



# KÜBERTURVALISUSE AASTARAAMAT 2025





RIIGI INFOSÜSTEEMI AMET



# Küberturvalisuse aastaraamat 2025

# Sisukord

## EESSÖNA

6

### Küberturvalisem Eesti algab sinust

Kuidas tulla toime rekordilise arvu küberrünnakute ja turvanõrkustega, millega eelmisel aastal silmitsi seisime, kirjutab Gert Auväärt, RIA peadirektori asetäitja küberturvalisuse alal.

## 2024. AASTA ÜLEVAADE

8

### Veel üks rekordiaasta, mida polnud vaja

Seda, et 2024. aasta tuleb küberruumis vaikne ja rahulik, ei oodanud meist keegi. Aga me ei osanud arvata ka seda, et möjuga intsidentide arv rekordkõrgelt tasemelt kahekordistub.

14

### Ukraina sõda: küberründed tulid rindejoonele lähemale

Möödunud aasta 19. novembril täitus tuhat päeva Venemaa täiemahulise sissetungi algusest Ukrainasse, sellest kauemgi on kestnud võitlus küberruumis.

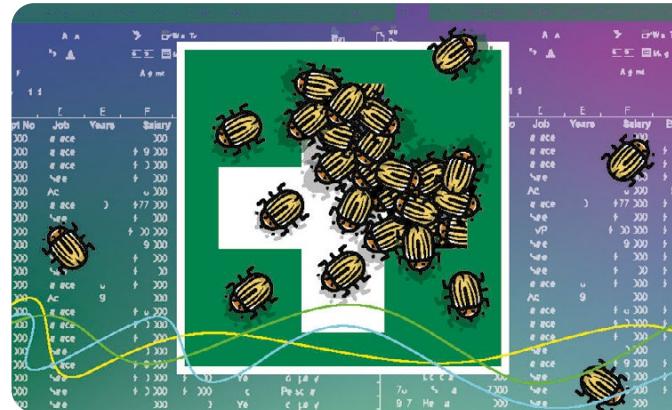
16

### SSSCP juht: Venemaa tegutseb küberruumis varjatumalt

Millised ründekatsed on õnnestunud ära hoida, saame teada intervjuust Ukraina side- ja teabekaitseteenistuse (SSSCP) juhi brigaadikindral Oleksandr Potiga.



Foto: SSSCP



18

### Hiiglasliku andmelekke õppetunnid

Elmise aasta alguses tungisid kurjategijad Allium UPI serverisse ning varastasid seal sadade tuhandete eestlaste andmed.

20

### Vene luure kübersurve lääneriikidele kasvab

Eesti riigiasutusi 2020. aastal tabanud küberruünakud omistati Venemaa sõjaväeluure (GRU) väeosale 29 155.

24

### Õngitsejad ise konksu otsas

Rahvusvahelise politseioperatsiooniga suleti õngitsuskelmidele teenuseid pakkunud platvorm LabHost. Eesti politsei oli haarangu ettevalmistamisel kandev roll.

26

### Ummistusründed: rohkem kisa, vähem villa

Registreerisime rohkem ummistusründeid kui kunagi varem, kuid tänu kaitsemeetmetele langes möjuga rünnakute osakaal.

28

### Petturid lahkusid miljonitega

Kahjustid kokku lüües peame taas tõdema, et lõppenud aasta oli petturitele edukas.

32

### Lunavara ohvrid, koolid ja ettevõtted

Nii ettevõtetes, koolides kui ka hambaravikeskuses avastati, et ründaja on tunginud nende süsteemidesse ja andmed lukustanud.

**34**

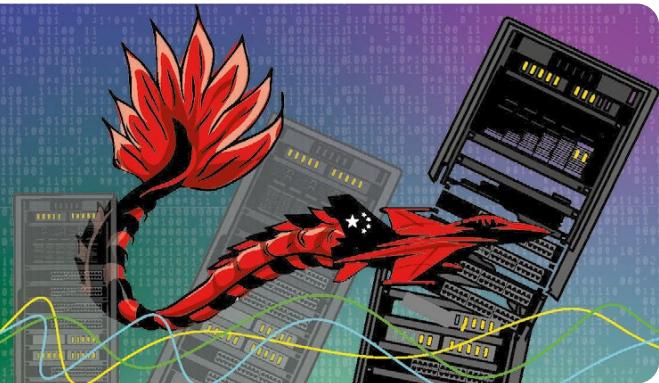
### **2024 tõi rekordarvu turvanörkuseid**

Ründajate röömuks pole haavatava tarkvara kasutajatel selle uuendamisega kiiret.

**36**

### **2024: sündmused rahvusvahelises küberruumis**

Mõjutustegevus valimiste ümber, Hiina häkkerid telekomiettevõtetes ja CrowdStrike'i põhjustatud ulatuslik katkestus IT-süsteemides.



**40**

### **Punane draakon sirutab tiibu**

Hiina eesmärgile saada 2050. aastaks maailm juhtivaks jõuks aitavad omalt poolt kaasa selle riigi küberrühmitused.

**42**

### **Küberturvalisus on Eesti riigi jätkusuutlikkuse küsimus**

Küberturvalisus pole pelgalt IT-probleem, vaid riigi jätkusuutlikkuse küsimus, kirjutavad **Taavi Viilukas, Irina Klementi ja Kaido Tee** justiits-ja digiministeeriumi riikliku küberturvalisuse osakonnast.

**44**

**44**

### **Eesti koolid küberturvaliseks**

Koolide tase on küberturvalisuse osas üsna köikuv ja tervikuna pole olukord eriti rõõmustav.

**48**

### **Ennetustegevused: vanavanematest lasteni**

Korraldasime õpitubasid vanematele, kampaania noorematele ning andsime välja juhendmaterjalid lastele ja nende vanematele.

**50**

### **ELi sammud küberturvalisuse vallas**

Mida Euroopa Liit 2024. aastal küberturvalisuse vallas korda saatis ning mida on oodata 2025. aastast?

**52**

### **Kuidas teha Eesti küberpiir lühemaks?**

Kuna kümne aastaga on riiklike andmekogude arv peaaegu kolmekordistunud, on piknenud ka meie küberpiir, mis vajab valvet ja kaitset.

**54**

### **E-hääletus: 20 aastat arengut**

2025. aasta oktoobris toimuvad kohaliku omavalitsuse volikogu valimised tähistavad e-hääletamise 20. aastapäeva.

**56**

### **Mida oodata 2025. aastalt küberruumis?**



# Küber turvalisem EESTI ALGAB SINUST

Kuidas tulla toime rekordilise arvu küber rünnakute ja turvanõrkustega, millega eelmisel aastal silmitsi seisime? Alustada tuleb endast ja seejärel aidata lähedasi, kirjutab **Gert Auväärt**, RIA peadirektori asetäitja küber turvalisuse alal.

**A**lustame positiivse noodiga. Möödunud aastal tegi meie elu tehnoloogia valdkonnas suure hüppe edasi. See avas uusi võimalusi majanduses ja teaduses. Samas toetub see võidakäik järjest keerulise male digitaalsele infrastruktuurile, mis omakorda loob üha uusi võimalusi ka küber kurjategijatele.

Kümme aastat tagasi ei osanud keegi karta, et küber kuritegevus võtab sellised mastaabid – praeguseks on tegu maailma suuruselt kolmandaks „majandusega“ USA ja Hiina järel.

Oleme jõudnud ajajärku, kus igaüks – olgu ta üksikisik, ettevõte või riik – peab vaatama küber turvalisust ühe esmavajadusena. Kui astud tänavale, siis ju kontrollid, kas rahakott ja võtmed on turvalises kohas, sama tähelepanelikkust eeldame kõigilt ka nutiseadet või arvutit kasutades, tagamaks nii andmete kaitset.

## KAITSEME EESTI DIGITAALSET PIIRI

Riigi infosüsteemi amet (RIA) arendab ja haldab Eesti digiriigi põhialuseid, osutades samal ajal keskelt riigi küber turvet. RIA reageerib ohtudele, ennetab probleeme ja kaitseb meie

digitaalseid piire. Tagamaks Eesti vastupanuvõime digiriigina, on vaja ühendada strateegiliselt küber turvalisus kõikidesse tegevusvaldkondadesse, arvestades kohalikke eripärasid ka rahvusvahelises koostöös. Lisaks riiklike teenustele kaitsmisele panustab RIA kriitilise infrastruktuuri vastupidavusse ja elanike teadlikkusse küberohitudest.

Uus Eesti küberstrateegia 2024–2030 keskendub just nende eesmärkide saavutamisele. Muutunud julgeolekuolukord nõuab, et vaataksem üle küber turvalisuse, teabekaitse ja kriisiohje seadused, et need vastaksid parimatele praktikatele ja tagaksid Eesti riigi teenuste toimimise.

## REKORDILISELT KÜBER RÜNNAKUID

RIA registreeris möödunud aastal Eestis rekordilised 6515 mõjuga küberintidenti. Maailmas registreeriti rekordilised 40 287 turvanõrkust, mida saab küber rünnakuteks ära kasutada – tegemist pole pelgalt arvuga, vaid hoiatusega, et kurjategijate võimalused ja rüündepind suurenevad ning ohupilt halveneb.

Häkkerid tungisid USA telekomiettevõtetes-



Gert Auvärt

Foto: Jaku Farra

se, Rumeenias pidid ametivõimud presidendi-valimiste esimese vooru tühistama ning maailmamajandust raputasid suured andmelekded ja tarkvaravead. Kübellünnakud pole enam pelgalt tehnoloogiline probleem – need mõjutavad valimisi, majandust ja isegi ühiskondade põhistruktuure.

Eesti on digitaalne edulugu, mis on meile toonud ka suure vastutuse. Meie riiklike andmekogude kolmekordistumine viimase kümnendi jooksul on suurendanud ründepinda ning röhutab vajadust jagatud ja töhusate küberturbelahenduste järele. Ja seda nii erasektori kui riigi poolt. Siin tulebki mängu RIA: pakkudes selliseid keskseid teenuseid nagu X-tee ja autentimisteenus, aitame vähendada dubleerimist ning võimaldame asutustel keskenduda oma põhitegevusele.

Kindlustunnet loob ka maailmas ainulaadne RIA küberreserv, mis koosneb RIA ja teiste riigi IT-majade ekspertidest, samuti Kaitseväe küberkaitseüksuse liikmetest. Kui kriitiliselt tähtsad teenused on ulatusliku küberintsidendi töltu häiritud ning teenuseid pakkuv asutus või ettevõte jäab olukorra kiirel lahendamisel oma joududega hätta, siis on võimalik kutsuda appi

küberreserv. See ei eksisteeri pelgalt paberil, vaid on praeguseks kolmel korral ka kögil kolmel tasandil aktiveeritud ja suurtel õppustel ristset saanud.

## IGAÜHEL ON ROLL KÜBERTURVALISUSES

Küberturvalisuse keskmes on inimesed. Iga üksikisiku või ettevõtte andmed ja vara on kaitstud niivõrd, kuivõrd head on nende teadmised küberhügieenist. Just seetõttu keskendusime möödunud aastal oluliselt kübereadlikkuse töstmisele: korraldasime vägagi hästi vastu võetud õpitube vanemaealistele, pakkusime noortele suunatud juhendeid ning uuendasime ennetusportaali itvaatlik.ee, kuhu lisasime praktilisi nõuandeid petuskeemide vältimeks ja intsidendist teavitamiseks. Köik ei peagi ise olema eksperdid, aga on hea, kui info on hõlpsalt leitav. RIA loodud kübertest on kahe aastaaga aidanud rohkem kui 21 000 inimesel täieda oma teadmisi küberhügieeni vallas, muutes selle oluliseks tööriistaks ka ettevõtetele ja asutustele.

Iga üksikisiku või ettevõtte andmed ja vara on kaitstud niivõrd, **kuivõrd head on nende teadmised küberhügieenist.**

Tehnoloogia areng ja küberkurjategijate oskuste tõus viitavad sellele, et tulevikus seisame töenäoliselt silmitsi veelgi keerukamate ohtudega, sealhulgas tehisintellekti kasutamise ja suurenendu andmeleketeega. Kestlik turvalisus nõub küberturvalisuse integreerimist kõigisse protsessidesse ja igaühe ellu.

Seekordne aastaraamat on rohkem kui lihtsalt ülevaade sündmustest. See on kutse tegutsemisele – iga inimese, organisatsiooni ja riigi tasandil. Ainult koostöös suudame tagada, et Eesti küberrumu oleks mitte ainult kaitstud, vaid valmis ka tuleviku väljakutseteks. ●

# VEEL ÜKS REKORDI- AASTA, mida polnud vaja

Seda, et 2024. aasta tuleb küberruumis vaikne ja rahulik nagu pühapäeva hommik Eesti väikelinnas, ei oodanud meist keegi. Aga me ei osanud arvata ka seda, et CERT-EE registreeritud mõjuga intsidentide arv rekordkõrgelt tasemelt kahekordistub.

**K**ui 2023. aastal saime kirja 3314 mõjuga intsidenti, siis eelmisel aastal 6515. Ööpäev läbi valves olev CERT-EE seisretiim registreeris iga päev keskmiselt 18 intsidenti. Mille arvelt see kasv tuli?

## PETULEHTEDE JA ÖNGITSUSTE TUULES

Õnneks mitte selliste juhtumite arvelt, mis oleks meie ühiskonda alustaladeni raputanud ja mõjutanud korraga sadade tuhandete inimeste elu.

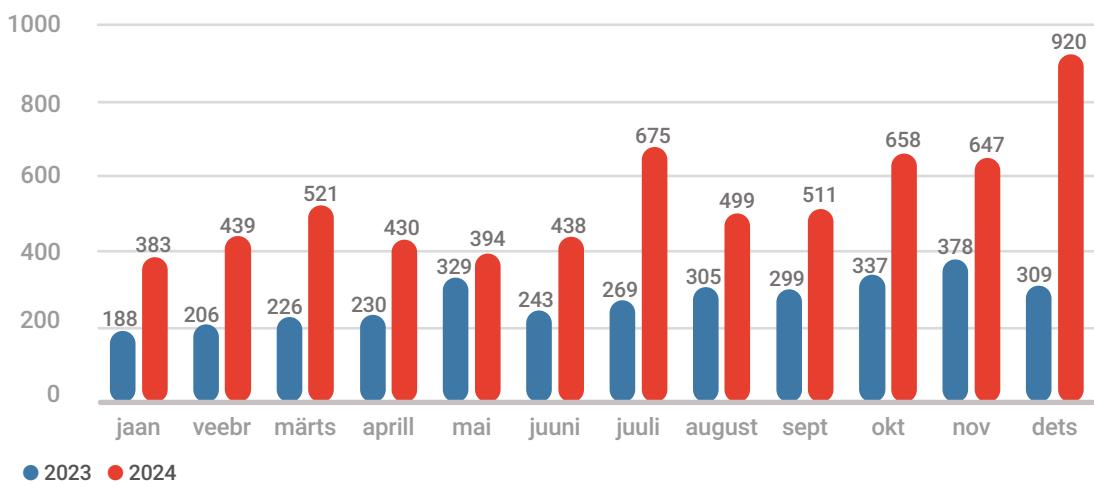
Nii nagu varasematel aastatel, moodustasid mullugi suurima osa mõjuga intsidentidest kõik-võimalikud öngitsus- ja petulehed. Nende hulk kasvas aastaga ligi 2,5 korda ja osakaal kerkis varasema poole pealt kahele kolmandikule.

Öngitsuste ja pettuse vallas on pilt kirju kui lapitekk. On klassikalisi pettusi, kus kasutajale näidatakse tema kodupanga omaga ärvahetamiseni sarnast petulehte. Kui ohver arvab, et PIN-koodi sisestades pääseb ta ligi oma kontolle, siis tegelikult avab ta seda tehes ukse pettuteile, kes samal ajal ehtsal pangalehel ohvri rahale küüned taha ajavad. Kui ohvri taskud on tühjaks tehtud, piüüavad nad vahel võtta tema nimel ka laenu ja sellegi enda kontrolli all olevalle kontole kanda.

Jätkuvalt levivad tuntud kullerifirmade nimel saadetavad petukirjad ja -sõnumid, mis meelitavad pakki kättesaamiseks libalehele oma pangakaardi andmeid sisestama. Õnge lähevad ka need, kes pole ammu ühtki pakki tellinud, aga



## Mõjuga intsidentide hulk kuude lõikes



● 2023 ● 2024

paraku meenub see alles hiljem, kui kontoväljavõtet uurides selgub, et lahkunud pole lubatud paar eurot, vaid sajad või tuhanded eurod.

Lisaks neile leidsime möödunud aastal kuhjaga investeeringispettuste lehti, mis kutsuvad muinasjutuliste tootlustega. Pärast vahapealset mõõna on aktsiate kõrval taas kuum kaup kõik-

**Kui aga ühel päeval tekib tahtmine oma algne rahapaigutus koos rammusa lisaga välja võtta, algab lõputu venitamine ja lisatingimuste seadmine.**

võimalikud krüptovääringud, üks eksootilisem kui teine. Enamasti alustatakse petulehtedel „investeeringisega“ tasa ja targu: esmalt riskitakse mõnekümne või mõnesaja euroga. Kui see kosub mõne nädalaga poole võrra ja algne summa koos lisandunud tootlusega õnnestub oma kontole kanda, kasvavad enesekindlus ja ahnus sama tempoga nagu närvuvad ettevaatlikkus ja kriitikameel. Teisele ringile minnakse väiksema umbusu ja suurema summaga.

Kuna ekraanil kerkib investeering kui pärmitaigen, innustab see raha veelgi lisama. Mõnel juhul panustatakse lisaks enda säästude-

le laenuraha. Kui aga ühel päeval tekib tahtmine oma algne rahapaigutus koos rammusa lisaga välja võtta, algab lõputu venitamine ja lisatingimuste seadmine. Mõnel juhul nõutakse raha väljavõtmiseks uusi sissemakseid, kuid reeglinäätavat petturite saagiks ka need. Raha sealset koju ei tule ja mõne aja möödudes kaob internetiavarustest ka veebleht, mille kaudu pettus toime pandi.

Selliste lehtede avastamise järel saab CERT-EE nende majutajatele palve petulehed maha võtta, et ohvrite hulka piirata, aga ega meie silmad ja käed kõikjale ulatu. Seepärast on esmatähtis siiski tavakasutajate teadlikkus varitsevatest ohtudest ja kriitiline meel. Kõikvõimalike pettuse kohta loe lähemalt lk 28.

### TEENUSEKATKESTUSI IGASSE PÄEVA

Õngitsuste ja pettuse järel moodustavad kolmenda suure rühma teenusekatkestused, mida registreerisime eelmise aasta iga päeva kohta keskeltläbi kaks. Sageli pole nende põhjuseks pahatahtlik rünne, vaid seadme- või tarkvara-riike või hoopis heatahtlik arendaja või administraator, kes mõnd toodet või teenust seadistades tahtis parimat, aga välja kukkus teisiti.

Sinna kategooriasse langeb eelmise aasta kurikuulsaim tarkvaraauendus, mille tagajärjeks oli ajaloo üks suuremaid IT-katkestusi. 19. juuli varahommikul saatis CrowdStrike väl-

ja uuenduse oma turbetarkvarale Falcon Sensor, mida kasutavad eelkõige suuremad ettevõtted ja asutused, et kaitsta arvuteid pahavara ja muude ohtude eest. 8,5 miljonit Windowsi arvutit, milleni see viga-ne tarkvaraauendus jõudis, jooksid kokku ja lõpetasid koostöö, näidates kasutajatele nn sinist surmaekraani.

Seetõttu jäi ära üle 5000 lennu, paljud pangad Brasiliast Uus-Meremaani teatasid teenusekatkestustest, oli häireid hädaabinumbrite ja haiglate töös, osa tele- ja raadiojaamu ei saanud oma programme edastada, tanklates ei saanud kütuse eest maksta... Seda nimekirja võiks pikalt jätkata. Süsteemide taastamine võttis nädalaid, sest nõudis käsitööd. Kui püüti selle vea põhjustatud kahjusid kokku liita, jõuti kiirelt 10 miljardi dollarini.

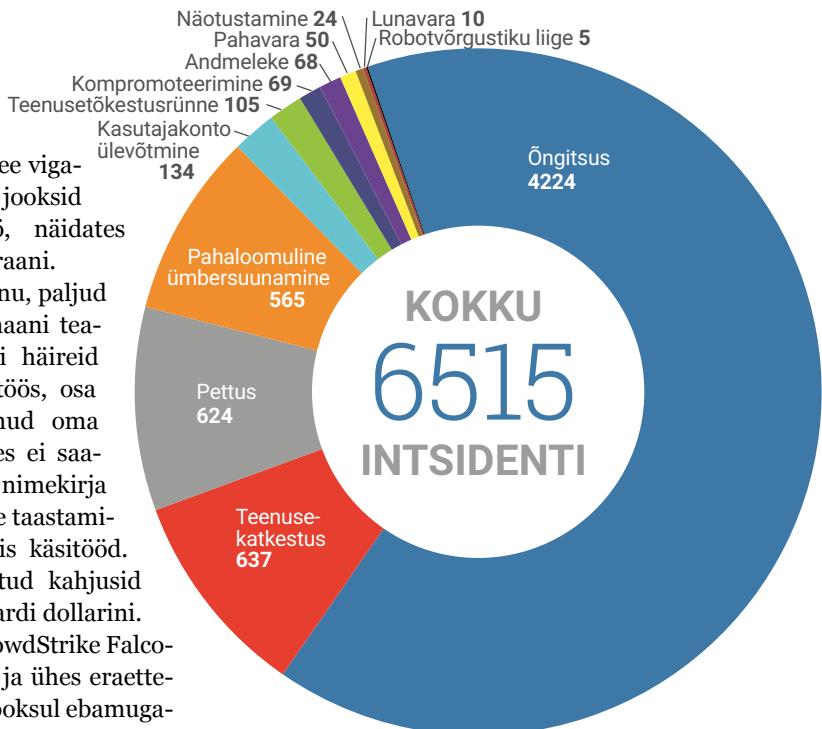
Eestil vedas, kuna siin on CrowdStrike Falconi kasutajaid vähe. Ühes riigi- ja ühes eraettevõttes tekitas see mõne tunni jooksul ebamugavust ning Tallinna lennujaamas tuli Ryanairi lendudele reisijaid registreerida käsitsi, mistõttu kulus selleks tavapärasest rohkem aega, aga muus osas pääsesime.

**Pärast CrowdStrike'i kahetsusväärset juhtumit kõlanud küsimustele, kas tarkvaraauendustega tasub kiirustada, oli ja on meie vastus „jah“.**

Pärast seda kahetsusväärset juhtumit kõlanud küsimustele, kas tarkvaraauendustega tasub kiirustada, oli ja on meie vastus „jah“. Uuendustega viivitamisest tekkivad riskid on oluliselt suuremad. Nende kohta saab lugeda lk 34.

Kui CrowdStrike'i põhjustatud katkestustest pääsesime, siis teise tundud küberturbefirma Cloudflare'i tõrgete tõttu oli septembri kolmandal esmaspäeval häireid ligi 200 avaliku sektori veebilehe töös, millele RIA ummistusrünnete vastu kaitset pakub.

## Mõjuga intsidendid 2024. aastal



Mobiilioperaatoritel oli törkeid nii andmekui ka kõnesidega, sealhulgas hädaabinumbrega. Juhul, kui koduoperaatori võrgus on

probleeme, aga on vaja kohe hädaabinumbriile helistada, tuleks telefonis eemaldada SIM-kaart. Sel juhul kasutab telefon 112-le kõne-de tegemiseks mõne teise operaatori võru.

Oli häireid riikliku autentimisteenuse TARA, Smart-ID, mobiil-ID ja ID-kaardi töös. Enamasti polnud katkestused piinavalt pikad või sattusid öisele ajale, mil enamik meist magab, mitte ei anna digiallkirju ega sisene internetipanga.

### ROHKEM UMMISTUSRÜNDEID, VÄHEM KAHJU

Veebilehed ja teenused võivad olla kättesaadud ka ummistusrünnete tõttu. Nende tõrjumisel ei lastud meil eelmisel aastal hing tõmmata. Suurem ründeaktiivsus algas pärast Venemaa algatatud täiemahulise sõja algust Ukrai-

## Mõjuga intsidentide hulk kahekordistus



nas ja on seal alates aasta-aastalt kasvanud. 2024 purustas rekordid nii rünnakute hulga kui ka nende mahu poolest. Ühe avaliku sektori veebilehtede vastu suunatud rünnakulaine käigus tehti nelja tunniga ligi kolm miljardit pahaloomulist pärtingut – tavaolukorras oleks sellise mahu täitumiseks pidanud ootama üle veerandsaja aasta.

Kui 2022. aastal oli edukas iga kolmas rünnak, siis mullu langes mõjuga ummistusrünnete osakaal 18 protsendile.

Ent rünnakute hulgast ja mahust olulisem mõõdik on nende mõju. Selles osas on meil pigem häid uudiseid: kui 2022. aastal oli edukas iga kolmas rünnak, siis mullu langes mõjuga ummistusrünnete osakaal 18 protsendile. Mõne veeblehe töös oli rünnakute töttu lühiajalis katkestusi või toimisid need tavapärasest aeglasemalt, aga suurt kahju ei õnnestunud nendega tekitada. Teenusetökestusrünnetest ja nende tagajärgedest kirjutame lk 26.

### LEKKISID ÜLE 700 000 INIMESE ANDMED

Eelmisel aastal registreerisime 68 andmeleket, mida on ligi poole rohkem kui 2023. aastal. Küll selgus, et eksamite infosüsteemi GitHubi

lehel olid testandmete asemel kõigile kättesaadavad sadade inimeste isikuandmed, küll võis jäätmejaama iseteeninduses näha lisaks enda andmetele kõigi teiste klientide tehinguid ja isikukoode.

Ent kui kõik teised möödunud aasta lekked kokku liita, kahvatub tulemus apteegi- ja haigla-kaupadega tegeleva ettevõtte Allium UPI juhumi kõrval. See ettevõte haldab Apotheeka, Apotheka Beauty ja Pet City kliendi-kaardisüsteemi, kus hoitud andmetele said ründajad ligi. Eduka ründe käigus varastati ligi 700 000 isikukoodi, üle 400 000 e-posti aadressi, kümned tuhanded telefoninumbrid ja koduseid aadresse. Info pärines kliendibaasi varukoopiast, kus hoiti andmeid aastatest 2014–2020. Need, kelle andmed

selle rünnaku käigus varastati, peaks olema kõikvõimalike pettuse ja öngitsuste osas varasemast veel ettevaatlikumad. Sellest kahetsusväärsest andmelekkest loe lähemalt lk 18.

### RÜNNAK SULARAHARINGLUSE VASTU

Erinevalt Apothekast, mille kliendiandmed lekkisid, pole Hansab ettevõte, mida paljud nimepidi teavad. Kuid vähe on neid, kes selle teenustega kokku ei puutu. Hansab täidab Eestis Swedbanki, Luminori ja LHV sularahaautoomaate, viib pensione koju, väljastab koostöös politsei- ja piirivalveametiga ID-kaarte ja passeening teeb taustal palju muud olulist. Teisisõnu: kui nende teenuste töö üleöö katkeks, tunneks seda peaagu kõik.

1. märtsi lõuna paiku hakkasid Hansabi serverid ootamatult taaskäivituma. See, et midagi on väga valesti, sai selgeks mõne minutiga. Hädaabinõuna ja suurema kahju ärahoidmiseks ühendati end internetist lahti ja isoleeriti võrk. Ent suur kahju oli juba sündinud: selgus, et kustutatud oli kogu ettevõtte virtualiseerimiskeskond – ründaja oli jöudnud süsteemi Püha Graalini, nagu Hansabi juht Kristo Timberg ajakirjanduses meenutas.

Kriis räsis ettevõtet, aga see ei kasvanud riiklikuks hädaolukorraks. Sularaha Eesti pangautomaatidest ega kauplustest otsa ei lõppenud ja need, kes ootasid kuu alguses koju oma pensioni, selle ka said. Paljude teenuste tagamiseks – sealhulgas sularahaautomaatide haldamine, kaubandusvõrgust toodud sularaha töötlemine ja klientide kontodele kandmine – mindi üle nn käsijuhtimisele.

Sel korral läks suhteliselt hästi, aga pikemate maksehäirete ja sularaharingluse katkestuste puhuks tasuks varuda sularaha, et maksta ühe nädala hädapärase kulutuste eest.

## KURITÖÖ JA KARISTUS

Kui vahel võib tekkida arvamus, et küberruumis tegutsedes on kurjategijad anonnüümsed ja seadusesilm nendeni ei jõua, siis möödunud aasta pakkus küllaga vastupidiseid näiteid, mis selle müüdi kummutavad.

Eelmises aastaraamatus kirjutasime, kuidas geenitestimise ettevõtte Asper Biogene'i süsteemidest varastati ligi 10 000 inimese andmed, sealhulgas geeni- ja terviseandmed.

Politsei alustas kriminaalmenetlust, mille käigus kogutud töendid viitavad, et kahe kuu jooksul toimetas neljaliikmeline grupp andmete varastamise nimel visa järjekindlusega. Esmalt otsiti ja leiti süsteemist turvaauk, mille kaudu saadi ligi infosüsteemi kasutajatunnustele ja parooliräsidele ehk krüpteeritud salasõnadele. Järgmise sammuna murti ühe töötaja parooliräsi lahti ja tema kontoga süsteemi sisenedes paigaldati sinna pahavara. Selle abil saadi ligi ka tundlikele terviseandmetele ja laaditi need alla. Seejärel esitati 45 000-eurone lunarahanõue.

Rünnaku taga olnud rühmituses kandis juhivat rolli Venemaa Föderatsiooni kodanik

Vladislav Rõbakov, kelle reisisihtkohtade valik kuivas kokku, kuna seoses Asper Biogene'i vastu tehtud küberriündega on ta nüüd rahvusvaheliselt tagaotsitav.

Asper Biogene'i andmelekke järel algatas paralleelselt menetluse ka andmekaitse inspektsioon, mis leidis, et ettevõtte infoturbes oli tõsiseid puudujääke ning määras rikkumiste eest 85 000 eurot trahvi. Nende lausete kirjutamise ajal polnud otsus veel jõustunud.

2020. aastal tabas Eesti riigiasutusi rünnak, mille käigus varastati majandus- ja kommunikatsioniministeeriumi haldusalast 350 GB jagu andmeid ja sotsiaalministeeriumi haldusalast info ligi 10 000 koroonasse nakatunu kohata. Kaitsepolitsei ja keskkriminaalpolitsei joudsid rünnakuid uurides kolme meheni, kes olid

.....

**Pikemate maksehäirete ja sularaharingluse katkestuste puhuks tasuks varuda sularaha, et maksta ühe nädala hädapärase kulutuste eest.**

.....

rünnaku ajal Venemaa sõjaväeluure (GRU) palgal: väeosaga 29 155 küberküsst juhtinud koloneli Juri Denissovi ning tema alluvate Nikolai Kortšagini ja Vitali Ševtšenkonni. Nemadki on nüüd rahvusvaheliselt tagaotsitavad. Sel teemal saab pikemalt lugeda lk 20.

Eelmisel aastal mõistis Harju maakohus reaalse vanglakaristuse Tallinna noormehele, kes müüs kurjategijatele öngitsuskomplekte ja nõustas neid rünnete läbiviimisel. Tema tööriist, mida ta suhtlusrakenduse Telegram vahendusel müüs, oli spetsialiseerunud kaheastmelisest autentimisest möödapääsemiseks. See võimaldas kurjategijatel öngitseda inimeste kasutajatunnuseid ning seeläbi ligipääse Microsoft 365, PayPali, Google'i, Yahoo, Dropboxi ja Binance'i kontodele.

Sellest, kes olid Allium UPI ja Hansabi vastu sooritatud rünnakute taga, loodame kirjutada mõnes järgnevas aastaraamatus. Seniks aga olgem IT-vaatlikud! ●

# UKRAINA SODA: küberründed tulid rindejoonele lähemale

Möödunud aasta 19. novembril täitus tuhat päeva Venemaa täiemahulise sissetungi algusest Ukrainasse, sellest kauemgi on kestnud võitlus küberruumis, mis toetab sõjalisi eesmärke.

Kriitiliste ehk väga suure mõjuga intsidentide arv oli 2024. aastal languses, intsidentide koguarv ning ründed valitsusasutuste ja kohalike omavalitsustele vastu aga tõusid. Jätkuvad tavapäraselt küberkuritegevus rahalistel eesmärkidel, riiklike sidemetega rühmituste ründekatsed kriitilise infrastruktuuri vastu ning varjatud ründed küberluure eesmärgil.

## KÜBERRÜNDED TOETAVAD SÕJALISI EESMÄRKE

Tähelepanuväärsse trendina võib esile tuua küberrünnete järjest süsteemsema rakendamise sõjaliste eesmärkide toetuseks. Julgeolekuja kaitsesektorivastaseid küberründeid tehti rohkem kui aasta varem ning vaenlane tõhustas viise koguda luureinfot Ukraina kaitseväelaste seadmete kaudu.

Küberturbeettevõtte Mandiant analüütikud kirjutasid Vene riikliku taustaga rühmituse

APT44 järjepidevast tegevusest langenud Ukraina kaitseväelaste telefonide ja muude varastatud seadmete häkkimisel ning sealт vestluste ja andmete kasutamisel. Et jälgida vägede liikumist ja logistikaahelaid, on vaenlase kübertegevused seega kolinud kohati otse rindejoonele.

Nii kaitseväelaste kui ka tsiviilelanike puhul on järjest levinumaks ründevektoriks erinevad suhtlusrakendused. Nende kaudu levitatakse pahavara nii rahalise kasu kui luure eesmärgil, samuti on kompromiteeritud rakenduste abil võimalik määrata kasutajate, näiteks sõjaliste üksuste asukohaandmeid.

Seetõttu otsustas Ukraina rahvusliku julgeoleku ja kaitse nõukogu septembris keelustada Telegrami kasutamise valitsusasutuste, kaitsesektori ja kriitilise taristu ettevõtete töötajate seadmetes. Piiranguga tuli omal initsiatiivil kaasa Kiievi riiklik ülikool, mis keelas Telegrami ülikooli töötajatele ning soovitas ka tudengi-



tel selle kasutamist vähendada. Siiski on Telegram jätkuvalt Ukrainas üks peamisi suhtlus- ja uudisteplatvorme ning ka pärast piiranguid jäeti selle kasutamise võimalus alles neile ametiisikutele, kelle roll nõuab pidevat avalikkusega suhtlemist.

#### SEE ÖNNETU DETSEMBER

Samamoodi nagu 2023. aastal, toimus Ukraina elanikele köige tuntavama mõjuga küberruunnak läinud aasta detsembris. Sel korral rünnati ligi 60 riiklikku andmebaasi ja registrit, millest sõltuvad inimestele vajalikud digitaalsed teenused: sünni- või surmatõendite väljastamine, abielu registreerimine, kinnisvaratehingud, pärimistoimingud ja kõikvõimalikud muud notariteenused. Mõjutatud olid ka riigipiidi Diia mitukümmend teenust, mis ei saanud vajalike andmebaasidega ühendust. Ründe üksikasjade kohta on raamatut trükki minemise ajal teada üsna vähe, ent Ukraina ametivõimud kahtlustavad Vene sõjaväeluure seotust.

Ehkki mõneks ajaks tuli üle minna paberile ja pliiatsile, suudeti osa teenuseid uue aasta alguseks taastada ning ka ülejäänute puhul on eba-mugavused tänu varukoopiatele loodetavasti ajutised.

#### Mis on APT44?

- ➥ Vene sõjaväeluurega seotud tehniliselt kõrgetasemeline häkkerirühmitus, tuntud ka kui **Sandworm**.
- ➥ Üks peamisi riikliku taustaga küberohustajaid Ukrainas, kuid tegutseb ka mujal.
- ➥ Aktiivne nii kriitilise taristu häiringute, küberluure kui ka mõjuoperatsioonide vallas.
- ➥ Aastatel 2015 ja 2016 ründas Ukraina elektrivõrku, põhjustades voolukatkestuse sadadele tuhandetele inimestele.
- ➥ Aastal 2017 ründas Ukraina vörke **NotPetya** hävitusvaraga, mis levis kiiresti üle maailma ja põhjustas hinnanguliselt 10–11 miljardit dollarit kogukahju.
- ➥ 2024 kevadel proovis rünnata Ukraina energia- ja veevarustustaristut, ent ukrainlastel õnnestus see katse törjuda.

Küll aga annab rünnak tunnistust sellest, et täiemahulist vallutussõda läbi viiv agressor püüab jätkuvalt rünnata ja kahjustada ka riigi elutähtsat tsiviiltaristut. ●

# SSSCIP JUHT: Venemaa tegutseb küberruumis varjatumalt

---

Millised ründekatsed on õnnestunud ära hoida, saame teada intervjuust CERT-EE hea koostööpartneri, Ukraina side- ja teabekaitseteenistuse (SSSCIP) juhi brigaadikindral **Oleksandr Potiga**.

---

Kuidas on Vene küberrünnevõimed 2024. aastal arenenud? Milliseid muutusi märkate vörreltes eelmise aastaga?

2023. aastal nägime Vene häkkerirühmituste hävitavaid küberründeid, mis olid suunatud IT-ettevõtete ja telekommunikatsiooniettevõtete vastu. 2023. aastal kannatas hävitavate rünnete all vähemalt 11 internetiteenuse pakkujat, rünnete kulminatsiooniks oli küberrünnak Kyivstarile 2023. aasta detsembris. Kõigi nende rünnetega kaasnesid lekked ja andmete avaldamine Vene sotsiaalmeediavõrgustikes.

2024. aastal hakkas Venemaa jätk-järgult loobuma küberrünnete avalikust esiletoomisest. Fookus on nihkumas küberluureoperatsioonidele sõja ja poliitikaga seotud süsteemides, kus eesmärk on võimalikult kaua märkamatuks jäädva. Sihtmärgid on Ukraina julgeoleku- ja kaitsesektor ning ettevõtted, mis neid otsestelt toetavad.

Lisaks on 2024. aastal märgatavalts kasvanud Vene rahaliselt motiveeritud rühmituste tegevus – sihitud küberründed suurtele organisatsioonidele ning erinevad petuskeemid raha omistamiseks. Usume, et küberkuritegevusega seotud häkkerirühmitused tegutsevad Vene-

maa valitsuse juhtimisel või nõusolekul, kuna osa neist tegeleb nii rahavargustega kui ka täidab küberespionaaži ülesandeid.

**Kas olete näinud tehisaru poolt võimestatud küberründeid Venemaalt? Kas tehisaru laiem kasutamine on kaasa toonud mingi olulise muutuse?**

Võib öelda, et tehisaru juba kasutatakse küberriinnakute läbiviimiseks, näiteks ukrainakeelseste andmepüügimeilide loomiseks või häkkerite ja ohvrite vahelise suhtluse arendamiseks sõnumirakendustes või e-posti teel. Tehisaru komponentide kasutamine kasvab kindlasti veelgi.

**2024. aastal nägime vaid ühte laialt kajastatud rünnet Ukraina kritilise taristu vastu – see oli riigiregistrite rünne detsembris. Pole kahtlust, et vaenlane kriitilist taristut ründab, järelikult on teie kaitse enamasti olnud töhus. Millised kriitilised sektorid olid läinud aastal kõige suurema lõögi all?**

Töepoolest, 2024. aasta lõppes kõrge profiliiga ründega Ukraina justiitsministeeriumi registrite vastu. Samas katseid kriitlist taristut rünnata tuvastasime kogu aasta välitel.



Foto: SSSCP

Oleksandr Poti

Näiteks märtsis avastati **UAC-0002** (tuntud ka kui Sandworm) ettevalmistused küberrünnakuteks, mille eesmärk oli häirida umbes 20 energia-, vee- ja soojusvarustussektori ettevõtte võrkude stabiilset toimimist kümnes Ukraina piirkonnas. Küberrünnakud püüti läbi viia kompromiteeritud tarneahelate kaudu, täpselt Ukraina ettevõtete kaudu, kes arendavad spetsiaalset tarkvara tööstussüsteemide jaoks.

Tänu operatiivmeetmetele küberrünnakute ettevalmistuste tuvastamiseks ja kiirele reageerimisele suudeti need ründed ära hoida. Huvitaval kombel on selle tegevuse kuupäevad korrelatsioonis 2024. aasta kevadel Ukraina infrastruktuurirajatiste pihta tehtud raketirünnakutega. Ilmselt olid need küberrünnakud möeldud raketirünnakute mõju suurendamiseks.

Lisaks võib mainida küberintsidenti, kus ühes Ukraina energiasektori ettevõttes avastati uus, **FrostyGoopi** nime kandev spetsiaalne ründevara tööstussüsteemide vastu. See viitab taas sellele, et venelased täiustavad pidevalt oma tööriisti ja kavandavad edasisi küberrünnakuid kriitilisele taristule.

#### Kuidas iseloomustate Vene häktiviste, kes Ukrainat ründavad? Kas nad on eelköige lihtsalt tüütused või ikkagi arvestatav oht?

Me ei saa öelda, et Venemaa häktivistid annaksid kübersõtta märkimisväärset panust vörreledes juba tundt Venemaa riiklikult toetatud häkkerühmitustega. Siiski on oluline mõista, et sellises totalitaarses riigis nagu Venemaa

pole iseseisvaid häktiviste. Mingil määral on nad kõik kontrolli all ja töötavad Venemaa valitsuse heaks. Kasvav oht on see, et kõik need häktivistid on kaadrireserv Venemaa eriteenistustele, kes hakkavad neid lõpuks ka keerulise-matesse küberrünnakutesse kaasama.

#### Kas te näete nüüd, kus konflikti on kaasatud Põhja-Korea, ka küberruumis sealtkandist rohkem ründeid?

Praegu ei ole me tuvastanud ühtegi küberrünnakut, mida võiksime seostada Põhja-Koreast pärit häkkerühmituste tegevusega. Siiski ei saa välistada, et nad võivad mingil hetkel olla seotud küberoperatsioonide läbiviimisega, kuna Venemaa suhtlus Põhja-Koreaga kasvab iga päevaga.

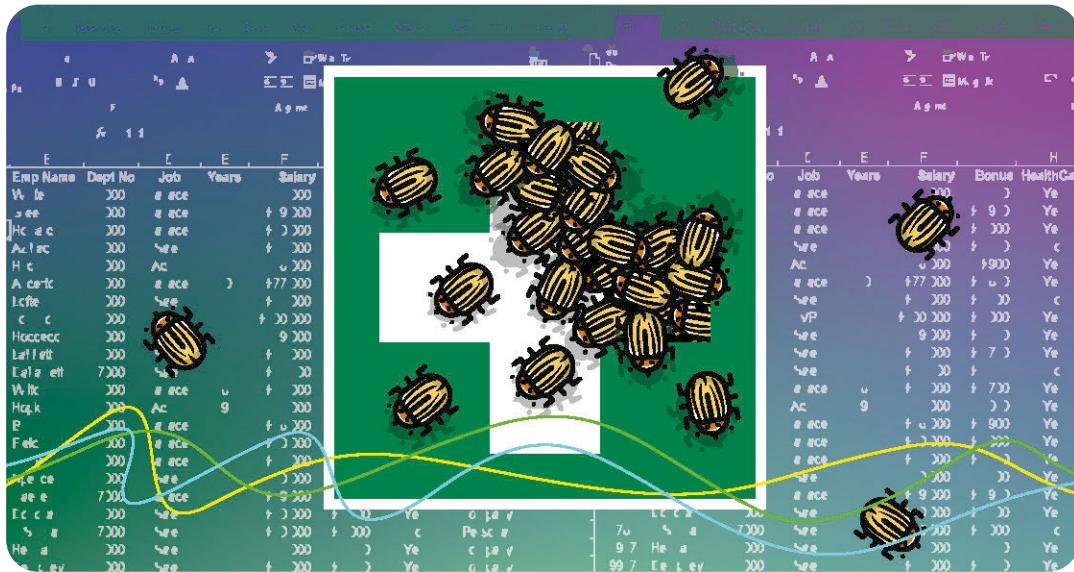
#### Mis on 2025. aastal teie meeles suurimad küberohud Ukrainas ja ka maailmas laiemalt?

2025. aastaks prognoosime Ukraina julgeoleku- ja kaitsesektori ning kaitsetööstuskompleksi vastu suunatud küberluureoperatsioonide kasvu. Arvestades, et Venemaa valmistub potentsiaalseks sõjaks NATOGa, intensiivistub ka küberluure liikmesriikide sõjaliste organisatsioonide vastu.

Lisaks sagenevad hävitavad küberrünnakud kriitilisele taristule ning need on korrelatsioonis füüsilise sabotaazi tegevusega, mida Venemaa on NATO liikmesriikide vastu juba alustanud.

Arvestades, et Venemaa valmistub potentsiaalseks sõjaks NATOGa, intensiivistub ka küberluure liikmesriikide sõjaliste organisatsioonide vastu.

Meil on märkimisväärne rahaliselt motiveeritud küberrünnakute arv Venemaalt Ukraina kommertsettevõtete vastu, mis kasvab jätkuvalt ja levib tõenäoliselt ka NATO riikidesse. Seda soodustab tehisaru kasutamine selliste küberrünnakute läbiviimiseks ja küberkurjategijate koostöö Venemaa valitsusega, mis pakub neile kaitset rahvusvahelise õigusemõistmise eest. ●



# Hiiglasliku ANDMELEKKE õppetunnid

Eelmise aasta alguses tungisid kurjategijad Allium UPI serverisse ning varastasid sealд andmed Apotheka, Apotheka Beauty ja Pet City klientide kohta. Lekkisid ligi 700 000 isikukoodi, üle 400 000 e-posti aadressi, kümned tuhanded telefoninumbrid ja kodused aadressid. Miks ja kuidas see juhtus?

**E**estis, Lätis ja Leedus apteegi- ja haiglakaupadega tegelev ettevõte Allium UPI andis 2024. aasta veebruaris nii politsei- ja piirivalveametile (PPA) kui ka riigi infosüsteemi ameti (RIA) intendentide käsitlemise osakonnale (CERT-EE) teada, et nende hallatavasse kliendikaardisüsteemi on ebbaseaduslikult sisenetud. Sissetungi järel laeti

alla seda lojaalsusprogrammi kasutavate ettevõtete Apotheka, Apotheka Beauty OÜ ja PetCity OÜ klientide isikukoode, ostuandmeid ja kontaktandmeid.

Alustatud kriminaalmenetluse käigus tuvatas PPA, et UPI andmebaasist laeti ebbaseaduslikult alla ligi 700 000 Apotheka, Apotheka Beauty ja Pet City kliendikaardi omaniku isiku-

koodi, üle 400 000 e-posti aadressi, ligi 60 000 koduaadressi ja umbes 30 000 telefoninumbrit. Mõnel juhul oli võimalik tuvastada ka ostetud käsimüügiravimeid ja muid apteegikaupu, kuid mitte ostetud retseptiravimeid. Kuna paroole, pangakaardi ega muid finantsandmeid kliendiprogrammis ei talletatud, ei saanud kurjategijad neid varastada. Info päringes kliendi-baasi varukoopiast, kus hoiti andmeid aastatest 2014–2020.

### MIKS SEE JUHTUS?

Tõsistest tagajärgedega küberriünnak ettevõtte või asutuse vastu algab sageli mõne töötaja kasutajakonto ülevõtmisest. Kasutajanime ja parooli teadasaamiseks võivad kurjategijad kasutada näiteks pahvara, mille töötaja tõmbab oma arvutisse nakatunud e-kirja manusega või kahtlastest kohast leitud piraattarkvaraga.

Selleks, et kurjategijad ei pääseks töötaja lekinud parooliga kohe süsteemi sisse, tuleb kasutada kaheastmelist autentimist. Samuti peaksid olema internetist ligipääsetavad ainult need infosüsteemid ja teenused, mille puhul see on tingimata vajalik, ja kõik need tuleks paigutada VPNi või muu turvalahenduse taha.

Et küberkuritegevus on väga rahvusvaheline, võivad lekinud andmed liikuda veel aastaid hiljem erinevate riikide ja grupeeringu vahel, kes neid erinevate küberriünnakute toimepanemiseks kasutavad.

### ANDMED ON ISIKLIK VARA

See juhtum tõi taas Eesti avalikkuse ette tundlike isikuandmete kaitse teema. Aja möödudes usaldavad aina rohkemad inimesed oma andmed aina enamate teenusepakkujate käte. Seda tehes loodavad nad, et teenusepakkujad panustavad tõsimeelselt nende antud andmete kaitsmisesse. Paraku see alati nii ei ole, kuid viimaste aastate sarnased intsidentid on siiski tõstnud nii ettevõtete kui inimeste teadlikkust ning tegutsemisvalmidust.

Samas tasub meil klientidena kriitiliselt suhtuda oma isikuandmete jagamisse, mh kliendikontode tarbeks. Väike soodustus või veidi mugavam asjaajamine ei pruugi seda riski väärta olla. ●

## Õppetunnid tormi silmast

**Selline kogemus on kui külm dušš,  
meenutab Allium UPI juhatuse liige  
Marika Pensa.**

Möödunud aasta talvel varastasid kurjategijad Apotheka kliendiandmebaasi varukoopia. Selle kahetsusväärse juhtumi järel pöörame ettevõtjana veel rohkem tähelepanu süsteemi turvalisusele.

Kurjategijad ei maga ja kasutavad ära iga nõrkuse, mis süsteemi peremehel võib olla teravdatud tähelepanuta jäänud.

Esimene õppetund on lihtne: turvalisuse tagamine ei lõpe kunagi, vaid on pidevalt jätkuv protsess. See on nagu jalgrattasõit ehk peab pidevalt edasi liikuma, et püsti jäada. Küberriünnaku ohvriks või sihtmärgiks sattunud ettevõttele on selline kogemus kui külm dušš, kuid samas ka meeldetuletus ja põhjus oma süsteemid üle vaadata. Küberturvalisus pole enam see, mille kohta inglise keeles öeldakse *nice to have*.

Veel üks õppetund juhtunust on, et kurjategija jaoks ei jagune maailm ettevõtluseks, riigiks, klientideks ja muudeks selgelt piiritletud osadeks. Ka töhus tegevus kuritegevuse vastu saab olla ainult ühendatud kollektiivkaitse, milles on oma roll nii üksiktöötajal, ettevõttel, riigil jne. Seepärast on meil väga hea meel, et oleme saanud teha töhusat koostööd Eesti riigiasutustega politsei- ja piirivalveametist riigi infosüsteemi ameti ja andmekaitse inspektsioonini. Me kõik saame aru, et oleme ühel pool rindejoont, mille teisel pool on rahvusvahelised kriminaalid. Loodame, et kuriteo toime pannud kurjategijad tabatakse ja võetakse vastutusele.

Küberkuritegevuse tõkestamine vajab jätkuvalt ja kasvavalt meie kõigi tähelepanu ja küsimus pole selles, kas see juhtub, vaid millal, millises mastaabis ja valdkonnas.

Pole kuulikindlaid inimesi ega süsteeme, kuid töhus kaitse väliste rünnete vastu võib päästa elu ja andmed.

# VENE LUURE kübersurve lääneriikidele kasvab

Põhjaliku uurimise tulemusena omistati mitmeid Eesti riigiasutusi  
2020. aastal tabanud küberrünnakud Venemaa sõjaväeluure  
(GRU) väeosale 29 155.

Juhumi niidiotsad hakkasid neli aastat tagasi hargnema sellest, et majandus- ja kommunikatsiooniministeeriumi (MKM) töötaja märkas oma arvutis kummaliisi anomalaiaid. Esmalt kahtlustas ta Eestis tollal massiliselt levinud pahavara. Kui aga arvuti puuhastamine probleemi ei lahendanud, teavitas ta juhtunust RIA intendentide käsitlemise osakonda (CERT-EE).

## PROBLEEM OLI SUUREM KUI ESMALT PAISTIS

Kiiresti selgus, et probleem on hoopis laiem. Ministeeriumi süsteemidesse oli ehitatud tagauks, mille kaudu oli välja viidud suures koguses andmeid – 350 gigabaiti. Riigisalused jäid küll puutumata, aga kurjategijate käte langes hulgaliselt ministeeriumi tööd puudutavat siseteavet: strategia- ja töödokumente, personaliinfot, kirjavahetust ettevõtetega jne.



Juri  
Denisssov



Nikolai  
Kortšagin



Vitali  
Šeštšenko

Küberruumis jälgjajades avastati, et samasuguse käekirjaga rünnakud olid toimunud veel mitme asutuse ja ettevõtte, sealhulgas välisministeeriumi ning tervise ja heaolu infosüsteemide keskuse (TEHIK) vastu. Kui ministeeriumi veebiserveritest said kurjategijad käte ainult avalikke andmeid, siis TEHIKu süsteemides pääsesid nad ligi umbes 10 000 koroonaviirusesse nakatunud inimese isikuandmetele.

Süüdlaste väljaselgitamiseks viisid kaitsepolitsei ja keskkriminaalpolitsei läbi uurimise, mis jõudis välja kolme meheni, kes olid rünnaku ajal olnud GRU teenistuses: väeosaga 29 155 küberüksust juhtinud koloneli **Juri Denissovi** ning tema alluvate **Nikolai Kortšagini** ja **Vitali Šeštšenkoni**. Harju maakohus võttis Venemaal elavad kahtlusulased 2024. aasta sügisel riigiprokuratuuri taotlusel tagaselja vahi alla ja nad kuulutati ka rahvusvaheliselt tagaotsitavaks.



See on ühtlasi esimene juhtum, mille puhul Eesti omistas riigivastased küberründed ametlikult kuritegude väidetavale toimepanijale. Rünnete omistamist koordineerib Eestis välisministeerium ning selle eesmärk on suunata riike küberuumis vastutustundlikult käituma ja neid vajadusel korrale kutsuda.

### SIHKUL ON UKRAINA LIITLASED

Samal ajal kulmineerus Eesti ja veel üheksa riigi ühisoperaatsioon Toy Soldier, mille tulemuse na seostati luureüksusega 29 155 veel suur hulk Ukrainat ning teda toetanud NATO ja ELi riike tabanud küberündeid. Muu hulgas panid USA võimud välja kümne miljoni dollari suuruse pearaha kuue Venemaa kodaniku tabamiseks, kelle hulgas olid ka Eesti poolt tagaotsitavad Denissov ja Kortšagin.

Teadaolevalt on 29 155 juba kolmas GRU väeos, mis on loonud oma kübervõimekuse.

## Kaitsepolitsei: küberoperatsioonid on osa Venemaa hübriidsõjast

Kaitsepolitsei peadirektori Margo Pallosoni sõnul kuulub 29 155 küberallüksuse eesmärki de hulka luureinfo kogumine, tundliku teabe targuste ja lekitamistega mainekahju tekitamine ning süsteematiiline sabotaaz andmete ja arvutisüsteemide hävitamisega. Sellele grupile omistati ametlikult küll 2020. aasta ründed, aga tegelikult on erinevate Vene küberluureüksuste ründed kogu aeg jätkunud nii Eesti kui ka teiste riikide vastu.

Vene eriteenistustute arsenalis on füüsилised ja küberhendid järjest rohkem läbi põimunud ning on töenäoline, et küberrünnetega saadud teavet võidakse ära kasutada ka füüslistes operatsioonides. Küberoperatsioonid on Venemaa sõjalise doktriini järgi oluline hübriidsõja komponent. Sõltumata meetoditest üritab Venemaa hübriidrünnakute abil ka teistele riikidele oma tahet peale suruda, ebastabiilsust külvata, hirmutada ja segadust tekitada.

USA süüdistuse järgi on nende põhitähelepanu koondunud viimastel aastatel Ukrainale, kus nad korraldasid 2022. aasta alguses – kuu aega enne Vene vägede suurt sissetungi – hävitava WhisperGate'i pahavararünnaku. Sihikule võeti mitmed Ukraina valitsus- ja õiguskaitseasutused ning hädaabitteenistused. Ründeks kasutati hävitusrvara ehk siis eesmärk polnud mitte süsteemide ülevõtmine, vaid täielikult kasutuskõlbmatuks muutmine. Kuna pahavara levitamine Ukrainas toimus ühe USA ettevõtte teenustesse kaudu, oli võimalik süüdlased Ühendriikides ka vastutusele võtta.

Mujal maailmas on USA riigiasutuste andmeil olnud küberüksuse põhieesmärk Ukrainale rahvusvahelise abi andmise takistamine. Nii NATO riikides kui ka teistes Euroopa, Keskkasiasia ja Ladina-Ameerika maades on nad rünnanud riigiasutusi ja kriitilist taristut, sealhulgas pangandust, tervishoidu, transpordi- ja energiasectorit. Näiteks on kübergrupp näotustanud veebilehti, kaardistanud taristut ning varastanud andmeid, mida nad on kas müünud või lekitanud. Microsoft andis sellele GRU küberüksusele koodnime Cadet Blizzard ja juhtis tähelepanu, et nad on rünnanud Ukrainas ja teistes Euroopa riikides ka IT-teenuste pakkujaid ja tarkvaraarendajaid, kes osutavad avalikule sektorile teenuseid, et siis nende kaudu tegeliku sihtmärgini jõuda.

Selle GRU kübergruppi meetodid pole tingimata väga keerulised ega rafineeritud. Sihtmärikidele ligi päsemiseks on nad nii Eestis kui ka mujal kasutanud juba varem avalikuks tulnud turvanörkusi – näiteks haavatavusi meili- ja veebiserverites – ning süsteemidest varastatud kasutajatunnuseid. Turvavigade väljaselgitamiseks ja ekspluateerimiseks, andmete väljaviiimiseks ning oma jälgede varjamiseks on üksus appi võtnud infoturbekogukonnas levinud tööriistad.

### JUHTUMI ÕPPETUNNID

Viimastel aastatel on küberturbe olukord kogu maailmas muutunud järjest keerulisemaks nii kasvanud geopolitiiliste pingete kui ka uute tehnoloogiliste arengute töttu, mida on oma tegevuse laiendamiseks kasutanud ära ka riiklike küberühmitused.

Eesti on seetõttu oluliselt suurendanud investeringuid küberterbesse ja kriitilise taristu kaitsesse ning siin on oluline roll RIA pakutavatel kesksetel teenustel: aitame riigiasutustel oma vörke turvata, otsime pidevalt haavatavusi ning teavitame asutusi ja ettevõtteid leitud probleemidest. Kui intsident on ikkagi toimunud, tulevad CERT-EE eksperdid vajadusel appi selle põhjuste uurimisel ja olukorra lahendamisel.

Kuigi enamikule Eesti eraettevõtetest pole küberintsidentidest teavitamine kohustuslik, tasub seda kindlasti teha. See aitab CERT-EE-i Eesti küberruumis toimuvast parema ülevaate saada ning ettevõtteid ja kogu riiki paremini kaitsta. Samamoodi võimaldab see ka riiklike küberündajate tegevust tuvastada.

Riiklike küberüksuste tegevust iseloomustab järgepidevus: kui rünnaku katse üks kord nurjub, võib oodata selle kordumist. Kõige suuremas ohus on kahtlemata valitsusasutused ja kriitilise taristu ettevõtted, aga tarneahela kaudu ka neile teenuseid pakkuvad firmad, näiteks IT- või raamatupidamisettevõtted. Sageli kasutatakse samasugust skeemi korraga mitme ettevõtte ja asutuse vastu, mistõttu on iga infokild suure pildi kokkupanekul oluline. Esmapilgul vähetähtis anomaalia võib lähemal uurimisel osutuda tösiseks küberündeeks.

Lõppkokkuvõttes vastutab iga organisatsioon oma süsteemide kaitsmise eest ise ja väga palju sõltub sellest, kuivõrd oluliseks juhtkond infoturvet peab. Vajadusel tuletab küberturva-

## ..... Lõppkokkuvõttes vastutab iga organisatsioon oma süsteemide kaitsmise eest ise. .....

lisuse tähtsust meelete RIA järelevalveosakond, mis on hoogsalt oma haaret laiendanud ning alustanud viimase kolme aasta jooksul ligi 150 järelevalvemenetlust. Suur osa järelevalve tööst on ennetuslik ehk siis ei reageerita ainult ilmsiks tulnud probleemidele, vaid ohuprognoside põhjal kontrollitakse olukorda kriitiliselt tähtsates asutustes ja ettevõtetes pidevalt. ●

## Kuidas ennast küberluurajate eest kaitsta?

Riiklikud küberühmitused kasutavad enamasti samu meetodeid ja tööriistu kui majanduslikku kasu himustavad küberkurjategijad, mistõttu kehtivad tavapärased infoturbe soovitused. Siiski juhime mõnele aspektile veel eraldi tähelepanu.

➥ Igasuguste küberünnete avastamiseks on äärmiselt oluline säilitada süsteemide logisid. Seejuures tuleks logida võimalikult suurt hulka erinevat infot (nt tulemüüri logid), et hiljem aru saada, mida ja kuidas ründajad tegid. Logidest on mõistagi kasu ainult siis, kui neid osatakse ka lugeda ja häiretele kohe reageeritakse. Eriti hoolikalt peaks monitoorima kaugligipääsu võimaldavaid lahendusi ja kontosid, mis neid kasutavad.

➥ Sisevõrk tuleks sõltuvalt organisatsiooni tökkorraldusest segmenteerida ehk osadeks jagada ning anda ligipääsuõigused ainult vastavalt vajadusele. Administraatorid peavad kindlasti kasutama erinevaid kontosid: tavakasutaja õigustega kontot igapäevasteks tegevusteks ja suuremate õigustega kontot ainult siis, kui seda on tarvis. Loomulikult ei tohiks paroole eri keskkondades ristkasutada ning kõigis süsteemides, kus see on võimalik, tuleks rakendada kahestameline autentimine.

➥ Keskhaldus tuleb hoida ajakohane ning loobuda vananenud tarkvarade ja seadmete kasutamisest – ühekordne investeering taakvara körvaldamiseks võib näida suur, aga see aitab vältida hoopis suuremat kahju.

➥ Kui kasutatakse mõne välise partneri teenuseid, tasub arvestada ka tarneahela riske. Kindlasti peab väliste partnerite ligipääse oma süsteemidele regulaarselt auditeerima ja andma neile ainult minimaalsed tööks vajalikud õigused.

USA küberturbeagentuuri CISA detailsemad tehnilised soovitused leiad [www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a](http://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a).

# ÕNGITSEJAD ise konksu otsas

Rahvusvahelise politseioperatsiooniga **PhishOFF** suleti maailma üks suuremaid õngitsuskelmidele teenuseid pakkunud platvorme **LabHost**, mille tegevuse tõttu sai kahju üle miljoni inimese. Eesti politseil oli haarangu ettevalmistamisel kandev roll.

Kui aastaid tagasi võis visata nalja lihtsaksoliste „Nigeeria kirjad“ üle, mis lubasid meeletuid rahasummasid, siis praeguseks on küberpettused teinud läbi suure arenguhüppe. Nende taga on tihti laia haardega rahvusvahelised võrgustikud ja organiseeritud kuritegevus.

Tegu on terve masinavärgiga, kus on paika pandud tööjaotus: ühed kurjategijad tungivad süsteemidesse sisse, teised loovad virtuaalkeskondi, kus asuvad näiteks õngitsuslehed, ning kolmandad möttlevad välja lahendusi, mis varastatud andmete abil inimese pangakonto võimalikult kiiresti ja tõhusalt tühjaks teevad, ning kõige lõpuks aitavad kurigelikult teenitud raha puhtaks pesta. Spetsialiseerunud platvormide kaudu saab teenusena sisse osta õngitsusi ja teenusetõkestusründeid, aga ka lunavara ja muud pahavara.

## ÜLE MILJONI KANNATANU

Üks suuremaid selliseid masinavärke, mis keskendus just õngitsuspettuse korraldamisele, oli **LabHost**. See võeti maha aprillis 2024 kulumineerunud rahvusvahelise politseioperatsiooniga PhishOFF, milles oli väga oluline ka Eesti politsei panus.

Europoli juhtimisel viis päeva kestnud haarrangutega peeti üle maailma kinni 37 pettuste korraldajat. Operatsioonis osales 18 riiki, enamik neist Euroopast, aga kaasatud olid ka USA, Kanada, Austraalia ja Uus-Meremaa.

2021. aastal tegevust alustanud LabHost oli avalik platvorm, mis pakkus teenusena ettevalmistatud libalehti, õngitsussüsteemi ja levitamislahendusi (SMS, e-post) ning müüs edasi ka samal platvormil kogutud andmeid. Mitu tuhat püsikliendist kurjategijat oli endale soetanud ligipääsu andmepüügi paketile, millega kelmusi toime panna. Komplekti kuulusid muu hulgas kümnete riikide suuremate pankade ja teenuste võltsitud veebilehed, millega oli võimalik iniimestelt välja petta autentimisandmeid ja varastada pangakontodelt raha.

Kõrgema taseme pakettide hinnad jäid 230 ja 350 euro vaheline kuus, kuid pakuti ka kvartalija aastatellimus. Arveldamine toimus krüptorahas ja teadaolevalt teenis LabHost oma teenuste müügiga ligikaudu miljon eurot, aga ohvritele tekitatud kahju oli palju kordi suurem. Platvorm võttis enda kanda kõige tüütumad ja aeganõudvamad küberkuriteo töölöigid ning administraatorid pakkusid tehniliste küsimustega hättä jäänud kurjategijatele spetsiaalselt selleks loodud Telegrami kanali kaudu abi.

Rahvusvahelise uurimise käigus tuvastati vähemalt 66 000 veebilehte, mida ligi 10 000 kurjategijat kasutas andmete või raha välja petmiseks. Üle maailma sai selle platvormi kaudu kannatada üle miljoni inimese. LabHosti vahendusel liikusid 480 000 pangakaardi andmed, 64 000 PIN-koodi ja rohkem kui miljon salasõna. Varastatud raha liigutati jälgede varjamiseks erinevate pangakontode vahel ning

vöeti lõpuks sularahas välja. Eesti suunal tegi platvormi kaudu õngitsusründeid kuni 30 kurjategijat, kellest kümme kond aktiivsemat peeti eri riikides kinni.

Põhja prefektuuri küber- ja majanduskuritegude talituse juht **Hannes Kelt** rääkis, et tema üksus hakkas paar aastat tagasi uurima massilist õngitsuslinkide lainet, kus kasutati ära Eestis tegutsevate pankade nimesid. „Jälgede kogumine ja andmete analüüs viis meid LabHostini. Kaasasime ka teisi riike, kes alustasid samuti uurimist, ning tulemuseks on seni ühe suurema seesuguse platvormi sulgemine,“ ütles Kelt.

## KURJATEGIJAID HEIDUTATI KOLME TARKVARAGA

Kelti juhitava talituse roll oli mõjutada ja heidutada LabHosti platvormil tegutsenud kurjategijaid kolme tarkvara abil. Esimene tööriist oli mõeldud kõigi aktiivsete õngitsustes kasutatud veebilehtede neutraliseerimiseks. Pärast mitu kuud kestnud infokorjet ja analüüsi suletigi aprillis 2024 kõik petukeskkonnad ja nendega seotud tuhanded petulehed.

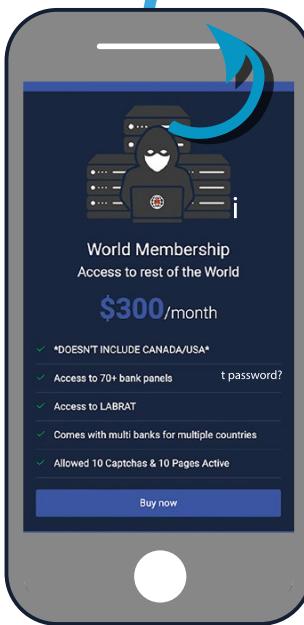
Samal ajal peeti haarangute käigus kinni kümneid kuritegude organiseerijaid, aga platvormi teenuseid kasutanud madalamana taseme pätte oli üle maailma tuhandeid. Selleks, et jõuda ka nendeni, loid Põhja prefektuuri eksperdid teise programmi, mis on oma olemuselt mõne sotsiaalmeedia- või sisujagamiskeskonna sarnane.

Kui komertsplatvormid saadavad kasutajale aasta lõpus ülevaate (*2024 wrapped*), milliseid pilte nad on jaganud, milliseid postitusi teinud või millist muusikat kõige rohkem kuulanud, siis 700 aktiivsemat petukeskkondi kasutanud kurjategijat said oma tegemistest politseilt samasuguse detailse kokkuvõtte, mille lõpus oli soovitus võimalikult kiiresti ise politseiga ühendust võtta ja oma kuriteod üles tunnistada – mida paljud ka tegid. Lisaks saateti 1500-le vähem aktiivselle kurjategijale nende tegemistest veel kirjalik kokkuvõte, et ka nemad saaksid aru, et petukeskkondades toi-

metades pole nad anonüümsed ega kaitstud.

Kolmandat tööriista kasutati kurjategijate omavahelistes vestluskeskkondades. Üle vöeti seal tegutsenud juturobot ja vestlusesse hakati edastama politseiinfot. Näiteks saateti kurjategijatele heidutuseks videoid ja sõnumeid kinnipidamistest ning näiteid platvormil kogutud töenditest. Eesmärk oli politsei sõnumit võimendada ja demonstreerida, et ka krüpteeritud suhtluskeskkondades pole täielik anonüümsus tagatud.

„Sedalaadi heidutust on vaja just vähem kogenud kurjategijatele, et neid varakult tagasi õigele teele nügida. Kokkuvõttes oli operatsioon väga edukas, mida tunnistasid lõpuks ka LabHosti võtmefiguurid, hoiatades ise oma kliente ning soovidades neil põgeneda ja oma seadmed hävitada,“ rääkis Kelt.



## VÕITLUS JÄTKUB

Kelt rõhutas, et sellises mahus rahvusvahelised operatsioonid nõuavad väga head koostööd ja koordineerimist. „Ühise pingutusega sulgesime platvormi, mis lõi võimalused tegutsemiseks tuhandetele kelmidele. Paraku ei ole tegu ainukese sellise keskkonnaga ning politsei töö kelmide peatamiseks jätkub. Kelmus on globaalne kuriteoliik ning ka väga suure platvormi kinnipanek ei too lõplikku lahendust, sest kurjategijad on väga motiveeritud uusi kelmuste viise looma ja kasutama.“

RIA intendentide käitlemise osakond CERT-EE tuvastab iga kuu mitusada õngitsus- ja petulehte. CERT-EE piirab lehtede ligipääsu, teavitab veebimajutajaid ja jagab infot ka oma rahvusvaheliste partneritega. Viimastel aastatel on kolmepoolne koostöö politsei ja Eestis tegutsevate pankadega läinud nii töhusaks, et leitud petuleht on võimalik maha võtta sisuliselt mõne minuti jooksul ja andmepüük kinni panna. ●

Põhja prefektuuri küber- ja majanduskuritegude talitus pälvis panuse eest PhishOFFi ettevalmistamisel 2024. aastal Europoli kõige innovaatilisema politseioperatsiooni auhinna.

# UMMISTUSRÜNDDED: rohkem kära, vähem villa

Eelmisel aastal registreeris CERT-EE rohkem ummistusründeid kui kunagi varem, kuid tänu kaitsemeetmetele langes mõjuga rünnakute osakaal. Uue trendina suunati rünnakute põhijoud nimeserverite vastu.

CERT-EE registreeris eelmisel aastal 580 ummistusrünnet. Seda on 93 võrra rohkem kui 2023. aastal ning koguni poolteist korda rohkem kui 2021. ja 2022. aastal kokku.

Nii nagu ründajad otsivad pidevalt uusi viise, kuidas enim kahju tekitada, täiendab CERT-EE oma DDoS-kaitset, et neidsamu ründajaid peata. Mida rohkem CERT-EE kaitse taga olevaid veeblehti rünnatakse, seda paremini on võimalik oma DDoS-kaitsemeetmeid tõhustata.

## Mis on DDoS?

Ummistusrünne (DDoS) on küberrünnak, mille käigus suunatakse sihtmärgile suur hulk pahaloomulisi pärtinguid, et selle serverid üle koormata ja muuta teenus kasutajatele kättesaadatuks. Kuna Eestile suunatud teenusetökestusrünnakud on enamjaolt poliitiliselt motiveeritud, siis sageli on nende sihtmärgiks valitud teenused, mille katkemine mõjutaks võimalikult paljusid inimesi: riiklikud e-teenused, pangad, transpordisektor jmt.

da. Tänu sellele oli vaatamata hirmutavalt kõrgele rünnakute arvule mõjuga rünnakute osakaal vaid 18 protsendi. See on märkimisväärne areng vörreldes sellele eelnenud aastaga, mil see näitaja oli 27 protsendi.

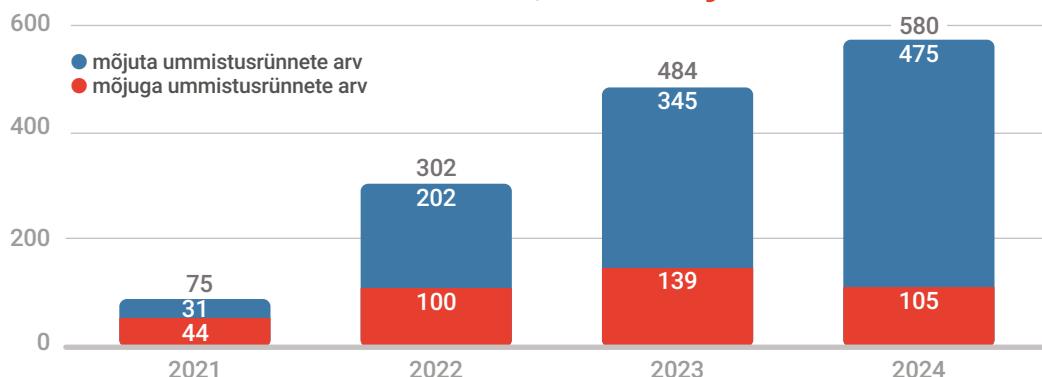
## SIHIKULE VÕETI NIMESERVERID

Üheks märkimisväärsemaks 2024. aasta trendiks oli see, et pahalased hakkasid üha enam veebiserverite asemel ründama nimeservereid.

Nimeserver teisendab IP-aadressid domeenideks. Tänu sellele ei pea me meeles pidama ja aadressireale kirjutama numbrijada 142.250.189.206, vaid google.com. Nimeserverid ei paku ise veebisisu, aga aitavad leida tee selleni. Kui ründajatel õnnestub nimeserverid ummistusründega rivist välja viia, ei saa kasutajad veeblehele enam ligi hoolimata sellest, et lehte teenindav veebiserver on täie tervise juures.

Kuna Eesti asutuste veebiserverid on viimasate aastate jooksul olnud pideva tule all, on neid paremini kaitsmata hakatud. Seetõttu pidid ründajad taktikat muutma ning võtma sihikule hoopis nimeserverid, mida on veidi raskem kaitsta.

## Ummistusrünnete arv kasvas, kuid mõju vähenes



Selliste rünnakute laine algas 2024 mais, mil Eesti asutuste nimeserveritele suunatud ummistusrünnete osakaal hüppas tavapäraselt kolmelt kuni kaheksalt protsendilt 69 protsendile. Veebiserverite vastu suunatud rünnakute arv samal ajal kahanes. Aasta viimastel kuudel moodustasid nimeserverite vastu suunatud rünned juba keskmiselt 90 protsendi kõikidest CERT-EE registreeritud teenusetõkestusrünnakutest.

Selline trend viitab selgelt sellele, et ründajad kohanevad kaitsemeetmetega ja otsivad pidevalt uusi haavatavusi, mida ära kasutada. Kui sihtmärgiks langevad süsteemid, mis on interneti toimimiseks kriitilise tähtsusega, võivad rünnakute tagajärjed olla ulatuslikumad kui lihtsalt üksikute veebisaitide rivist välja viimine. See muutus tähendab, et asutused ja ettevõtted peavad senisest enam panustama ka nimeserverite kaitsesse, kuna need moodustavad interneti selgroo.

### UMMISTUSRÜNNETE HULK JA MAHT KASVAVAD ENDISELT

Geopolitiiliste pingete tõttu ootame 2025. aastalt ummistusrünnete arvu jätkuvat kasvu. Need jäädvad populaarseks mõjutusvahendiks nii riiklikest toetatud rühmitustest kui sõltumatute hääktivistide jaoks. Tänu selle ründeliigi kasvavale populaarsusele tekib juurde platvorme ja teenusepakkujaid, kellelt saab DDoS-rünnakuid tellida. See omakorda muudab rünnakud võimsamaks ja kätesaadavaks ka vähem kogenud küberründajatele. Kõik see kergitab üldist ohutaset küberrummis.

### Nelja tunniga 26 aasta koormus

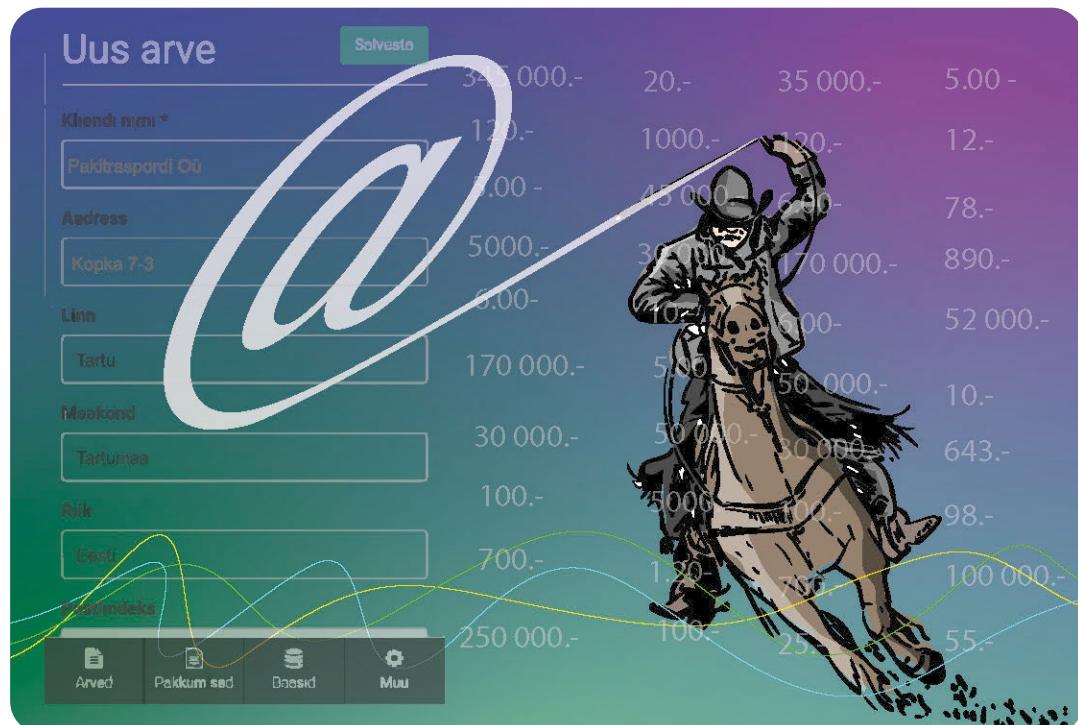
Märtsis toimus Eesti avaliku sektori vastu ummistusrünnete laine, mis oli oma mahu poolest rekordiline. Pahalased suutsid kolme asutuse veeblehe suunal teha ligi 2,8 miljardit pahaloomulist päringut, ja seda vaid nelja tunniga. Tavaolukorras oleks sellise mahu täitmiseks kulunud ligi 26 aastat.

Selle ründelaine taga olid kaks Vene hääktivistide rühmitust, kelle sihtmärgiks olid 16 Eesti riigiasutust.

Ennenägematutel rünnakumahtudele vaatamata oli mõju eelmainitud kolme veeblehe teenusele minimaalne.

Pahalaste kasuks rääkisid küll tohutud päringumahud, kuid rünnak ise polnud kuigi keerukas. Tänu DDoS-kaitsele ja CERT-EE aktiivsele reageerimisele enamik päringuid sihtmärkideni ei jöudnudki. Nõnda olid ülejäänud 13st rünnatud veeblehest lühiajaliselt mõjutatud vaid kolm ning kümne lehe puhul polnud rünnakuid isegi tunda.

Samuti võib oodata, et ründajad keskenduvad interneti toimimise seisukohast kriitilistele komponentidele: nimeserverid, pilveteenused ja autentimisteenused, millest sõltuvad paljud teised teenused. Tehisintellekti ja masinõppe toel muutuvad ummistusrünned dünaamilisemaks – neid saab reaalajas kohandada, et vältida kaitsemeetmeid ja muuta nende törjumine keerukamaks. ●



# PETTURID lahkusid miljonitega

Hoolimata teavitustööst, mida politsei- ja piirivalveamet, RIA ja teised asutused teevad, peame kahjusid ja pettusi kokku lüües taas kurbusega tõdema, et lõppenud aasta oli petturitele edukas.

**K**ui 2023. aastal registreeris CERT-EE kokku 546 mõjuga pettust, siis 2024. aastal 624 intsidenti. Eelmise aasta esimese 11 kuu jooksul kaotasid Eesti inimesed pettustega seitse miljonit eurot, ülevad politsei- ja piirivalveameti andmed. Kuna

paljud inimesed ei teavita juhtunust, võime eeldada, et tegelik kahjusumma on oluliselt suurem.

Aga miks ometi nii suur hulk pettusi õnnestub? Sellel on erinevad põhjused. Esiteks on petised aja jooksul järjest targemaks saanud ja

nende kirjad tunduvad töetriuud. Teiseks on meil köigil kiire ja proovime mitut asja korraga teha ning sealjuures valvsus kaob. Kolmandaks on paljud inimesed hakanud üha rohkem e-poodidest kaupa tellima, mis tähendab, et sageli ootamegi postipakki ja kui saabub petturi saadetud sõnum, tundub see ehtne olevat.

## ETTEVÖTTEID KIMBUTASID ARVEPETTUSED

Arvepettus on võrdlemisi levinud pettuse liik, kus ettevõttete või asutusele saadetakse tema koostööpartneri nimelt völtsarve. Völtsarve erineb tegelikust enamasti vaid muudetud pangakonto andmete poolest ja seetõttu võib pettus kergesti õnnestuda. Ettevõte kannab teadmalt raha kurjategijatele, koostööpartner aga ootab jätkuvalt ülekannet.

Seda pettuseliki pole lihtne ära tunda, sest tihilugu võtavad kurjategijad õige kirjavahetusüle ja ohvrile jääb mulje, et ta suhtleb oma äripartneriga edasi. Samas ei ole pangakontode muutmine just väga levinud praktika ja see võiks mõjuda ohu märgina.

Novembris teavitati meid neljast arvepettuse juhtumist, mille kogukahju oli ligi 300 000 eurot.

Esimesel juhul kandis Eesti ettevõte üle 170 000 euro petturite kontrolli all olevale kontole. Petturid olid kompromiteerinud ettevõtte meilikonto ja jälgisid selle kaudu toimunud kirjavahetust tarnijaga. Sobival hetkel saatsid nad Eesti ettevõttele selle välismaise tarnija nimel arve, millel oli muudetud arvelduskonto number. Paraku tegi ettevõte selle alusel makse.

Teisel puhul langes arvepettuse ohvriks riigile kuuluv ettevõte. Ettevõtte üldaadressile saabunud arve nägi välja nagu ehtne ja ka sellel olnud summa vastas ootustele, kuid arvel olnud kontonumber oli muudetud. Ettevõte kandis ligi 30 000 eurot petturatele. Pettus tuli välja, kui koostööpartner, kelleni raha ei jöudnud, palus saata maksekinnituse.

Kolmas õnnetu näide puudutab uue auto ostmist. Eesti ettevõte oli kuu aja jooksul olnud kirjavahetuses Saksamaal asuva automüürjaga. Selle kirjavahetuse käigus täideti leping ja sooritati makse vastavalt saadud pangarekvisitiidele. Kui joudis kätte auto üleandmise hetk, sel-

## Kuidas vältida arvepettust?

### ■ Tõsta arvepettuste osas teadlikkust.

Kõik, kes sinu ettevõttes või asutuses arveid kinnitavad, võiksid teada arvepettuse olemust ja tunnuseid. Alustuseks jaga hendega RIA blogis ([ria.ee/blogi/levivad-arvepettused-kontrolli-enne-kui-maksad](http://ria.ee/blogi/levivad-arvepettused-kontrolli-enne-kui-maksad)) ilmunud postitust ja räägi oma töötajatele, millega on tegemist.

### ■ Lepi kokku arvete kinnitamise protseduur.

Näiteks loo reegel, et kui arve rekvisiidid on muutunud, tuleb arve saatjaga võtta ühendust alternatiivse kanali kaudu, näiteks telefoni teel. Ühendust tuleks võtta mõne teadaoleva kontaktiga, selle asemel et telefoninumbrit arvelt vaadata. Petis võib ka arvel olevad kontaktandmed enda omade vastu vahetada.

### ■ Kui sul või raamatupidajal tekib kahtlus, et ülekanne on tehtud valele kontole, võta viivitamatult ühendust oma pangaga.

Välkmaksete ajastul on reageerimisaega napilt, kuid väga kiirelt reageerides võib pangal olla võimalik ülekanne tagasi kutsuda.

### ■ Kui oled tuvastanud völtsarve koostööpartneri nimelt või kahtlustad seda, võta kohe koostööpartneriga ühendust.

Kasuta selleks erinevat kanalit kui see, millega arve saabus. Sellisel moel käitudes võib saada probleemile kiirelt jälile, et see ei liiguks järgmiste ohvriteni.

gus, et pangakonto ei kuulunud auto müüjale ja ligi 60 000 euro suurune makse oli tehtud pettuse kontole. Petturid olid võtnud kirjavahetuse üle ja muutnud arvel olevaid pangarekvisiite.

Neljandal juhul sattus tööstusettevõte arvepettuse ohvriks. Petisel õnnestus sobival hetkel sekkuda kirjavahetusse ja esitada völtsarve. Kuna ettevõte pidi just järgmise osamakse tegevma, siis tundus kõik õige ja tasuti ärvahetamiseni sarnane arve. Raamatupidaja ei osanud kahtlustada rekvisiitide muutumist.

## KRÜPTOBUUM TÕI UUED PETTUSED

Üha enam näeme ka krüptorahaga seotud pettusi. Kuna tegemist on valdkonnaga, millega seostub kiire ja lihtne teenimisvõimalus, siis on ka petturid hakanud heausksete inimeste pealt kasu lõikama. Oleme näinud erinevaid skeeme, kuid enamasti toimuvad need järgmiselt: esmalt pakutakse inimesele teenimisvõimalust ja aidatakse tal teha sissemakse krüptovääringutega kauplemise platvormil. Alustatakse väiksemate summadega, näiteks palutakse kanda 250 eurot krüptovaluutaga tegelevasse keskkonda. Kui inimene on esmase makse teinud, siis näidatakse talle, kui suurt tulu selle pealt teenib. Inimene võtab teenitud summa välja, aga teadagi, süües kasvab isu. Seega tekib soov uesti oma raha investeerida ja seekord juba rohkem. Sel korral kannab inimene petiste kontole juba kordades suurema summa, aga mõne aja pärast selgub, et edaspidi tuleb ka raha kättesaaduse eest tasu maksta. Inimene maksab veelgi juurde, kuid ei saa kätte ei esialgset summat ega ka juurde makstud raha.

## Politsei tabas õngitsuskomplektide valmistaja

Keskkriminaalpolitsei esitas 5. juunil kahtluse 22-aastasele noormehele, kes müüs rakenduses Telegram enda valmistatud õngitsuskomplekte. Need võimaldasid üles seada õngitsuslehti ja seeläbi inimeste kasutajatunnuseid koguda. Nii oli võimalik mitmete keskkondade, nt Microsoft 365, PayPali, Google'i, Dropboxi ja Binance'i kahestmelisest autentimisest mööda pääseda.

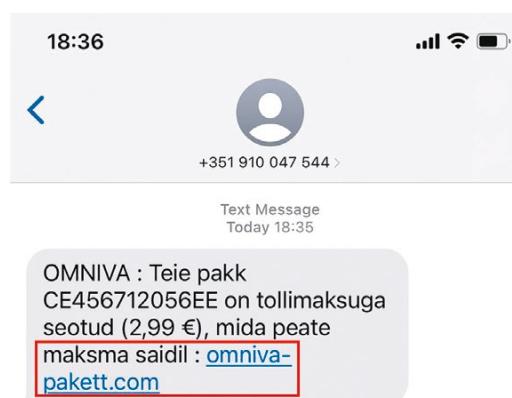
See juhtum toob esile, et küberkuritegevus on muutumas teenusepõhisemaks ehk sageli on rünnete läbivija ja seda võimaldavate lahenduste pakkuja erinevad isikud. Selliseid teenuseid loovad petturid on ka politsei huviobjidis, sest küberkurjategijatest on saamas üha olulisem lüli rahvusvahelise organiseeritud kuritegevuse maailmas. Oluline on selline ahel juba algjärgus peatada.

Vahel jäetakse ka mulje, et tegemist on tööpakkumisega. Esmalt lepitakse kokku töötasu, mille saamiseks peab inimene tegema mingi hulga krüptorahaga seotud ülesandeid. Seejärel selgub, et teenistuse kättesaamiseks küsitakse lisamaksu. Näiteks kui on kokku lepitud, et töötasu on 10 000 eurot, siis peab töötaja esmalt tasuma 20 protsendi makse, et oma palk kätte saada. Suure tulu ootuses maksabki töötaja nõutud summa, kuid nii enda kui lubatud raha näeb ta sama palju kui oma kõrvu. Enamasti jäavad sel moel kaotatud summad 2000–3000 euro kanti, kuid oleme saanud teateid ka palju suurematest kahjustest.

## JÄTKUSID NII PANKADE KUI KA POSTITEENUSE PAKKUJATE NIMEL SAADETUD PETTUSED

Taas saime hulgaliselt teateid õngitsuskirjadest ja SMSidest, mis on saadetud kas postiteenuse pakkuja või panga nimel. See pettuseliik on olnud populaarne juba aastaid ja vaibumise märke pole näha. Laias laastus jagunevad need õngitsused kaheks.

1. Omniva, DPD või DHL nimel saadetakse e-kiri või SMS, milles väidetakse, et pakki ei õnnestu kohale toimetada kas vale aadressi, maksmata tarnekulude või tollimaksu tõttu. Tihtilugu küsitakse neis sõnumites paari eurot kas tollimaksu või postiteenuse eest tasumiseks. Kui aga kasutaja oma pangakaardiandmed sisestab, võetakse kontolt maha oluliselt suurem summa. Enamasti ulatuvad selliste pettuse kahjusummad mõnesajast kuni paarikümne tuhande euronni.



L 23.11.2024 18:24

LHV (noreply@lhv.ee) <system@sentr-via.netsuite.com>  
Lugukeetud klient... - [#484651]

Peatelt on käes andmete uuendamise aeg

Lugukeetud klient!

Sooame olla Sulle parim pangateenuse partner ja seepärast on oluline, et Sinu kontaktandmed on alati äriahased.

<https://google.lt/amp/jeanchevalley>.  
 Ann online.fr/kohauixi88gka2wglofhrrwm1ho andmete uuendamise tähtaeg 25.11.2024.  
 Click or tap to follow link.

Sisene

Küsime tekkimisel palume ühendust võtta meili või telefoni teel.

Palume sellele e-kirjale mitte vastata. Tegemist on automaatse teavitusega.

Meeldivat koostööd soovides,

Carmen Rado.

2. Postkasti saabub mõne populaarse panga nimel saabunud e-kiri, milles palutakse oma andmeid uuendada. Kirja saatjaks on suvaline aadress ja kirja sees on kahtlane link, mis ei kuulu nimetatud pangale. Tavaliselt rõhutatakse neis kirjadest, et asjaga on kiire ja selles on määratud tähtaeg. Kahjuks paljud inimesed ei märka neid ohukohti ja lähevadki oma andmeid uuendama. Kasutaja suunatakse lehele, kus on vaja näiteks Smart-IDga sisse logida ja sisestada oma PIN-koodid.

Nende mõlema juhtumi puhul võib kasutaja olla üsna kindel, et oma raha ta tagasi ei saa. Kõige olulisem on jälgida kirjas või sõnumis olevat linki – kas selles olev domeen on õige. Enamasti saab kahtlastest aadressist aru, et tegemist pole õige kirjaga. Pangad ei saada andmete uuendamiseks e-kirja, milles on link, vaid paluvad andmeid uuendada ainult panga ametlikus rakenduses või ametlikul veebilehel. Ka Omnia ega teised postiteenuse pakkujad ei lase andmeid sisestada kahtlastel veeblehtedel. ●

Kõige olulisem on jälgida kirjas või sõnumis olevat linki – **kas selles olev domeen on õige**.

## Neli näidet õnnestunud pettustest

1. Augustis sai Kalle (siin ja edaspidi nimed 1. muudetud) Omnilalt sõnumi, milles väideti, et pakk on vale aadressi töttu tagastatud ja paluti uuendada tarneaadressi. Öngitsuslehel paluti valida õige pakiautomaat ja tasuda selle eest neli eurot. Kasutaja sisestas oma kaardianimed ja märkas, et leht jääb laadima ega pööranud sellele rohkem tähelepanu. Hommikul aga avastas ta, et kontolt on võetud üle 1300 euro. Kalle sulges pangakaardi, kuid juba kadunud raha ta tagasi ei saanud.

2. Septembris müüs Malle Facebooki Marketplace'i keskkonnas külmkappi. Ostja väitis, et ei saa ise kaubale järele tulla, kuid soovib kasutada Cargobusi kullertenust. Seejärel saadeti Mallele link ja suunati ta näiliselt Cargobusi lehele makset tegema, et kinnitada külmkapi transport. Heauskne inimene sisestas lehele oma pangakaardiandmed ja hetk hiljem oli kontolt 3900 eurot kadunud. Kahjuks ei õnnestunud seda makset tagasi kutsuda ja petise tegevus läks korda.

3. Oktoobris sai Helle justkui LHV pangalt 3. kirja, milles kutsuti üles oma andmeid uuendama. Helle sisestas pangaandmed saadetud lingi alt avanenud lehele ja avastas öhtul, et tema kontolt on võetud 950 eurot. Pärast seda proovis ta panka nii helistada kui ka kirjutada, kuid kuna tegemist oli töövälise ajaga, õnnestus pangaga suhelda alles järgmisel hommikul. Kahjuks ei olnud enam midagi teha ja tuli leppida raha kaotusega.

4. Ülle broneeris majutuse veebisaidil Booking.com. Esmalt luges ta teiste küllastajate hinnanguid ning vaatas majutusasutuse fotosid ja maksumust – pakkumine tundus suurepäane. Keskkonnas oli hotellist mitukümmend fotot ja samuti oli paarkümmend kasutajat jätnud positiivse tagasiside. Kuigi tasumine peaks toimuma Booking.com-i kaudu, edastas majutusteenuse pakuja Üllele eraldi pangakonto, millele ta raha üle kandis. Pärast makse sooritamist kadus omanik nagu tina tuhka ja majutuskoht oli portaalist maha võetud.

# LUNAVARA OHVRID, koolid ja ettevõtted

Ehkki kogu ühiskonda raputanud lunavararünnakutest pääses Eesti ka eelmisel aastal, avastati nii ettevõtetes, koolides kui ka hambaravikeskuses, et ründaja on tunginud nende süsteemidesse ja andmed lukustanud.

**I**unavararünnak on üks ebameeldivamaid küberrünnaku vorme, kuna see võib seisata organisatsiooni töö ja sealda ohtu isikuandmed. Kuigi globaalselt lunavararünnakute arv ja nendest tulenev kahju 2024. aastal kasvasid, räägivad meile teadaolevad andmed Eesti kohta teist keelt. CERT-EE registreeris kümmekond lunavarajuhtumit, mis on vähem kui varasematel aastatel. Seejuures tuleb arvestada, et suur osa ohvritest ei tea-vita meid.

## KAKS KOOLI, KAKS ERINEVAT LUGU

2024. aastal said lunavararünnakutega pihta kaks Eesti kooli. Tallinna Tervishoiu Kõrgkool pidi juuni alguses – eksamiperiodil, mil kooli-personalil on niigi käed-jalad tööd täis – hakka ma võitlema rünnaku tagajärgedega. Ründaja krüpteeris kooli serveris ligi pooleteise terabaidi jagu andmeid, sealhulgas enam kui 200 töötaja ja tudengi faile. Õnneks oli koolil olemas värske varukoopia, mille abil õnnestus failid ja teenused järgmiseks päevaks taastada.

Kaks nädalat enne uue kooliaasta algust, 16. augustil avastasid Järvamaa Kutsehariduskeskuse töötajad, et kooli kõikides serverites

olevad andmed on krüpteeritud. Selle rünnaku põhjustatud kahju oli aga suurem, kuna andmetest polnud varukoopiat.

## RÜNNAKUD, MIS PEATASID ETTEVÕTETE TÖÖ

Juuli lõpus tabas lunavararünnak Tartus tegutsevat väikeettevõtet. Selle käigus krüpteeris pahavara failid neljas arvutis. Ettevõtte tavapä-rane töö katkes.

Umbes nädal hiljem seiskas andmeid krüp-teeriv pahavara töö ühes Löuna-Eesti jaekau-bandusettevõttes. Seal pääsesid ründajad ligi ka varundusserverile, mistõttu ei saanud andmeid varukoopiast taastada.

Novembri esimesel päeval tabas lunavararünnak hambaravikliinikut. Ka selle andmeid polnud võimalik taastada, kuna puudus toimiv varukoopia.

## MIKS SELLISED RÜNNAKUD JUHTUVAD?

2024. aastal toimunud lunavararünnakute põhjuseid analüüsides kerkivad esile RDP ehk kaugtöölaua rakenduse ning võrguseadmetega seotud haavatavused.



Peaaegu igal kolmandal juhul tungisid ründajad süsteemi läbi kaugtöölaua rakenduse, kus kasutati nõrku paroole ja kus puudusid täiendavad turvameetmed nagu VPN, kaheastmeline autentimine, IP-põhised piirangud, logimine ja monitooring. Nende juhtumite valguses soovitame RDP kasutajatel lugeda RIA kodulehel olevat ohuhinnangut ([ria.ee/media/929/download](http://ria.ee/media/929/download)), kus kirjutame kaugtöölaua protokolliga kaasnevatest riskidest ja nende maandamise võimalustest.

2024. aastal langes mitu organisatsiooni lunavararünnaku ohvriks, kuna nende võrguseadmed olid vananenud, tarkvara uuendamata või haldusliides turvaliselt seadistamata. Ühel juhul oli internetis avalikult kättesaadav võrguseadme haldusliides ja muutmata vaikimisi administratoriparool, samal ajal ootas serveri tarkvara uuendamist. Teisel puhul oli kasutuses ruuter, mille tarkvaras oli ammu teada turvanõrkus,

## Mida teha, kui oled lunavararünnaku ohver?

- ➥ Eemalda nakatunud seade võrgust (ära unusta juhtmevaba võrku).
- ➥ Teavita CERT-EEd ([cert@cert.ee](mailto:cert@cert.ee)), kes juhendab intsidendi lahendamisel ja annab soovitusi, kuidas end edaspidi selliste rünnete eest kaitsta.
- ➥ Nakatumise korral tasub operatsiooni-süsteem taastada tagavarakoopiast või paigaldada see taasnakatumise vältimiseks uuesti. Enne tagavarakoopiast taastamist tuleb veenduda, et see pole pahavaraga nakatunud.
- ➥ Enne ründajatega ühenduse võtmist kaalu riske: pole garantii, et lunaraha maksmisel dekrüpteerib kurjategija failid või ei avalda varastatud andmeid. Samuti saadab see kurjategijatele sõnumi, et nende tegevus on edukas ja nad võivad sind ka järgmine kord ohvriks valida.

kuid seadme tootja lõpetas turvauuenduste väljastamise juba 2022. aastal. Sellisel puhul tuleks soetada uus seade. Mõne ostuga viivitamine võib väga kalliks maksma minna.

**Peaaegu igal kolmandal juhul tungisid ründajad süsteemi läbi kaugtöölaua rakenduse, kus kasutati nõrku paroole ja kus puudusid täiendavad turvameetmed.**

### NAKATUMISE VIIS SELGUSSETU

Mitmel juhul jääb täpne viis, kuidas lunavara süsteemi sattus, selgusetuks. Sageli on teadmatuse põhjuseks logide puudumine. Vahel kustutavad kurjategijad oma jälgede varjamiseks logid, aga pahatihti ei pea nad sedagi tegema, sest logisid lihtsalt pole. Kui pole teada, kuidas ründajad süsteemi tungisid, võivad kutsumata külalised sama ukse kaudu peagi naasta. ●

# 2024 tõi rekordarvu TURVANÖRKUSI

Eelmisel aastal registreeriti üle 40 000 turvanörkuse.

Neid jagus populaarsetesse sisuhaldustarkvaradesse, võrguseadmetesse, e-poe platvormidele ja mujale. Ründajate röömuks pole haavatava tarkvara kasutajatel selle uuendamisega kiiret.

**A**ugusti teine nädal algas transpordiametis keskmisest suurema ehmatusega. Pärast seda, kui üks kaitsesüsteem teavitas kahtlastest tegevusest asutuse võrgus, asuti lähemalt uurima, milles asi. Üsna pea oli ebameeldiv töde teada: ründaja oli kompromiteerinud süsteemi, mille kaudu hallatakse transpordiameti töötajate arvuteid ja muid seadmeid, ning saanud sellele administraatori õigustega ligipääsu. Ehkki algselt oli õhus ka võimalus, et ründaja on varastanud andmeid, lükkas hilisem uurimine selle oletuse ümber.

Lahendus, mida transpordiamet oma seadmete kaughalduseks kasutas, oli Fortineti Forti-ClientEMS. Selles oli kriitiline turvanörkus

(CVE-2023-48788), mille Fortinet avalikustas 12. märtsil koos tarkvara uue versiooniga, mis vea parandas. Paraku jäi transpordiametil see turvalisuse seisukohast hädavajalik uuendus paigaldamata. Ründajad leidsid haavatava süsteemi, kasutasid võimalust ja marssisid sisse.

## ÜKS PALJUDEST

Paraku on selliseid lugusid mitu, neid on nii avalikust kui ka erasektorist.

Veebruari alguses teatas riigiasutus, et nende VPN-serverid on kompromiteeritud. Jaanuaris alanud rünnakuks kasutati Ivanti turvanörkusi, mis olid rünnaku ajaks avaldatud olnud tosin päeva.

Augustis teavitas CERT-EE ühe veebipoe haldajat, et nende kasutataval platvormil Magento on avastatud kriitiline turvanörkus. Paraku ei reageerinud poe haldaja meie teavitusele ja novembris veebipood mainitud turvanörkust kasutades kompromiteeriti.

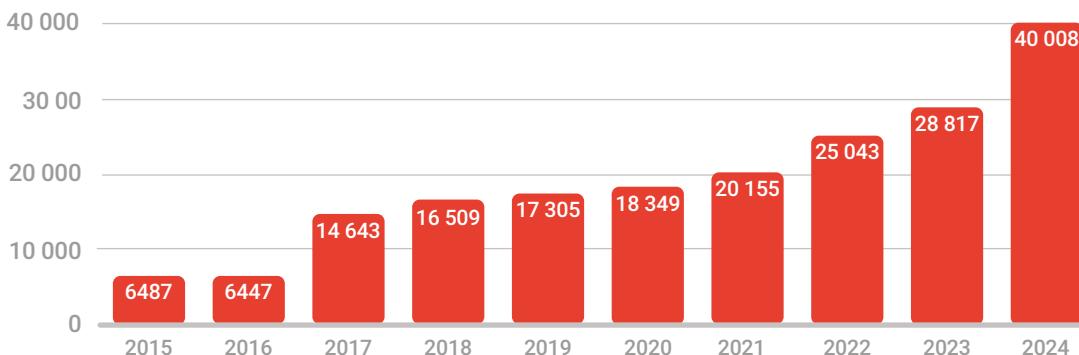
CERT-EE otsib Eesti küberruumis kriitiliste turvanörkustega süsteeme. Leidmise korral anname ohus olevate veebilehtede või seadmete omanikele sellest teada ja pakume nõu, kuidas haavatavus parandada.

Kui 2023. aastal saatis CERT-EE välja 2427 teavitust, siis möödunud aastal juba üle kolme korra rohkem ehk 7955. Mullu saadetutest suurima osa ehk 2462 moodustasid hoiatused WordPressi ja selle pistikprogrammide ning

## Kuidas kaitsta end turvanörkuste ärakasutamise vastu?

- ➥ Hoia kõigi süsteemide operatsiooni-süsteem või püsivara, rakendused jm tarkvara ajakohasena.
- ➥ Vaheta välja lõppenud tööeaga seadmed, millele tootja enam turvauendusi ei paku.
- ➥ Kaitse oma vörku ja administreerimisiideid. Kasuta VPNi ja luba ligipääs seadmetele, eriti süsteemide haldusliidestele, vaid kindlatelt IP-aadressidelt.

## Registreeritud turvanõrkuste arv 2015–2024



Allikas: nvd.nist.gov

263 Magento turvanõrkuste kohta. Sadu teavitsi saatsime ka kriitilise haavatavusega võrguseadme ja võrguhaldussüsteemide omanikele.

### NULLPÄEVA TURVANÕRKUSE ÄRAKASUTAMINE EESTIS

23. oktoobril avalikustati info FortiManageri nullpäeva turvanõrkuse (CVE-2024-47575) kohta. FortiManageri kriitilisel funktsionaalsusel puudus autentimine ja ründaja sai süsteemis käivitada endale sobivaid käsklusi. FortiNet oli oma kliente mõni päev varem võimalikust turvanõrkusest teavitanud ja soovitanud tarkvara uuendada ning seadmeid täiendavalt kaitsta. Eestis oli seda turvanõrkust ära kasutatud aga juba 22. oktoobril ja ründajad olid saanud ühe organisatsiooni kaks serverit enda kontrolli alla.

### MIS MUJAL MAAILMAS TOIMUS?

2024. aastal suurenes oluliselt avastatud turvanõrkuste hulk. Raporteeriti kokku 40 008 turvanõrkust, mida on võrreldes 2023. aasta 28 817 haavatavusega kolmandiku võrra rohkem.

Ülemaailmse trendidena saab välja tuua võrguseadmete püsivaras ja võrguhaldussüsteemides olevate nullpäeva turvanõrkuste kuritarvitamise. Siia sobivad näiteks kaks Ivanti tarkvarade nullpäeva turvanõrkust (CVE-2023-46805 ja CVE-2024-21887), mida kasutasid ära Hiinaga seotud rühmitused. Need haavatavused võimal-

### CERT-EE avastas Palo Alto tarkvarast olulise haavatavuse

CERT-EE avastas ja kirjeldas Palo Alto Networksi operatsioonisüsteemi PAN OS kasutavates seadmetes olulise haavatavuse (CVE-2024-3393). Selle kaudu oli võimalik panna tulemürү hanguma ehk viia see teenusetökestuse seisundisse, saates seadmele spetsiaalse pahatahtliku võrgupaketi. Teenusetökestuse seisundis tulemürү toob endaga kaasa võrguliikluse peatumise – pole võimalik kasutada internetiühendust ega üle võrgu toimivaid e-teenuseid. CERT-EE ja Palo Alto insenerid tuvastasid koostöös probleemi põhjuse ja Palo Alto andis välja parandatud versiooni PAN OS-ist.

davad autentimisest möödumist ja käsusüsti.

Küberkurjategijad otsivad jätkuvalt ka vanade turvanõrkustega seadmeid, et kasutada neid turvanõrkusi näiteks lunavararünnakuks või seadme liitmiseks oma robotvõrgustikuga.

Tavapäraselt palju kriitilisi turvanõrkusi leiti ka veebi sisuhaldussüsteemides ja e-poe tarkvarades.

Nullpäeva turvanõrkuste rohkus ja vanade haavatavuste jätkuv kuritarvitamine näitavad selgelt, et selle probleemiga tuleb tegeleda süsteemsel: panna paika ja järgida turvanõrkuste haldamise protsesse ja kaitsta oma organisatsiooni võrku täiendavate meetmetega. ●

# 2024: sündmused rahvusvahelises küberruumis

Mõjutustegevus valimiste ümber, Hiina häkkerid telekomiettevõtetes ja CrowdStrike'i põhjustatud ulatuslik katkestus IT-süsteemides.

**2024** oli erakordne valimiste aasta – lisaks presidendi- valimistele USA-s, üldvalimistele Ühendkuningriigis ja Euroopa Parlamendi valimistele toimusid üld- või kohalikud valimised veel ligi sadakonnas riigis üle terve maailma. Paljude riikide jaoks tähendas see lisasurvet küberruumis nii teenusetõkestusrünnete, erakondade veeblehtede näotustamiskatsete kui ka inimeste eelistusi vormivate infooperatsioonide näol.

## RUMEEENIAS TÜHISTATI PRESIDENDIVALIMISTE ESIMENE VOOR

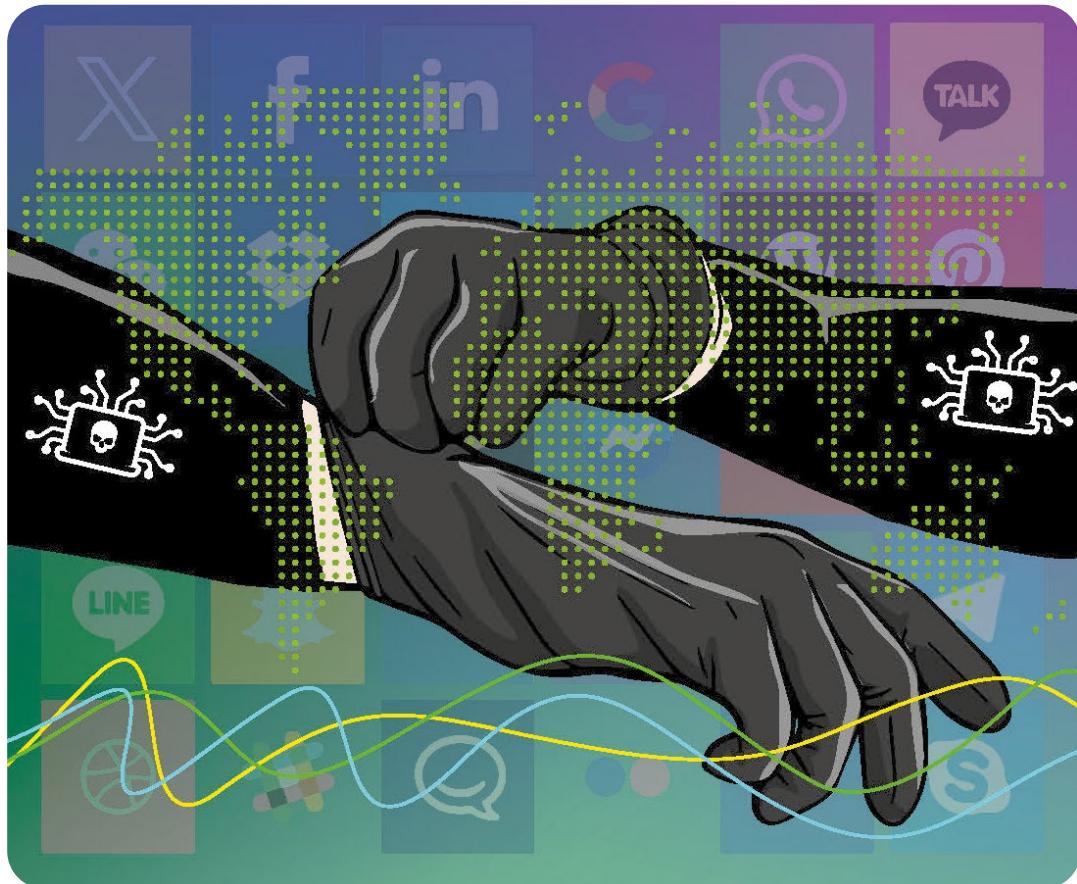
Infooperatsioon valimiste kontekstis tähendab üldiselt väljamöeldud uudiste või pooltõdede koordineeritud levitamist ja võimendamist sotsiaalmeedias, eesmärgiga tuua mõnede kandidaadile häält või vastupidi, neid ära viia. Kui seliseid infooperatsioone viivad läbi välisriigid, on

asi eriti hull – sisuliselt on tegemist välise sekkumisega riigi demokraatlikeesse protsessidesse.

Aasta drastilisim näide on Rumeeniast, kus konstitutsionikohus otsustas tühistada novembris toimunud presidendifinalimiste 1. vooru tulemused. Nimelt oli riigi luureteenistuse andmetel Venemaa korraldanud koordineeritud mõjutuskampaania TikTokis paremäärmuslasest kandidaadi toetuseks. Samuti leidsid luureteenistused, et valimiste taristu vastu tehti rohkem kui 85 000 küberrünnet erinevatel eesmärkidel: ligipääsu hankimiseks, valimistega seotud info muutmiseks ja selle kätesaadavuse takistamiseks.

## SALT TYPHOON TELEKOMIETTEVÕTES

Nii Iraan, Hiina kui Venemaa üritasid mõjutada ka Ameerika Ühendriikide presidendifinalimisi. Aasta viimastel kuudel hakkasid meedias



levima uudised Hiina riikliku taustaga häkkerte edukast sissetungist mitme suure Ameerika telekomiettevõtte – nende hulgas AT&T, T-Mobile ja Verizon – taristusse. Sissetungiga on seotud rühmitus **Salt Typhoon** ning teadaolevalt on tegemist ulatuslikema küberluure eesmärgil tehtud ründega lääne telekommunikatsioonisektori vastu.

Valge Maja hinnangu kohaselt on Hiina häkkrid varitsenud telekomiettevõtetes juba aasta või paar ning lisaks USA-le on mõjutatud ka mitmed Euroopa ja Kagu-Aasia riigid. Salt Typhooni tegevus jöudis meediasse algsest seetõttu, et neil olevat õnnestunud pealt kuulata ka mitme Ameerika tipp-poliitiku kõnesid kuni asepresidendi ja presidendi välja.

Lisaks luurehuvidega ohustajatele ründasid telekomisektorit ka tavalised küberkurjategijad. Oktoobris langes ohvriks Prantsuse suurustelt teine internetiteenuse pakkuja Free, millelt

varastati andmebaas 19 miljoni kliendikonto kohta ning prooviti see tumeveebis rahaks teha.

.....  
**Hiina häkkrid on varitsenud telekomiettevõtetes juba aasta või paar ning lisaks USA-le on mõjutatud ka mitmed Euroopa ja Kagu-Aasia riigid.**  
.....

Juba mainitud USA telekomiettevõtet AT&T mõjutas kevadel ka **Snowflake**'i andmelao kompromiteerimine, mis oli ühtlasi üks aasta suurima ulatusega ründeid teenusepakkujaga kaudu. Snowflake on pilvepõhine platvorm, mida kliendid saavad kasutada suurte andmehulkade hoidmiseks ja analüüsimeks.



Andmevargustele keskenduv rühmitus **Shiny Hunters** leidis tumeveebis müügilt mõned Snowflake'i kasutajakontode ligipääsutunnesed ning haistas võimalust jõuda nende abil Snowflake'i kõrge profiliiga klientide tundlike andmeteni. Snowflake'i andmevargus puudutas kokku vähemalt üheksa suurettevõtte miljoneid kliente. Nende hulgas oli ka Ticketmasteri piletimüügiettevõte ning andmelekke tagajärvel tekkin muu hulgas segadus niigi defitsiitsete Taylor Swifti kontserdituuri piletitega.

### CROWDSTRIKE'I TARKVARAVIGA PEATAS MILJONITE ARVUTITE TÖÖ

Kui enamasti seostatakse suure mõjuga kübertsidentide pahatahtlike rünnetega ning neid aitavad ära hoida küberturbeettevõtted oma kaitselahendustega, siis üks ajaloo suurim IT-intsident oli maineka küberettevõtte **Crowdstrike** enda hiigelopardus.

Nimelt laskis ettevõte läinud aasta suvel ringlusse vigase uuenduse ühe oma peamise toote, Crowdstrike Falconi platvormile, mis põhjustas 19. juulil miljonite Windowsi süsteemide töö peatumise. Selle tagajärvel tühistati lende

### Crowdstrike'i üleilmne IT-katkestus

Ööl vastu 19. juulit kell 4.24 andis CrowdStrike välja regulaarse turvauuenduse pilvepõhisele Crowdstrike Falconi viirusetõrjesüsteemi sensorile. Seekordne uuendus oli aga vigane. Automaatselt uuendatud sensor mõjutas paljude Windowsi süsteemide alusseadeid sellisel moel, et need lakkasid töötamast. Hinnanguliselt katkes globaalselt vähemalt 8,5 miljoni seadme töö. See tõi kaasa häireid ja sulgemisi lennuliikluses, finantssektoris, tervishoius, kaubanduses ja meedias mitmel pool maailmas, globaalset kahju hinnatakse miljardites dollarites.

Crowdstrike sai veast kiiresti aru ja andis samal ööl kell 5.27 välja parandatud uuenduse. Juba rikutud seadmed tulid aga taastada käsitsi, mistõttu kestsid katkestused sõltuvalt sektorist ja ettevõttest mõnest tunnist kuni päevade ja nädalateni.

Ameerikas ja Euroopas, häireid oli Ühendkuningriigi rongiliikluses, katkes uudisteagentuuri tegevus Soomes ning suleti kaubanduskeskus Austraalias – need on vaid mõned näited maailma tabanud katkestustest. Ka Eesti ei jäänud sellest puutumata – Elektrilevis oli osa arvuteid mõne tunni jagu pausil ning Tallinna lennujaamas käis nt Ryanairi lendudele registreerimine käsitsi.

### RÜNNAKUD TERVISHOIUSEKTORI VASTU

Küberrünnetega mõjutatakse ka elutähtsaid teenuseid ning nagu ka varasematel aastatel, olid mitmed tõsised intsidendid seotud tervishoiusektoriga. Seejuures paistis silma, et sageli riinnati mitte tervishoiuasutusi otse, vaid mõnda kriitilise tähtsusega teenusepakkujat.

Veebruaris ründas **BlackCat** lunavararühmitus USA ettevõtet **Change Healthcare**, mis toob kokku patsiendid, arstid ja kindlustusseltsid. Selle tõttu oli terves riigis häiritud tervishoiuteenuste eest arvete esitamine ja patsientidele kompenseerimine ning tervishoiuasutused olevat kandnud kümnedesesse miljonitesse dollariettesse ulatuvat kogukahju. Lisaks varastati ründe käigus 100 miljoni ehk ligikaudu iga kolmanda ameeriklase tundlikke andmeid, mille eest mõni kuu hiljem täiendavat lunaraha nõuti.

Veebruaris põhjustas lunavararünnak **Rumeenia** meditsiinisektori infosüsteemi vastu olukorra, kus sadakond haiglat pidi oma süsteemid võrgust eemaldama ning retsepte ja haiguslugusid ajutiselt käsitsi kirjutama. Juuni alguses tabas lunavararünnak aga patoloogia- ja diagnostikateenusepakkujat **Synnovis**, millel on koostöö mitme suure Londoni haiglaga. Seetõttu ei saanud mitu päeva teha vere kiiranallüüse ega vereülekaneid, mistõttu tuli edasi lükata operatsioone ja tühistada vastuvõtte.

### HELSINGI LINNAVALITSUSEST LEKKISID INIMESTE ANDMED

Andmelekked on muutunud tänapäeva digitaliseerunud ühiskonnas üsna tavalseks, ent aasta 2024 tõi mõned eriti silmatorkavad juhtumid. Mai algus töi halva uudise meie põhjanaabritele, kui selgus, et **Helsingi linnavalitsuse** haridusosakonda on tabanud küberrünnak ja selle

tulemusel varastatud kuni 150 000 inimese andmed, sealhulgas laste ja noorte isiku- ja terviseandmed.

Rünne toimus läbi aegunud tarkvaraga servi, mis oli otsustatud välja vahetada, ent hool-dustööde pingelise graafiku töttu oli see edasi lükatud. Kuna tõsised andmelekded on Soome ühiskonda raputanud ka varem, otsustas valitus kaasata juhtumi uurimisse eriti tõsistest õnnestuse uurimise ja ennetusega tegeleva ohutusjuurdlusameti.

Mai esimesel nädalal sai teatavaks, et **Ühendkuningriigi kaitseministeeriumi** kasutatava palgaarvestustarkvara kaudu lekkisid rohkem kui 225 000 Ühendkuningriigi kaitseväe tegevteenistuja, veterani ja reservisti isikuandmed. Andmete seas olid näiteks nimed ja pangakonto andmed – vaenulike riikide luureteenistustele kahtlemata huvitav info.

Lekke põhjustanud rünnak olevat saanud võimalikuks teenusepakkaja ebapiisava küberturvalisuse taseme töttu. See tõi taas esile probleemi, mille üle paljud riigid, sealhulgas Eesti, pead murravad: kuidas leevendada kriitilise tähtsusega sektorites neid küberriske, mis kaasnevad välistete teenusepakkujatega.

## SÜVAVÖLTSINGU TÖTTU KADUS 25 MILJONIT DOLLARIT

Läinud aastal ennustasime, et kiirelt arenev tehisaru muudab mängu ka kübermaastikul. 2024. aastal muutusid suurte keelemuodelite toel tõepärasmaks ja ka vähem levinud keeltes korrektsemaks miljonid öngitsuskirjad ja -sõnumid. Ehmatavamad arengud olid aga seotud süvavöltsgingu (ingl *deepfake*) tehnoloogia-ga nii häältes kui pildis.

Veebruaris oli Hongkongi politsei sunnitud tegelema juhtumiga, kus ühe rahvusvahelise suurfirma finantstöötaja osales videokõnes oma kollegidega ja tegi hiljem ettevõtte kontolt 25 miljoni dollari suuruse ülekanne, nagu talle teada-tuttav finantsjuht oli videokõnes korralduse andnud. Kogu videokõne aga osutus völtsginguks – kollegide asemel olid ekraanil süvavöltsgunga loodud kujutised, kes nägid välja täiesti tõepärased ning rääkisid kollegide häälega.

Kui völtsvideote tegemine vajab natuke pingutust ja aega, siis konkreetse inimese häale ära

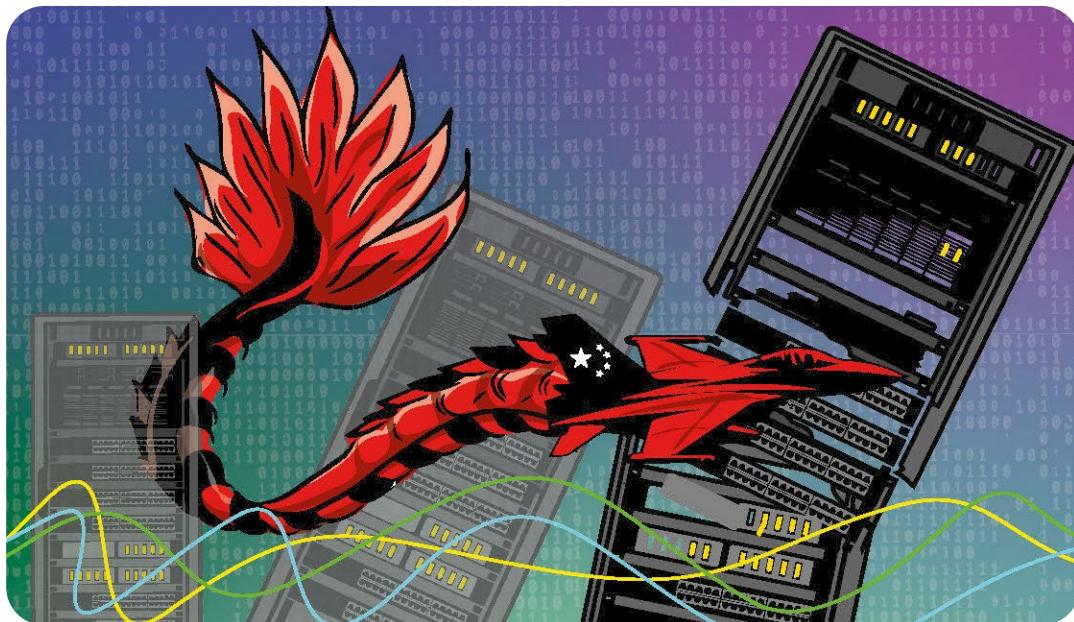
õppimine võtab levinud tarkvaral vaid kümme-kond minutit. Ameerikast näiteks on teada juhum, kus pereemale helistas võõras mees ja väitis, et tema tütar on põhjustanud liiklusõnnetusse ning nõudis kulude hüvitamist. Usutavuse lisamiseks anti telefon vahepeal tütrele, kes tundus pabinas, tunnistas oma süüd ja soovitas emal nõustuda. Tegelikult olid aga petturid võltsinud tütre häält.

**Kui völtsvideote tegemine vajab natuke pingutust ja aega, siis konkreetse inimese häale ära õppimine võtab levinud tarkvaral vaid kümme-kond minutit.**

Kui sageli kasutatakse völtshäale loomiseks konkreetse inimese internetist leitud kõne näidiseid (näiteks videot TikTokis või esinemist konverentsil), siis antud juhul oli tütar saanud eelnevatel päevadel kummaliisi telefonikõnesid, mida ta kohe ei taibanud katkestada. Perekond usub, et see oli vajalik petturite kasutatavale tehisarutööriistale tütre häale ja kõnemaneeri õpetamiseks.

## HÄKTIVISTIDE OMAVAHELINE KOOSTÖÖ PARANEB

Viimastel aastatel nii Eesti kui ka mujal maailma küberruumis mürgeldanud häktivistid näitasid oma meelsust ka 2024. aastal, püüdes küberrünnetega häirida nende silmis vaenulike riikide igapäevaelu. Fookuses olid ka neis riikides toimuvad tippsündmused, nagu näiteks Pariisi olümpiamängud või jalgpalli EM. Peamiselt oli tegemist lihtsakoeliste ummistusrünnetega riigi veeblehtede vastu ja enamasti ei olnud Neil möju. Küll aga näib, et erinevate häktivistide rühmituste koostöö aegamööda paraneb ning nii suudetakse ajuti oma tegevust ka geograafiliselt laiendada. Kreml-meelsete häktivistide sihtmärkide hulka lisandus näiteks Lõuna-Korea, kes mõistis hukka Põhja-Korea sõdurite kaasumise Venemaa peetavasse sõtta Ukrainas. ●



# PUNANE DRAAKON sirutab tiibu

Hiina eesmärgile saada 2050. aastaks maailma juhtivaks jõuks aitavad omalt poolt kaasa selle riigi küberrühmitused. Hiinaga seotud küberohud võib jagada kolmeksi: küberrünnakud, tehnoloogiline sõltuvus ja andmete levik Hiina.

Hiiлага seotud rühmitused on ilmselt kõige võimekamad ja keerulisemaid küberoperatsioone läbi viivad läänevastased jõud. Näiteks USA senaator Mark Warner töi välja, et Hiinaga seotud toimijate tegevused on nii tõised, et Venemaa omad tunduvad nende kõrval lapsemänguna. Venemaga vörreledes toimetab Hiina tihti varjatu-

malt, sest nende eesmärk pole teenuse halvamine, vaid küberspionaaž või eelpositsioneerimine. Kuigi Hiinaga seotud küberrühmitusi on palju, toome siin esile kolm eriilmelist „taifuuni“.

## TAIFUUNIDE LAINETES

2024. aasta sügisel teatasid USA võimud, et Hiinaga seotud rühmitusel **Salt Typhoon** on õnnes-

tunud tungida Ameerika telekomiettevõtete süsteemidesse. Tänu sellele said nad ligi kõnelogi-dele, krüpteerimata tekstisõnumitele ning isegi president Donald Trumpi ja presidendikandidaat Kamala Harrise meeskonna kõnedele.

Teine tegija, **Flax Typhoon** on saanud enda kontrolli alla mitusada tuhat seadet üle maailma, luues nn zombiseadmetest koosneva armee ehk botneti.

Kolmas taifuun, **Volt Typhoon** peidab ennast Ameerika kriitilises infrastruktuuris ning Valge Maja hinnangul pole nende eesmärk seal mitte niivõrd andmeid varastada, kuivõrd olla valmis halvama eluliselt olulisi teenuseid (vesi, side, käte jm), kui Hiinal peaks seda vaja minema.

#### „MADE IN CHINA“

Töenäoliselt on su telefon tehtud Hiinas. Kui sul on robotolmuimeja, siis küllap ka see. Ja kuumaõhufrüüt. Meie kodudes ja kontorites on raske leida asju, mis pole tehtud Hiinas, kui neid, mis on. Kuigi esialgu võib tunduda, et kuna Hiinas toodetud kaup on soodsam ja seega meile kui tarbijatele kasulik, siis tegelikult pole see pilt nii mustvalge. Nimelt on Hiinas toodetud kaup soodsam mitte ainult tänu odavamale tööjõule, vaid ka Hiina riigi toetusele oma tööstusele.

Selline tegevus aga võib kaasa tuua selle, et ülejäänud maailma firmad ei suuda Hiina ettevõtetega konkureerida ja ühel hetkel võime avastada ennast olukorras, kus meile olulised teenused ja tooted sõltuvad Hiina tootjatest.

Näiteks tõi Elering oma varustuskindluse aruandes välja, et Eesti päikesenergia paigaldistes on väga suur osa ühel Hiina inverterite tootjal ja see võib kaasa tuua olulisi riske varustuskindlusele. Näiteks on need haavatavamad küberrünnakutele, andmeid jälgib Hiina riik, hooldus ja hankimine sõltub ühest tootjast.

#### TIKTOK LUURAB SINU JÄRELE

Ilmselt on paljud kuulnud, et TikTok luurab sinu järele ja saab ligi su andmetele. Aga mis selles halba on? „Minul ei ole ju midagi varjata!“ ütleb keskmene eestlane. Andmed on inimese isiklik vara ja nendega peaks ringi käima vastutustundlikult. Euroopa andmekaitsemäärus (GDPR) just seda reguleeribki. Hiina seadused on aga teistsugused. Nimelt on Hiina sea-

## Kolm rünnakut, milles kahtlustatakse Hiina rühmitusi

**Salt Typhooni** läbiviidav häkkimine algas 2024. aasta kevadel ja kestab siiani. Avaliku info kohaselt pääses rühmitus vähemalt 80 telekomiettevõtte vörku üle maailma ja seda rünnakut peetakse üheks hullemaks küberrünna kuks ajaloos. Ründajail önnestus tungida ka Donald Trumpi telefoni. Ameerika valitsusasutused kahtlustavad, et ligi päaseti krüpteerimata tekstivahetusele (näiteks SMS) ja muudele andmetele. Täpsem uurimine käib, kahju ulatus on hetkel teadmata.

**Flax Typhoon** nakatas üle 200 000 seadme (ruuterid, valvekaamerad jne), moodustas nendest nn robotvõrgustiku, mida kasutati küberrünnette läbiviimiseks.

Suurbritannia kaitseministeeriumisse tungisid häkkerid, kes varastasid rohkem kui 270 000 praeguse ja endise sõjavälase andmed. Andmete hulgas olid ees- ja pere-nimi, pangaandmed, aadress ja muud isikuandmed. Rünnakus kahtlustatakse Hiinaga seotud toimijaid.

duse kohaselt kohustatud kõik firmad oma andmeid riigiga jagama – seda on kohtus avalikult kinnitanud ka TikTok tegevjuht. Peale selle, et kommunistlik parti saab teada, millised kassivõi tantsuvideoid sulle meeldivad, kogub TikTok andmeid ka sinu seadme, kontaktide, kalendri, teiste rakenduste, wifi-ühenduse jms kohta. Samuti kasutatakse kõiki neid andmeid, et arendada Hiinas tehisintellekti.

Muide, mäletad oma kuumaõhufrüütüri – kui see on ühendatud internetti, saadab ka see kogutud andmed Hiinasse.

Hiina on maailma üks võimsamaid riike, mis on esitanud avaliku väljakutse demokraatlikele riikidele ja üritab suurendada oma mõjuvõimu ka kübermaailmas, kasutades selleks erinevaid viise. RIA soovitab köikidel asutustel ja ettevõttel hoolikalt hinnata oma tarneahela usaldusväärust ning eraisikutel kaaluda, mis rakendusi ja tooteid nad kasutavad. ●

# KÜBERTURVALISUS

## on Eesti riigi jätkusuutlikkuse küsimus

Küberturvalisus pole pelgalt IT-probleem, vaid riigi jätkusuutlikkuse küsimus, kirjutavad Taavi Viilukas, Irina Klementi ja Kaido Tee justiits- ja digiministeeriumi riikliku küberturvalisuse osakonnast.

Digitaalne närvivõrk, millega sõltuvad meie avaliku ja erasektori teenused, on äärmiselt keerukas. Selle iga sõlme töökindlus sõltub teiste sõlmude olemasolust ja terviklikkusest. Kui üks neist muutub kättesaamatuks, mõjutab see kõiki teisi süsteeme ja teenuseid, mis sellest sõltuvad. Selline ristsõltuvus tähendab, et küberturvalisus pole asi iseeneses, vaid väga oluline osa tervikpildis, millele tuleb pidevalt tähelepanu pöörata.

### VAJAB SUUNDA JA SIHTI

Kui küberturvalisuse valdkonnas puuduks riiklik poliitika ja strateegiline suund, oleks see võrreldav Browni liikumisega, kus kõik osakesed liiguvad juhuslikult, kuid ilma ühise eesmärgita. Kujutagem ette riiki, kus küberturvalisust juhitakse vaid üksikute projektide ja juhuslike otsuste abil. Iga asutus ja organisatsioon tegutseks oma parima äranägemise järgi, kuid tulemuseks oleks killustatud süsteem, mis ei suuda ohtudele tõhusalt reageerida ega tagada

kriitiliste teenuste toimepidevust. Pole kahtlust, et selline riik oleks kergelt haavatav.

Seetõttu on äärmiselt oluline, et digitaalselt arenenud riigid, sealhulgas Eesti, loovad ja rakendavad küberturvalisuses poliitikat, mis tugineb pikaajalisele visioonile ja süsteemsele lähenemisele. Nii inimesed, ettevõtted, kriitiline taristu kui ka avalik sektor peavad ühisest eesmärgist aru saama ja selle nimel pingutama. Ühtne poliitika tagab, et küberturvalisuse meetmed on koordineeritud ja vastastikku toteavad ning võimaldavad muutuvatele ohtudele kiiresti ja paindlilikult reageerida. Vaid nii saab riik olla piisavalt kaitstud ja vastupidav.

Riiklike infosüsteemide arhitektuur peab arvestama võimalikke ristsõltuvusi ja riske. On hädavajalik, et iga uue süsteemi või tehnoloogia integreerimisel hinnatakse selle mõju kogu süsteemile ning lähtutakse riskianalüüsist. Riskihindamine pole ühekordne projekt, vaid järjepidev tegevus, mis peab sammu pidama muutuva ohupildi ja tehnoloogia arenguga.



Kaido Tee, Irina Klementi ja Taavi Viilukas.

Foto: Jüriits- ja Digidoministerium

Küberturvalisus pole pelgalt IT-probleem, vaid riigi jätkusuutlikkuse küsimus. Sarnaselt süsteemide vastupidavuse testimisega ja regulaarse riskihindamisega tuleb analüüsida ka organisatsiooni või riigi kui terviku vastupanuvõimet.

### ÜHTNE ÕIGUSRUUM

Muutunud julgeolekuolukorra tõttu tuleb keskenduda sellele, et küberturvalisuse, võrgu- ja teabekaitse ning kriisiohje õigusruum oleks ühtlustatud, vastaks parimale praktikale ning tagaks Eesti riigi teenuste toimimise ja turvalisuse ka keerulistest olukordades.

Lähiajal on oluline, et rahvusvahelised direktiivid saaks Eesti õigusesse üle võetud nii, et oleks tagatud tasakaal riigikaitse, ettevõtlusvabaduse ja küberturvalisuse nõuete vahel.

Euroopa Liidu (EL) direktiivid on oluline osa Eesti küberturvalisuse raamistikust, kuid nende rakendamisel tuleb vältida jäiku ja läbimõtlema ta lahendusi. Pahatihti märkame, et eestlastele on kombeks teha Vene lollus Saksa täpsusega. See tähendab, et ELi direktiivid ja regulatsioonid võetakse formaalselt ja täpselt üle, kuid unustatakse eesmärk ja saadav kasu. Tark lähenemine ELi direktiivide rakendamisel tähendab, et iga regulatsiooni mõju analüüsatakse ja kohandatakse kohalikele oludele vastavaks.

Näiteks võttes Eestis üle NIS2 direktiivi, mis määrab küberturvalisuse nõuded olulistele teenuseosutajatele, tuleb keskenduda mitte ainult tehniliste nõuete formaalsele täitmisele, vaid prioriseerida kohaliku ettevõtluse arendamist ja riigi digitaalse vastupanuvõime tugevdamist. Tuleb arvestada kohalike ettevõtete suurust, sektorite eripärasid ja taristu arengutaset. Nii tagame, et regulatsioonid aitavad töepooltest parandada turvalisust ega muuta koormavaks bürokraatiamasinaks. Viimasel juhul saavad konkurentsieelise hoopis suuremad rahvusvahelised ettevõtted, kellel on ressursid ja kogemused küberturvalisuse nõuetega kiiresti kohandada. See poleks mõistagi Eesti huvides.

### VAATAME TULEVIKKU

Küberturvalisuse poliitikakujundajana keskendume lisaks hetkeprobleemide lahendamisele ka kaugemale tulevikule. Kümmekonna aasta jooksul muudab kvantarvuti areng täielikult andmekaitse ja küberturvalisuse valdkonda, murdes lahti seni turvalise ja kindla krüptograafia. Sellest tulenevalt peame juba praegu mõtlema kvantarvutuskindlatele algoritmidele ehk postkvant krüptograafiale.

.....

**Kümmekonna aasta jooksul muudab kvantarvuti areng täielikult andmekaitse ja küberturvalisuse valdkonda.**

.....

Küberturvalisuse tagamisel ei piisa ainult füüsилiste, tehniliste ja protseduuriliste meetmete rakendamisest, vaid tarvis on süsteemset ja kogukondlikku lähenemist riigi kui terviku kaitseks. Küberturvalisus on riigi jätkusuutlikkuse küsimus ja me ei tohi seda alahinnata. Selleks, et olla paremini kaitstud, peame ühendama oma teadmised ja oskused ning tegema koostööd mitte ainult avalikus sektoris, vaid ka erasektoriga ja rahvusvaheliselt. Küberturvalisus nõubab ühset „meie“ mõtteviisi, kus unustatakse üksteisele näpuga näitamine, „sina või mina“ lähenemine ja töötatakse koostöös ühise eesmärgi nimel. Vaid nii saame tagada meie digiriigi turvalisuse. ●

# EESTI KOOLID küberturvaliseks!

Eestis kehtivad küberturvalisuse nõuded ligi tuhandele haridusasutusele, alustades kohalikele omavalitsustele kuuluvatest lastaedadest ja koolidest kuni suurte avalik-õiguslike ülikoolideni välja. Koolide tase on selles vallas üsna kõikuv ja tervikuna pole olukord eriti röõmustav.

**RIA** registreerib igal aastal kümneid haridusasutusi tabanud küberintsidente, millest suur osa oleks võimalik üsna kerge vaevaga ära hoida. Koolides tuleb ette andmelekkeid, kontode ja veeblehtede kaaperdamisi ning pettusi, aga ka ummistas- ja lunavararündeid ning palju muudki. Vaatame levinumatele ohtudele lähemalt otса ja anname soovitusi nende vältimeks.

## LEKKISID ÕPILASTE JA KOOLITÖÖTAJATE ANDMED

Viiimase paari aasta jooksul on Eestis teada kolm juhtumit, kus on lekinud õpilaste ja koolitöötajate isikuandmed ning vähemalt ühel juhul panid kurjategijad need ka müüki. Tegu oli peamiselt kontakt- ja kontoadmetega ehk õnneks mitte kõige tundlikuma infoga.

Samas võivad koolid kokku puutuda ka tundlike, õpilaste tervist puudutavate andmetega.

Hariduslike erivajadustega laste arengukaartides võidakse muu hulgas kirjeldada lapse käitumisraskusi ja terviseprobleeme, samuti kokkupuuteid politseiga. Sellise info avalikuks tulek võib tõsiselt kahjustada lapse tulevikku.

Õpilaste terviseandmetega puutuvad kokku ka koolide tervishoiutöötajad. Üks ohukohti on see, kui koolioe arvuti asub samas võrgus, mida kasutab kogu ülejäänud koolipere (ja kõik teised, kel on salasõna). Infoturbe huvides tuleks kooli võrk segmenteerida ehk luua eraldi alamvõrgud vastavalt vajadusele näiteks õpetajatele, õpilastele, koolitöötajatele ja meditsiinipersonalile. Tegemist ei ole eriti keerulise ettevõtmisega, aga tihti jäetakse see teadmatusest tegemata.

Haridusasutuste piisavalt turvamata arvutivõrke on kasutatud isegi kuritegude toimepäinemiseks, muu hulgas narkoäriks, mille uurimiseks on politsei pidanud koolidega ühendust võtma. Seega ohustavad küberintsidentid isikuandmete kõrval ka koolitöötajate ja laiemalt



koolide mainet. Samamoodi võivad mainekahju tuua ikka ja jälle ette tulevad lood, kus mõne koolitöötaja, õpetaja või õpilase konto võetakse üle ning tema nimel saadetakse massiliselt ebasündsa sisuga kirju või läkitatakse teistele koolipere liikmetele ja lapsevanematele õngitsusi.

.....

## Õppematerjalide hävimine küberrünnaku või tehnilise tõrke tõttu tähendab õpetajatele tundide uuesti ettevalmis- tamiseks tohutut lisatööd.

.....

Selliseid juhtumeid aitab enamasti ära hoida tähelepanelikkus ja küberhügieeni soovituste järgimine. Konto ülevõtmiseni viib tihti õngitluslingi või pahavaraga faili avamine, uuenda-

mata tarkvara, laokile jäetud paber salasõnaga või õpetaja lahti unustatud arvuti, mis on jäanud silma mõnele üleannetule koolijütsile. Kontode kaitseks soovitame kindlasti sisse lülitada mitmeastmeline autentimine.

### **AASTATEPIKKUNE TÖÖ VÕIB HETKEGA KUSTUDA**

Suur osa küberintsidentidest saab tegelikult alguse erinevatest tehnilikatest probleemidest, mitte kellegi pahatahtlikkusest. Tänapäeval on oluline osa õppematerjalidest loodud digitaalsel kujul ja ka õppetöö tulemusi jäädvustatakse koolides sageli ainult digitaalselt. Õppematerjalide hävimine tehnilise tõrke või küberrünnaku tõttu tähendab õpetajatele tundide uuesti ettevalmis-tamiseks tohutut lisatööd. Aastate jooksul nähitud vaev võib olla hetkega nullitud. Hinnete kustumine või pahatahtlik muutmine võib aga põhjustada õpilastele suurt segadust ja hilismaid probleeme oma õpitulemuste töendamisel.



2024. aasta augustis hävisid lunavararünna-ku tõttu kõik Järvamaa Kutsehariduskeskuse serverites olnud andmed, millest polnud varukoopiaid. Paremini läks juunis lunavaraga pihta saanud Tallinna Tervishoiu Kõrgkoolil, kus õnnestus töötajate ja tudengite failid järgmiseks päevaks varunduse abil taastada. Need juhtumid näitavad taas kord andmete varundamise tähtsust ja kindlasti tuleks varukoopiaid hoida muudest süsteemidest lahus.

Peale selle korraldatakse Eesti koolide vastu üsna tihti ummistusründeid, mille tulemusena võib olla kooli internetiühendus ja kogu töö mõnda aega häiritud. Ründemustreid vaadates on põhjust arvata, et paljude juhtumite taga on ilmselt kooliõpilased – sedalaadi ründeid on

.....  
Küberturbe nõuete rakendamine võib alguses tunduda koolijuhiile keerulise ülesandena, aga kui seda teha samm-sammult ja kindla plaani järgi, on see jõukohane.  
.....

võimalik lihtsalt korraldada, sealhulgas küberjategijatelt teenusena tellida. Samas peaksid koolide infosüsteemid olema üles ehitatud nii, et neid ei saaks selliste massrünnetega häirida.

## Soovitused koolidele küberturbega alustamisel

1. Kuna väga paljud küberohud on ärahoitavad töötajate küberateadmiste parandamisega, soovitame köigepealt kasutusele võtta RIA pakutav tasuta Kübertest, millega on ühinenud juba sadakond kooli.
2. Haridasutuse juhil tasub infoturbe teemat kindlasti kooli omanikuga arutada nii ressursside eraldamise kui ka töökorralduse mõttes: näiteks kas oleks mõistlik korraldada

Kõiki riske pole kunagi võimalik nulli viia ja iga intendent on õppimiskoht – koolides infoturbe eest vastutavatel inimestel tasub kindlasti oma kogemusi kolleegidega jagada, et üksteiselt oleks võimalik õppida ja mõnes teises koolis ei juhuks samamoodi. Paraku üritatakse need lood enamasti maha vaikida. Kui aga probleemidest kogukonnas ei räägita, ei teki ka ohuteadlikkust ja arvatake ekslikult, et midagi ei juhtugi. Nagu öeldakse: tark õpib teiste vigastest, rumal enda omadest.

## KOOLIJUHIL TASUB OMANIKUGA NÕU PIDADA

Alati ei sõltu koolide küberturvalisus ainult nende enda tegevusest. Lõppenud aastal oli korduvalt probleeme näiteks haridus- ja teadusministeeriumi hallatava eksamite infosüsteemiga ja õppekeskkonnaga Moodle, mis näitab kesksetesse e-teenusesse investeeringimise olulisust.

Samas on Eestis ka mitmeid eraettevõtete pakutavaid platvorme (nt e-päevikud) ja teenuseid, mille kasutamisele pole koolil sisuliselt alternatiive, sest konkurents on väike või puudub sootuks. Seaduse järgi peavad teenuste sisseostmisel tagama andmete kaitse siiski asutused ise. Seda on võimalik saavutada teadliku ja läbimõeldud väljast tellimisega, milleks on abi RIA loodud veebikoolitusest. Koolidel on mõistlik seljad kokku panna ning oma vajadused üheskoos läbi arutada, et neil oleks suhtlu-

kõigi omavalitsuse allasutuste infoturve ühiselt, palgata väline teenusepakkuja vms.

3. RIA on koostanud haridasutustele eraldi Eesti infoturbestandardi (E-ITS) profili, kus on välja toodud just neile vajalikud turvanõuded. Samas tasub meeles pidada, et profiil vajab siiski konkreetse asutuse eripärade põhjal kohendamist.
4. Profil algab juhile mõeldud soovitustega, sest tal on oluline roll infoturbe eestvedamisel oma asutuses. Konkreetsemate tehniliste nõuete täitmiseks tasub juhil määrata vastutav inimene kas oma asutusest või väljastpoolt (nt infoturbejuht, IT-spetsialist või arvutiõpetaja).

ses teenusepakkujatega tugevam jõuõlg. Perearstide seltsi kogemus on näidanud, et niimoodi koostööd tehes on võimalik kergemini teenuslepingutes vajalikke muudatusi saavutada.

Küberturbe nõuete rakendamine võib alguses tunduda koolijuhiile keerulise ülesandena, aga kui seda teha samm-sammult ja kindla plaani järgi, on see jõukohane. RIA eksperdid näevad oma töös pidevalt, et küberturvalisuse tase ei sõltu enamasti kooli suurusest, vaid juhi suhtumisest: kuivõrd oluliseks peab ta seda, et koolipere andmed on kaitstud ning et tänapäeva-vaseid õppe- ja töövahendeid saab kasutada turvaliselt, küberohte kartmata.

Enamik Eesti haridasasutusi kuulub kohaliike omavalitsustele ja sõltub neist eelarveliselt, mistõttu tasub koolijuhil küberturvalisuse parandamiseks kindlasti oma valla- või linnavalitsusega nõu pidada. Arvestades seda, et omavalitsustel on palju allasutusi, mis kasutavad sageli ühiseid infosüsteeme, võib neil olla mõistlik korraldada küberturvet keskselt – ükskõik, kas vajalikku personali palgates või mõnelt ettevõttelt teenust sisse ostes. Kogu omavalitsust hõlmava mudeli on Eestis valinud näiteks Pärnu linn ja Saaremaa vald.

RIA korraldab regulaarselt infopäevi-koolitusi, mis abistavad küberturvalisuse nõuete rakendamisel, ja paljud neist üritustest on mõeldud just haridasasutustele. Samuti on RIA eksperdid valmis koole küberturbe nõuete osas otse nõustama ja kõik küsimused on oodatud aadressil [kikk@ria.ee](mailto:kikk@ria.ee). ●

**5.** Küberturbe töhusaks korraldamiseks on vaja kõigepealt teada, millised IT-varad koolile üldse kuuluvad. Selleks tuleb koostada ülevaade kasutusel olevatest seadmetest-tarkvaradest ning vaadata üle koolitöötajate ja õpilaste ligipääsud süsteemidele ja võrkudele. Kooli lõpetanud õpilaste ja lahkinud töötajate juurdepääsud on vaja kohe sulgeda.

**6.** Teise praktilise sammuna tuleks panna paika kooli infoturbekord ehk kuidas kooli IT-seadmeid ja -süsteeme turvaliselt kasutada.

**7.** IT-teenuste sisseostmisel on vaja kriitilise pilguga üle vaadata lepingud, et oleks täpselt

## RIA järelevalve hakkab koole sagedamini külastama

Viimasel ajal on haridasasutustele rohkem tähelepanu pööranud ka RIA järelevalveosal, kuna küberintsidentide suur arv viitab sellele, et koolid ei tegele infoturbega piisavalt.

2025. aastal on plaanis kontrollida riigigümnaasiume ja avalik-õiguslikke ülikoole ning ilmselt jõutakse ka mõne omavalitsusele kuuluva koolini. Järelevalve eesmärk pole kedagi karistada, vaid hoida edaspidi ära suuri andmelekkeid ja katkestusi olulistes õppesüsteemides. Selleks tuvastatakse turvanõrkused ja puudused küberturbe nõuete täitmisel ning suunatakse asutusi leitud probleeme mõistliku aja jooksul kõrvaldama. Seejuures saab ka asutus ise kaasa rääkida, mis ajaks ta jõuab asjad korda teha.

Kui kokkulepetest ei peeta kinni või keeldutakse üldse järelevalvega koostööst, siis on RIA-i võimalik määrata sunniraha, kuid reaalselt on sunniraha määramiseni jõutud önneks vaid vähestel juhtudel.

Lisaks puudustele kõrvaldamisele konkreetses asutuses võimaldab järelevalve saada RIA-i parema ülevaate küberturbe olukorras terves valdkonnas, juhtida tähelepanu levinud probleemidele, suunata paremini ennetustegevusi ning teha vajadusel ettepanekuid ka õigusaktide muutmiseks või lisaraha eraldamiseks.

teada, mida teenus hõlmab ja kuidas lahendataks turvaintsidente.

**8.** Koolis infoturbe eest vastutaval inimesel tasub kindlasti tutvuda kolme RIA loodud E-ITSi rakendamise e-koolitusega DigiRiigi Akadeemias aadressil [digiriigiakadeemia.ee](http://digiriigiakadeemia.ee). Koolitused on enamasti läbitavad tunni aja jooksul, annavad valdkonnast ülevaate ja jagavad praktilisi soovitusi.

➥ E-ITSi ABC

➥ E-ITSi rakendamine

➥ Turvaline väljast tellimine

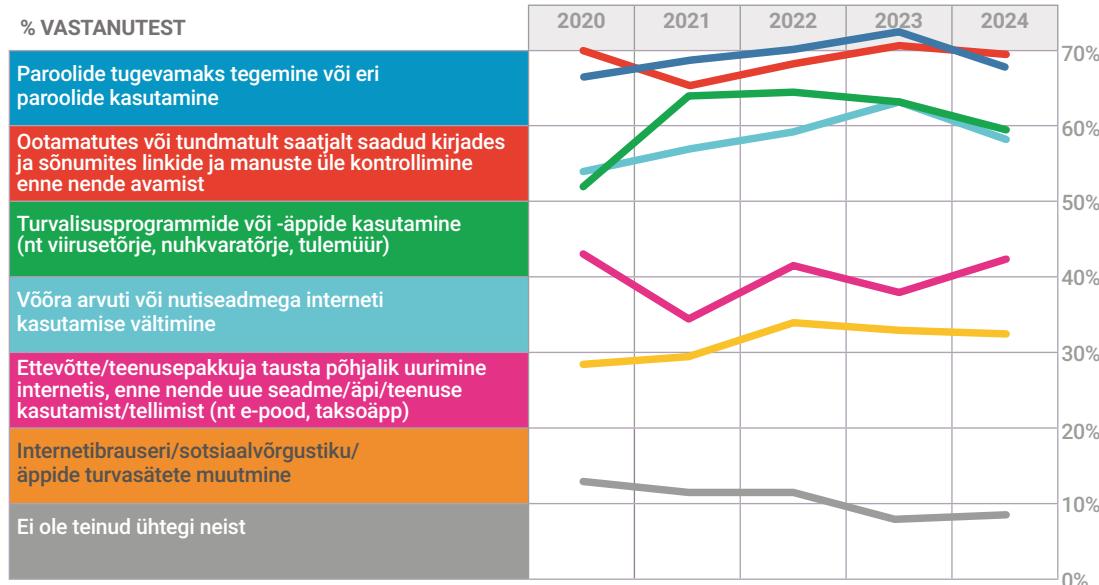
# ENNUS-TEGEVUSED vanavanematest lasteni

Ka küberturbes kehtib reegel: ennetus on soodsam kui tagajärgedega tegelemine. Sellest lähtuvalt korraldasime möödunud aastal õpitubasid vanemaealistele, kampaania noorematele ning andsime välja juhendmaterjalid lastele ja nende vanematele.

**A**astatega on Eesti inimeste teadlikkus küberohtudest valdavalt paranenud. Statistikaameti andmeil on inimesi, kes pole küberruumis astunud ühtegi sammu oma turvalisuse tagamiseks, alla kümne

protsendi. Ligi kolmveerand netikasutajaid uurib põhjalikult e-kirju ja sõnumeid, mis on saabunud ootamatult või tundmatult saatjalt, ning 70 protsendi arvestab ka soovitust, et salasõnad peavad olema tugevad ja erinoma täpsed.

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





## KÕIK POLE NII ROOSILINE

Teisalt esineb ka murettekitavaid trende. 16–24-aastased kontrollivad küll hooliga teenusepakkija või ettevõtte tausta, ent muude heade praktikate rakendamine (näiteks paroolide tugevdamine, turvasätete muutmine või viirusetörje kasutamine) on langenud.

Varasemalt on RIA tellitud uuringutest selgunud, et inimesed kipuvad küberruumis liialt usaldama oma kriitilist mõtlemist ning valdav on ka hoiak, et ei usuta mõne küberruunnaku ohvriks langemist. Liigne enesekindlus pärnsib ohutunnet ja teeb inimesed virtuaalmaailmas haavatavamaks.

## ÕPITOAD VANEMAEALISTELE JA KAMPAANIA NOORTELE

Vanemaalistel inimestel võib vahel olla raskusi internetist usaldusväärse info leidmisega. Seetõttu panime seljad kokku BCS Koolitusega, et pakkuda kesk- ja vanemaalistele silmast silma formaadis küberturvalisuse õpitube. Tasuta töötubades õpetati ära tundma internetiga seotud ohte ning oma arvuteid ja nutiseadmeid paremini kaitsuma. Eesti eri paikades toimunud õpitoad osutusid populaarseks ning uusi teadmisi käis kogumas pea 500 inimest. Osalejad pidasid saadud infot väga väärthuslikuks ning sarnaseid lühikoolitusi teadmiste ja oskuste värskendamiseks oodatakse ka tulevikus.

Oktoobris ehk rahvusvahelisel küberturvalisuse kuul seadsime fookuse noorematele. Tänavatel ja veebis nähtav olnud teavituskampaania kutsus üles järgima elementaarseid küberhügieeni reegleid ja leidma veidi aega, et aidata oma lähedastel olla IT-vaatlik.

Küberturvalisuse kuul ilmus rohkelt temaatilisi lugusid veebis, raadios, ajalehtedes ja sot-

siaalmeedias. Muu kõrval jõudis ETV eetrisse lühisaadete sari „IT-vaatlik“, mille episoodides jagasid küberarkust eksperdid RIAs, politseist, pangaliidust, ülikoolilist ja mujalt. Saadetes räägiti nutiseadmete turvalisusest, pettuse äratundmisest, turvalisest kaugtööst ning muust olulisest. Sarja esimesed 15 saadet jõudsid ligi 200 000 silmapaarini. Kel need vaatamata, saavad seda teha nii IT-vaatliku veeblehel, ERRI arhiivis kui ka voogedastusplatvormil Jupiter.

## JUHENDID LASTELE JA NENDE VANEMATELE

Kõige noorematele internetikasutajatele lõime mängulised juhendid, mis sisaldavad ristsõnu ja harjutusi ning tutvustavad küberteremasid lastele arusaadaval ja huvipakkaval viisil. Statistikaameti andmetel jälgivad pea pooled lapsevanemad oma alla 16-aastaste laste tegemisi sotsiaalvõrgustikes, mängukeskkondades või muudes veebiportaalides. Sama palju on neid, kes on pannud lapse seadmele sisulised piirangud, kasutades selleks näiteks mõnda vanemliku kontrolli rakendust.

70 protsendi lapsevanematest räägib oma lapsega ohtudest küberruumis ning jagab ka vastavaid käitumisõpetusi. Kuigi lapse ja vanema vahelist vestlust ei asenda miski, andsime sügise hakul välja just lastele ja nende vanematele suunatud „Turvaliselt internetis“ juhendid. Juhendmaterjalid leiab ennetusportaalil [itvaatlik.ee](http://itvaatlik.ee) ning esimesed 2000 eksemplari lastele mõeldud materjalidest jõudsid kiirelt soovijateni üle Eesti. Peagi on oodata uut kogust populaarseid juhendeid, et olulised teadmised küberohtudest jõuaks veelgi rohkemate laste ja nende vanemateni. ●

# ELI SAMMUD küberturvalisuse vallas

Mida Euroopa Liit 2024. aastal küberturvalisuse vallas korda  
saatis ning mida on oodata 2025. aastast?

## 2024

aasta juulis suvepuhkusele suunduvatest lennureisijatest oskas vaid mõni üksik arvestada võimalusega, et pikisilmi oodatud reis jäab küberintsidendi tõttu ootamatult ära. USA küberbetarkvara pakkuja ebaõnnestunud versiooniuendus põhjustas Windowsi operatsioonisüsteemiga arvutites katkematu taaskäivitamise, tuues kaasa miljardeid eurosid kahju ning häirides lennuliiklust, börsie, teleülekandeid ja tootmist.

Küberintsidentide mõju üldsusele lähiaastatel aina tõuseb ning käed rüpes istumine leevendust ei too. Milliseid samme astub Euroopa Liit (EL), et tagada inimeste, ettevõtete ja ühiskondade toimimine küberrünnete kuldajastul?

„Küberrünnete osas niipea paremaks ei lähe ning aina enam peame mõtlema mõeldamatutle.“ Sellise mõtte ütles DG CONNECTi ehk küberturvalisuse eest vastutava peadirektoraadi pealik Robert Viola 2025. aasta jaanuaris. Tema tõdemus ning aina sagenevad pealkirjad küberrünnetest aitavad aru saada, milks on EL viimastel aastatel küberturvalisuse vallas vastu võtnud hulga õigusakte. Nende abil soovitakse tõsta Euroopa inimeste, ettevõtete ja asutuste küberkerksust. Digihendustest on saanud ühiskonna toimimise oluline osa, mitte pelgalt mugavam alternatiiv füüsilistele teenustele.

Sellepärast on paslik vaadata, mida EL 2024. aastal küberturvalisuse vallas korda saatis ning mida on oodata 2025. aastast.

### NIS2

2023. aasta jaanuaris jõustus ELi küberturvalisuse 2. direktiiv ehk NIS2, mille eesmärk on tagada ühtlaselt kõrge küberturvalisus üle ELi. Riikidel oli aega 2024. aasta oktoobrini, et see oma riigi õigusesse üle võtta, kuid Eesti jäi ühes 20 teise liikmesriigiga ajahäätta. Eelnõu koostajate hinnangul pidurdasid protsessi pidev suuniste täpsustamine ja sektori pääringud. Eesmärk on NIS2 üle võtta 2025. aasta keskpaigaks. Siis selgub lõplikult, kui paljusid uusi ettevõtteid direktiiv mõjutab. Direktiiv aitab elutähtsatel ja olulistel teenusepakkujatel läheneda küberturvalisusele strateegiliselt ning määratleb, kuidas ja keda ründe korral teavitada ning määratleb küberturvalisuse tagamise baasnõuded.

### KÜBERKERKSUSE MÄÄRUS

2024. aasta 10. oktoobril võtsid liikmesriigid vastu küberkerksuse määrase (ingl Cyber Resilience Act, CRA), mis paneb paika digielementide ning internetti ühendatud seadmete nagu nutitelerite ja kodukaamerate küberturvalisuse nõuded. Määrus tagab, et digikomponentidega tooted, näiteks asjade interneti lahendused, püsivad turvalised kogu tarneahela ulatuses ning elutsükli ajal.

CRA eesmärk on kehtestada ühtsed küberturvalisuse nõuded riist- ja tarkvaratoodetele, välvides õigusaktide kattumist. Määrus kohaldub toodetele, mis on otseselt või kaudselt ühendatud teise seadme või sidevõrguga, välja



arvatud tooted, millele juba kehtivad ELi õigusnormid, näiteks meditsiiniseadmed, lennundustooted ja sõidukid. Tooted peavad omama CE-märgist, mis kinnitab vastavust määritusele ning ohutus-, tervishoiu- ja keskkonnakaitse-nõuetele. See aitab tarbijatel mõista, kas toode on kübervaline, ning kaitseb tarbijaid ja ettevõtteid ebaturvaliste digitoodete eest.

Erinevalt NIS2st on CRA rakendamiseks aega 2027. aasta detsembrini. Euroopa Komisjon peab koostöös liikmesriikidega looma esmalt üldised standardid (tüüp A) ja seejärel enam kui 20 tootekategooria standardid (tüüp C). Ettevõtted, kes soovivad toodetele ise vastuvushinnanguid teha, peavad järgima oma kategooria tüüp C standardeid. Kui kõik kulgeb plaanipäraselt, valmivad peamised standardid 2026. aasta sügiseks.

## KÜBERSOLIDAARSUSE MÄÄRUS

2024. aasta detsembris võtsid liikmesriigid vastu küber solidaarsuse määrase (ingl Cyber Solidarity Act), et tugevdada ELi tasandil oluliste ja ulatuslike (enam kui kahte riiki möjutavate) küberohutude avastamist, ennetamist ja reageerimist.

2025. jaanuaris avalikustatud määrus hõlmab kolme peamist meedet, milleks on Euroopa kübervalalisuse hoiatussüsteem küberohutude reaalajas avastamiseks ja neile reageerimiseks; kübervalalisuse hädaolukorra mehhanism, mis parandab valmisolekut ja reageerimisvõimet ulatuslike küberintidentide korral, ning küberintidentide läbivaatamise mehhanism, mille abil analüüsatakse ulatuslikke küber-

intidentide ning tehakse soovitusi ELi kübervalisuse parandamiseks.

Möödunud aastal said eelmainitud seadustele lisaks punkti veel kaks küberialast regulatsiooni: aasta lõpus kiideti heaks kübervalalisuse seaduse (CSA+) muudatus, mis puudutab hallatud turbeteenuseid, ning määrus, mis paneb paika piiriüleste elektrivoogude kübernöuded.

## MIDA TOOB 2025. AASTA?

Eelmisel aastal saadeti kübervalalisuse reguleerimise osas palju korda. Tänavu asub EL revideerima kübervalalisuse määrust, mis käsiteb Euroopa Liidu kübervalalisuse ameti ehk ENISA rolli ja kübervalalisuse sertifitseerimise raamistikku. Viie aasta tagune õigusakt vajab värs kendamist, et kajastada ENISA muutunud kohustusi ja täiustada kübervalalisuse valdkonnas toimuva sertifitseerimist.

Samuti hakatakse ajakohastama küberintidentide ja kriisidele reageerimise raamistikku, mis valmis 2017. aastal. Maailm on sellest ajast muutunud ning ELi valmisolek ja kerkus vajavad palju suuremat tähelepanu. Euroopa Komisjon on aastat alustanud agaralt, kui tutvustas 15. jaanuaril oma ettekujutust, kuidas tõsta tervishoiualdkonna kübervalalisuse taset.

Kuigi leidub kahtlejaid, kes peavad ELi samme kübervalalisuse vallas ebapiisavaks, soovib enamik eksperte õigusrahу, et olema solevaid meetmeid töhusalt rakendada. ELil ja liikmesriikidel, sealhulgas Eestil, tuleb nüüd keskenduda õigusaktide elluviimisele ja toetada sihtühmi nende nõuete tätmisel. ●

# Kuidas teha EESTI KÜBERPIIR lühemaks?

Kuna kümne aastaga on riiklike andmekogude arv peaaegu kolmekordistunud, on pikenenud ka meie küberpiir, mis vajab valvet ja kaitset. Seda saab lühendada, kui võtta kasutusele RIA pakutavad kesksed teenused.

**P**ahatahtlike ja kutsumata külaliste kodust eemale hoidmiseks on meil kombeks lukustada uks. Visamaid sissetungijaid see aga ei takista – nende jaoks on vaja keerukamat ja targemat heidutust, ennetust ja tõkestust. Riigi küberturvalisuse tagamisel tuleb mõelda sarnaselt.

Totalitaarsete režiimide kombel enda lahtiühendamine maailmast võib tunduda parima „lukuna“, kuid uks selle küljes on õhutihed. Uks taga, õues, on värske õhk, kuid seepool kipub hapnik otsa saama. Küberi kon-

teksti tõlgituna teeb lahtiühendamine katki väga paljud teenused, millele igapäevaselt toetume.

## KÜBERTURVALISUS ON MEIE KÖIGI VASTUTUS

Riigikaitset käsitletakse laiapindsena, sama lähenemist on mõistlik rakendada ka küberkaitse vankri ette. Iga asutus, ettevõte, pere ja inimene saab midagi ära teha, et kogu riigi küberruum oleks turvalisem.

Riik pakub mitmeid võimalusi, et end küberturvalisuse alal harida ja saadud tead-



misi kontrollida. RIA avaldab regulaarseid ülevaateid, kui hea või halb ilm küberruumis parasjagu valitseb. Kirjeldame olulisemaid intsideente, et lugejad saaksid õppida teiste, mitte enda vigadest. Pakume e-õppakeskkonda Kübertest ja ennetusportaali itvaatlik.ee.

Riigiasutused saavad RIA teenuste seast rakendada terve hulga meetmeid, mis aitavad kurjad käed riiklikest süsteemidest eemal hoida ning seeläbi tagada inimestele õigel hetkel vaja-like teenuste kättesaadavus.

## KÜBERPIIR PIKENEBS

Siiski on mündil ka teine külg. Viimase kümne aastaga on riiklike andmekogude arv kasvanud ligikaudu 500-lt 1400-le, mis tähendab ründerpinna märkimisväärset suurenemist ehk lihtsalt väljendudes – oleme pea kolm korda suurem sihtmärk.

Seda võib käitleda kui riigipiiri kolmekordset pikenenist, mis nõub töhusamaid ja targetmaid meetmeid, et meie silmad jõuksid nende ni, kes kurja plaanivad, ja pahatahtlik tegevus eristuks selgete piirjoontega. Siinjuures ei saa jäätta tähelepanuta, et ka küberrünnakute maht kasvab iga aastaga. Rünnakute keerukuse kasvule lisab hoogu tehisintellekti võidakäik.

## KÕIKE EI PEA ISE TEGEMA

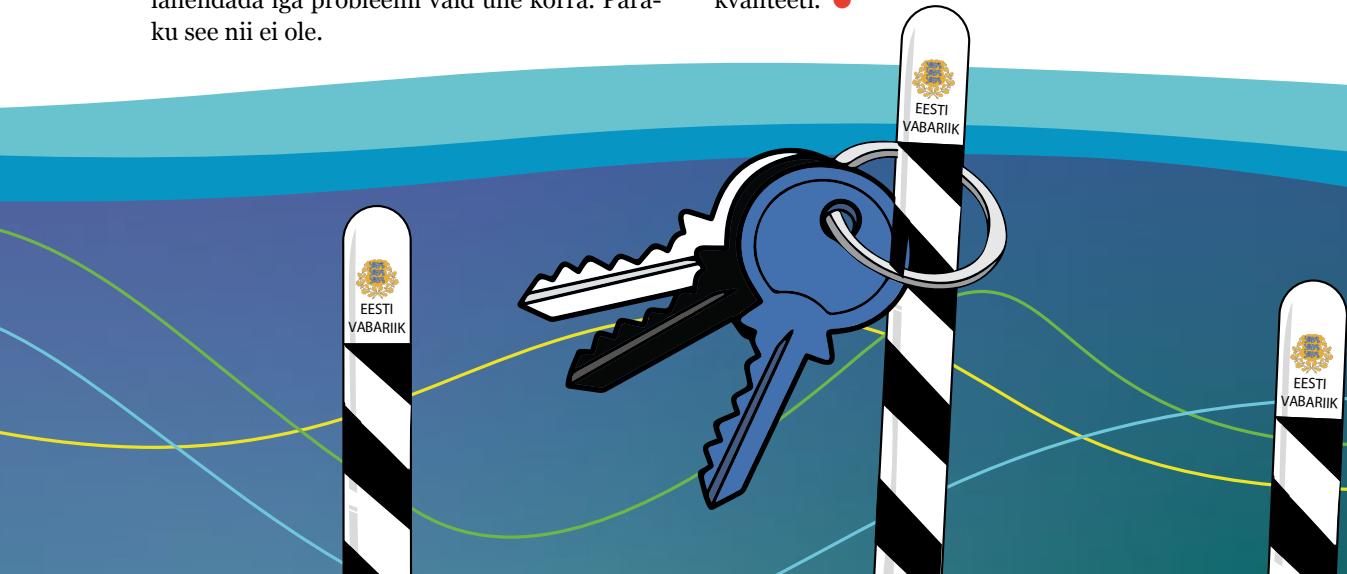
Riigil on arvukalt asutusi, neil kõigil hulk pakutavaid teenuseid, mida toetab kogukas infotehnoloogiline infrastruktuur: alates klassikalistest serveritest ja võrkudest kuni erilahenduseks loodud tarkvaradeni välja. Ideaalis võiks säärase hiiglasliku ja keeruka masinavärgi sees lahendada iga probleemi vaid ühe korra. Paraku see nii ei ole.

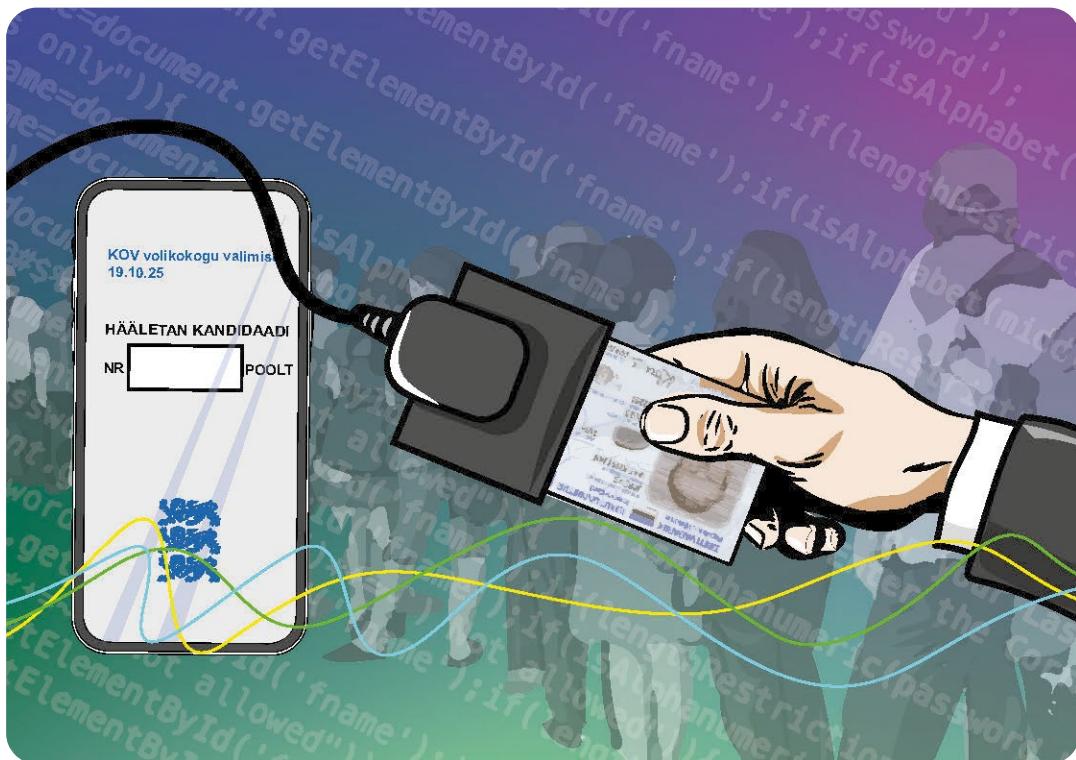
Kui ühe käega aitab RIA hoida klassikalist kübertyrvalisust, siis ameti teise käe ülesanne on luua ja pakkuda teenusena teistele asutustele neid süsteemide komponente, mis on kõikjal põhimõtteliselt ühetaolisid või rahuldavad samasugust vajadust. Olgu selleks riiklik autentimisteenus, turvaline andmevahetuskiht X-tee, riigiportaal esti.ee või riiklik postkast. RIA teenused on just need tehnilised ehitusklotsid, mida igal asutusel pole otstarbekas ise ehitada, hooldada ja üleval pidada. Loodud ühe korra, et teised ei peaks seda tegema – printsipi, mille poole riigina püüdlemee.

RIA teenused on just need tehnilised ehitusklotsid, mida igal asutusel pole otstarbekas ise ehitada, hooldada ja üleval pidada.

RIA teenuste laialdane kasutus aitab muuta riiklikku küberpiiri lühemaks. Bonusena ei pea iga asutus enam kõike ise tegema – jagame koormust, hoiame fookust sellel, mis on iga asutuse põhiülesanne. Taaskasutame kõike, mis on ühetaoline, ja arendame ise ainult seda, mis on enda äri spetsiifiline.

Seeläbi vabaneb ressurss – nii inimesed, raha kui ka aeg –, mida suunata inimestele suurema väärtsuse loomisesse ja loodud väärtsuse (küber) kaitsmisse. Vähendame kvantiteeti, et tõsta kvaliteeti. ●





# E-HÄÄLETUS: 20 aastat arengut

2025. aasta oktoobris toimuvad kohaliku omavalitsuse volikogu valimised tähistavad e-hääletamise 20. aastapäeva.

**E**elmisel aastal toimunud Euroopa Parlamendi valimised möödusid rahulikult. Valimisprotsess, sealhulgas elektrooniline hääletamine ja häälte kontrollimine, toimis sujuvalt ja ootuspäraselt. Ka olukord küberrindel oli valimisnädalal suhteliselt vaikne – ründeid valimiste süsteemide vastu ei tuvastatud. Kuigi valimisnädala alguses pidasid mõned veebirauserid valijarakenduse käivitatavat faili ekslikult pahavaraks, oli lahen-

dus kiire tänu töhusale koostööle Google'iga.

E-hääletusplatvormi usaldusvärsust kinnitas ka valijate rekordiline aktiivsus kontrollrakenduse kasutamisel – ligi kümme protsendti hääletanitest kontrollis oma e-hääle jõudmist RIA kogumisserverisse, mis on kõigi aegade parim tulemus. Mida kõrgem on oma hääle kontrollijate osakaal, seda suurema kindluse saavad ka valimiste korraldajad, et süsteeme ja valijate arvuteid pole kompromiteeritud.

## KUUS KESKMISE TASEME RISKI

Tehnoloogia areng on toonud lauale uued küsimused meie e-teenuste turvalisuse osas. Nendele vastamiseks uuris teaduste akadeemia küberturvalisuse komisjon, kuidas tagada Eesti e-teenuste turvalisus, ja avaldas oktoobris analüüsiga tulemused.

E-hääletamise juures ei leitud ühtegi kõrget või väga kõrget riski. Leiti kuus võimalikku keskmise taseme riski, mille leevendamisega seotud tegevusi tuleks jätkata. Nendeks on demokraatlike valimiste usaldusväärssust kahjustavate kampaaniate tasakaalustamine; püsiv töö kehtivate hääletusviisiide turvalisuse ja usaldatavuse tagamisel; nutiseadme valijarakenduse autentsuse ja tervikluse kontrolli meetodi väljaarendamine; e-hääletamise protokolli täiendamine auditeeritavuse ja vaadeldavuse töstmiseks; valimiste auditeerimise ja vaatlemise protsesside edasiarendamine ning valimiste infosüsteemide töökindluse jätkuv arendus.

Ülejäänud 25 riski hinnati madalaks, sealjuures avalikkuses palju arutletud võimalused, et keegi e-valimiskastis hääli kustutaks või muudaks, sest süsteemi sisse ehitatud kontroll-mehhanismid hoiaavad sellised katsed ära.

## E-HÄÄLETAMINE NUTITELEFONIDESSE

Eesti e-teenuste edulugu on rajatud kasutaja-sõbralikkusele ja innovatsioonile. Ka e-hääletamine järgib seda arengut ja on liikumas sinna, kus on kasutajad – nutitelefonidesse. Mobiiltelefonidele väljatöötatud valijarakenduse ehk m-rakenduse prototüüp on oluline samm tulevikku, mille abil saab e-hääletamine uue, mugavama ja lihtsamini ligipääsetava vormi.

**Lõplik otsus, kas kõik riskid on piisavalt maandatud või vastuvõetavad, jäääb vabariigi valimiskomisjoni teha.**

Praeguseks on valmis saanud m-rakenduse tehniline prototüüp, mille abil on testitud häälte andmist, edastamist ja vastuvõtmist. Hetkel käib

## Valimiste rollijaotus

**Riigi valimisteenistus** (RVT) tegeleb valimiste korraldamisega nii jaoskondades kui ka elektrooniliselt.

**Vabariigi valimiskomisjon** (VVK) teeb järelevalvet, registreerib kandidaatid ning teeb kindlaks lõplikud hääletamis- ja valimistulemused, tegeleb valimiskaebuste ja -rikkumiste ning valimiste usaldusväärssuse küsimustega.

**Riigi infosüsteemi amet** (RIA) on valimiste korraldajatele tehnoloogia- ja innovatsiooni-partner, mh haldab valimistega seotud infosüsteeme ja tagab valimiste küberturvalisuse.

koostöö tehnoloogiaettevõtetega ja valimiste korraldajatega riskide kahandamiseks. Teadupärast erineb rakenduste allalaadimine telefoni nende levitamisest arvutite operatsioonisüsteemides ning see käib äppipoodide kaudu.

Läbipaistvsus ja auditeeritavus on võtme-küsimus ning see eeldab tihedat koostööd rakenduspoodide omanikega (Google ja Apple), et leida parimad lahendused rakenduse terviklikkuse tagamiseks. Lõplik otsus, kas kõik riskid on piisavalt maandatud või vastuvõetavad, jäääb vabariigi valimiskomisjoni teha.

## E-HÄÄLETAMINE TÄHISTAB 20. AASTAPÄEVA

13.–19. oktoobrini 2025 toimuvad kohaliku omavalitsuse volikogu valimised. Ettevalmistused käivad täiskiirusel, et tagada sujuv ja turvaline valimisprotsess. Seekordsed valimised saavad olema oluline verstapost Eesti e-hääletuse ajaloos, sest tähistatame 20 aasta täitumist e-hääletuse esmakordsest kasutamisest Eestis. Selle aja jooksul on Eesti e-hääletuse lahendus olnud eeskuju kogu maailmale, töestades, et tehnoloogia suudab lisada valimisprotsessile väärust ning suurendada usaldusväärssust ja turvalisust.

E-valimiste turvalisuse tagamiseks võetakse järgmistel valimistel kasutusele mitu tehnoloogilist uuendust, sealhulgas Smart-ID valija autentimiseks ning krüptograafia vallas elliptiliste köverate rakendamine. ●

# Mida oodata 2025. AASTALT küberruumis?



## Järjekordne küberintsidentide rekord

Nagu ses aastaraamatus välja toodud, purunes 2024. aastal Eesti küberruumis registreeritud mõjuga intsidentide rekord. Vaadates 2024. aasta teist poolt, eriti selle viimaseid kuid ja nädalaid, prognoosime kasvutrendi jätkumist ka alanud aastal. Usume, et tõusunurk pole enam sama järsk, kuid on naiivne loota, et see languseks pöörab. Edasisele töösulele aitavad kaasa kurjategijate kasvav võimekus ning ühiskonnas üha leviv teadlikkus, et intsidenti korral tuleks teavita da RIA intsidentide käsitlemise osakonda aadressil cert@cert.ee või raport.cert.ee.

## Kasvab väga suure mõjuga intsidendi toimumise tõenäosus

Küberturvalisus ei saa kunagi valmis. Tehnoloogia areneb pidevalt ning koos sellega kasvavad ka kurjategijate või riikliku taustaga grupeeringu te võimalused kahju teha, olgu see raha teenimise, saladuste varastamise või mõne elutähta teenuse toimimise häirimise eesmärgil. Tegelikult, nagu on meie regiooni inimestele väga selgelt näidanud Läänemerel alates 2023. aasta oktoobrikuust toimunud arengud, piisab olulise taristu rivist välja viimiseks ka palju lihtsakoelisematest meetoditest kui arenenud küberühendvõimekus. Vaja on vaid ühte mitte liiga heas korras laeva, mille ankurgi ei taha pardal püsida.

Ükskõik kui hästi RIA küberintsidendi ennetamiseks ja törjumiseks valmis-tub ning ükskõik kui tõsiselt Eesti riigiasutused, ettevõtted ja inimesed end kaitsta püüavad, on ründajal alati lihtsam. Kui kujutada meie



küberruumi ette silmapiirini laiuva suvise Eestimaa aasana, kus õitsevad lilled, laulavad linnud ja mängivad lapsed, tuleb sinna juurde möelda ka kõrge aed, mis peaks tagama kurjade joudude jäämise väljapoole seda kaunidust. Aed peab olema läbimatult absoluutsetl igas kohas ehk küberruumi kaitsjate tähelepanu peab ulatuma pidevalt igale meetrile. Vastavõistkonnal on aga vaja vaid üht redelit, mille abil kiiresti üle ronida, või üht tööriista, millega auk tekitada. Sellistes tingimustes võib midagi tõsist juhtuda pigem varem kui hiljem.

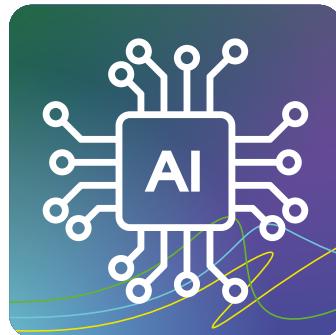
## Hiina-küsimuse kajastus muudab inimeste käitumist

2024. aasta viimastel kuudel oli Eesti ajakirjanduses mitmeid, muu hulgas ka kübermõõtmega Hiina-teemalisi uudiseid. Nende hulgas sai laiemat kajastust küsimus, kas Eesti pealinn peaks tegema kommunikatsiooni Hiina valitsuse kontrollitaval platvormil TikTok, mis arenas küsimuseks, kas riik peaks Hiina valitsusele AI-d treeniva TikToki ära keelama. Teine suurem teema oli Eestis müügile tulnud Hiina ettevõtte BYD elektriautod, mis on ühendatud Hiinas paiknevate serveritega, kuhu jõudvatele andmetele pääsevad ligi selle riigi ametivõimud. Veel tekkis poleemika sellest, kas Hiinas toodetud ruuterid on turvalised ja kas neid peaks kasutama. Need kõik olid väga õiged küsimused, sarnaselt nendega, mis esitati septembris riigikogu Hiina sõprusrühma liikmetele, kes osaliselt võõrustajate raha eest kohapeal visiidil käisid. Kõige taustaks veel hiinlaste sõprus meie idanaabriga, käitumine



viimase Ukraina-vastase agressiooni taustal ning manöövrid Taiwani ümber.

Hiina-teema ei kao 2025. aastal ega edaspidigi. Usume, et ettevaatuselole sundivad punased lipukesed kinnistuvad üha rohkemates peades. Kui ikka ühest riigist pärit tooted jagavad igaühe andmeid selle riigi võimudega ning see riik on paljudes globaalsetes väärusküsimustes meie ja meie liitlastega mitte just samal pool vastasseisu tähistavat rindejoont, tasub vähemalt üheksa korda möelda, kas peaks selle uue Hiina vidina ostma või lubama oma lapsel telefoni TikToki laadida.



## Tehisintellekt jätkab võidukäiku

Tehisintellekt (AI) jätkab arenomist seitsmepenikoormasaabastega. Lisaks ka eesti keeles saadetavate öngitsuskirjade täiuslomisele kasutavad küberkurjategijad AI-rakendusi ründekoodi kirjutamiseks. Tagantjärele on muu hulgas selgunud, et 2023. a lõpus Israeli ja Hamasi konflikti laines pihta saanud Eesti katlamajade ja veejaamade vastu korraldatud rünnakutes kasutati samuti tehisaru abil loodud koodi. Üks maailma tuntumaid AI-arendajaid OpenAI tunnistas oktoobris 2024, et nende ChatGPT mudelit on kasutatud rünnete ettevalmistamiseks, sh pahvara arendamiseks, valeinfo levitamiseks ja öngitsuste loomiseks. Kõnealusel raportis on ära märgitud nii Hiina, Iraan kui Venemaa. Muidugi saab tehisintellekti kasutada ka kaitsvam pool, mistõttu töötavad järgmised aastad tulla põnevad.



## Kas järjekordne suur andmeleke?

Kirjutasime andmekaitsest ka eelmise küberturvalisuse aastaraamatu prograamiks, kuna 2023. aastal leidis aset paar suuremat andmeleket. Väljendasime lootust, et „nende kaasuste jõudmine avalikkuse ette töstab asutustele ja ettevõtete soovi ja suutlikkust neile usaldatud isikuandmeid asjakohaselt

kaitsta“. Vaid mõni päev pärast selle teksti ilmumist sai RIA teada, et aset on leidnud järjekordne – ja töesti väga-väga suur – isikuandmete leke, millest kirjutame seekordses väljaandes. Önnekse pole seejärel mastaapsid andmelekkeid Eestis olnud, kuid pole põhjust arvata, et eelmine jäab viimaseks.

# Küberturvalisuse aastaraamat 2025

---

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





Loe edasi: [www.ria.ee](http://www.ria.ee)