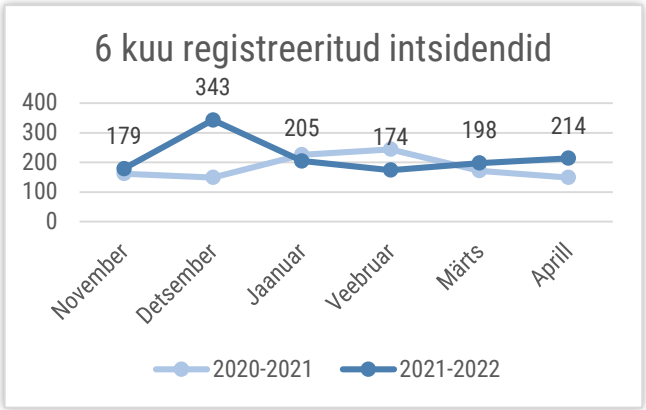
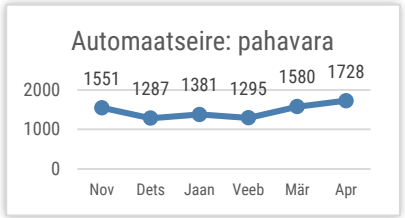
# Olukord küberruumis – aprill 2022

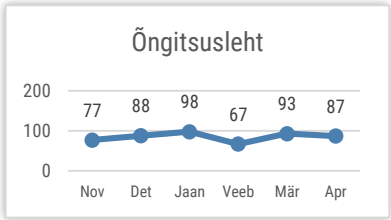
- Aprillis registreerisime 214 mõjuga intsidenti, mis on viimase aasta keskmisest veidi kõrgem näitaja.
- Aprillis sooritati teenusetõkestusründeid Eesti riigiasutuste ja ettevõtete veebilehtede vastu.
- Avaldasime küberruumi kvartaliülevaate ja koostasime ohuhinnangu kriitilisest turvanõrkusest Spring4Shell.
- Jätkusid küberründed nii Ukraina kui ka toetavate riikide vastu.




*CERT-EE-le teavitatud intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.*




*Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.*




*Õngitsuslehed moodustavad jätkuvalt kõige suurema osa CERT-EE registreeritud intsidentidest*

# Olukord Eesti küberruumis

Alates 21.aprillist hakati sooritama **teenuse-tõkestusründeid Eesti riigiasutuste ja elutähtsa ning olulise teenuse osutajate veebilehtede vastu.** Rünnakute sihtmärkideks olid muuhulgas eesti.ee, id.ee, ccdcoe.org, tallinn-airport.ee, zone.ee, elron.ee, politsei.ee, vm.ee, president.ee ja RIA nimeserverid. Rünnakute tõttu toimisid mitmed neist veebilehtedest tavapärasest aeglasemalt või polnud ajutiselt kättesaadavad, kuid üldiselt saame öelda et ummistusründed olid suurema mõjuta. Rünnakud kestsid kuni 25.aprilli õhtuni, kuid suur osa neist hajutati RIA-s kasutusele võetud vastumeetmete abil.

Kahjuks ei möödunud ka aprill ilma **teenuste katkestusteta**. Neljal korral ei olnud kättesaadav Maksu- ja Tolliameti veebileht emta.ee. Katkestused toimusid 1. aprillil, 3. aprillil, 6. aprillil ja 27. aprillil. Tõrkeid põhjustasid seadistusviga veebirakenduse tulemüüris ja süsteemi rike. 6.aprillil lakkas Tartu Ülikooli Kliinikumi veebilehe töö ligi 3 tunniks. 11.aprillil ajavahemikul 12.35 kuni 12.48 ei toiminud digiretseptid, kindlustatuse kontroll ega teised avalikud Haigekassa teenuseid üle x-tee. 13.aprillil ajavahemikul 13.20 kuni 14.10 oli häiritud Elisa võrgus Mobiil-ID kasutamine, mistõttu esines probleeme m-IDga e-teenustesse sisenemisel ja digiallkirja andmisel. 26.aprillil katkesid äriregistri e-teenused riistvararikke tõttu.

Aprillis sooritati hajutatud **teenusetõkestusründeid (DDoS**) meelelahutusettevõtte veebilehe vastu. Ründed toimusid 11. aprillil ja 18. aprillil. Rünnaku mõjul ei olnud võimalik veebilehte külastada ning ei toiminud piletimüük.

Tallinnas tegutsev ettevõte **langes arvepettuse ohvriks**, mille tulemusel saadi üle 17 000 euro kahju. Kurjategijad saatsid ettevõttele kirja, kus paluti tasuda varem saadetud arve, aga seekord teha makse uuele pangakontole. Selliste juhtumite puhul tuleks alati küsida endale teadaolevalt kontaktilt üle, kas tegemist on ikkagi legitiimse kirjaga. Tõenäoliselt oli koostööpartneri meilikonto kompromiteeritud ning seeläbi saadud ligipääs nende andmetele.

Jätkusid **ka erinevad finantspettused**, millest meid teavitati 18 korral. Krüpotorahapettuste kahjude suurus ulatus 10 000 eurost kuni 300 000 USA dollarini. Petuskeeme oli erinevaid ja mõnel juhul tegi kasutaja ise petturitele makseid lootes heale investeerimisvõimalusele, kuid oli ka juhtum kus varastati krüptorahakott. Nägime ka mitmeid Facebooki kaudu tehtud petuskeeme, mis üldjuhul jätsid kasutajale mulje usaldusväärsest müügitehingust, aga peale ülekande tegemist kadusid nii müüja kui ka müügikuulutus ning ostja jäi ilma rahast ja kaubast.

# Tegevused küberturvalisuse parandamisel Eestis

Avaldasime ohuhinnangu märtsi lõpus avalikuks tulnud **Java Spring veebiraamistikuga seotud kriitilise turvanõrkuse** kohta. Spring on üle maailma laialdaselt kasutusel olev raamistik, mis lihtsustab ja kiirendab Java programmeerimiskeelega rakenduste arendamist. Seda kasutatakse ka Eestis ja küberturbeettevõtte Check Point analüüsi kohaselt ohustab iga kuuendat organisatsiooni üle maailma Sping4Shell turvanõrkuse ärakasutamine. Ohuhinnagus toome välja haavatavuse mõju Eestis ja soovitused turvajuhtidele, kuidas turvanõrkused paigata.

Aasta esimeses **kvartaliülevaates** kirjutasime Venemaa agressioonist Ukrainas ja kuidas see on mõjutanud küberruumi, mida oleme teinud vastupidavuse suurendamiseks küberruumis, sõjaga kaasnenud häktivismi lainest ja taas levima hakanud tegevjuhi petuskeemist. Kvartaliülevaate täistekst on leitav RIA kodulehelt.

Korraldasime **lauaõppuse** Narva Linnavalitsusega, mille käigus mängisime läbi olukorra, kus riskid realiseeruvad ja tekib reaalne kahju kuna infoturbemeetmed on rakendamata. Õppuse järelmid on koostamisel ja tulevikus on plaanis ka teiste asutustega sarnaseid üritusi korraldada.

Sulgesime **ISKE portaali** ja viisime ISKE rakendusjuhendi ning ohtude ja meetmete kataloogid üle E-ITS portaali. Ühtlasi pikendasime E-ITS koolituste kestvust juunikuuni ja neile saab registreeruda E-ITS portaalis.

Töötasime välja **rakenduse, mis kaitseb õngitsuste ja pahavara eest**. Rakendus blokeerib pahavara ja õngitsusi ning filtreerib DNSi abil kasutaja eest pahatahtlikke linke. Rohkem infot leiab siit.

**Kohtusime transpordi- ja tervishoiuteenuse sektorite** esindajatega ning rääkisime neile olukorrast küberruumis ja kuidas hetkeolukord võib neid mõjutada. Tõime välja olulised puudused ettevõtete tegevustes infoturbe korraldamisel ja võrgu- ja infosüsteemidele turvameetmete rakendamisel.

**Lõpetasime ühe menetluse, tegime ühe ettekirjutuse ja teostasime jätkutegevusi 7 ettevõtte järelevalvemenetlustega**. Järelevalvemenetlustes on kõrgendatud tähelepanu all turvameetmete rakendamine, IT-riskianalüüs ja riskide haldamine, intsidentide käsitlemise haldus ja turvalise e-posti ning veebileheserveri toimimise korraldamine.

# Rahvusvaheline keskkond

Microsoft teatas aprilli lõpus, et nad on tuvastanud vähemalt kuus Venemaa riiklike sidemetega küberrühmitust, mis on Venemaa invasiooni algusest Ukraina vastu korraldanud üle 237 operatsiooni. Osad destruktiivsed ründed kestavad senini ja ohustavad tsiviilisikute eluolu. Raportis sedastatakse, et Venemaa küberründed paistavad olevat korrelatsioonis riigi kineetiliste sõjaliste operatsioonidega.

Möödunud kuul olid Ukraina kõrval ka mitmed teised Euroopa riigid poliitiliselt motiveeritud küberrünnakute sihtmärgiks. Venemeelne küberrühmitus KillNet korraldas järjepidevalt teenusetõkestusründeid (DDoS) Ukrainat toetavate riikide pihta, lisaks **Eestile** olid sihtmärgiks ka näiteks Tšehhi ja Rumeenia riigiasutuste, ettevõtete ja meediaorganisatsioonide veebilehed.

Euroopa riigid olid ka õngitsuskampaaniate sihtmärgiks. CERT-UA hoiatas aprillis, et on tuvastanud kaks uut Venemaaga seostatud rühmituse Gamaredoni õngitsuskampaaniat: üks sihib Ukraina organisatsioone ja teine ELi riikide asutusi. Kampaaniate eesmärk olevat süsteeme nuhkvaraga nakatada. Peibutusteemana kasutatakse ära sõja temaatikat, näiteks Ukraina kohalikule omavalitsusele saadetud kirja teema oli „*Information on war criminals of the Russian Federation*".

Venemaa küberrühmitusi tabasid aprillis ka mõned tagasilöögid. Näiteks olevat Vene sõjaväeluurega seotud rühmitus Sandworm proovinud rivist välja lüüa Ukraina suurt energiaettevõtet, kuid ebaõnnestus. Häkkerid proovisid elektrialajaamade ühendused katkestada kasutades uut versiooni pahavara Industroyer2. Seda tööstuslikke juhtimissüsteeme (ICS) ründavat pahavara kasutas Sandworm ka 2016. aasta detsembris Ukraina elektrisüsteemi pihta tehtud rünnakus, mis jättis osa Kiievist elektrita. Nüüd õnnestus rünne energiaettevõtte pihta aegsasti tuvastada ja võrku kaitsta.

Ka õiguskaitseorganeid saatis aprillis edu. Europoli koordineeritud rahvusvaheline politseioperatsioon võttis maha ebaseadusliku andmete müügifoorumi RaidForums. Võimud võtsid üle foorumi infrastruktuuri ning vahistasid selle administraatori ja kaks kaasosalist. Andmete seas oli info miljonite krediitkaartide ja pangakontode kohta, samuti ka veebikontode kasutajanimede ja nendega seotud paroolide kohta.

Rahaliselt motiveeritud küberrühmitus Hive0117 sihib õngitsuskirjadega telekommunikatsiooni- ja tööstusettevõtteid Ida Euroopas, näiteks **Eestis**, Leedus ja Venemaal. Venekeelsetes õngitsuskirjades jäljendatakse Venemaa riiklikku kohtutäiturite teenistust.