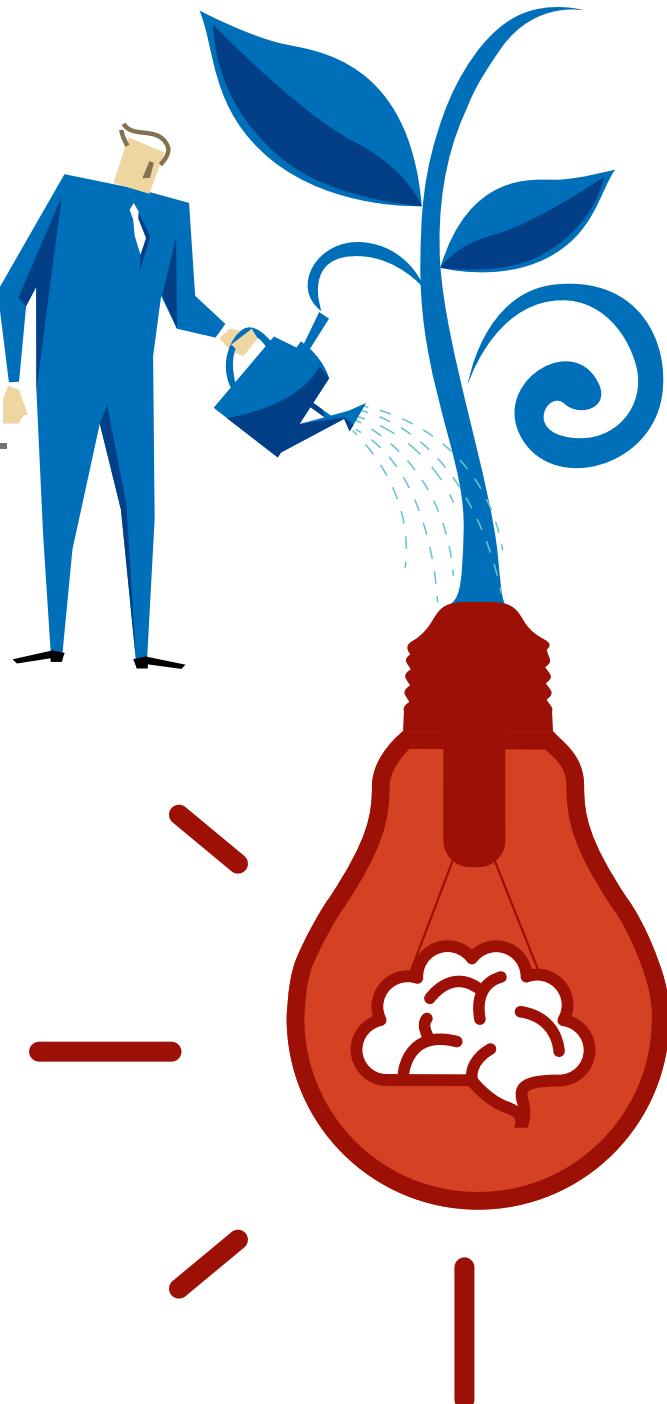
RIA ja Ettevõtluse ja Innovatsiooni Sihtasutus (EIS) töötasid välja innovatsioonitoetuse küberturbe-ettevõtetele, et edendada selle valdkonna toote- ja teenusearendust.

Kellele see mõeldud on ja kuidas seda taotleda?

Küberinnovatsioonitoetuse eesmärk on aidata teha ettevõtetel esimene samm koostöö suunas teadus- ja innovatsiooni-asutustega. Toetuse saamiseks peaks küberturvalisuse teenust või toodet arendav ettevõte kirjutama valmis projekti koostöös mõne teadus-arendusasutusega. Olgu selleks mõni ülikool või Euroopa Horisondi teadusprojektis osalenud teadusmahukas ettevõte. Toetust kaasfinaantseerib Euroopa küberkompetentsikeskus (ECCC) ja tema liikmed.

KUNI 100 000 EUROT

Kuna toetuse summa on 60 000 – 100 000 eurot ja projekti omafinantseerimise määr on sõltuvalt ettevõtte suurusest 30–50 protsendi, siis võiks projekti eelarve olla vähemalt 90 000 eurot.



Projekt võiks ette näha näiteks kontseptsiooni tõendust (*proof-of-concept*); prototüübi valmistamist või testimist; komponentide arendust, testimist või demonstreerimist; tootekatsetust; töös-

tuslikku eksperimenti või teostatavusuuringut. Samuti võib ühes projektis olla kombinatsioon mitmest eelmainitud tegevusest.

Üldine eesmärk on toetada toote- ja teenusearendust küberturvalisuse valdkonnas, kuid spetsiifilisemalt näiteks küberturvalisuse automatiserimises, tehisintellekti kasutamises küberturvalisuse tagamiseks, tööriistade väljatöötamises, mis toetaks üleminekut kvantarvutikindlatele krüptograafilistele algoritmidele, või kosmosevaldkonnaga seotud tehnoloogias.

Kuna küberinnovatsiooni-toetuse üks põhieesmärke on teadlaste ja ärivaldkonna koostöö edendamine, peegeldavad seda ka toetuse tingimused.

FOOKUS PÕHIÄRIL

Projekti kirjutamisel on oluline keskenduda oma põhiäri arendamisele ja mõelda läbi, kuidas saaks koostöö mõne teaduri-ga seda uuendusliku lähenemise kaudu toetada.

Toetussummad viitavad sellele, et tegemist on vaid esimeste sammudega. Kui koostöö osutub edukaks, on ettevõtetel võimalik suurema mahuga teadus-arendus-innovatsiooniprojektide jaoks saada tuge EISi pakutavast rakendusuuringute programmist või juba Euroopa Horisondi projektitaotlusvoorudest.

Kuna küberinnovatsioonitoetuse üks põhieesmärke on teadlaste ja ärivaldkonna koostöö edendamine, peegeldavad seda ka toetuse tingimused. Näiteks peaks koguprojektist vähemalt 40 protsendi minema teadus- ja arendusasutusele. Ülejäänud 60 protsendi projekti kuludest võib ettevõte kasutada oma projektmeeskonda doktorandi või doktorikraadiga inimese palkamiseks, nõustamisteenusteks (nt intellektuaalomandi

KÜBERKIIRENDI OOTAB UUSI IDUETTEVÖTTEID

2023. aastast on RIA TAK osakond koostöös Tehnopoly Startup Inkubaatoriga korraldanud küberturvalisuse valdkonna iduettevõtetele kiirendiprogrammi nimega Küberkiirendi.

Kuna seda programmi pikendati 2028. aastani, ootame nii 2026. kui ka 2027. aasta kevadsuvvel avaldusi liitumiseks järgmisse Küberkiirendi lennuga. Igasse lendu võtame vastu kuus-seitse iduettevõtet, kes tegutsevad küberturvalisuse valdkonnas. Iduettevõtted saavad seitsme kuu jooksul ekspertidel tiptassemel tuge ja 60 000 eurot oma idee arendamiseks.

Kandidaatimiseks peaks ettevõte pakkuma küberturvalisuse tooteid või teenuseid. 2025. aasta fookus oli sarnane innovatsioonitoetuse temaatikaga: küberturbe automatiseerimine, tehisintellekti kasutamine küberturvalisuse tagamiseks, kvantarvutikindlatele lahendustele üleminek, kosmosetehnoloogiad ja manipuleerimisrünnakute ennetamine.

2026. aasta fookusteemad avaldame kandidaatimise avanedes, kuid põhitelg on sama: kuidas uute ja teaduspõhiste lahendustega teha küberturvalisust kiiremaks, paremaks ja kättesaadavamaks.

jaoks), metroloogiaks, akrediteerimiseks, sertifitseerimiseks või projektmeeskonna tööjöu- ja tegevuskuludeks.

KUIDAS ALUSTADA?

EISi kodulehel on lisainformatsioon ja viited, kus ja kuidas taotlust esitada, kuid enne seda soovitame ettevõtjatel mõelda läbi võimalikud projektipartnerid, kelle poole innovatsiooniküsimusega pöörduda. Mõni ülikool tegeleb rohkem krüptograafiaga, mõni tehisintellektiga, mõne teadusmahuka ettevõtte portfellis on kosmosevaldkond.

Kui ideid on palju, aga partnereid napib, tasub võtta ühendust RIA küberturvalisuse keskuse teaduse ja arenduse koordineerimisosakonnaga (TAK) ja me aitame leida hea partneri. ●

EU CYBERNET laieneb itta

Euroopa Komisjon pikendas kolme aasta võrra RIA juhitavat ja ELi rahastatavat küberturvalisuse arenguabi projekti EU CyberNet. See toob uued partnerid ja võimaluse viia ELi abi Kagu-Aasia ning India ookeani piirkonda.

EU CyberNet on Eesti ja Euroopa küberturbekogukondadele hästi tundud. Kuue aasta jooksul oleme selle kaudu kasvatatud globaalset vastupanuvõimet kübertuhudele, eksportinud Eesti kogemusi turvalise digiriigi arhitektuurist ning aidanud Eesti tehnoloogiaettevõtetel kaugetel maaadel uusi ulksi avada. Ent vähesed teavad, et alates 2025. aasta kevadest töötas projektimeeskond koos RIA juhtkonnaga projekti jätkumise nimel.

Augustis saime röömustada, et suur pingutus tasus end ära: Euroopa Komisjon kuulutas EU CyberNeti teise etapi võitjaks RIA ja Saksamaa arengukoostööagentuuri GIZ ühispakkumise.

TEINE ETAPP: UUED PARTNERLUSED JA LAIENEV HAARE

EU CyberNeti teine etapp algas 2025. aasta septembris. RIA panustab projekti tehnilise võimekuse ja küberturbeekspertiisiga, GIZ eelkõige pikajalise arengukoostöö kogemusega. Ühelt poolt

LAC4

EU CyberNeti raames asutas RIA Ladina-Ameerika ja Kariibi mere piirkonnas tegutsemiseks regionaalne küberturbealase kompetentsikeskusse LAC4. See Dominikaani Vabariiki loodud koolitusasutus, millel on praeguseks 16 liikmesriiki, on saanud ELi üheks tuntuimaks kaubamärgiks piirkonnas, mis jätkab tegevust eraldiseisva RIA projektina.

suurendab uue strateegilise partneri lisandumine EU CyberNeti võimekust, teisalt kasvab projektijuhtimise keerukus.

Kui esimeses etapis viis EU CyberNet küberturbealast teadmist ja abi Ladina-Ameerika ja Kariibi mere piirkonda, siis teise etapi lepinguga lisandus mandaat pakkuda seda ka India ja Vaikse ookeani piirkonnas (Filipiinid, Indoneesia, Tai Kuningriik, Vietnam, Malaisia, Fidži jm). Väljakutse ei ole kergete killast, kuid usume, et eelnev kogemus ja põhjamaine kaalukus aitavad meil eesmärgid täita.

KOOLITUSED JA KONSULTATSIOONID

EU CyberNeti põhitegevused hõlmavad laia spektrit koolitusi ja konsultatsioone. Oleme toetanud algusjärgus CSIRTe (küberintsidentide lahendamise tiime), pakkunud tehnilisi koolitusi kogenud meeskondadele, nõustanud valitsusi küberturvalisuse strateegiate ja õigusaktide osas, viinud läbi kriisijuhtimise õppusi ning aidanud partneritel valmistuda rahvusvahelisteks küberdiplomaatia foorumiteks ÜROs. Ühe prioriteedina oleme panustanud järgmise põlvkonna talentide arengusse, kaasates noori ja edendades soolist mitmekesisust küberturvalisuse karjääririvalikul.

Oluliseks edulooks on kujunenud EU CyberNeti ekspertide võrgustik. Selles on nüüd ligi 600 spetsialisti valitsustest, teadusasutustest ja erasektorist. Ekspertvõrgustiku kaudu on EU CyberNet oluliselt laiendanud pakutava tehnilise abi mitmekesisust ja kvaliteeti ning on valmis toetama kõiki ELi või liikmesriikide rahastusega küberturvalisuse algatusi üle maailma.



Praeguseks on EU CyberNet korraldanud üle 250 tegevuse maailma eri paigus. Koolitustesse ja õppustesse oleme kaasanud üle 13 000 õppuri enam kui sajast riigist.

LOOME JA HOIAME KOGUKONDI

Läbi aastate on otse selzt partnerriikidele suunatud abitegevuste kõrval projekti portfooliosse tekkinud terve rida Euroopa Komisjonile ja ELi institutsioonidele suunatud tegevusi: näiteks ELi rahastusega küberprojektide kogukonna kohtumised, igakuiseid EU CyberNeti klubüüritused, ekspertide kiirkursused ja suvekoolid. Sellised algatused soodustavad teadmiste ja heade praktikate vahetust ning aitavad kaasa ELi kübergümnaasiumide arendamisele.

Praeguseks on EU CyberNet korraldanud üle 250 tegevuse maailma eri paigus.

Projekti kodulehelt leitav ja peamiselt Euroopa Komisjoni tarbeks ehitatud kaardistustööriist (Mapping Tool) pakub ajakohast ülevaadet kõigi ELi rahastatud kübergümnaasiumide algatustele kohta üle maailma. Meie pakutav konsolideeritud vaade projektide kohta võimaldab ELil paremat koordineerimist ja strateegilist planeerimist ning vähendab dubleerivate tegevuste rahastamist. ●

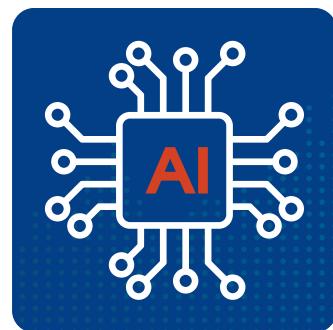
Mida oodata 2026. AASTALT küberruumis?

TEHISINTELLEKTI EI PEATA ENAM KEEGI

Tehisaru (AI) ning suurte keelemu-delite areng jätkub tohutu tempoga. Loomulikult lihtsustab see meie igapäevaelu, võimaldades küsida AI käest aina keerulisemaid küsimusi ning saada üha informeeritumaid vastuseid. Kuid samuti rõõmustab vastaspool – kurjategijad ja agressiivselt meeblestatud režiimid, kes saavad AI abil järjest tõhusalt oma sihtmärke rünnata.

2025. aastal nägid meie Ukraina sõbrad, et Venemaa ründas neid

pahavaraga, mis kasutab sisemisi AI-algoritme. Samuti hakkasid Vene riikliku taustaga ohustajad mullu ka teiste riikide valitsus- ja kaitsevägede vastu suunatud rünnakutes kasutama pahvara, mis suudab ise genereerida pahaloomulisi käske. Nägime ka Hiina soodsa ja korralikult töötava keelemuodeli nimega DeepSeek turule tulekut. Selle osas pole peamine mure (veel) naabrite või teiste ründamine, vaid Deep-



Seeki sisestatud info jagamine erinevate Hiina valitsus- ja julgeolekuasutustega.

TÄIENEV ÕIGUSRUUM TOOB KÜBERTURBE FOKUSESSE

1. jaanuaril 2026 hakkas kehtima küberturvalisuse seaduse (KüTS) muutmise seadus, millega võeti Eesti õigusesse üle Euroopa Liidu küberturvalisuse 2. direktiiv ehk NIS2. Eesti ettevõtete ja asutuste arv, kes peavad seal sätestatud nõudeid järgima, kasvas umbes 3500 pealt ligi 6500 juurde. Direktiivi eesmärk on tõsta küberturvalisuse taset terves ELis.

See kehtestab juhatuse liikmete isikliku vastutuse kübernõuetega täitmise eest ning senisest suuremad võimalikud trahvid nende rikkumise korral (kuni 10 miljonit eurot või kaks protsendi aastakäbest). Küberturvalisus töuseb



senisest rohkem juhtkondade teadvusesse.

KüTSi seni kehtinud versiooni järgi oli köigile seaduse kohaldumisalasse kuuluvatel asutustel ja ettevõtetel kohustus vastata Eesti

infoturbestandardile (E-ITS), mis aitab suurematel ja võimekamatel organisatsioonidel oma infoturbega mötestatult tegeleda. Nüüdsest tullakse väiksematele piltlikult öeldes poolele teelee vastu, kuna nende osaks jäab rakendada vaid RIA poolt eelmisel aastal paika pandud üldnõudeid ehk esmaseid infoturbemeetmeid. Need vähendavad oluliselt halduskoormust ning sätestavad väiksemate asutustele jaoks mõistetavalta ja jõukohaselt just nende jaoks olulisimad turbameetmed. Vöib loota, et infoturvet pärisele rakendada püüdvate väikeorganisatsioonide arv suureneb hüppeliselt.

PURUNEB JÄRJEKORDNE MÕJUGA INTSIDENTIDE REKORD

2025. aastal purunes Eesti küberruumis järkordne registreeritud mõjuga intsidentide rekord. Uus näitaja on 10 185, mis tähistab ühtlasi esimest viiekohalist vastavat arvu ühe kalendriaasta lõikes (2024. aastal oli see näitaja umbes kolmandiku ja aasta varem pea kolm korda väiksem). Nähes, kuidas pidevalt kasvava võimekusega kurjategijad mötlevad välja aina uusi ja edukaid petuskeeme, peame kahjuks progoosima



kasvutrendi jätkumist ka alanud aastal. Tõenäoliselt pole see küll sama kiire kui mullu, aga kõigil tasub meeles pidada, et igale lingile ei tasu klikkida ega sisestada ootamatu telefonikoone peale PIN-kode. Kui siiski satud küberintsidenti ohvriks, teavita sellest cert@cert.ee või raport.cert.ee.

UUS TASE PÕHJALA-BALTI REGIONAALSES KÜBERKOOSTÖÖS

Detsembris 2025 alustas sisulise tööga Taani vedamisel ellu kutsutud Põhjala-Balti küberkonsortsium ehk Nordic Baltic Cyber Consortium (NBCC). Selles osaleb seitse riiki: lisaks RIA poolt esindatavale Eestile Läti, Leedu, Soome, Taani, Norra ja Island. Rootsi peaks NBCC liikmeks saama hilisemas faasis.

NBCC eesmärk on tugevdada piirkonna koostööd ning paremini ennetada ja avastada küberründakuid. Selleks tuleb üles ehitada ühiskasutatavad infojagamise ja analüüsimise tööriistad ning suurendada küberohuteadmust, kaasates infoallikaid ka erasektori. NBCC pöörab tähelepanu ka innovatsioonile ning avaliku ja erasektori koostöö edendamisele.

Riikidevahelist koostööd toetab ka Euroopa Liit programmi „Digtalne Euroopa“ kaudu. Projekti



nelja-aastane kogueelarve on ligikaudu 14 miljonit eurot. NBCC algatus on ELi küberolidaarsuse määrase kontekstis piirilene küberkeskus (Cross-Border Cyber Hub). Võrgustik peaks hakkama aktiivselt infot vahetama teiste selliste küberkeskustega ELis, moodustades osa üleeuroopalisest küberturvalisuse hoiatussüsteemist.

LIIGUME VEELGI KESKSEMA KÜBERKAITSE POOLE

1. juunil 2025 alustas tööd RIA juhimiskeskus, mis tegeleb varem CERT-EE vastutada olnud Eesti küberruumi seirega ning RIA teenuste toimimise reaalajas jälgimise ja juhimisega. Tegu on piltlikult oeldes RIA südame ja närvisüsteemiga, kes ohu korral käitub häirekeskusena. Loodi see selleks, et meile harjumuspärane Eesti digiriik toimiks katkestusteta ja oleks valmis kohe reageerima nii tehnilistele tõrgetele kui ka küberohitudele.

2026. aastal hakkame seda laiendama riigi teistele e-teenustele, eesmärgiga tekitada senisest laiem pilt Eesti küberruumis toimuvast. Luuakse kliendisöbralikud lahendused, mille abil saavad teenuste omanikud jagada RIAsse automaatselt infot nende teenuste kättesaadavuse ja tõrgete kohta.

Selles rollis hakkab RIA käituma kui riiklik küberjuhimiskeskus või GovSOC (Government Security Operations Centre). RIAsse koonduv avaliku sektori olukorrateadlikkus võimaldab paremini juhtida ja koordineerida suure mõjuga küberintsidentide lahendamist ning hoida riigi kriitilistel teenustel silma peal 24 tundi ööpäevas.



Küberturvalisuse aastaraamat 2026

Väljaandja: **Riigi Infosüsteemi Amet**

Pärnu mnt 139a, 11317 Tallinn

Kujundus: **Martin Mileiko** (Profimeedia)

Illustratsioonid: **Andres Varustin, Martin Mileiko**

Trükk: **K-Print**

ISSN 3059-8494

Loe edasi: **[ria.ee](#)** ja **[itvaatlik.ee](#)**