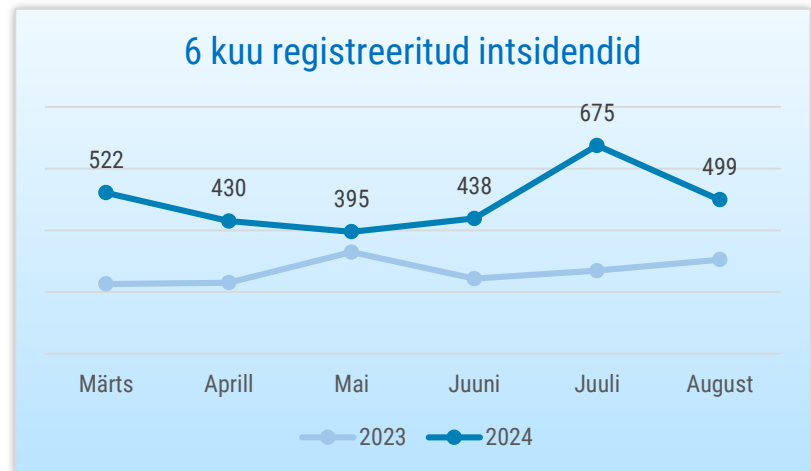




OLUKORD KÜBERRUUMIS

AUGUST 2024

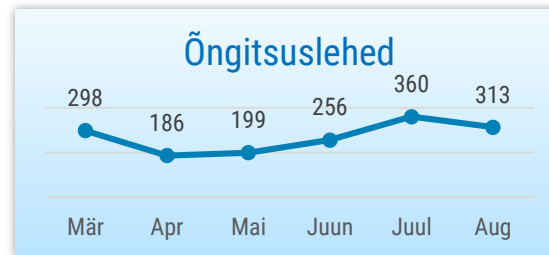
- Augustis registreerisime **499 mõjuga intsidenti**, mis on viimase poole aasta keskmisest veidi kõrgem näitaja.
- Augustis registreerisime kaks **lunavararünnet** ja nägime massilist **Omniva nimel saadetud õngitsussõnumite** levikut.
- Viisime läbi rahvusvahelise tüdrukute **küberlaagri CyberWizards**. Käisime podcastis „Olukorrast digiriigis“ rääkimas küberturvalisuse olulisusest ja hetkeolukorrast riigis.
- Trumpi kampaaniameeskonna teatel tungiti nende **sisesuhtlusvõrgustikku**. Ukraina eksperdid avastasid **pahavarakampania**, mis sihtis Ukraina valitsusasutusi.



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

Augustis nägime taas mitmeid teenusekatkestusi. 6. augustil ajavahemikul 17.25 kuni 18.15 oli tõrkeid e-politsei infosüsteemi Apollo ja piirikontrolli infosüsteemi PIKO töös. Patrullid ei saanud süsteeme kasutada, kuna x-tee päringud ei läinud läbi. Intsidendi põhjustas riistvaralise turvamooduli töö katkemine. Samal päeval oli probleeme ka e-äriregistrist kirjade saatmisel. Intsidendi ajal ei saanud äriregistri kasutajad esitada esmakande ega muudatuste avaldusi, milles oli vaja kinnitada e-posti aadress. Probleem, mille põhjustas viga e-posti tarkvaras, lahenes 6. augustil kell 20.02. 22.augustil katkes TeliaTV töö ajavahemikul 16.45 kuni 19.20, mil Androidi digiboksi kasutajatel ei õnnestunud teleteenust kasutada. 24. augustil ajavahemikul 3.59 kuni 10.30 oli katkestusi Rahandusministeeriumi infotehnoloogiakeskuse (RMIT) hallatavate veebilehtede töös. Rike,

mille põhjustas RMITi nimeserveri seadistusviga, mõjutas 67 veebilehte.

15. augustil laekus CERT-EE-le info, et Transpordiameti lõppkasutajate seadmete keskhaldussüsteem on kompromiteeritud ja ründaja on saanud sellele haldusõigustega ligipääsu. Transpordiamet koostöös CERT-EE ja partneritega viis läbi analüüsi, mille käigus selgus, et ründaja kasutas märtsis avalikustatud haavatavust (CVE-2023-48788) Fortineti tarkvaras. Hetkel teadaolevalt õnnestus ründajal koodi kaugkäivitada, kuid kõik vajalikud väljuvad ühendused mõjutatud masinast ebaõnnestusid.

Augustis registreerisime kaks lunavararünnet. 16. augustil toimus lunavararünnak Järvamaa Kutsehariduskeskuse vastu, mille tulemusel kõik serverid krüpteeriti. Intsidendil oli suur mõju kooli tegevusele, kuna hävisid kõik serveris olnud andmed. Serveritest varukoopiaid ei olnud, sest süsteemi

kogumaht oli väga suur. 17. augustil krüpteeris lunavara Lõuna-Eesti jaekaubandusettevõtte serveris olnud andmed. Kuna ründajad pääsesid ligi ka varundusserverile, siis kustutati ka varukoopia ära. Rünnaku tõttu ettevõtte töö seiskus. Sel aastal oleme näinud kokku seitset lunavararünnet.

Sel kuul levisid massiliselt Omniva nimel saadetud õngitsussõnumid. Sõnumite sisu oli erinev, kuid peamiselt väideti, et pakki ei saa kohale toimetada vale aadressi tõttu ja kutsuti üles oma andmeid uuendama. Mõnes sõnumis nõuti ka saatekulu või tollimaksu tasumist. Kõigi sõnumitega oli kaasas kahtlane link, mis viis kasutaja õngitsuslehele. Tuletame taas meelde, et postifirmad ei saada taolisi sõnumeid ega palu kasutajatel oma andmeid sisestada tundmatutele linkidele. Näeme, et viimastel kuudel on õngitsuslehtede loomine hoogustunud. Kindlasti ei tohiks sõnumis olevat linki avada ja oma andmeid sisestada.



Tegevused küberturvalisuse parandamisel Eestis

29. juulist kuni 3. augustini viisime läbi rahvusvahelise tüdrukute küberlaagri CyberWizards, mis toimus sel aastal juba teist korda.

Laagri eesmärk on populariseerida neidude seas küberturvalisuse valdkonda huvitava töökohana, sest praegu on vaid umbes viiendik sel alal töötajatest naissoost. Laagris osales 95 tüdrukut vanuses 13–16-aastat, kellest pooled tulid Eestist ja ülejäänud välisriikidest. Esindatud olid Läti, Leedu, Tšehhi, Poola, Itaalia, Ungari, Prantsusmaa, Ukraina ja Küprose tüdrukud. Tüdrukutega jagasid lisaks RIA töötajatele oma kogemusi ka küberturvalisuse eksperdid Clarified Security-st, Teliast, SEB pangast ja PPA-st.

RIA analüüsi- ja ennetusosakonna juhataja Märt Hiietamm käis koos majandus- ja kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna juhi asetäitja ning küberriskide

halduse juhi Irina Klementiga podcastis "Olukorrast digiriigis" rääkimas küberturvalisuse olulisusest ja hetkeolukorrast riigis.

Muutunud julgeolekuolukorra tõttu on juunis kinnitatud uus riiklikküberturvalisuse strateegiat esmajärjekorras just meie digiriigi kerksuse suurendamisele keskendumine ja mõlemad saatekülalised pidasid üheks suuremaks probleemiks antud valdkonnas inimeste suhtumist. Küberturvalisuse strateegiaga 2024-2030 saad tutvuda [siin](#).

Avaldasime tehisintellekti ja masinõppe tehnoloogia turvalisuse uuringu juurde kuuluvad õppevideod, mida saad vaadata [siit](#). Uuringu ja videotega tasub [tutvuda](#) kõigil Eesti asutustel ja ettevõtetel, kes kavatsevad tehisaru kasutusele võtta.

Juulikuus lõppesid Eesti äpi arendustööd ja sügisest algab rakenduse avalik testimine. Eesti

äpp on riigiportaal eesti.ee täiendav esitluskiht mobiilseadmes, mis võimaldab ühest kohast leida kõik olulisemad riigi teenused. Sügisel on kõigil huvilistel võimalus Eesti.ee mobiilirakendust testida. Selleks saab testija kasutada mobiilirakenduse vahendusel pakutavaid teenuseid ja anda tagasisidet teenuste kasutajamugavuse kohta.

27. ja 29. augustil viisime läbi infopäevad haridusametuste juhtidele. Infopäeval rääkisime andmekaitsest, infoturbe nõutest ja nende täitmise järelevalvest. Haridusametustele kehtestati infoturbe nõuded 2022. aastal jõustunud küberturvalisuse seadusega, mis tähendab et erinevatel õppeasutustel tuleb luua infoturbe halduse süsteem, et kaitsta oma teenuseid, vara ning teavet. Peagi lisame ka toimunud ürituse salvestuse RIA kodulehele.



Rahvusvaheline keskkond

USA presidendikandidaat Donald Trumpi kampaaniameeskonna [teatel tungiti nende sisesuhtlusvõrgustikku](#).

Meeskonna esindaja süüdistas küberründes Iraani, ent konkreetseid tõendeid selle kohta seni esitatud ei ole. Küll aga viitab kampaaniameeskonna esindaja hiljutisele Microsofti [analüüsile](#), kus kirjeldati mitmeid valimistesse sekkumise operatsioone, mida seostatakse erinevate Iraani küberrühmitustega. Analüüsis oli välja toodud, et juunis kasutas Iraan üht häkitud meilikontot, saatmaks sõnumeid kampaania heaks töötavale kõrgele ametnikule. Saadetud sõnumid sisaldasid pahaloomulist linki. USA väljaanne Politico kinnitas, et neile saadeti anonüümselt e-posti kontolt Trumpi kampaaniaga seotud dokumente.

Ukraina eksperdid [avastasid juulis pahavarakampaania, mis sihtis Ukraina valitsusasutusi ning püüdis neid nakatada tagaukse-tüüpi](#)

pahavaraga. Üle saja seadme puhul on teada ka nende nakatumine. Ohvritele saadeti Ukraina julgeolekuteenistust (SBU) matkiv e-kiri, mis nõudis kasutajalt teatud dokumentide edastamist ning sisaldas linki .zip laiendiga arhiivile. Lingile vajutades käivitus arvutis pahavara, mis võimaldab seadme kaugelt oma kontrolli alla võtta.

USA-s Floridas tegutsev andmevahendus-ettevõtte National Public Data, mille teenuseid kasutatakse taustakontrollide tegemisel, [tunnistas suurt andmeleket kuid tagasi toimunud küberründe tagajärjel](#). Meedia hinnangul võib leke puudutada praktiliselt kõiki ameeriklasi – väidetavalt on lekkinud andmebaasis 2,9 miljardit andmerida, sealhulgas nimi, sotsiaalkindlustusnumber, aadress ja e-posti aadress. Kui alguses üritasid kurjategijad andmeid müüa, siis hiljem paisati need tasuta tumeveebi.

Ettevõttele heidetakse muuhulgas ette, et andmevargusest kuni selle tunnistamiseni kulus aega üle nelja kuu ning algne sissetung olevat toimunud juba 2023 detsembris.

Maailma üks suuremaid naftatöötlejaid Halliburton [langes küberrünaku ohvriks](#), mille tõttu oli ettevõtte tegevus häiritud. Rünaku täpsemad asjaolud ja mõju pole veel teada, kuid osad eksperdid viitavad võimalikule lunavararünakule. Suured naftafirmad on varemgi langenud mõjukate küberrünakute ohvriks: 2021. aastal tabas Colonial Pipeline'i lunavararünnak, mille tõttu tekkis USA osades osariikides kütusepuudus.

USA pooljuhtide tootja Microchip Technology [teatas, et mitmes nende tehases on küberründe tõttu tootmine häiritud](#). Kahtlane võrguliiklus tuvastati 17. augustil, misjärel tuli osa süsteeme võrgust isoleerida ning see mõjutas tootmist osades tehastes.