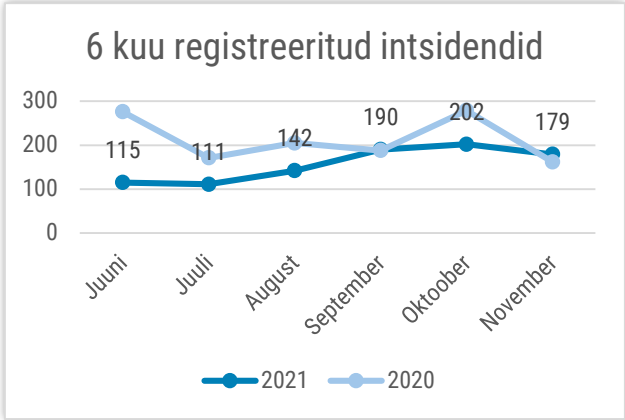
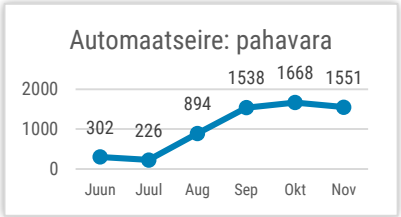
Olukord küberruumis – november 2021

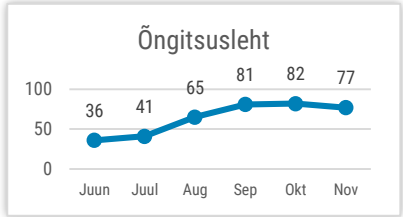
- Novembris teavitati meid 179st intsidendist, mis on aasta keskmisel tasemel. Lisaks tuvastati automaatseire käigus vähemalt 1551 seadet, mis on pahavaraga nakatunud.
- Nägime suurema mõjuga teenustõkestusrünnakuid nii avaliku sektori, aga taas ka haridussektori suunas.
- Uuendasime itvaatlik.ee ennetusportaali.
- Kriitilise informatsiooni infrastruktuuri kaitse infopäeva on võimalik järele vaadata RIA Facebooki lehelt.
- Novembris tabati küberkurjategijaid mitmes riigis.



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

Novembris nägime taaskord hulka teenustõkestusründeid (hajutatud rünne ehk DDoS), millest mõnel oli suurem mõju kui teistel. 22. novembri varahommikul toimus DDoS rünnak Siseministeeriumi infotehnoloogia- ja arenduskeskuse ehk SMITi teenuste vastu. Selle tagajärjel oli umbes tunni jooksul häiritud SMITi nimeservereid kasutavate teenuste ja veebilehtede töö, kuid teenused ei katkenud täielikult.

Teenustõkestusründeid nägime jätkuvalt haridussektoris, nagu ka oktoobris ja septembris. Lõuna-Eestis ja Kesk-Eestis asuvate gümnaasiumite ja põhikoolide suunas tehtud rünnakud enamasti nende tööd ei häirinud. Küll aga mõjutasid rünnakud lühiajaliselt õppeinfosüsteemi Tahvel ning Haridus- ja Noorteameti Moodle e-õppekeskkonna toimimist: kestsid need vahemikus kuus minutit kuni veidi üle tunni.

Novembris saime teada neljast juhtumist, mil Eesti inimeste andmed olid kolmandatele osapooltele kättesaadavad. Näiteks ühe organisatsiooni meililisti kuuluv meilikonto kompromiteeriti, mille käigus sai meililisti sisu ründajale teatavaks; ühe 2013. aastaga lõppenud Euroopa projekti kodulehe kaudu lekkisid kasutajate andmed, kus olid ka Eesti isikutega seostatavaid kirjeid; ning turvanõrkuse tõttu oli kahe keskkonna kasutajatele näha piiratud hulk andmeid teiste kasutajate kohta. Kõigi nimetatud intsidentide kohta tehti teavitus mõjutatud osapooltele ja andmekaitseinspektsioonile.

Kolmel korral teavitati meid lunavararünnakust. Teavitajate kahju oli enamasti süsteemidele taastamisele kulunud aeg ja tööjõukulu.

Ühe Eestis tegutseva suure panga kaarditerminalidega tekkisid 1. novembril poole päeva jooksul tõrked korraliste hooldustööde käigus.

Tegevused küberturvalisuse parandamisel Eestis

Korraldasime 9. novembril Eesti elutähtsate teenuste osutajatele ja teistele kriitilise tähtsusega taristu partneritele infopäeva. Rääkisime nii olukorrast küberruumis, kui ka turvatestimisest ja tarneahelate turvalisusest. Infopäeva ülekanne on järelvaadatav RIA Facebooki leheküljel.

Novembris avalikustasime uue ennetusveebi itvaatlik.ee. Viimased kaks aastat on sellele veebilehele üles pandud materjale, mis on seotud lühiajaliste kampaaniatega (näiteks 2019. aastal vanemaealistele ja 2020. aastal ettevõtjatele mõeldud kampaaniamaterjalid). Uuenduskuuri tulemusel saime staatilise kampaanialehe asemele tervikliku lahenduse, kuhu aegamööda aina rohkem infot lisada. Hetkel on sealt võimalik leida nii tavakodanikele kui ka ettevõtjatele mõeldud näpunäiteid ja küberhügieeni põhimõtteid, samuti suunatakse riigiettevõtteid rohkem uue infoturbestandardi E-ITS suunas.

Uus infoturbestandard hakkab vaikselt jõudma asutusteni. Ka novembris korraldasime mitmeid koolitusi E-ITSi rakendajatele, arutasime eesrindlike pilootijatega kitsaskohti ja valmistasime ette juriidilisi dokumente, et E-ITSi rakendamine läheks ka regulatsiooni mõttes sujuvalt.

Jätkasime novembris tavapäraseid koolitusi infoturbe teadlikkuse tõstmisest. Oleme neid korraldanud juba aastaid nii infoturbejuhtidele, aga ka ettevõtete-asutuste juhtidele ja eraldi ka tervishoiuteenuste osutajatele. Kõigi nende koolituste eesmärk on teadvustada riske ja ohtusid, mis mõjutavad organisatsiooni tegevust ja toimimist.

Tegime 24. novembril avalikuks informatsiooni, et teadlased tuvastasid 2011. aastal ID-kaardist turvanõrkuse, mis võimaldas 120 000 kaardiga ilma PIN-koode teadmata digiallkirju anda. Selleks, et rünne läbi viia, pidi ründaja enda kätte saama kasutaja ID-kaardi ning ID-kaart pidi olema kehtiv (kaardi kaotamise korral üldjuhul sellest teavitatakse ning sertifikaadid peatatakse või tühistatakse). ID-kaartide kuritarvitustest teateid ei olnud ega ole siiani. Uut avalikustatud infot kajastasid teiste seas sügavamalt näiteks Eesti Rahvusringhäälingu saade Pealtnägija, aga ka Geeniuse portaal.

Rahvusvaheline keskkond

November võis nii mõnegi küberkurjategija jala võbisema võtta, sest teateid arreteeritud ametikaaslastest saabus omajagu. Näiteks teatas USA justiitsministeerium, et on kinni pidanud ja süüdistuste esitanud kahele REvili liikmele. Üks neist on Ukraina kodanik Jaroslav Vasinskyi (22a), kes olevat ka sel suvel rahvusvahelise tarkvaraettevõtte Kaseya pihta tehtud lunavararünnaku taga. Teine vahistatu on Vene kodanikust Jevgeni Poljanin (28a), kellele laekunud 6,1 miljonit dollarit lunaraha konfiskeeriti.

Kuu lõpus infomeeris Interpol, et viis läbi rahvusvahelise operatsiooni, mille tulemusel arreteeriti 1003 isikut, kes tegelesid näiteks armupettustega, investeerimiskelmustega, rahapesu ja ebaseaduslike hasartmängudega. Lisaks külmutasid võimud 2350 pangakontot ja üle 27 miljoni dollari. Selle kõige tuules teatas novembris BlackMatter-i küberrühmitus võimude surve tõttu tegevuse lõpetamisest.

Siiski ei toonud november õiguskaitseorganitele ainult häid uudiseid. 13. novembril pääsesid häkkerid ligi USA Föderaalse Juurdlusbüroo (FBI) serverile, kust saatsid kümneid tuhandeid võltsitud e-kirju. Need ei sisaldanud pahavara, aga imiteerisid FBI hoiatusi, mis saadetakse välja nendele, kelle võrku on sisse murtud ja andmed varastatud. FBI sõnul said häkkerid tarkvara seadistusvea tõttu ligi portaalile, mis ei ole osa FBI ühtsest e-maili süsteemist.

Mõjukaid andmelekkeid oli aga küll. Näiteks lekkis USA-s Utah osariigis asuvast radioloogiakeskusest (UIA) 582 170 patsiendi info. Lekkisid inimeste ees- ja perekonnanimi, e-maili aadress, sünnikuupäev, isikukood, tervisekindlustuse poliisi number, meditsiiniline info (diagnoosid, ravi, retseptid).

Samuti tabas andmeleke ühe maailma suurima veebimajutaja ja domeenide registeerija GoDaddy võrku. Nii lekkisid 1,2 miljoni GoDaddy kliendi e-maili aadress ja kliendinumber, mis tõenäoliselt soodustab nende pihta õngitsusrünnete tegemist.

Märkimist väärib ka see, et häkkerid pääsesid ligi USA kaitsetööstuse ettevõte Electronic Warfare Associates (EWA) meilisüsteemile ja varastasid sealt isikute kohta infot. Varastati inimeste nimesid, isikukoode ja infot juhilubade kohta. EWA pakub elektroonilisi seadmeid USA valitsusele, sh kaitseministeeriumile ja siseministeeriumile.

Ent alati ei pruugigi häkkerite eesmärk olla andmeid varastada. Näiteks Austraalia Queenslandi osariigi vee-ettevõtte (SunWater) teatas novembris, et häkkerid luusisid 9 kuud nende serveris ringi. Kliendiinfot alla ei laetud, vaid ründajad süstisid serverisse pahavara, mille eesmärk oli suurendada ühe videoplatvormi külastatavust.