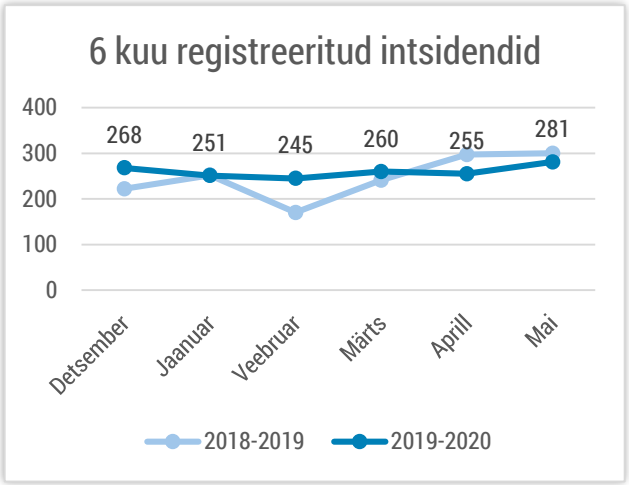
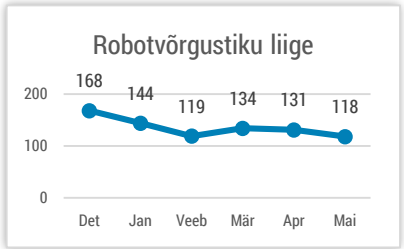
Olukord küberruumis – mai 2020

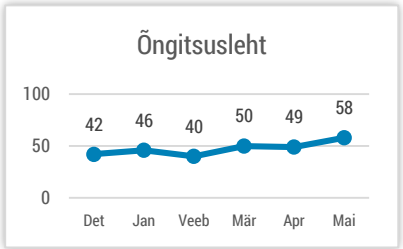
- Mais registreerisime 281 intsidenti, mis on tavapärasest veidi kõrgem näitaja.
- Märkimisväärseid koroonaviirusega seotud intsidente ei olnud näha ei Eestis ega mujal maailmas.
- Õngitsuskampaaniad kestavad, taas püüti internetipanka imiteerides ohvritelt raha varastada.
- Avaldasime inglisekeelse ülevaate Eesti küberturvalisuse maastikust ning korraldasime seda tutvustava seminari „Cyber Security in Estonia 2020: What Has Changed“.
- Lunavaraga ründavad rühmitused ähvardavad maksmata jätmise korral ohvri andmed avalikustada.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede hulk on kasvamas. Eelkõige on märgata kontoandmeid õngitsevaid lehti.

Olukord Eesti küberruumis

Mais märkimisväärseid COVID-19 viiruse levikuga või eriolukorraga seotud intsidente Eesti küberruumis me ei täheldanud. Tervishoiuteenustes (digiretsept, tervise infosüsteemi kesksüsteem jt) esines üksikuid lühiajalisi teenusekatkestusi või häireid, mille põhjustasid kas administreerimis- või tarkvaravead, mis kiirelt parandati ning mille mõju ei olnud märkimisväärne.

Mai keskel nägime taaskord internetipankade lehekülgi imiteerivaid õngitsuskampaaniaid, mis Eesti elanikke mullu pidevalt kimbutasid. SEB klientide Smart-ID kontode andmeid koguv lehekülg eemaldati 14. mai lõunaks, kuid samal päeval pärastlõunal tehti teine katse uue lehega. Kaks päeva hiljem 16. mail 13:40 algas kolmas kampaania, kus samuti imiteeriti SEB panga lehte. Kõik õngitsuslehed said eemaldatud.

Maikuust alates oleme näinud mitu lainet sarnase käekirjaga õngitsuskirju, mis üritavad kätte saada kasutajate meilikontode andmeid.

Smart-ID kasutajate suunas oleme näinud ka teisi rünnakukatseid. Mai alguses veensid petturid telefoni teel ohvrit looma Smart-ID konto. Konto jäi petturite kontrolli alla ja seda kasutati mitme finantsteenuse pakkuja juures teenuste ostmiseks.

Üks Eesti veebipood teatas, et nende serverisse on sisse murtud, sealt andmed kopeeritud, seejärel kustutatud ja nõutud lunaraha, vastasel juhul lubati andmed avalikustada. Väljapressijate kätte sattusid räsi kujul kasutajate paroolid, müügiarved, tellimused ja muud andmed. Ettevõte taastas kustutatud andmed varuversioonist, andmete avalikustamisest meile märku antud ei ole. Sarnast väljapressimismeetodit kasutavad tänapäeval ka lunavaraga tegelevad kuritegelikud organisatsioonid, kes enne failide krüpteerimist andmed endale kopeerivad ja lunaraha mittemaksmise puhul andmed avalikustada lubavad. Eesti veebipoe puhul aga lunavara kasutamist ei täheldatud.

27. mai õhtul katkes tarkvararikke tõttu ühes Riigipilve kolmest saidist andmekeskuse andmesalvestus-süsteemi töö. 28. mai hommikuks said enamus kliente oma andmetele ja teenustele taas ligi. Intsidendi tõttu polnud 27. mai õhtust kella kuni 28. mai hommikuni kättesaadavad näiteks majandus- ja kommunikatsiooniministeeriumi ja Lennuameti veebilehed.

Mais nägime üht pikemaajalist teenustõkestusrünnakut, kui üle 20 tunni jooksul rünnati üht finantsteenust pakkuva ettevõtte kodulehte. Leht ei olnud kättesaadav enam kui kümne tunni jooksul.

Tegevused küberturvalisuse parandamisel Eestis

Korraldasime veebiseminari "Cyber Security in Estonia 2020: What Has Changed", kus erinevate Eesti küberturvalisusega seotud asutuste esindajad arutlesid küberturvalisuse väljakutsete üle pandeemia tõttu muutunud keskkonnas. Tallinnas Kultuurikatlas toimunud seminari jälgis veebiülekande vahendusel üle poole tuhande silmapaari nii Eestist, aga ka pea 50st riigist üle maailma.

Küsimust „Mis on muutunud?" ajendas küsima hiljuti välja antud inglisekeelne kompendium "Cyber Security in Estonia 2020", kus kirjeldasime olukorda küberruumis enne pandeemia levikut üle maailma. Raamat annab ülevaate sellest, kuidas küberturvalisust Eestis korraldatakse ning mis 2020. aastal Eesti jaoks oluline on. RIA küberturvalisuse teenistuse kõrval on raamatus PPA küberkuritegude büroo, Kaitsepolitseiameti, Välisluureameti, Majandus- ja kommunikatsiooni-ministeeriumi, Välisministeeriumi, Kaitseministeeriumi, Andmekaitse inspektsiooni, Kaitseväe küberväejuhatuse, Kaitseliidu küberkaitseüksuse, NATO CCDCOE ja Eesti Infoturbe Assotsiatsiooni EISA ülevaated oma tegevustest ja täna olulistest teemadest.

Kutsume kõiki avaliku sektori teenistujaid läbima DigiTesti uut õppemoodulit. RIA pakub avalikule sektorile küberteadlikkuse tõstmiseks ja hindamiseks e-õppe-keskkonda DigiTest. Selleks, et hoida DigiTesti sisu ajakohasena, täiendame seda igal aastal uue õppemooduliga. Käesoleva aasta küsimustik, kursus ja test on saadaval siit.

Mai lõpus teavitasime avalikkust Magento tarkvara toe lõppemisest ja vajadusest veebipoode üle viia uuele versioonile. Nimelt on Magento 1. versioon Eestis väga levinud kodulehe ja e-poe platvormi tarkvara, kuid tootjapoolne tugi selle Enterprise versioonile lõpeb 30. juunil ära. Sõltuvalt versioonist võib tugi hõlmata nii kvaliteediparandusi kui ka turvaaukude lappimist. Turvalise kauplemise jätkamiseks soovitame uuendada tarkvara järgmisele versioonile.

Tegemist ei ole ainult 1. versiooni elutsükli lõpuga: Magento Commerce 2 (endine Enterprise Edition) tarkvara kasutavad veebipoodnikud peaksid olema teadlikud ka sellest, et tootja ei toeta ka enam versioone 2.0, 2.1 ja 2.2 ning need tuleks uuendada Magento 2.3 versioonile.

Mais lõpetasime menetlused viie kohaliku omavalitsuse suhtes ning tegime viiele omavalitsusele ettekirjutused küberturvalisusega seotud puuduste kõrvaldamiseks.

Rahvusvaheline keskkond

Märkimisväärseid COVID-19 viiruse levikuga või eriolukorraga seotud intsidente maikuus näha ei olnud.

Euroopa üks suuremaid erameditsiini võrgustikke Fresenius sai pihta lunavararünnakuga, mille käigus kurjategijad ähvardasid avaldada ka ettevõtte võrkudest varastatud andmed. Freseniuse teatel patsientide ravi rünnaku tõttu ei katkenud. Lunavararühmitus demonstreeris, et neil on tundlikke patsiendiandmeid ja avaldas 200 patsiendi nimed ja muud terviseandmed mai keskel. Tegemist on viimasel ajal üha tavapärasema olukorraga, kus küsitakse lunavara nii failide lahti krüpteerimiseks kui ka avalikustamise vältimiseks.

Jätkuvad teated suurematest andmeleketest. Odavlennufirma Easyjet teatas, et jaanuarikuus lekkisid üheksa miljoni kasutaja isikuandmed, nende hulgas 2200 kliendi pangakaartide andmed koos CVV koodidega. Lunavara Maze operaatorid andsid märku, et nad kompromiteerisid juba 2019. aasta augustis Costa Rica panga Banco BCR ning nende käes on peale muu siseinfo ka 4 miljoni kliendi krediitkaardiandmed. (Kurjategijad kritiseerisid panka nõrkade turvameetmete pärast ning mai lõpus alustasid kliendiandmete avalikustamist, et survestada panka maksma neile lunaraha.) Mai alguses pani häkkerite rühmitus Shiny Hunters tumeveebi korraga müüki 11 ettevõtte klientide andmebaasid, mille leketest ettevõtted ise teadlikud ei olnud. Lekete hulgas oli näiteks 90 miljoni Indoneesia veebipoe Tokopedia kliendi andmed ja USAs toidu kohalevedu pakkuva ettevõtte Homechef 8 miljoni kasutaja andmed. Andmebaaside eest küsis rühmitus tasu vahemikus 1500-3500 dollarit.

Uurijad paljastasid Hiinaga seostatud küberrühmituse Naikon pikaaegse spionaažitegevuse valitsusasutuste suunal Aasia ja Okeaania regioonis. Rühmitus oli viis aastat olnud pea nähtamatu pärast seda, kui 2015. aastal nende luuretegevust dokumenteeriti.

Norra riiklik investeerimisfond sai BEC-ründe tõttu 10 miljonit USA dollarit kahju. Meilisüsteemile ligipääsu saanud kurjategijad jälgisid kuude jooksul, milliseid kanaleid kaudu ülekandeid korraldatakse. Seejärel loodi ühele vastutavatest töötajatest võltskasutaja, mille kaudu suunati rahavoog fondist kurjategijate kontole.

USA riikliku julgeoleku agentuur NSA tegi harvaesineva avaliku hoiatuse, et Venemaa valitsusasutustega seostatud küberrühmitus Sandworm kasutab ära koodikaugkäivitamise turvanõrkust meiliserverites laialdaselt kasutatavas Exim tarkvaras. Sandworm on rühmitus, kes kellele on omistatud näiteks mullu Gruusiat tabanud veebilehtede näotustamise ja telejaamade rünnak, 2017. aastal maailmas hävingut külvanud NotPetya ning 2016. aastal Ukrainas elektrivarustuse katkestanud rünnaku taga.