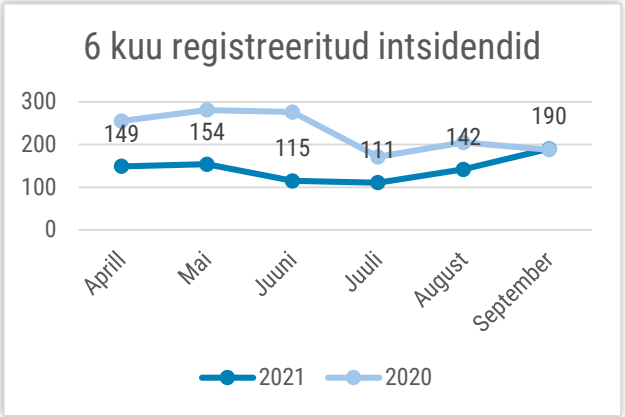
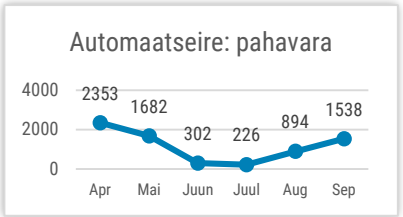
RIIGI INFOSÜSTEEMI AMET

Olukord küberruumis – september 2021

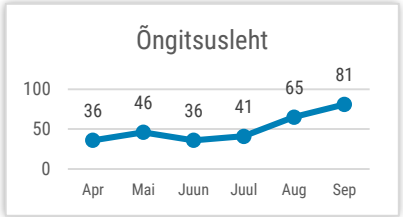
- Septembris registreerisime 190 mõjuga intsidenti, mis on selle aasta kõrgeim näitaja. Sellele lisanduvad automaatseirest tuvastatud intsidendid.
- Kooliaasta algusega kaasnes hulk teenustõkestusrünnakuid, mis mõjutasid nii koole, aga ka teisi Eesti teenusepakkujaid.
- Pakkusime elutähtsate teenuste osutajatele võimalust kontrollida oma veebiteenuste turvalisust.
- Saksamaa omistas poliitikute vastu tehtud rünnakud Venemaa sõjaväeluure küberüksusele.



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

Septembrikuus algas taas kooliaasta, mis tähendab, et ka haridusasutustega seotud intsidendid paistsid uue hooga silma. Meile anti teada korduvatest hajutatud teenustõkestusrünnakutest (DDoS) haridusasutuste ja –teenuste vastu, näiteks õppeinfosüsteemi Tahvel suunas. Samuti nägime DDoS rünnakute sihtmärkidena Haridus- ja Noorteameti (HARNO) pakutava õpikeskkonda moodle.edu.ee. Kokku kümmekond rünnakut mõjutasid teenuste kättesaadavust paarist minutist paari tunnini. Oluline on märkida, et rünnakud on mõjutanud ka Tallinna Tehnikaülikooli, Tartu Ülikooli Kliinikumi ja HARNOga seotud nimeservereid. CERT-EE on pakkunud omalt poolt infrastruktuurialast tuge.

Septembris registreerisime kolm lunavararünnakut. Kuu alguses teavitas üks väiksem kaubandusettevõte, et raamatupidaja arvutist oli lunavara liikunud edasi teistesse tööjaamadesse. Ettevõte sai andmed varukoopiast taastatud.

Ka teised lunavarateavitused olid seotud seekord raamatupidamisega. Ühe ettevõtte raamatupidamistarkvara krüpteeriti, krüptimiseks kasutati REvil/Sodinokibi tööriista. Kuna ettevõttele IT-teenuse pakkujal õnnestus andmed taastada, jäi suurem kahju olemata. Taaskord murti sisse läbi valesti seadistatud kaugtöölaua protokolli (RDP).

Kolmas lunavaraintsident juhtus raamatupidamisettevõttega. Rünnakuks kasutati taas Revil lunavara, mis krüpteeris lisaks arvutile ka sellega ühendatud tagavarakoopia ning seiskas seeläbi ettevõtte tegevuse. Lunavara paigaldamiseks kasutati kaugjuurdepääsu-tarkvara TeamViewer. CERT-EE edastas rünnaku ohvriks langenud ettevõttele Revil lunavara dekrüptori, mille abil õnnestus andmed taastada.

Septembri alguses tuvastasime mitmeid õngitsus- ja pahavarakampaaniaid, millest enamik jäljendasid SEB panka. Leidsime ka mitmeid teiste pankade portaale jäljendavaid õngitsuslehti, ent nende levitamiseks laialdasi õngitsuskirjade laineid meie teada ei kasutatud.. Lisaks toimus endiselt ohtralt juba suvel alanud petukõnesid Swedbanki nimel.

Tegevused küberturvalisuse parandamisel Eestis

Pakkusime suve lõpus elutähtsate teenuste osutajatele võimalust kontrollida oma veebiteenuste turvalisust CERT-EE tehnilise tööriistaga, mis on spetsialiseerunud veebidele ning võimeline tuvastama tuhandeid erinevaid turvanõrkusi. Tänaseks on seda kasutanud ligi kolmkümmend elutähtsa teenuse osutajat, kellest paljudel aitas teenus tuvastada nii keskmise kui ka kõrge tasemega turvanõrkusi. Kõik ettevõtted, kes oma veebiteenuseid kontrollida soovisid, said RIA-lt krüpteeritud raporti tulemuste kohta ning soovi korral edasist nõu tulemuste tõlgendamisel ja puuduste kõrvaldamisel.

Septembris kohtusime Eesti küberturbeettevõtetega järjekordsel küberhommikusöögil. Arutasime olukorda küberruumis, Euroopa Liidu uut küberkerksuse akti ning Euroopa Komisjoni ettepanekut ühise küberüksuse (Joint Cyber Unit) loomiseks. Küberhommikusöök on RIA ja EISA korraldatav ürituste seeria, kus võõrustamise teatepulk liigub Eesti küberettevõtete vahel. Seekord oli võõrustajaks Cybers.

CERT-EE täiustas oma igapäevast kübervaldkonna uudiskirja, mis sisaldab kokkuvõtet nii Eesti kui rahvusvahelises meedias ilmuvatest tähtsamatest küber- ja IT-uudistest. Septembrist alates sisaldab uudiskiri ka lühikest kokkuvõtet ööpäeva sündmustest Eesti küberruumis. Uudiskirjaga liitumiseks tuleb saata e-kiri teemaga „Subscribe“ aadressile certnews@cert.ee (liitumiseks on vajalik asutuse või organisatsiooni meiliaadress, erameiliaadressile uudiskirja tellida ei saa).

Selle aasta kolmandas kvartaliülevaates kirjutasime krüptorahaga seotud petuskeemidest, taakvara (legacy) probleemist ning Confluence'i tarkvara turvaaugu ärakasutamisest ka Eesti küberruumis. Kvartaliülevaate täistekst on leitav RIA kodulehelt.

Rahvusvaheline keskkond

Saksamaa teatas, et Venemaa sõjaväeluure GRU-ga seotud ohustaja nimega Ghostwriter proovib varastada nende parlamendiliikmete andmeid. Õngitsuskirjade abil olevat proovitud ligi pääseda Bundestagi ja ka liidumaade parlamentide liikmetele. Saksa välisministeeriumi esindaja sõnul olevat küberrünnaku eesmärk desinformatsioon ja mõjutusoperatsioonid. Saksamaa kutsus Venemaad üles vaenulikku tegevust lõpetama. Selle tuules esitas ka Euroopa Liit Venemaale ametliku süüdistuse pahatahtliku kübertegevuse eest, mis sekkub EL-i liikmesriikide valimistesse ja poliitikasse. EL-i teatel ründab Venemaa Ghostwriteri-nimelise kampaaniaga liikmesriikide (mitte ainult Saksamaa) parlamente, ametnikke, poliitikuid, ajakirjanikke ja tsiviilisikuid.

Lisaks teatas Saksamaa, et enne nende 26. septembril toimunud parlamendivalimisi oli teenusetõkestusrünnaku tõttu häiritud valimiste veebilehe töö. Veebileht oli maas mõned minutid. Muud valimisteks vajalikus IT-süsteemid rünnakust mõjutatud ei olnud, seda tõenäoliselt DDoS lisakaitse tõttu.

Möödunud kuul tegi maailmas omajagu kahju ka lunavara. Näiteks sai Lõuna-Aafrika Vabariigi justiitsministeerium pihta lunavaraga, mis krüpteeris kõik ministeeriumi süsteemid. Seega muutusid nii sisemised kui ka välimised elektroonilised teenused kättesaamatuks. Intsidendi tõttu käivitati varuplaan: nt muudeti manuaalseks kohtuistungite salvestamine ja õiguslike dokumentide väljastamine. Püsti pandi ka uus e-maili süsteem, mis viitab, et ründajatele ei makstud lunaraha.

Lisaks sai lunavaraga pihta ka USA põllumeeste ühistu (NEW Cooperative), ründajaks oli BlackMatter-i rühmitus. Häkkerid nõudsid ühistult 5,9 miljonit dollarit, et varastatud andmeid ei lekitataks ning dekrüpteerimisvõtme saamiseks. Ühistu sõnul olid lunavarast mõjutatud osad ettevõtte seadmetest ja süsteemidest, mistõttu lülitati lunavara edasise leviku tõkestamiseks süsteemid välja.

Venemaal tegutsev küberrühmitus REvil, mis juulis teadmata põhjustel internetist kadus, hakkas uuesti tööle. 7. septembril käivitusid taas REvili maksmise, läbirääkimiste ja andmete lekitamise veebilehed. Juba on nad teatanud ka oma uutest ohvritest.

Ukrainas võtsid Prantsuse, Ukraina ja USA õiguskaitseorganid koos Europoli ning Interpoliga kinni kaks Ukraina lunavaraoperaatorit. Politseioperatsioon päädis kahe inimese arreteerimisega, läbi otsiti seitse kinnistut, konfiskeeriti 370 000 dollarit sularaha ja kaks luksusautot väärtuses 217 000 dollarit ning külmutati 1,3 miljoni dollari väärtuses krüptorahasid.