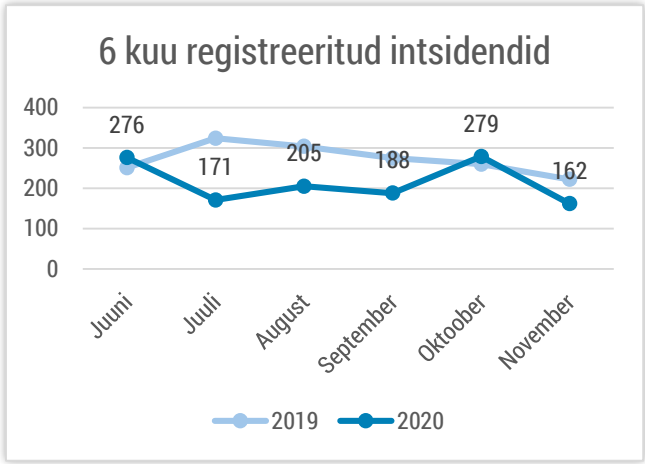
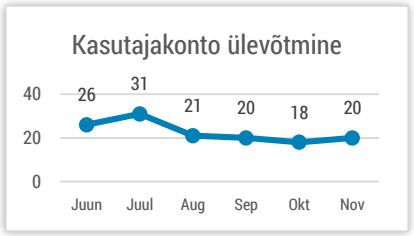
Olukord küberruumis – november 2020

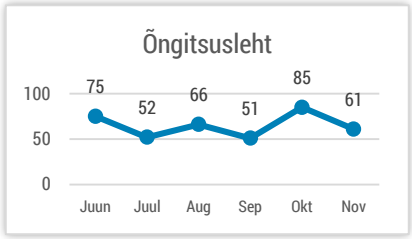
- Novembris registreerisime 162 intsidenti.
- Eesti kolme ministeeriumi haldusalade veebiserveritest varastati märkimisväärne hulk andmeid.
- Kurjategijad ähvardavad jätkuvalt teenusepakkujaid teenustõkestusrünnakutega ja teevad näidisrünnakuid.
- Emoteti pahavara levib Eestis suures mahus.
- Pakume aasta lõpuni eakatele nõuandetelefonil küberturvalisuse nõuandeid.
- Lunavararünnakud maailmas jätkuvad.



Intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.



Teated kontode ülevõtmisest on aasta jooksul stabiliseerunud.



Õngitsuslehtede hulk on jätkuvalt kõrgel tasemel. Õngitsetakse nii kontoandmeid, kui ka petetakse välja raha.

Olukord Eesti küberruumis

Novembris tuvastasime kolmel erineval juhul rünnakuid riigiametite võrkude vastu, mille tagajärjel said kurjategijad teatud ulatuses ligipääsu Majandus- ja Kommunikatsiooniministeeriumi (MKM) haldusala, Sotsiaalministeeriumi (SoM) haldusala ja Välisministeeriumi (VäM) serveritele. Kõigi rünnakute puhul märkasime sarnast käekirja ja rünnakute tagajärjel oli kurjategijatel ligipääs olulisele hulgale isikuandmetele, MKMi haldusala puhul ka „Asutusesiseseks kasutamiseks" mõeldud andmetele. Täpsemalt on võimalik lugeda RIA kodulehel pressiteatest ning ulatuslikust intsidendi kajastusest Eesti meedias.

Toetasime rünnakust mõjutatud asutusi jõu ja nõuga ning suutsime tuvastada, kuidas rünnak ellu viidi. Kõigi kolme ründe käekiri puhul rünnati veebilehti majutavat serverit. Ühel juhul õnnestus ründajatel ligi pääseda haldusala serveritele, ülejäänud kahel puhul veebiserverist kaugemale ei jõutud. Oleme alustanud järelevalve-menetlust, Andmekaitse inspektsioon oma menetlust ja keskkriminaalpolitsei kriminaalmenetlust seoses süsteemidele ebaseadusliku ligipääsu hankimisega.

Novembris saime teada taas DDoS rünnetest, mille puhul saadeti sihtmärgile rünnaku alguse ajal väljapressimis-kiri, kus nõuti raha rünnakust loobumiste eest. Sihtmärkideks on Eestis olnud septembrist alates telekomiettevõtted ja pangad, keda rünnati ka novembrikuus. Asutustel on enamasti taoliste rünnakute vastu kasutusel kaitsemeetmed, mistõttu on rünnakute mõju minimaalne.

Novembris teatas üks Eestisse registreeritud krüptoraha kauplemisplatvormi pakkuv ettevõte, et platvormi turvanõrkuse abil varastati neilt suures ulatuses Bitcoini ja Ethereumi krüptovaluutat.

Saame pidevalt teada uutest Emotetiga nakatunud seadmetest Eesti küberruumis. Oleme Emoteti pahavarast kirjutanud oma kuuülevaadetes alates augustist, tegemist on paljudele teistele pahavaraperekondadele ligipääsu müüva pahavaraga, mille kaudu võidakse varastada ohvrilt andmeid või saada laiaulatuslikum ligipääs tema seadme kaudu teistele süsteemidele. Novembris teavitati meid veel umbes 150st nakatunud seadmest. See viitab omakorda, et tegelik nakatunud seadmete arv on palju suurem. Emoteti tagajärjel toimunud rünnakute osas võime hinnata, et tegelik kahju selgub oluliselt hiljem, kui kurjategijatel on ära tehtud uurimistöö, et millistesse asutustesse nad oma pahavaraga sisse said.

Tegevused küberturvalisuse parandamisel Eestis

Seoses novembris tuvastatud rünnakutega Eesti riigiasutuste serverite vastu, mis kasutasid ära veebiserverite kriitilisi haavatavusi, koostas CERT-EE soovitused elutähtsate ja oluliste teenuste osutajatele taoliste intsidentide vältimiseks. Nendega tasub tutvuda kõigil küberturvalisuse poole püüdlevatel asutustel. Põhjalikumad soovitused saadeti mõjutatud asutustele ning neile, kes teadaolevalt kasutavad sama tarkvara, mille kaudu rünnakud toimusid. Täiendava info saamiseks on asutuste ja infoturbejuhtidel võimalus pöörduda cert@cert.ee.

Jätkasime novembris vanemaealisele venekeelsele elanikkonnale suunatud teavitustegevustega ning avasime infoliini telefonil 683 0962, kuhu helistades saab kolmapäeviti kella 13 – 15 vahel nõu ja abi erinevate küberturvalisuse küsimuste ja probleemidega. Infoliin jääb avatuks aasta lõpuni. Samuti jagasime infomaterjale raamatukogudele, kus on suurem venekeelne lugejaskond, ning viisime koostöös Väärikate Ülikooliga läbi kaheosalise virtuaalse õpitoa küberturvalisuse teemadel. Õpitoa põhjal on valminud ka kaheosaline venekeelne koolitusvideo, mis on leitav siin.

Korraldasime RIA koostööpartnerite infopäeva "Tark e-riik", mis toimus esmakordselt virtuaalselt ja kahepäevasena, 17. – 18. novembril. Teiste teemade hulgas käsitleti infopäeval olukorda Eesti küberruumis, anti ülevaade äsja lõppenud teavituskampaaniast "Ole IT-vaatlik" ning järgmise aasta plaanidest teavitustegevuste vallas. RIA infopäeva esitlusi on võimalik järele vaadata meie Youtube'i kanalilt.

Novembri alguses avaldasime juhised, kuidas turvaliselt seadistada enda või oma pereliikme nutitelefon. Need nõuanded on saadaval siit.

Rahvusvaheline keskkond

Novembris leidis aset mitu lunavararünnakut, mis põhjustasid nii rahalist kahju kui ka andmekadu. Märkimisväärsemate ohvritena võib välja tuua näiteks Brasiilia ülemkohtu või Itaalia alkoholitootja Campari, kellelt küsis Ragnar Locker rühmitus 15€ miljonit lunaraha. Maailma üks suuremaid mänguasjade tootjaid Mattel teatas suvisest rünnakust, kus andmed krüpteeriti eelneva TrickBoti pahavaraga nakatumise kaudu ja COVID teadustööga seotud biotehnoloogiaettevõtte Miltenyi Bioteci rünnati uudse Mount Lockeri lunavaraga. Küberkurjategijad on lisaks tavapärasetele võtetele saanud ligipääsu sihtmärgi võrkudesse läbi Google Drive'i ning Facebooki reklaamide.

USA justiitsministeerium konfiskeeris ajaloo suurimas ulatuses - üle miljardi dollari väärtuses - krüptovaluutat, mis oli seotud pimeveebi Silk Road platvormiga, kus kaubeldi eri kuritegelike teenustega, alates narkootikumide müügist kuni palgamõrvadeni välja.

Kuigi võidujooks COVID-19 vaktsiini leiutamise nimel on lõpusirgele jõudmas, siis on jätkuvalt paljastatud küberrünnakuid (peamiselt Venemaa, Hiina ja Põhja-Korea suunalt), mille eesmärgiks on varastada salastatud vaktsiinide uuringu ja arendamisega seotud teavet.

Novembris teatas rünnakutest oma taristu vastu mitmed suure mõjuga asutused üle maailma: elutähtsate teenuste osutajad (Jaapani tuumaenergia sektor), teadus- ja tervishoiuasutused (Vermonti Ülikooli haigla) kui ka muus mõttes globaalse mõjuga organisatsioonide vastu (Manchester United'i jalgpalliklubi).

Novembrikuus leidis aset ka mitu suuremahulist andmeleket, millest tundlikuim oli 16 miljoni COVID-19 nakatunud brasiillase isikuandmete leke. Pimeveebist leiti müügist ka 17 ettevõtte lekkest kogutud 34 miljoni kasutaja andmetega andmekogu.

Novembrikuus avaldati ka pikk nimekiri turvanõrkustest, mis võimaldasid ligi 50 000 paikamata Fortineti VPN-serverit ohustada. Nimekirjas leidus seadmeid, mis kuuluvad muuhulgas mitmetele pankadele, suurtele ettevõtetele ning valitsusasutustele. ˇ

Virtuaalse privaatvõrgu teenust pakkuv ettevõte VpnMentor tuvastas 380 miljoni sissekandega andmebaasi, mida kuritarvitati Spotify kasutajakontode ülevõtmiseks.

Kaugtööajastul tuleb tähelepanu pöörata ka laiemalt levinud vestlustarkvarale – näiteks sai novembris tähelepanu Microsoft Teams'i uuenduse nime all levitatav pahavara.