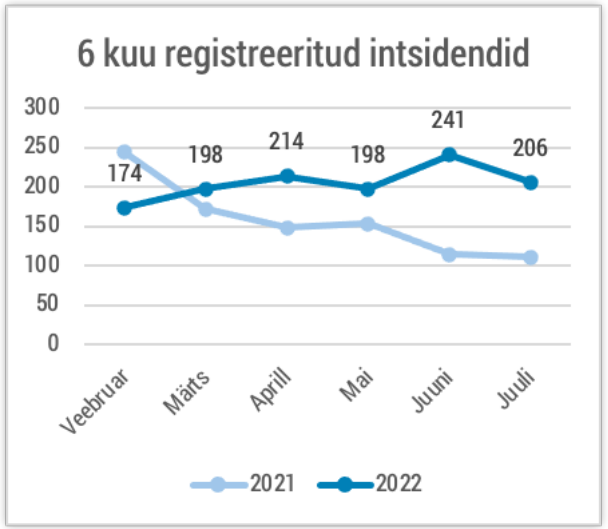
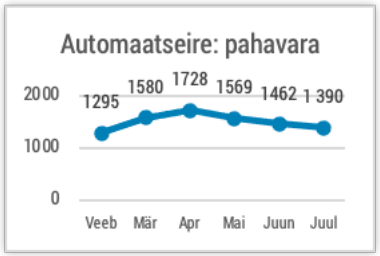
Olukord küberruumis – juuli 2022

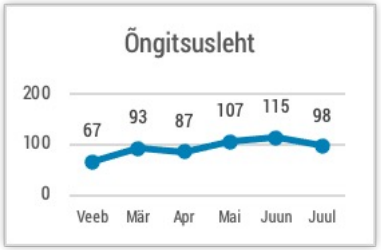
- Juulis registreerisime 206 mõjuga intsidenti, mis on viimase poole aasta keskmine tase.
- Katkestused tabasid Tallinna lennujaama ja Eesti Panga veebilehte ning Telia teenuseid.
- Jätkusid ummistusründed Eesti suunas, kuid tänu kaitsemeetmetele polnud neil mõju.
- Algatasime seitse uut järelevalvemenetlust ja tegime ühe ettekirjutuse.
- Rünnati Ukraina üht suurimat ringhäälingut eesmärgiga levitada valeinfot presidendi tervise kohta.
- Küberrünnakud tabasid Läti riiklikku tele- ja raadiokeskust ning Soome uudisteagentuuri STT.



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

Juulis nägime taas mitmeid **teenusekatkestusi**. 9. juulil katkes kolmveerand tunniks Tallinna lennujaama veebilehe töö, 12. juulil polnud kuue tunni jooksul kättesaadav Eesti Panga veebileht ja 18. juulil tõrkus rohkem kui viie tunni jooksul Mobiil-ID. 19. juuli pärastlõunal tekkisid tõrked Telia teenustega – ei toiminud lühinumbrid ega mobiilne parkimine -, mis taastusid järgmisel hommikul. 21. juuli ööl katkes Eesti Hariduse ja Teaduse Andmesidevõrgu EENet nimeserverite töö, mistõttu polnud kättesaadavad mitmed veebilehed. 21. juuli hommikul ei saanud seadistusvea tõttu ligi pooleteist tunni jooksul siseneda riigiportaali eesti.ee.

Jätkusid **teenusetõkestusründed**. 2. juulil tabas ummistusrünne Vabariigi Presidendi veebilehte, 7. juulil üritati masspäringutega üle koormata Tallinna lennujaama ja Vabariigi Valitsuse veebileht. Tänu kaitsemeetmetele polnud neil rünnakutel mõju.

Juulis saime teate ühest **lunavarajuhtumist**. Ettevõte tegi oma IT-süsteemides muudatusi, mille käigus jäeti avatuks mõned mittevajalikud, kuid küberkurjategijate seas kõrgelt hinnatud teenused. Vaid kaks päeva hiljem olid failid lunavara poolt krüpteeritud. Andmed taastati varukoopiast ja väljapressijatel jäi tasu saamata, aga on oht, et pärast süsteemi kompromiteerimist tehti seal muudki kurja.

Üks lunavararühmitus oli aga lisanud Eesti ettevõtte oma **andmelekete** veebilehele. Osade lunavararünnakute puhul ründaja mitte üksnes ei krüpteeri ohvri andmed, vaid ka varastab need. Juhul, kui ohver väljapressijale dekrüpteerimisvõtme eest ei maksa, kasutab kurjategija järgmise mõjutusvahendina ähvardust andmed avalikustada.

Ühele linnavalitsusele kuuluvatest ja avalikuks kasutamiseks mõeldud arvutitest leiti **klahvinuhk** (*keylogger*), mis varastas paroole ning muid tundlikke andmeid. See juhtum annab põhjuse korrata soovitust kasutada mitmeastmelist autentimist ja erinevatel kontodel erinevaid paroole. Mõlemad sammud muudavad küberkurjategijate elu keerulisemaks.

Tegevused küberturvalisuse parandamisel Eestis

Aasta teises kvartaliülevaates kirjutasime Eestit tabanud teenustõkestusrünnete lainetest ja nende mõjust, Facebookis levinud kontode ülevõtmisest uuel moel, nutikaid kodumasinaid ohustavatest turvanõrkustest ja uuest küberturvalisuse direktiivist (tuntud kui NIS 2.0). Kvartaliülevaate täistekst on leitav RIA kodulehelt.

Otsime arenduspartnereid, kes arendaks edasi ja hooldaks Eesti Infoturbestandardi (E-ITS) portaali ning looks selle tarbeks uusi lahendusi. Raamhanke maksumus on miljon eurot ning leping sõlmitakse neljaks aastaks.

Avaldasime ID-tarkvara uue versiooni. Suurim muudatus on toe lõppemine Windowsi 32-bitistele operatsioonisüsteemidele, mis on tingitud sellest, et mainitud operatsioonisüsteemidele ei arendata enam hädavajalikke tarkvarakomponente ning see mõjutab ka ID-tarkvara toimimist nendes süsteemides. Uuendustest kirjutasime täpsemalt RIA kodulehel.

Algatasime seitse uut **järelevalvemenetlust** ja tegime ühe ettekirjutuse. Järelevalvemenetluste eesmärgiks on kontrollida elutähtsat teenust osutavates ettevõtetes küberturvalisuse nõuete täitmist nii organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamise vaatenurgast.

Juulis jätkus Raadio 4 eetris venekeelne küberteadmistele keskenduv raadiosari „Введи пароль“ („Sisesta parool“) ja ühtlasi kestab ka teavituskampaania, mis juhib tähelepanu turvalisele küberkäitumisele. Saated on Raadio 4 eetris igal esmaspäeval kuni augusti lõpuni ning neid saab järgi kuulata RIA IT-vaatliku portaalis.

Rahvusvaheline keskkond

Euroopa Liidu kõrge esindaja mõistis juulis hukka venemeelsete häkkerite pidevad teenusetõkestus-rünnakud (DDoS) Euroopa riikide ja partnerite vastu. Avalik deklaratsioon rõhutas, et EL uurib pahatahtlikku kübertegevust, mis mõjutab rahvusvahelist rahu, turvalisust ja stabiilsust.

Juulis tabasid küberrünnakud meie naabermaid. Kuu alguses sai ummistusrünnetega pihta Läti riiklik tele- ja raadiokeskus (LVRTC), mis pakub andmesideteenust ning e-identiteedi teenuseid, nt e-allkirjastamist. Ründed olid täpselt sihitud ja tehniliselt hästi läbi viidud, kuid asutus tõrjus need edukalt ning suuremat mõju neil polnud. Juuli lõpus rünnati Soome uudisteagentuuri STT. Rünnaku tagajärjel oli agentuur sunnitud mõned süsteemid võrgust eemaldama.

Kehvemini läks Albaanial, kus küberkurjategijate sihtmärgiks oli mitmeid e-teenuseid pakkuv infoühiskonna agentuur (AKSHI). Rünnaku tõttu polnud ühe päeva jooksul enamik riiklikke e-teenuseid kättesaadavad. Pressiteate kohaselt polnud Albaania varem nii massiivse küberünnaku ohvriks langenud ja see pärines väljastpoolt Albaaniat.

Jätkusid sõjaga seotud küberründed: rünnati Ukraina üht suurimat ringhäälingut eesmärgiga levitada valeinfot Ukraina presidendi tervise kohta. Ukraina nn IT-armee ründas aga Venemaa kinosid. Väidetavalt korraldati teenusetõkestusrünnakuid üle 80 kino vastu. Rünnete tõttu oli kinode veebilehtede töö häiritud ja nende kaudu ei saanud osta pileteid.

Ligi kahe miljoni kliendiga Prantsusmaa mobiili-operaatorit tabas Lockbiti lunavara. Selle tõttu olid häiritud osad teenused, võimalik oli ka andmeleke. Küberrühmitus Lockbit on rünnanud, näiteks, maailma üht suurimat IT-konsultatsiooniettevõtet Accenture ja Taani tuulegeneraatorite tootjat Vestas..

Kanada ühe suurima mobiili- ja internetipakkuja Rogers teenusekatkestus mõjutas juulis riigi transpordi-, pangandus- ja hädaabiteenuseid, sh 911 hädaabinumbrit. Üle 15 tunni kestnud katkestuse põhjustas tuumikvõrgu ebaõnnestunud uuendus.