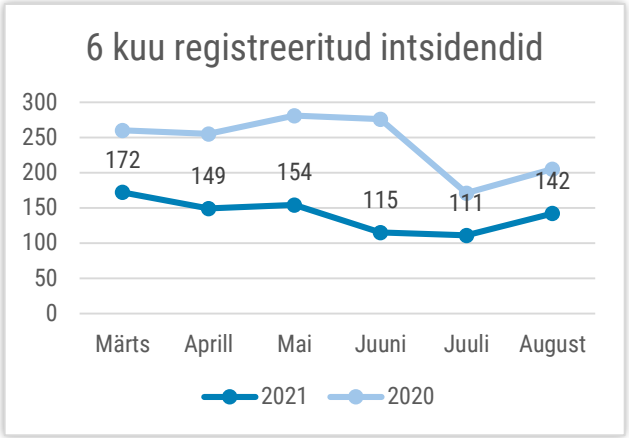
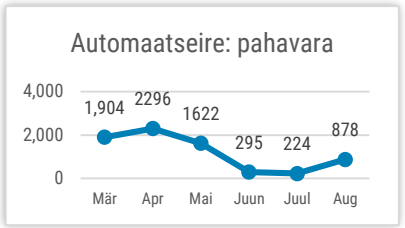
Olukord küberruumis – august 2021

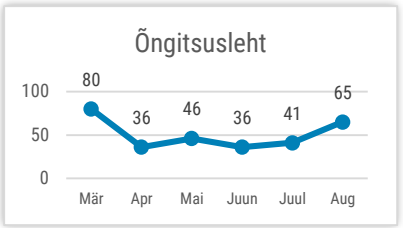
- Augustis registreerisime 142 mõjuga intsidenti, automaatseirega edastasime võrkude omanikele lisaks tuhandeid teateid nakatumistest ja turvanõrkustest.
- Populaarne siseveebiplatvorm Confluence teatas turvanõrkusest, mida ründajad hakkasid massiliselt ära kasutama. Haavatavaid servereid oli ka Eestis.
- Kohtusime haiglate esindajatega ja tellisime elutähtsate teenuste osutajate küberturvalisuse parandamiseks taaskord turvateste.
- Rahvusvaheliselt on jätkuvalt päevakajalised suure mõjuga lunavararünnakud.



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 üha suurema osa kõigist mõjuga Intsidentidest.

Olukord Eesti küberruumis

Augusti lõpus teatas maailmas laialdaselt kasutatava Confluence'i wiki-platvormi tootja Atlassian, et nende tootes on kriitiline turvanõrkus, mille parandamiseks oli vaja tarkvara uuendada. Confluence on kasutusel tihtipeale äriprotsesside dokumentatsiooniks või siis asutuste siseveebideks. Septembri alguseks suutsid ründajad haavatavust juba ära kasutada ning üritasid automatiseeritud süsteemide abil sisse pääseda avalikku interneti avatud Confluence'i serveritesse üle maailma, sealhulgas Eestis. Tihti päädis sissesaamine sellega, et need serverid suunati krüptoraha kaevandama, kuid välistatud pole ka andmete vargus või muutmine.

Meile teadaolevalt saadi sisse ka kolme riigiasutuse siseveebidesse. Täpne mõju – kas andmeid on varastatud või lehekülgi muudetud – pole veel lõpuni selge. Intsident näitab järjekordselt seda, et turvanõrkuste avalikustamise ja turvapaikade kättesaamise puhul tuleks süsteeme uuendada võimalikult kiiresti.

Augusti keskel teavitas üks Tallinna jäätmekäitlusettevõte neid tabanud lunavararünnakust. Esmalt krüpteeris pahavara ühes arvutis olnud failid ja liikus sealt edasi ettevõtte failiserverisse. Ettevõtte sõnul nakatus ka failiserveri varukoopia.

Harjumaa metallitööstussektori ettevõtte äripartner langes arvepettuse ohvriks. Nimelt kompromiteerisid petturid Eesti ettevõtte ja kliendi vahelise kirjavahetuse. Kui meilivestlus jõudis arvete maksmiseni, sekkusid petturid, saates kliendile ettevõtte nimel arve, millel oli muudetud arvelduskonto number. Kuna klient ei kontrollinud saatja meiliaadressi ega arve autentsust, kandis ta üle kümne tuhane euro petturite kontrolli all olnud pangakontole.

Augustis teavitati meid paarist suurema mõjuga teenustõkestusründest – üks oli suunatud riigiameti vastu, kuid selle mõju oli minimaalne vastava kaitsemehhanismi rakendumise pärast. Teine oli suunatud ühe ülikooli vastu, kuid paari tunni jooksul mitmes laines tehtud rünnak mõjutas nimeserverite ummistamise tõttu ka teisi haridusasutusi üle Eesti.

Väiksema mõjuga DDoS rünnakuid – mis võivad olla lühiajaliselt suunatud kodukasutajate või veebilehtede vastu – näeme automatiseeritud seire käigus rohkemgi. Augustis tuvastasime DDoS rünnakuid kokku 130 erineva IP-aadressi suunas.

Augusti lõpus teavitas meid üks isik armupettusest. Ohvri sõnul petsid Venemaal abivajavat pruuti kehastanud kurjategijad temalt välja 31 000 eurot.

Tegevused küberturvalisuse parandamisel Eestis

Osalesime augusti alguses järjekordsel arvamusfestivalil, et rääkida küberturvalisusest ja info-operatsioonidest. Küberturvalisuse teenistuse juht Gert Auväärt panustas arutellu “Maailmapoliitika jõujooned ÜRO Julgeolekunõukogu areenil – Eesti ÜRO Julgeolekunõukogus”. CERT-EE pealik Tõnu Tammer rääkis arutelus pealkirjaga „Sinu Tik-Toki tantsu mõju“, tehnoloogiaosakonna juht Andrus Padar arutelus „21. sajandi infosõda, milleks ja kuidas seda peetakse ja kuidas meist igaühest võib saada infosõdur“. Juhtivanalüütik Lauri Tankler juhtis diskussiooni internetitrollidest ning EU Cyberneti väljaõppe koordinaator Erkki Leego diskussiooni kaugtööst.

Suvega said läbi elutähtsaid teenuseid osutavatele asutustele (ETO) tellitud turvatestid. Tellime taolisi turvateste teenuseosutajatele, kes on selleks soovi avaldanud, et aidata parandada üldist infosüsteemide turvalisust ja riskide hindamist. Pärast turvatestide läbiviimist esitletakse tulemusi nii asutuste juhtkondadele, kui ka IT- ja turvajuhtidele. RIA tellib riigi jaoks elutähtsate ja oluliste teenuste osutajatele turvatestimisi 2012. aastast, tänavu testiti kuut asutust ja ettevõtet.

Augustis kohtusime Eesti haiglate IT- ja infoturbejuhtidega, et arutada nendega küberturvalisuse hetkeolukorda ja koostöövõimalusi. Tervishoiusektor ja selle toimepidevus on RIA jaoks juba mitu aastat olnud prioriteetne, eriti pandeemia kontekstis.

Jätkame Eesti infoturbestandardi ehk E-ITSi tutvustamise ja juurutamisega (E-ITS peaks pika üleminekuperioodi järel aastaks 2024 välja vahetama senise avaliku sektori infoturbestandardi ISKE). Pärast juulikuist suvepuhkust jätkusid augustis infoturbe halduse baaskoolitused rakendajatele, suurem hoog saab koolitustele sisse septembris. Koolitustele on võimalik registreeruda infoturbestandardi koduleheküljel eits.ria.ee.

Rahvusvaheline keskkond

Augustis tõmbas rahvusvahelises küberuumis tähelepanu rühmitus Lockbit 2.0. Kuu keskel ründasid nad lunavaraga üht maailma suurimat IT-konsultatsiooniettevõtet Accenture'i. Rühmituse sõnul ei pääsenud nad ettevõtte võrku n-ö klassikalisel moel (nt turvanõrkust ära kasutades), vaid ettevõtte nn *insaideri* abiga. Enne failide krüpteerimist laadisid ründajad oma sõnul alla ka 6 terabaiti andmeid. Ettevõtte väitel õnnestus neil nakatunud süsteemid varunduse abil taastada ning rünnak kliente ei mõjutanud.

Lockbit pääses augustis ligi ka lennuettevõtetele Bangkok Airways ja Ethiopian Airlines, mille süsteemidest varastas (ja hiljem lekitas) andmeid reisijate kohta. Rühmitus väitis, et sai lennuettevõtetesse sisse „tänu" Accenture kompromiteerimisele, Accenture lükkas rühmituse väite ümber, kinnitades et nende kaudu ei pääsetud ligi kellegi teise süsteemidele.

Lunavara kimbutas teisigi. Näiteks lõi lunavara mitmeks päevaks rivist välja Itaalia Lazio regiooni IT-süsteemid, sh COVID-19 vaktsineerimisportaali, mistõttu ei olnud võimalik end süsti saamisele registreerida.

Meditsiinivaldkond kannatas lunavara tõttu ka USA-s Ohios ja Lääne-Virginias, kus sihtmärgiks sattus Memorial Health haiglate ja kliinikute võrk. Rünnaku tõttu tuli kolme haigla erakorralist abi vajavad patsiendid suunata ümber teistesse haiglatesse ning tühistada korralisi läbivaatusi ja protseduure. Rünnaku taga arvatakse olevat Hive'i rühmitus.

Augustis ilmusid andmete kauplemisega tegelevasse veebifoorumisse RaidForums müüki Leedu välisministeeriumi e-kirjad. Müüja väitis, et müügiks pakutud 1,6 miljonis e-kirjas oli tundlikke teemasid ning dokumente. Lekke valguses teatas Leedu kaitseminister, et möödunud aasta novembris langes välisministeerium küberrünnaku ohvriks, mille autor olevat Venemaa sidemetega.

Positiivsemate teadete killast väärib märkimist, et alates 2019. aastast tegutsenud lunavararühmitus Ragnarok (tuntud ka kui Asnarok) lõpetas tegevuse. Lõppakordina avaldas rühmitus tumeveebis universaalse dekrüpteerimisvõtme.

Häkkerite rühmitus avalikustas augusti lõpus videod Iraani Evini vanglast, kus hoitakse poliitilisi vange. Lekkinud videotest, kus on näha nii 2020. kui ka 2021. aasta ajatempleid, paistab poliitvangide piinamist ja vangla üldiselt ebainimlikke tingimusi.

Valgevene opositsioonilised häkkerid (nn küberpartisanid) jätkasid materjali avalikustamist valitseva režiimi kukutamiseks. Materjalide hulgas olid näiteks videod kinnipidamisasutustest, kus pekstakse protestijaid, ning kõrgete riigiteenistujate kõnesalvestused, mis viitasid korruptsioonile.