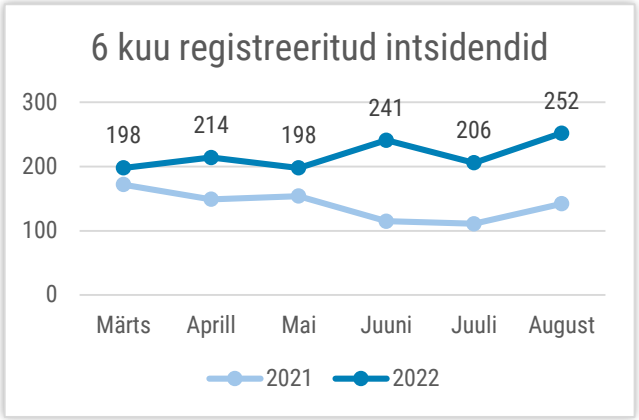
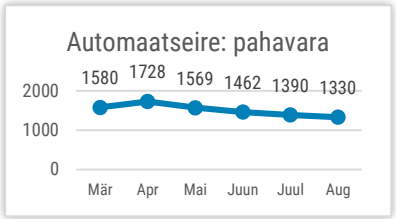
Olukord küberruumis – august 2022

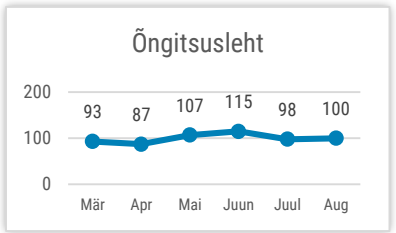
- Augustis registreerisime 252 mõjuga intsidenti, mis on viimase poole aasta kõige kõrgem näitaja.
- Augustis sagenesid teenusetõkestusründed Eesti riigiasutuste ja ettevõtete vastu, kuid vaatamata suuremahulistele rünnetele ei olnud neil märkimisväärset mõju.
- 30. augustil ei saanud kolme tunni vältel kasutada ID-kaarti, Mobiil-ID ega Smart-ID teenuseid autentimiseks.
- Nii Itaalias kui Montenegros rünnati digitaalset infrastruktuuri, mille tagajärjel olid paljud teenused rivist väljas.



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

Nagu viimastel kuudel juba tavaks, toimus mitmeid **teenusekatkestusi**. Kahel korral, 2. augustil ja 8. augustil, ei olnud võimalik tehniliste tõrgete tõttu külastada Elroni veebilehte ega osta rongipileteid. 15. augustil ajavahemikul 10.30 kuni 13.30 oli katkestus Tartu Ülikooli Kliinikumi registratuuri töös, mistõttu oli teenuste osutamine häiritud ja tavapärased tööprotsessid oluliselt aeglasemad. Probleemi põhjustas võrgulüliti seadistamine. 23. augustil ajavahemikul 12.10 kuni 13.15 olid häired Telia mobiilsideteenuste kasutamises, mis mõjutas nii kõnesid kui andmesidet. Telia kinnitusel ei olnud tegemist ründega, vaid tehnilise probleemiga. 30. augustil oli ligi kolmetunnine katkestus SK ID Solutions AS autentimisteenuste töös, muuhulgas olid häiritud ID-kaardi, Mobiil-ID ja Smart-ID kasutamine.

Alates 5. augustist kuni kuu lõpuni sagenesid **teenusetõkestusründed** (DDoS) Eesti riigiasutuste ja ettevõtete vastu, kuid tänu kasutusele võetud kaitsemeetmetele ei olnud neil suurt mõju. Kõige intensiivsemad ründed toimusid 16. ja 17. augustil ning väga tõenäoliselt korraldati need protestiks Narva tankimonumendi teisaldamise eest. Kõige nähtavam mõju oli 17. augustil toimunud emta.ee veebilehe vastasel rünnakul, kui ajavahemikul 12.30 kuni 13.40 ei olnud veebileht kättesaadav. Sihtmärkideks olid erinevad asutused ja ettevõtted, nende hulgas näiteks Riigikogu, Välisministeeriumi, Kaitseministeeriumi, Politsei- ja Piirivalveameti, SK ID Solutionsi, Eesti Kaitseväe, Omniva, Vabariigi Presidendi Kantselei, Maksu- ja Tolliameti, Elroni, eesti.ee, id.ee ja Tallinna Lennujaama veebilehed.

Augustis levisid näiliselt Politsei nimel saadetud nn sextortion-**väljapressimiskirjad**, milles väideti et kasutaja on toime pannud seksuaalkuriteo ja tema suhtes algatatakse menetlus. Kirjale paluti vastata ja saata oma põhjendused 48 tunni jooksul. Meile teadaolevalt peale vastamist saadeti kasutajale võltsitud trahviteade. Selliseid kirju tuleks eirata, ja kiri kas lihtsalt kustutada või saata edasi CERT-EE aadressile cert@cert.ee uurimiseks.

Lisaks väljapressimiskirjadele levisid ka **pahavaraga kirjad**, mis saadeti justkui Tallinna Ülikooli ja Swedbanki nimel. Mõlemal juhul oli kirja manusena kaasas pahavaraga fail. Tuletame meelde, et kahtlaste e-kirjade manuseid ei tohiks avada, vaid kiri tuleks ära kustutada. E-kirja teel pahavara saatmine on levinud viis kasutaja seadmele ligipääsu saamiseks ja üldjuhul saadetakse pahaloomulisi faile kas manuse või lingi teel.

Tegevused küberturvalisuse parandamisel Eestis

Seoses **sagenenud teenusetõkestusrünnetega**, jälgisime pidevalt nii olukorda küberruumis kui erinevatel kanalitel tehtud teavitusi. Jagasime kogukonnale ja partneritele jooksvalt infot ning pakkusime neile RIA kaitsemeetmeid. Kui tavapäraselt registreerime kuu jooksul kümmekond ummistusrünnakut, siis augustis toimus neid 65 korral.

Augustis saatsime CERT-EE meeskonna poolt erinevaid **teavitusi domeenide omanikele**. Hoiatasime domeenide omanikke, kelle haldusalasse kuulub Wordpressi kriitilise turvanõrkusega haavatav veebileht. Tegemist on päringute võltsimist võimaldava veaga, mille abil võib ründajal olla võimalik teostada päringuid ja ründeid veebiserveri ning tulemüüri taga olevate süsteemide suunas. Lisaks teavitasime neid, kelle haldusalas oli toimunud andmeleke ehk kelle kasutajatunnused olid sattunud tumeveebi müüki.

Sel sügisel on taas võimalik osaleda **infoturbe halduse baaskoolitustel**. Koolituse eesmärk on anda tulevastele Eesti infoturbestandardi (E-ITS) rakendajatele teadmised ja oskused standardi rakendamiseks. Kokku toimub 30 koolitust, täpsem info ja koolituste kuupäevad on leitavad E-ITS portaalis.

Alustasime **5 uut järelevalvemenetlust**, neist neli tervishoiuteenuste osutajate ja üks vedelkütusega varustaja suhtes. Järelevalvemenetluste eesmärgiks on kontrollida elutähtsat teenust osutavates ettevõtetes küberturvalisuse nõuete täitmist nii organisatsiooniliste, füüsiliste kui infotehniliste turvameetmete rakendamise vaatenurgast. Kõrgendatud tähelepanu all on teenuse osutamiseks ettevõtte arvutivõrgu- ja infosüsteemidele rakendatud turvameetmete kirjeldused, riskianalüüs ja riskide haldamine.

Lõime koos Nortaliga avalikule sektorile uue **keskse seansihaldusega autentimisteenuse**, mis tagab e-teenustesse ühekordse sisse- ja väljalogimise. Uus lahendus teeb e-teenuste kasutamise mugavamaks, kuna mitme keskkonna vahel liikudes piisab vaid ühekordsest autentimisest. Täpsemalt saab uue autentimisteenuse kohta lugeda RIA veebilehelt.

Augustis jätkusid nii **venekeelne küberteadmisi õpetav raadiosari kui teavituskampaania**, mis juhtisid tähelepanu turvalisele küberkäitumisele. Kokku 13 saadet olid Raadio 4 eetris igal esmaspäeval ja kordusena laupäeval kuni augusti lõpuni ning neid saab järele kuulata RIA IT-vaatliku portaalis. Keskmiselt kogus iga saade kahe eetrisoleku peale üle 43000 unikaalse kuulaja.

Rahvusvaheline keskkond

Möödunud kuul toimus küberrünnak Montenegro riigi digitaalse infrastruktuuri pihta. Paljud teenused (sh transpordi, vee ja elektri) olid rivist väljas, nt tuli riigi elektrivõrk ümber lülitada manuaalsele režiimile. Montenegro teatel on rünnete taga Vene eriteenistused, kuid ründe ühe osa eest on vastutuse võtnud ka Cuba-nimelist lunavara kasutav kuritegelik küberrühmitus. Montenegro teavitas rünnakust teisi NATO riike, neile läksid appi eksperdid USAst ja Prantsusmaalt.

Augustis sai ka teatavaks, et juuli keskpaigas Albaaniat tabanud küberrünnakute taga olevat olnud Iraan. Ehkki Iraani küberluureoperatsioone on üle maailma palju täheldatud, siis teenuste tööd häirivad rünnakud Iraanist ühe NATO liikmesriigi pihta on ebatavaline.

Ka viimase kuu jooksul jätkusid küberründed seoses Venemaa agressiooniga Ukrainas. Näiteks ründas grupp venemeelseid häktiviste Ukraina riikliku tuumaenergia ettevõtte Energoatom veebilehte. Teine grupp Vene häktiviste ründas Soome parlamendi veebilehte.

Aktiivsed olid ka ukrainameelsed häkkerid. Näiteks teatas Anonymous, et nad häkkisid Venemaa suurima taksoteenuse Yandexi rakendust. Häkkerid olevat tellinud taksod kõik ühele aadressile, tekitades 1. septembril Moskva kesklinnas suure ummiku.

Lisaks oli aktiivne Ukraina küberpolitsei (SSU), mis sulges miljonist veebirobotist koosneva robotvõrgustiku ehk botifarmi, mida kasutati sotsiaalvõrgustikes valeinfo levitamiseks. Robotvõrgustiku eesmärk oli diskrediteerida Ukraina ametlikest allikatest pärinevat teavet ja destabiliseerida sotsiaalset ning poliitilist olukorda riigis.

Augustis oli ka mitmeid lunavararünnakuid kriitiliste teenuste pihta. Näiteks 1000-voodikohaga Prantsusmaa haigla töö oli LockBiti lunavara tõttu raskelt häiritud, sest haigla äritarkvara, salvestussüsteemid (täpsemalt radioloogia) ja patsientide vastuvõtuga seotud infosüsteemid olid rivist väljas. Paljud patsiendid suunati teistesse haiglatesse.

Kaks Itaalia energiasektori üksust olid küberrünnete sihtmärgiks – kütusehiiglane Eni ja energiaagentuur GSE. Viimase eest võttis vastutuse lunavararühmitus BlackCat, mis enda sõnul varastas 700 GB andmeid, sh lepinguid, projektiinfot, raamatupidamisdokumente.

Lisaks oli elu häirivaid küberründeid ka tavaliste ettevõtete pihta. Näiteks Taanis pidid 175 7-Eleven kauplust lunavararünnaku tõttu oma uksed ajutiselt sulgema, sest ründe tõttu polnud võimalik kasutada kassasid ega võtta vastu makseid. Hollandis jällegi oli päevadeks häiritud 120 hambaravipraksise töö.