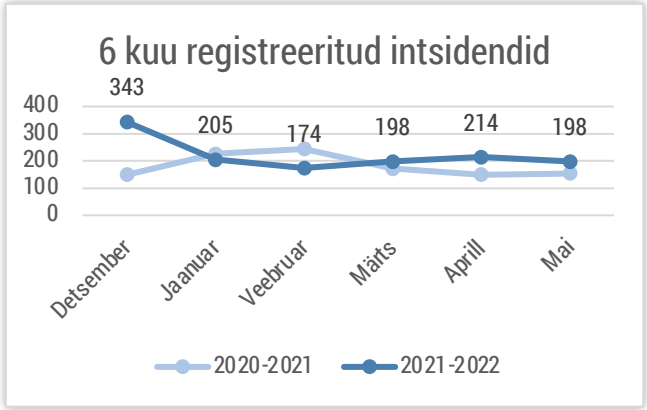
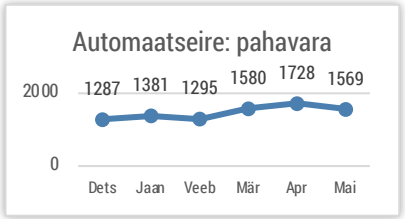
Olukord küberruumis – mai 2022

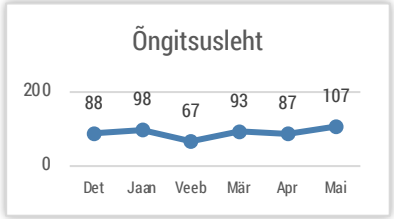
- Mais registreerisime 198 mõjuga intsidenti, mis on viimase aasta keskmisest veidi madalam näitaja.
- Mais jätkusid teenusetõkestusründed Eesti riigiasutuste veebilehtede vastu, kuid üldjuhul neil puudus suurem mõju tänu kasutusele võetud kaitsemeetmetele.
- Avaldasime RIA blogis mitu postitust ja hoiatasime Facebookis levivast kontode ülevõtmise skeemist.
- Jätkusid küberründed nii Ukraina, Venemaa kui ka Ukrainat 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

Kahel korral toimus **katkestus Haigekassa teenuste töös**. 3.mail ajavahemikul 10.46 kuni 10.58 ja 12. mail ajavahemikul 10.38 kuni 10.46 ei olnud võimalik kasutada digiretsepti, kindlustatuse kontrolli ega teisi avalikke Haigekaasa teenuseid üle X-tee.

4. mail ajavahemikul 9.30 kuni 11.00 katkes Smart-ID-ga autentimine ja allkirjastamine. 29. mail ajavahemikul 10.25 kuni 11.22 esines **tõrkeid kõigis SK ID Solutions teenustes**, nende hulgas ID-kaardi, Mobiil-ID ja Smart-ID kasutamises. Lisaks ei toiminud ka ID-kaartide, Mobiil-ID ja Smart-ID väljastamine. Tõrked põhjustas andmebaasi viga.

8. ja 9. mail sooritati **teenusetõkestusründeid** (DDoS) Välisministeeriumi, Siseministeeriumi ja Politsei- ja Piirivalveameti avalike veebide vastu. Kõige suurem mõju oli rünnak Välisministeeriumi veebilehele vm.ee, mis ei olnud 8. mail ajavahemikul 22.33 kuni 23.33 ja 9. mail ajavahemikul 7.49 kuni 11.45 kättesaadav. 28. mail sooritati lühiajalise katkestuse põhjustanud DDoS rünne Riigi Infosüsteemi Ameti veebilehe ria.ee vastu.

10. mail ajavahemikul 18.24-18.55 esines häireid **piirikontrolli infosüsteemis** PIKO, mistõttu polnud võimalik piiriületusi registreerida.

31.mail ajavahemikul 14.10 kuni 17.00 olid **keskse tulemüüri probleemidest tingitult häired** erinevates Siseministeeriumi infotehnoloogia ja arenduskeskuse (SMIT) hallatavates teenustes, nende hulgas UUSIS, PIKO, HKSOS, OIS, PÄVIS ja relvaregister.

Üks Tartu ettevõte langes **palgakonto-pettuse ohvriks**. Personalijuht sai kirja, milles end töötajana esitlenud petis palus kanda oma töötasu edaspidi uuele pangakontole. Andmeid üle kontrollimata tehti soovitud muudatus ja kanti palk ning puhkusetasu petturi kontrolli all olevale kontole. Soovitame alati taoliste kirjade puhul töötajalt või kliendilt üle küsida, kas tema ikka on selle kirja saatnud ja kas kirjas olev info vastab tõele.

Jätkuvalt levivad mitmesugused **õngitsuslehed**, mida registreerisime kokku 107 korral. Tihti on sellised petulehed tõetruult järgi tehtud ja kasutajal jääb mulje, et sisestab enda andmed näiteks panga veebilehele. Seetõttu on oluline alati kontrollida veebilehe aadressi, kus isiku- ja kontoandmeid sisestada palutakse. Enamasti näeb veebileht legitiimne välja, kuid aadressireal on näiteks swedbank.ee asemel hoopis swed-loged.com. Kahtluse korral võib alati panka või muule teenusepakkujale üle helistada ja kontrollida, kas tegemist on õige lehega.

Tegevused küberturvalisuse parandamisel Eestis

Avaldasime RIA blogis mitu uut postitust. Esimene neist on **Dahua videovalvekaamerate kriitiliste turvanõrkuste** kohta. 2021.aasta sügisel avaldati kaks kriitilist turvanõrkust, mis mõjutavad Dahua valveseadmeid ja mille kaudu on võimalik ründajal ilma paroolita haavatavate kaamerate haldusliidesesse ligi pääseda. 10. mai seisuga on Eestis ligi 1500 internetis nähtavat Dahua seadet. Ohuhinnangus andsime nõu, kuidas valvekaameraid ja muid seadmed turvaliselt seadistada ja kasutada. Teavitasime teenusepakkujaid nende klientidele kuuluvatest Dahua seadmetest, millel on turvauuendused tegemata.

Teine postitus kirjeldab **suuremahulist õngitsuskampaaniat**, mis sihib Eesti ettevõtteid. E-kirjade saatmiseks kasutatakse kompromiteeritud koostööpartnerite meilikontosid ja kuna saatja aadress oli korrektne, ei teki kirja saajal kahtlust ja avataksegi jagatud faili link. Peale lingi avamist suunati kasutaja õngitsuslehele oma kontoandmeid sisestama.

Kolmandas postituses räägime **tarneahelarünnakutest**, mis need on, millist mõju võivad avaldada ja kuidas end ründe eest kaitsta.

Taas levitati **Facebooki vestluste kaudu pahaloomulist linki,** millele vajutades võetakse kasutaja konto üle. Küberründajad saatsid Messengeris pahavaraga linki koos tekstiga „Kas see oled sina selles videos?“. Kui kasutaja klõpsas lingile, järgnes sellele konto ülevõtmine. Kirjutasime, mida peaks tegema sellises olukorras ja petuskeemist täpsemalt RIA veebilehel ja blogis.

Mais jätkusid baaskoolitused **Eesti infoturbestandardi rakendajatele**, mida viime läbi koostöös Tallinna Tehnikaülikooliga ning ka juunis on võimalik kahel koolitusel osaleda.

Alustasime **kaht uut järelevalvemenetlust** elektri- ja energiasektori ettevõtete üle, mille käigus kontrollime küberturvalisuse seaduse nõuete täitmist. Järelevalvemenetlustes on kõrgendatud tähelepanu all ettevõtte arvutivõrgu- ja infosüsteemidele rakendatud turvameetmete kirjeldused, riskianalüüs ja riskide haldamine. Lisaks koostasime ka ühe ettekirjutuse ja lõpetasime kaks menetlust.

Rahvusvaheline keskkond

Kremlimeelne häktivistide rühmitus KillNet jätkas maikuus teenusetõkestusrünnakuid Euroopa riikide pihta. Näiteks rünnati Itaalia riigiasutuste veebilehti ja Itaalia politsei teatel ka Eurovisioni lauluvõistlust (mille võitis Ukraina). Lisaks teatas KillNet „sõja“ kuulutamisest Ukrainale ja üheksale riigile, mis on Ukrainale abikäe ulatanud (sh Eestile).

Samas korraldavad ukrainameelsed häkkerid teenusetõkestusründeid Vene ja Valgevene veebilehtede pihta (sh valitsuse, sõjaväe, energiasektori, meediaväljaannete). Näiteks olevat Ukraina nn IT-armee korraldanud massiivse DDoS-ründe Venemaa alkoholiarvestuse infosüsteemi (EGAIS) pihta, mistõttu oli mai alguses Venemaal probleeme alkoholitarnetega.

Venemaa Sberbanki küberturbe juhi teatel on ründed panga pihta viimase kolme kuu jooksul jõuliselt kasvanud. Mai alguses olevat Sberbank tõrjunud suurima DDoS-ründe oma ajaloos, kui panga veebilehte ründas robotvõrgustik 27 000 seadmega.

Ukraina võtab ägedate küberrünnakute tõttu oma seadmete ja süsteemide kaitsmiseks paroolide asemel kasutusele füüsilised turvavõtmed. Selleks annetas USA ettevõte Yubico 20 000 nn võtit, millest vähemalt 6000 on Ukraina kriitilistes sektorites juba kasutusele võetud.

Häkkerid üle maailma kasutavad aina enam oma õngitsus- ja pahavarakampaaniates peibutusteemana ära sõja temaatikat. Näiteks sihivad küberturvalisuse ettevõtte CheckPointi teatel Hiina küberluurajad aktiivselt Vene riiklikke kaitseinstituute, mille fookuses on kõrgtehnoloogiliste kaitselahenduste uurimine ja arendus.

Costa Rica kuulutas küberrünnakute tõttu riigis välja eriolukorra. Juba üle kuu aja on Costa Rica riigiasutuste süsteemid ja teenused olnud rivist väljas, põhjuseks lunavararühmituse Conti ründed. Rühmitus nõudis 10 miljonit dollarit lunaraha, mida riik ei maksnud. Mai lõpus sai Costa Rica terviseteenistus pihta ka Hive-nimelise lunavaraga.

Samas tulid mais ka teated, et Conti lunavararühmitus on tegevust lõpetamas ja jagunemas ümber teistesse väiksematesse rühmitustesse. Arvatakse, et rühmitus korraldas sedavõrd avaliku ja jõulise rünnaku Costa Rica pihta fassaadiks ja enda reklaamimiseks.

Venemaa taustaga küberrühmitus BlackCat ründas lunavaraga Austria Kärnteni liidumaa süsteeme, mille käigus krüpteeriti väidetavalt tuhanded tööjaamad ja mitmed teenused olid häiritud. Rühmitus nõudis dekrüpteerimisvõtme eest 5 miljonit dollarit, mida liidumaa maksta ei plaani.