



# Trendid ja tähelepanekud küberruumis

II kvartal 2022

## 1. Eestit tabasid teenusetõkestusrünnete lained

### OLUKORD

Möödunud kvartalis andsid Eesti küberruumis tooni teenusetõkestusründed mitmete riigiasutuste ja elutähtsate ning oluliste teenuste osutajate vastu. Ründed toimusid lainetena: esimene ja suurima mõjuga laine toimus 21.-25. aprillil, mil rünnati 13 erinevat riigiga seotud või riigi jaoks oluliste teenuste veebilehte. Ajaliselt langes see kokku Eestis toimunud rahvusvahelise küberõppusega **Locked Shields**.

Teine laine leidis aset 8.-9. mail, Venemaal tähistatava võidupäeva paiku, kui ründeid sooritati muuhulgas Välisministeeriumi, Siseministeeriumi ja Politsei- ning Piirivalveameti veebilehtede vastu.

Kolmas laine algas 5. juunil, mil ligi nädala jooksul rünnati samuti riiklikke veebilehti, lisaks panku ja transpordiettevõtete kodulehti. Enamike sihtmärgiks valitud veebilehtede puhul olid rakendatud täiendavad kaitsemeetmed, mistõttu rünnete mõju oli väike. Siiski olid mõned veebilehed kuni mõne tunni jooksul kättesaamatud, põhjustades kasutajatele ebamugavusi.

### RIA HINNANG

Sihtmärkide valik ja rünnete ajastus kõnelevad ründajate soovist tekitada mainekahju ja häirida tavapäraseid teenuseid, et inimestes ebakindlust ja pahameelt tekitada. Rünnete taga on erinevad venemeelsed häkerite rühmitused, kes sotsiaalmeediagrupidest oma tegevusega kiitlevad. Sihikul ei ole ainult Eesti, vaid ka teised riigid, kes on Vene agressiooni Ukrainas hukka mõistnud ja Ukrainat toetanud.

Juuni lõpus leidsid aset sarnased teenusetõkestusründed Leedu ja Norra vastu, mõlema puhul ajendiks riikide otsus tõkestada sanktsioneeritud kaupade transport Venemaale oma territooriumi kaudu.

Eesti puhul kasutati rünnetes nii kompromiteeritud veebilehti, mis pandi kasutajate teadmata saatma ummistuspäringuid teatud sihtmärkide suunas, kui robotvõrgustikke. Ründelained olid erineva intensiivsusega, aprilli laine tippajal ulatus Eesti veebilehtede suunas tehtud pahaloomuliste päringute arv 700 miljonini mõne tunni jooksul.

Rünnete suhteliselt vähe märgatav mõju tulenes asjaolust, et enamike sihtmärkideks valitud veebilehtede haldajad olid osanud selleks varem valmistuda ning mõnel juhul pakkus CERT-EE ka täiendavat tuge.

### Mida sellest järeldada?

Taoline vaenulik tegevus küberruumis on praegusele ajale iseloomulik ning ühtlasi hea näide häktivismist, millest kirjutasime eelmises [kvartaliülevaates](#). Teenusetõkestusründed on ründajale üsna kulutõhus viis mingit efekti saavutada, seetõttu näeme taolisi laineid kindlasti veel.

Arvestama peab ka sellega, et isegi kui sihtmärgiks ei ole Eesti ettevõtted, võib teiste riikide vastu tehtud rünnatel olla kõrvalmõju näiteks ühiste andmekeskuste kaudu. Üldine juhend, kuidas ennast teenusetõkestusrünnete vastu kaitsta, on leitav [siit](#).

## 2. Kas see oled sina selles videos?

### OLUKORD

Nii aprillis kui mais hoiatasime Facebookis leviva kontode ülevõtmise laine eest. Taas hakkas levima skeem, kus vestluskasutaja saadeti kasutajale sõnum „Vaata mis ma leidsin“ või „Kas see oled sina selles videos?“. Sõnumi juurde oli lisatud pahaloomuline link, mis kutsus seda avama ja kasutaja suunatakse järgmisele veebilehele, kus toimub juba konto ülevõtmine.

Kontode ülevõtmine on CERT-EE registreeritud intsidentide hulgas tõusutrendis. Keskmiselt 20 korda kuus kaaperdatakse konto nii, et inimesel puudub ligipääs ja kontroll enda konto üle. Võrreldes eelmise aastaga on tõus ligi 40%. Statistika kajastavad ainult meile teada antud intsidendid, tegelikkuses juhtub seda kindlasti kordades rohkem.

Pärast seda, kui ründajad saavad inimese sotsiaalmeediakonto enda kätte, vahetavad nad selle parooli, telefoninumbri ja e-posti aadressi, mis muudab konto taastamise palju keerulisemaks. Konto tagasi saamine võib lausa võimatu olla ja selle kohta kirjutasime täpsemalt [RIA blogis](#).

### RIA HINNANG

Seekord toimus kontode ülevõtmine veel kiiremini ja lihtsamalt, kui tavaliselt. Enamasti toimub kontode kaaperdamine õngituslehe kaudu, kuhu inimene ise sisestab pahaaimamatult enda kasutajanime ja parooli.

Seekord piisas aga vaid ühest vales klõpsust, kui avada sõnumi teel saadetud link. Kasutaja ei pruukinud isegi aru saada, et midagi juhtus. Sarnast petuskeemi kasutati ka Instagramis, kus ei pidanud isegi sõbra saadetud lingile vajutama, piisas vaid lingi kuvatõmmisest ja tuttavale tagasi saatmisest.

Kasutajakontode andmete õngitsemine ja ülevõtmine on kurjategijatele lihtne ja odav viis sinu andmete kompromiteerimiseks. Seetõttu kordame üle mõned soovitusel:

- Kõige olulisem on olla teadlik ja tähelepanelik ning mitte avada sõnumi või e-maili teel saadetud suvalisi linke. Sõnumisaatja võib olla sinu tuttav, aga ka täiesti võõras inimene. Seega kui saad kiiret tegutsemist nõudva kahtlase sõnumi, siis ära ava linki.

- Konto ülevõtmine vaid ühele lingile klõpsamisega võib toimuda nii nutiseadmes kui ka arvutis ning selline ründemeetod toimib kõigis sotsiaalmeediakeskkondades. Lisakaitseks pakume RIA loodud Encrypted DNS rakendust, mis blokeerib pahavara ja õngitsusi ning filtreerib DNSi abil kasutaja eest pahatahtlikke linke. Rakendus on kasutatav nii Apple kui Android seadmetes ning selle saab alla laadida ametlikust rakenduste poest. Täpsema info seadistamise kohta leiad [siit](#).
- Saada kahtlased kirjad ja sõnumid RIA intsidentide käsitlemise osakonnale (**CERT-EE**), kasutades selleks <https://raport.cert.ee> keskkonda või [cert@cert.ee](mailto:cert@cert.ee) e-postiaadressi.

### 3. Nutikad kodumasinad ahvatlevad küberründajaid

#### OLUKORD

Maikus kirjutasime [RIA blogis](#) kahest kriitilisest turvanõrkusest, mis mõjutavad ühe tootja videovalvekaameraid. Turvanõrkuste abiga on ründajal potentsiaalselt võimalik haavatavad seadmed üle võtta ja kasutada neid videopildi jälgimiseks, tundliku informatsiooni (paroolid, ärisaladused vms) kogumiseks või liita seade robotvõrgustikuga, mida kasutatakse sihtmärkide ründamiseks hajusate ummistusrünnetega (DDoS).

Turvanõrkused avaldati küll juba 2021. aasta lõpul, kuid CERT-EE tuvastas möödunud kvartalis Eestis endiselt mitusada potentsiaalselt haavatavat seadet. Seejuures ei ole videovalvekaamerad ainukesed seadmed, mida inimesed internetiga ühendavad. Liikudes kaubanduskeskuste ringi, märkame üha rohkem erinevaid kodumasinaid, millel on selline võimekus olemas. Samuti tõuseb ettevõtete hulk, kes erinevaid IoT lahendusi pakuvad. Kuna selliseid seadmeid soetatakse üha rohkem, ei ole inimestel sageli ka täpset ülevaadet seadmetest, mis nende kodus internetti kasutavad.

#### RIA HINNANG

Värvõrgu (Internet of Things, IoT) seadmeid, nagu näiteks tolmuimejaid, videovalvekaameraid, lambipirne, külmkappe või nõudepesumasinaid ei seostata üldiselt küberohtudega, kuna need täidavad väga konkreetseid ülesandeid ja tunduvad ohutud. Seadmete trivialsuses peitub aga nende võlu ründajatele, sest tihtipeale ei ole need turvaliselt konfigureeritud – nad kasutavad vaikimisi seatud paroole, mis on internetist sageli kättesaadavad, neil on uuendamata tarkvara, mis sisaldab turvanõrkuseid või nõuavad nad töötamiseks ebavajalikult palju õiguseid, mida on ründajatel võimalik potentsiaalselt kuritarvitada.

Järgnevalt toome välja mitu soovitusi, mida peaks IoT-seadmete kasutamise puhul tähele panema.

- Vaheta ära kõik seadmetega seatud paroolid ja uuenda neid regulaarselt. Vaikimisi seatud seadmete paroolid on sageli hõlpsasti internetist leitavad või on neid kerge ära arvata.

- Kontrolli regulaarselt, kas erinevad IoT-seadmed vajavad tarkvarauuendusi. Uuenduste korral rakenda need. Aegunud tarkvaraga seadmed sisaldavad turvanõrkuseid, mida ründajatel on võimalik ära kasutada.
- Veendu, et seadmete haldusliidesed ei oleks kõikidele internetist kättesaadavad. Vajadusel loo selle jaoks näiteks vastavad piirangud koduse ruuteri haldusliideses. Mitmel interneti teenusepakujatel on haldusliidestest kasutamise juhendid enda kodulehel ka välja toodud.
- Võimalusel eralda koduvõrku kasutavad seadmed üksteisest. Näiteks loo eraldi võrk lambipirnid, nutikõlaritele ja anduritele samal ajal kui olulisi andmeid sisaldavad seadmed on eraldi võrgus. Koduvõrgu segmenteeritus tagab selle, et pahalastel ei oleks võimalik IoT-seadmete kompromiteerimise korral ligi pääseda näiteks sinu isiklikule arvutile.

### EL leppis kokku uutes ja rangemates küberturvalisuse nõuetes

#### OLUKORD

Viimastel aastatel on üle maailma kasvanud küberohud, seda nii tehnoloogia arengu, digitaliseerimise kui ka intensiivsema küberkuritegevuse tõttu. Nii on tõusnud ka vajadus senisest enam panustada riigiasutuste ja ettevõtete küberturvalisusse. Selleks on Euroopa Liidu liikmesriigid viimase aasta jooksul pidanud põhjalikke läbirääkimisi ja jõudnud kokkuleppele uues nn küberturvalisuse direktiivis ehk võrgu ja infosüsteemide turvalisuse direktiivis (tuntud ka kui NIS 2.0).

Uus direktiiv sedastab võrreldes praegu kehtivaga (nn NIS 1.0) rohkem sektoreid, mis on majanduse ja ühiskonna toimimise jaoks kriitilised ning peaksid oma küberturbesse panustama. Lisandunud on näiteks jäätmeäritlus, posti- ja kulriteenused, kosmosetööstus, keemiatööstus, elektriautode laadimispunktid, avalik sektor ja veel mitmed. Oluline on silmas pidada, et sektor ei tähenda automaatselt kõiki selle sektori asutusi ja ettevõtteid, vaid teatud üksused, mis riigi hinnangul mängivad ühiskonnaelul toimimisel tähtsat rolli.

Lisaks uutele nn kriitilistele sektoritele hakkavad NIS 2.0 direktiiviga selle kohustele kehtima senisest rangemad küberturvalisuse nõuded, suurenevad riikliku järelevalve hoovad, tõhustatakse rahvusvahelist koostööd ja palju muud.

#### RIA HINNANG

Uue direktiivi mõju Eestile võib hinnata keskmiseks. Eeskätt väljendub see selles, et tuleb muuta küberturvalisuse seadust, suureneb seaduse kohustuste hulk ja seetõttu kasvab halduskoormus nii riigiasutustele kui ka ettevõtetele. Samal ajal muutuvad aga Eesti elule olulised teenused küberrünnetele vastupidavamaks ja seega töökindlamaks. Kuna Eesti on oma küberturvalisuse seaduses juba seni olnud küllalt ambitsioonikas, siis ei too uued nõuded meile kursimuutust.

Üks läbirääkimistel suuremat arutelu tekitanud teema oli kohaldamisala ehk mis sektorid ja organisatsioonid peaksid küberturvalisuse nõudeid järgima. Näiteks üks tulisemaid teemasid oli avaliku sektori asutuste subjektide sekka arvamine, sest kõigi riikide jaoks ei olnud see vastuvõetav. Eestile ei olnud see otseselt probleem, sest

meil on juba praegu paljud riigiasutused ja ka kohalikud omavalitsused küberturvalisuse seaduse kohustused. Kompromissina leiti, et avalik sektor siiski on direktiivi skooabis (sh regionaalne tasand), kuid iga riik saab lähtuvalt oma avaliku sektori ülesehitusest seda kohandada.

Suurem aruteluteema oli ka säte, mille kohaselt peaksid selle direktiivi subjektid lisaks küberinsidentidele riigile kohustuslikus korras teada andma ka märkimisväärtest küberohtudest. Selle vastu olid mitmed riigid, sealhulgas Eesti, et vältida kõigile osalistele liigset halduskoormust. Nii jäi see nõue ka tekstist välja.

Uus küberturvalisuse direktiiv ühtlustab ja tõstab ELi küberturvalisuse taset. Samas on oluline silmas pidada, et direktiivi näol on tegemist miinimumharmoneerimisega, mis jätab igale riigile vabaduse rakendada direktiivist rangemaid meetmeid.

Nüüd, kus riigid on omavahel tekstis kokku leppinud, peavad formaalse kinnituse andma ka EL institutsioonid. See juhtub ilmselt septembris ning seejärel on riikidel aega 21 kuud, et vajalikud muudatused oma seadusandluses sisse viia.

#### LÄHEB HÄSTI: ↗

Lisaks värsketele Eesti infoturbestandardile E-ITS on valminud ka uuendus ja väga põhjalik [infoportaal](#), kust standardi senised (riigiasutused, elutähtsate ning oluliste teenuste osutajad) ja tulevased (nt koolid, pearearstid, erinevad teenusepakujad) rakendajad tekkivatele küsimustele vastused saavad.

Praegu Riigikogus menetluses olevate [küberturvalisuse seaduse](#) muudatuste vastuvõtmisel muutub E-ITS kohustuslikuks eeldatavalt alates 01.01.2023.

#### SAAKS PAREMINI: ⚠

Kuigi väljas on suur suvi, ei puhka paraku pätid. Viimastel nädalatel on Eesti elanikke kimbutamas järjekordne pettuste laviin: saadetakse massiliselt liba-SMSe, mille abil loodetakse inimestelt raha varastada. Ohvriks langevad reageerivad sageli liiga ettevaatamatult sõnumitele, mis matkivad nt SEB-d, DHLi ja Swedbanki. Sõnumis olev veebilink suunab kurjategijate kontrolli all olevale õngituslehele, kuhu sisestatud isiku- ja pangakaardiandmed jõuavadki nende kätte. Kokku on juuli alguse seisuga Eesti inimesed sel teel kaotanud mitukümmend tuhat eurot.

[Loe RIA pressiteatest](#), kuidas end petusõnumite vastu paremini kaitsta.

**Kokkuvõtte lõi RIA küberturvalisuse teenistus, et selgitada küberohtude trende laiale auditooriumile, sealhulgas lugejatele väljaspool Eestit. Olukorda küberruumis analüüsib RIA küberturvalisuse teenistus detailsemalt igakuistes kokkuvõtetes.**

Tehnilisemaid soovitusi jagab CERT-EE koolitustel ja RIA kodulehekülje kaudu.