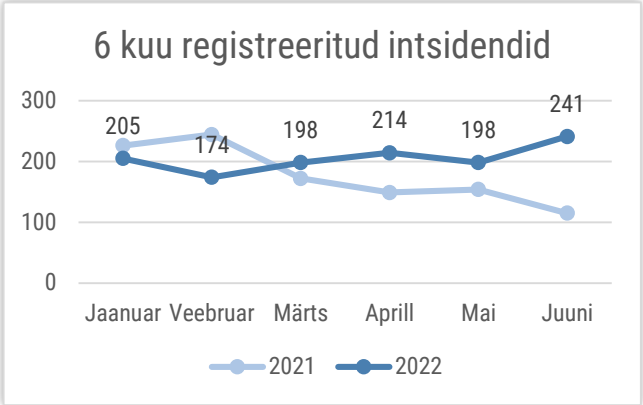
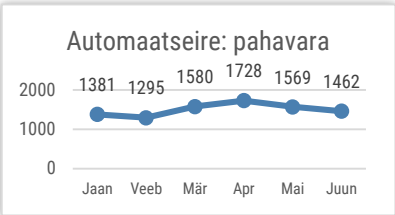
Olukord küberruumis – juuni 2022

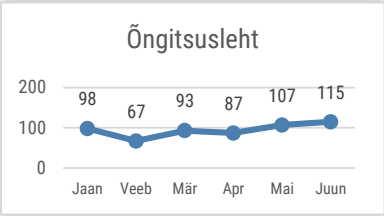
- Juunis registreerisime 241 mõjuga intsidenti, mis on viimase poole aasta kõige kõrgem näitaja.
- Jätkusid teenusetõkestusründed Eesti riigiasutuste ja elutähtsa teenuse osutajate vastu ning ettevõtted langesid erinevate pettuste ohvriks.
- Eetrisse jõudis venekeelne raadiosari ja algas teavituskampaania, mis juhib tähelepanu turvalisele küberkäitumisele.
- Juunis jätkusid sõjaga seotud küberründed nii Ukraina, Leedu kui ka Norra riigiasutuste 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

Alates 5. juunist kuni 9. juunini sooritati **teenusetõkestusründeid (DDoS)** Eesti riigiasutuste ja elutähtsa või olulise teenuse osutajate vastu. Rünnakud tabasid muuhulgas Vabariigi Presidendi veebilehte, transpordi- ja finantssektori portaale ja Riigi Infosüsteemi Ametit. Rünnakute maht ja mõju oli väiksem kui aprillis Eesti vastu sooritatud ummistusrünnetel, kuid osad teenused olid siiski kättesaamatud. Väiksem mõju oli neile teenustele, millele on rakendatud RIA poolt pakutav kaitse.

Kahel korral esines **tõrkeid Haigekassa põhiteenuste töös**. 11. juunil ajavahemikul 6.44 kuni 8.44 ja 28. juunil ajavahemikul 9.32 kuni 11.00 olid häiritud nii digiretsept kui ka kindlustatuse kontroll. Katkestus toimus turvaserveri vea tõttu. 11. juunil oli probleeme ka Haigekassa avaliku veebilehega, intsidendi põhjustasid Haigekassale teenust pakkuva Riigipilve tõrked.

16. juunil ajavahemikul 16.29 kuni 16.51 katkes **võrguseadme taaskäivituse tõttu** 29 Riigipilve virtual-masina töö. Mõjutatud olid Haigekassa, Keskkonna-ministeeriumi Infotehnoloogiakeskus, Kredex, Välisministeerium, Majandus- ja Kommunikatsiooni-ministeerium, Riigi Infosüsteemi Amet, Saaremaa Gümnaasium, Statistikaamet, Tervise ja Heaolu Infosüsteemide Keskus, Transpordiamet ning Ericsson.

27. juunil ajavahemikul 10.40 kuni 12.50 oli probleeme **piirikontrolli infosüsteemiga PIKO**, milles ei töötanud päringuid ja ei olnud võimalik registreerida piiriületusi ning mõjutatud olid kõik intsidendi kestel Eestisse saabuvad ja Eestist lahkuvad reisijad.

Vähemalt kaks Eesti ettevõtet langesid **arvepettuse ohvriks.** Petturid kompromiteerisid ühe ettevõtte välispartneri e-postkasti ja saatsid selle alt arve, millel muutsid pangarekvisiite. Heauskselt kandiski ettevõte petturite kontrolli all olnud kontole ligi 20 tuhat eurot. Kui partneri pangakonto andmeid ilma eelneva kommunikatsioonita muudetakse, soovitame partnerilt kindlasti üle küsida, kas muudatus ka päriselt aset leidis. Teise juhtumi puhul oli tegemist sarnase skeemiga ja kahju suurusjärk oli 8000 eurot. Täpsemalt saab skeemist lugeda siit.

Kaks ettevõtet sattusid **lunavararünnakute ohvriks**. Ühel juhul kasutati Locki Locker-nimelist lunavara ja süsteemidesse tungiti kasutades avatud pordiga kaugtöölaua protokolli (RDP). See on tavaline viis süsteemidesse häkkimiseks ja avaldasime märtsis sel teemal ohuhinnangu, kus soovitame kasutada VPNi ehk virtuaalset privaatvõrku. Teisel rünnakul kasutati Phobose lunavara, kõik võrgus olevad masinad krüpteeriti ja ettevõtte töö oli tugevalt häiritud.

Tegevused küberturvalisuse parandamisel Eestis

Juunis jõudis Raadio 4 eetrisse venekeelne küberteadmistele keskenduv **raadiosari** „Введи пароль“ („Sisesta parool“) ja ühtlasi alustasime ka **teavituskampaaniat**, mis juhib tähelepanu turvalisele küberkäitumisele. Nii raadiosaated kui ka kampaania on vene keeles, kuna Statistikaameti andmetest selgus, et võrreldes eestlastega on muu emakeelega elanike teadlikkus küberhügieenist märkimisväärselt madalam. Saated on Raadio 4 eetris igal esmaspäeval 13 nädalat järjest ning neid saab järgi kuulata RIA IT-vaatliku portaalis.

Avaldasime RIA blogis kolm uut postitust. Esimeses kirjutame **Confluence'i tarkvaras avastatud kriitilisest turvanõrkusest** ning toome välja vastumeetmed ja soovitused. Kuna Confluence tarkvara on Eestis laialdaselt kasutusel, võib turvanõrkus ka meie asutustele ja ettevõtetele mõju kaasa tuua.

Teises postituses aga tuletame meelde mida **pahaloomuliste e-kirjade** puhul tähele panna ja kuidas käituda. Viimasel ajal on taas hakanud rohkem levima Emotet pahavara, mida saadetakse just e-maili manuste kaudu.

Kolmandas postituses teeme ülevaate kriitlilisest **Follina turvanõrkusest** Windowsi operatsioonisüsteemides, mis on selle mõju Eestis ja maailmas ning kuidas täpselt turvanõrkust ära kasutatakse.

Osalesime koos PERHi ja Lastehaiglaga Euroopa Liidu küberturvalisuse ameti (ENISA) tervishoiusektori **küberõppusel Cyber Europe 2022**. Õppusel mängiti läbi mõned toimunud küberintsidendid ja see hõlmas nii tehniliste intsidentide lahendamist kui ka kommunikatsiooni poolt. Õppus oli suunatud tervishoiusektori infoturbejuhtidele, IT-osakondadele ja kriisijuhtimise tiimidele.

Hoiatasime juunis levima hakanud **liba-mobiilisõnumite eest**, mis näiliselt saadetakse SEB, Swedbanki või DHLi nimelt. Libasõnumites õhutatakse kiirelt tegutsema ja oma andmeid sisestama võltsitud veebilehele. Petulehtede veebiaadressid üritatakse muuta pankade omadega võimalikult sarnaseks, et inimeses suuremat usaldust tekitada. DHLi sõnumites kasutatakse ära olukorda, kus inimesed tellivad palju e-poodidest ja kasutaja suunatakse maksma lisatasu paki kättesaamiseks. Taoliste pettuste läbi kaotasid inimesed tuhandeid eurosid.

Alustasime **10 uut järelevalvemenetlust**, tegime 1 ettekirjutuse ja lõpetasime 2 menetlust. Järelevalvemenetluste eesmärgiks on kontrollida elutähtsat teenust osutavates ettevõtetes küberturvalisuse nõuete täitmist nii organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamise vaatenurgast.

Rahvusvaheline keskkond

Juunis jätkusid sõjaga seotud küberründed. Ukraina erikommunikatsiooni teenistus (SSCIP) hoiatas, et häkkerid püüavad ligi pääseda Ukraina riigiametnike telefonidele. Tegemist olevat nn *zero-click* häkkimisega ehk seadme omanik ei pea nakatumiseks isegi kuskil klõpsama.

Lisaks hoiatas CERT-UA, et Vene häkkerid on õngitsuskampaaniaga sihikule võtnud Ukraina meediaorganisatsioonid, nt raadiojaamad ja ajalehetoimetused. Kirjade (peibutus)teema oli "*nimekiri interaktiivsete kaartide linkidest*" ja neile oli lisatud samanimeline fail.

Kuid juuni tõi teateid ka töövõitudest. USA justiitsministeerium teatas, et võttis maha Vene RSocks-nimelise robotvõrgustiku, mille abil on kompromiteeritud miljoneid koduarvuteid, Androidi nutitelefone ja IoT-seadmeid üle maailma.

Kremlimeelsed häktivistid eesotsas rühmitusega KillNet korraldasid teenusetõkestusrünnakuid Leedu riigiasutuste ja kriitilise infrastruktuuri pihta. Rünnete ajendiks olevat see, et Leedu tõkestas vastava üleminekuperioodi lõppemise järel EL-i poolt sanktsioneeritud kaupade maismaatransiidi Venemaa ja Kaliningradi vahel. Killneti sõnul ei jäta nad ründeid enne, kui transiidikeeld Vene kaupadele tühistatakse.

Lisaks said kremlimeelsete häkkerite teenusetõkestusrünnakutega pihta ka Norra riigiasutused ja ettevõtted. Meedias on levinud info, et Norra saadik Moskvas kutsuti seal vaibale seoses kaebusega, et Norra tõkestab Vene kaupade liikumist läbi riigi Vene Arktika söekaevandustesse.

Microsoft avaldas Ukraina sõja esimesed küberi õppetunnid. Venemaa invasiooni küberstrateegia põhinevat MS hinnangul kolmel tegevussuunal: destruktiivsed ründed Ukrainas, sissetung võrkudesse ja luure väljaspool Ukrainat ning mõjutusoperatsioonid inimeste pihta üle maailma.

Juunis oli ka mõjukaid kuritegelikke küberründeid. Näiteks sai kuu alguses lunavararündega pihta Itaalia linn Palermo, mistõttu olid häiritud mitmed linna IT-teenused. Ründe järel lülitas linn kõik IT-süsteemid välja, nii et linnaelanikud pidid asutustega suhtlemiseks kasutama mh faksimasinaid.

Mitmes USA osariigis oli häiritud töötuhüvitise maksmine ja töötuks registreerimine, sest neid infosüsteeme pakkuv tarkvaraettevõte GSI sai pihta küberrünnakuga, mistõttu lülitati süsteemid välja. Näiteks Tennessee osariigi töötuprogrammis olevat umbes 12 000 inimest, kellele polnud võimalik toetust välja maksta.