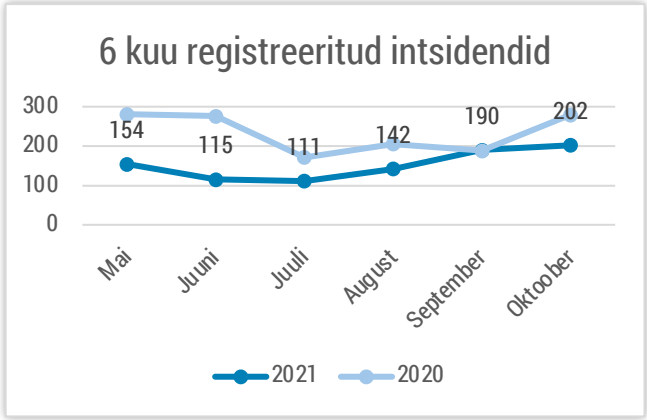
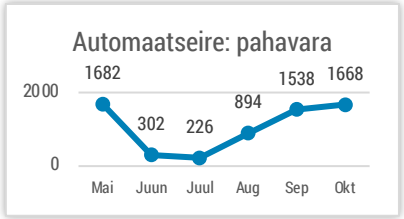
Olukord küberruumis – oktoober 2021

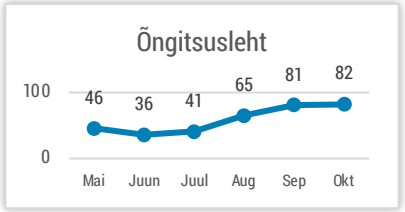
- Kohalike omavalitsuste valimiste eel ega ajal ei tuvastanud me ühtegi olulise mõjuga rünnakut valimiste tehnoloogiatele või hääletust mõjutavatele süsteemidele.
- Jätkusid teenusetõkestusründed koolide ja haridusteenuste vastu.
- Statistikaameti uuringust selgub, et Eesti elanike teadmised küberhügieenist on paranenud.
- Microsoft hoiatas, et Vene välisluureteenistuse (SVR) küberrühmitus APT29 kompab võimalusi globaalseteks tarneahelarünnakuteks.



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.



Õngitsusleheed moodustavad jätkuvalt kõige suurema osa CERT-EE registreeritud intsidentidest

Olukord Eesti küberruumis

Kohalike omavalitsuste valimiste eel ega ajal ei tuvastanud me ühtegi olulise mõjuga rünnakut valimiste tehnoloogiatele või hääletust mõjutavatele süsteemidele. Üksikutest käideldavuse intsidentidest kirjutasime ka RIA blogis. Meie hinnangul möödus valimiste periood rahulikult.

Oktoobris jätkusid teenusetõkestusründed (DDoS) koolide ja haridusteenuste vastu. Septembri lõpust oktoobri keskpaigani täheldati pidevaid rünnakuid ühe Tallinna kutseõppeasutuse suunas, 18.10 hommikul toimus ligi tunniajane DDoS ühe Kesk-Eesti kooli vastu, 20.10 vahemikus 11.30 – 14.40 toimus mitu ummistuskatset ühe Lõuna-Eesti kooli suunal, sama päeva pärastlõunal tehti ka kolmeminutiline rünnak haridus- ja noorteameti hallatava Moodle õppekeskkonna vastu. RIA hinnangul on nende taga sageli kooliõpilased.

Oktoobris teavitati meid kahest lunavararünnakust. Üks neist mõjutas suuremat ettevõtet, kes suutis taastada enamuse oma tööjaamadest varukoopiatest. Teine oli suunatud ühe Eestis tegutseva keemiatooteid valmistava ja müüva ettevõtte suunas. Lunavara krüpteeris serveris olnud failid ja peatas seeläbi mõneks ajaks firma töö.

Lunavara kõrval on kurjategijatel ka teisi viise ettevõtjaid häirida ja raha välja pressida. Üks autoremondiga tegelev väikeettevõte teatas, et nende serverist on kustutatud majandustarkvara ja selle andmebaas, mistõttu firma töö katkes. Ründaja jättis arvutisse kirja instruktsioonidega, kuidas temaga ühendust võtta, et raha eest andmed taastada ja vältida edasist leket.

Jätkuvalt levib küberruumis tohutult õngitsuskirju. Näiteks kompromiteeriti ühe haigla töötaja konto, kes oli ise õngitsuslehele oma andmed jätnud, ja tema konto alt saadeti omakorda tema kontaktidele tuhandeid kontandmeid küsivaid õngitsuskirju. Kontoandmete kõrval on jätkuvalt näha ka pangakontode andmeid õngitsevaid kirju.

Lisaks õngitsuskirjadele **levis oktoobris tavapärasest rohkem pahavara sisaldavaid e-kirju.** Näiteks levis näiliselt Eesti Kaubandus- ja Tööstuskoja nimel saadetud meil teemaga „Vaja hinnapakkumist“, millega kaasas oleva faili avamisel käivitati arvutis pahavara.

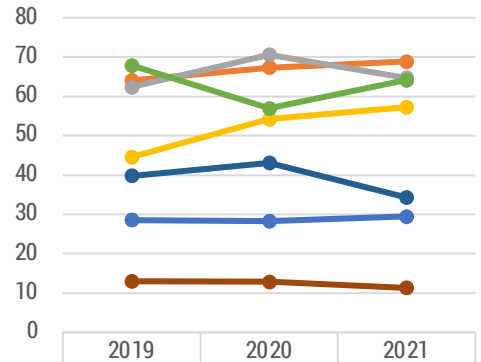
Tegevused küberturvalisuse parandamisel Eestis

Oktoobrikuu möödus meil suuresti kohalike valimiste tähe all. Oleme Riigi valimisteenistuse koostööpartnerid ning hoolitseme muu hulgas e-hääletuse Koguja teenuse toimimise, aga ka valimiste infosüsteemi (VIS3) arendamise eest. Tehnoloogilise toe kõrval hoidsime silma peal nii nende teenuste, aga ka üldiselt Eesti e-teenuste küberturvalisusel, millest kogu meie valimiste taristu sõltub.

Lisaks aitasime kokku panna riskihinnangud, hoolitsesime e-hääletajate kasutajatoe eest, toetasime valimisteenistuse kommunikatsioonispetsialiste, panime kokku küberhügieenikoolituse valimisjaoskondade töötajatele ning korraldasime jaoskondade seadmete logihaldust ja –seiret.

Nagu eelpool öeldud, möödusid valimised meie hinnangul rahulikult. Olulisemateks intsidentideks võib pidada käideldavuse tõrkeid. Näiteks katkes riigi autentimissüsteemi TARA turvalisussätete tõttu ligipääs VIS3-le laupäeval 45 minutiks. Samuti on oluline valimiste kättesaadavus kõigile osapooltele, seega kui Maci kasutajad ei saanud e-hääletamise esimesel päeval valijarakendust kasutada, oli vaja see probleem kiirelt lahendada.

Uurisime kolmandat aastat järjest koos statistikaametiga Eesti elanike küberhügieeni-käitumist. Oktoobris avaldatud andmed näitavad, et küberhügieeni-alane olukord on paranenud. Nende inimeste osakaal, kes ei tee midagi selleks, et enda küberturvalisust parandada, on langenud 12,9 protsendi pealt 11,3 protsendini. Rõõm on näha, et just vanemaealiste hulgas on kasvanud nende vastajate hulk, kes rõhutavad vajadust muuta oma paroolid tugevamaks.



	2019	2020	2021
Paroolid	64,1	67,3	68,9
lingid-manused	62,4	70,6	64,7
võõrad seadmed	44,6	54,2	57,3
Sätted	28,6	28,3	29,5
Turvaprogrammid	67,9	57	64,2
Taustauuring	39,8	43,1	34,3
Ei midagi	13	12,9	11,3

Rahvusvaheline keskkond

Oktoobri alguses lõi laineid Facebooki ja sellega seotud teenuste (Instagram, WhatsApp) ulatuslik teenusekatkestus. Facebooki teatel oli põhjuseks andmekeskuste vahelist võrguliiklust koordineerivatele ruuteritele tehtud konfiguratsioonimuudatused.

Mitmel pool maailmas sai küberrünnakutega pihta kriitiline taristu. Näiteks tabas Iisraelis Hadera linnas asuvat haiglat lunavara. Seetõttu tühistati mitte-kiireloomulised protseduurid, ent alternatiivsete süsteemide toel said ajakriitilised teenused jätkuda. Ründekatseid tehti ka teistele Iisraeli haiglatele.

Oktoober ilmestas, kuidas **meditsiinivaldkonna küberohud võivad esile kerkida ka mujal kui haiglates**. Nimelt kutsus insuliinipumpade tootja Medtronic küberohu tõttu tagasi osade oma insuliinipumpade kaugjuhtimiseks mõeldud puldid. Pulti sisse häkkides on võimalik sellega koguseid ja doseerimist manipuleerida nii, et see võib viia inimese surmani.

Ka mitu panka sai oktoobris küberrünnakuga pihta. Näiteks Ecuadori suurim pank (1,5 miljonit klienti) Banco Pinchincha pidi küberrünnaku tõttu suure osa oma arvutivõrgust välja lülitama. Samuti langes rünnaku ohvriks Pakistani riiklik pank (NBK).

Microsoft hoiatas, et Vene välisluureteenistuse (SVR) küberrühmitus APT29 (tuntud ka kui Nobelium) kompab võimalusi globaalseteks tarneahelarünnakuteks. Rühmitus katsetab sama lähenemist nagu 2020.a teatavaks saanud Solarwindsi rünnaku puhul, mille tulemusel pääseti mh ligi mitmele USA valitsusasutuse süsteemidele. Kui Solarwindsi puhul sihiti tarkvaratootjat, siis nüüd teenusepakkujaid, kes haldavad oma klientide eest nende pilveteenuseid ja teisi tehnoloogiaid.

Venemaa pälvis küberteemadel tähelepanu ka andmelekkega. Nimelt müüakse nö põrandaaluses foorumis 800 dollari eest miljonite Moskva autoomanike andmeid. 50 miljoni andmereaga andmebaasis on näiteks Moskva autoomanike täisnimed, sünniaastad, telefoninumbrid, VIN-koodid, numbrimärgid. Andmebaasi ostnud Vene väljaannete sõnul näivad andmed olevat tõesed. Pole selge, kuidas andmed lekkisid. Häkkeri enda sõnul sai ta need Moskva liikluspolitsei töötajalt.

Oktoobris sai ka teatavaks, et kuu varem tabas Argentiina rahvastikuregistrit (RENAPER) andmeleke. **Avalikuks said kõigi Argentiina kodanike isikuandmed**, sealhulgas ID-kaardi fotod, nimed, koduaadressid, sooidentiteeti puudutavad andmed jne.