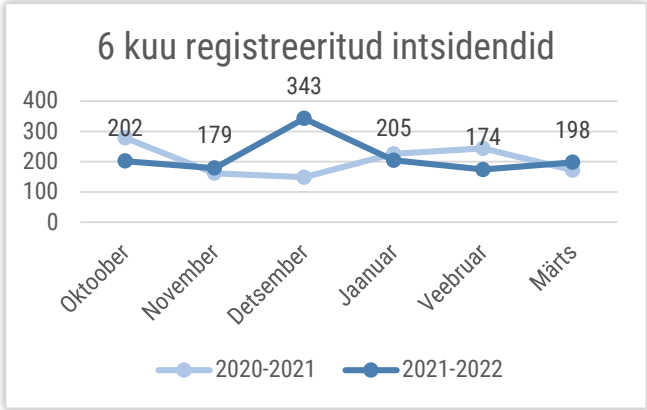
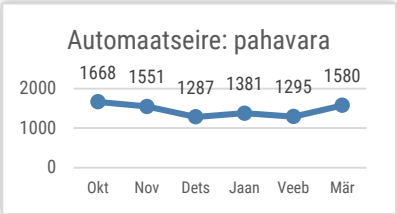
Olukord küberruumis – märts 2022

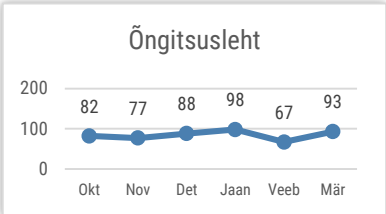
- Märtsis registreerisime 198 mõjuga intsidenti, mis on aasta keskmisel tasemel, kuid tõus võrreldes eelmise kuuga.
- Märtsis esines nii teenusekatkestusi, DDoS ründeid kui ka lunavaraga nakatumist.
- Hoiatasime uut tüüpi libakirjade eest, avaldasime mitu ohuhinnangut ning analüüsisime põhjalikult Ukrainas toimuvaid küberrünnakuid.
- Jätkusid küberrünnakud Ukraina vastu, neist kõige suurema mõjuga oli telekommunikatsiooniettevõtte Ukrtelekomi vastu suunatud küberrünne.



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

Nii nagu eelmisel kuul, **nägime ka märtsis mitmeid teenusekatkestusi**. Politsei- ja Piirivalveameti (PPA) biomeetriateenuse töös oli 4.märtsil ajavahemikul 10.37 kuni 17.40 ligi seitsmetunnine paus, mille jooksul ei toiminud PPA teenindustes sõrmejälgede ega fotode hõive, samuti oli probleeme piirikontrolliga. Intsidendi põhjustas probleem tarkvara sertifikaatidega. 16.märtsil esines häireid PPA isikutuvastus- ja menetlus-infosüsteemis UUSIS, mis põhjustas probleeme piirikontrolli infosüsteemis, relvaregistris ja isikut tõendavate dokumentide väljastamisel. Intsidendi põhjustas tarkvara viga. Nii Riigikohtu, Õiguskantsleri kui ka Majandus-ja Kommunikatsiooniministeeriumi veebilehed olid korduvalt kättesaamatud süsteemi tõrgete tõttu. Samuti esines katkestusi tervise infosüsteemi töös.

Jätkusid **teenustõkestusrünnakud (DDoS)** nii õppeinfosüsteemi Tahvel, koolide kui ka ERR pihta. Õppeinfosüsteemi Tahvel vastu korraldati DDoS rünne kuuel korral märtsis. 14.03 ajavahemikul 8.25 kuni 11.45 toimus neli DDoS rünnet ühe Raplamaal asuva kooli vastu. Neil rünnetel mõju ei olnud ja tavapärane töö jätkus. Eesti Rahvusringhäälingut (ERR) rünnati 21.03 ajavahemikul 18.34 kuni 18.36, häiritud oli veebilehtede töö ja otsestriiming. Teenuste töö taastus kell 19.

Paaril korral tuvastasime monitooringu abil võrguliikluse, mis on omane **pahavaraga nakatunud seadmega krüptoraha kaevamisele**. Tõenäoliselt olid ühe kohaliku omavalitsuse haldusalas olevad masinad pahavaraga nakatunud ning seadistatud krüptoraha kaevandama kolmanda osapoole jaoks. Selline tegevus kasutab palju ressursse ning selle mõjul on seade tavapärasest aeglasem ning ventilaatorid töötavad kiiremini.

Märtsis **levisid Tallinna Ülikooli ja Estonian Business Schooli nimel saadetud pahavaraga e-kirjad**. Kirjadele oli lisatud manusena pahavaraga nakatunud Exceli või ZIP-fail, selle avamisel ja makrode käivitamisel oli kurjategijatel võimalik saada ligipääs kasutaja seadmele. Kirjade pealkirjaks oli näiteks „Hinnapäring 10.03.2022 (Tallinna Ülikool)“ ja neis kutsuti esitama hinnapakkumisi kooli eelarvele. Riigivõrgus prooviti sarnaseid e-kirju saata rohkem kui 40 000 korral, aga paljud neist blokeeriti juba enne kasutajateni jõudmist. Taoliste e-kirjade puhul on oluline manust mitte avada, kiri edastada asutuse või ettevõtte IT-toele ning seejärel kustutada. Nii toimides e-kiri ega selles sisalduv pahavara arvutis ohtu ei kujuta.

Eesti ettevõtet tabas **lunavararünnak, mille käigus krüpteeriti raamatupidamistarkvara andmebaas ja tagavarakoopiad**, mis asusid samas serveris. Server oli avalikult kättesaadav RDP (Remote Desktop Protocol) lahenduse kaudu. Tihti on kaugtöölauatarkvara ebaturvaliselt seadistatud, mis tähendab et RDP jaoks lahti jäetud võrguühenduste kaudu saab arvutile või serverile ligi välisvõrgust. Nägime veel kahte taolist rünnakut märtsi jooksul.

Tegevused küberturvalisuse parandamisel Eestis

Avaldasime **ohuhinnangu** **lunavararünnakute ning kaugtöölaua protokolli RDP** (Remote Desktop Protocol) turvaliselt seadistamise kohta. Viimasel ajal oleme näinud, et enamus lunavararünnakuid sooritatakse just ebaturvaliselt seadistatud RDP kaudu. Anname ohuhinnangus soovitused, kuidas kaugtöölaua protokolli turvata.

Hoiatasime **uut tüüpi** **libakirjade eest**, mis kasutavad ära Venemaa sõda Ukraina vastu. Petukirjadega proovitakse koguda inimeste andmeid ja levitada pahavara. Samuti esinevad kurjategijad heategevusorganisatsioonidena ja küsivad heausksetelt inimestelt krüptorahas annetusi. Need annetused paraku abivajajateni ei jõua.

Avaldasime **uue** **ohuhinnangu** Ukraina vastastest küberrünnakutest ja nende võimalikust mõjust Eestis. Ohuhinnangus tõime välja, milliseid ründeid on kasutatud Ukraina vastu ja mida oleme Eesti küberruumis näinud viimaste kuude jooksul. CERT-EE igapäevane monitooring näitab, et haavatavuste otsimine ja nende pahatahtlik katsetamine on tavapärasest pisut aktiivsem. Ohuhinnangus andsime neli soovitust enda pettuste ja libakirjade eest kaitsmiseks.

Avaldasime **Eesti infoturbestandardi ehk E-ITSi** uue 2021.aasta versiooni ja uuendatud portaali. Uues versioonis on täiendatud moodulite tekste ja juhendeid ning lisatud videod. 2024. aastaks peavad kõik senised ISKE rakendajad üle minema kas Eesti infoturbestandardile või rahvusvaheliselt tunnustatud standardile ISO27001. E-ITSi on arendatud kooskõlas ISO27001-ga, kuid seejuures on E-ITSi eeliseks, et tegu etalonturbega, mis annab tüüpsete varade jaoks juba valmis meetmete komplektid.

Kohtusime Eesti Kaupmeeste Liidu, Eesti telekommunikatsiooni ettevõtetega ja Eesti Rahvusringhäälinguga ning andsime neile ülevaate julgeolekuolukorrast seoses sõjaga Ukrainas, olukorrast küberruumis ja peamistest ohtudest, mis nende endi sektoreid võivad mõjutada. Tutvustasime CERT-EE poolt pakutavaid avalikke tööriistu ja leppisime kokku edasised koostöövõimalused.

Hoiatasime **CERT-EE Twitteri** **konto** vahendusel erinevate märtsis levinud pahaloomuliste kirjade ja SMS-sõnumite osas. Soovitame hakata konto jälgijaks, et edaspidi jõuaks hoiatused pahavaraga kirjade või sõnumite kohta kiirelt kohale.

Analüüsisime põhjalikult **Ukrainat tabanud küberrünnakuid**, koondasime info kokku avalike allikate põhjal ja hindasime nende mõju. Kokkuvõte aitab paremini mõista, kuidas ja milleks küberrünnakuid sõja ajal kasutatakse ning miks ei ole laiaulatuslikku kübersõda toimunud.

Rahvusvaheline keskkond

Venemaa jätkuv agressioon Ukrainas oli märtsis nähtav ka küberruumis. Ukraina sai pihta kõige jõulisema küberrünnakuga invasiooni algusest, mis viis rivist välja riigi suurima telekommunikatsioonieттevõtte Ukrtelekomi. Ründe tõttu jäid inimesed ühenduseta üle riigi. Hinnanguliselt langes ühenduvus üle 80 protsendi võrreldes sõjaeelse ajaga. Kriitilisest infrastruktuurist sai märtsis teist korda küberrünnakuga pihta ka Ukraina telekom Triolan.

Lisaks tuvastati märtsis uut tüüpi hävituslikke pahavarasid, mille eesmärk on nakatatud seadmetest kogu info kustutada ja need kasutuskõlbmatuks muuta. Hävitusvaradega sihitakse aktiivselt Ukraina riigiasutusi ja ettevõtteid.

Ründajad kasutasid Ukraina kohalike omavalitsuste kompromiteeritud veebilehti valeinfo levitamiseks ja postitasid omavalitsuste nimel teateid Kiievi langemise kohta. Kompromiteeritud Ukraina uudistesaitidel (nt Ukraine 24) levitati *deepfake* videot Ukraina presidendist Volodõmõr Zelenskist.

Ukrainameelselt häälestatud häktivistide rühmitus Anonymous teatas kuu vältel paljudest rünnetest Venemaa organisatsioonide pihta. Näiteks teatati Venemaa keskpanga häkkimisest ja sealt varastatud dokumentide lekitamisest, samuti ka rünnetest Vene Õigeusu Kiriku ja Vene oligarhide investeerimisettevõtete pihta.

Ukraina julgeolekuteenistus SBU teatas, et nad on alates Venemaa sissetungist 24. veebruaril avastanud ja maha võtnud viis valeinfot levitavat robotvõrgusikku ehk nn trollifarmi.

Google'i teatel proovisid Venemaa häkkerid ligi pääseda ühe NATO kompetentsikeskuse ja mitme Ida-Euroopa riigi relvajõudude võrkudesse. Ligipääsu olevat proovitud saada õngitsuskampaania abil. Väidetavalt oli õngitsuste taga Venemaal tegutsev küberrühmitus nimega Callisto.

Ka küberkurjategijad olid märtsis aktiivsed. Rühmituse Lapsus$'i ohvrite nimekirja lisandusid mitmed suured tegijad, näiteks Microsoft, rahvusvaheline autentimis-ettevõte Okta ning IT- ja tarkvaraarendamise ettevõte Globant. Rühmituse *modus operandi* on tungida ohvri süsteemidesse, varastada andmed ning nõuda andmete mitte lekitamise eest raha. Kuu lõpus saabusid teated, et võimud pidasid Ühendkuningriigis kinni mitu rühmituse liiget, kes olid vanuses 16-21.

Küberründed häirisid viimase kuu jooksul elu üle maailma ja seda mitmel moel. Näiteks tabas Iisraeli valitsusasutuste veebilehti massiivne teenuse-tõkestusrünne (DDoS). Lunavara tõttu oli mitu päeva häiritud Kreeka riiklik postiteenus. UK kaitse-ministeeriumi teatel õnnestus tundmatutel ründajatel kompromiteerida mõned andmed sõjaväkke värbamise süsteemis, mille kaudu saavad inimesed end veebi teel sõjaväkke registreerida.