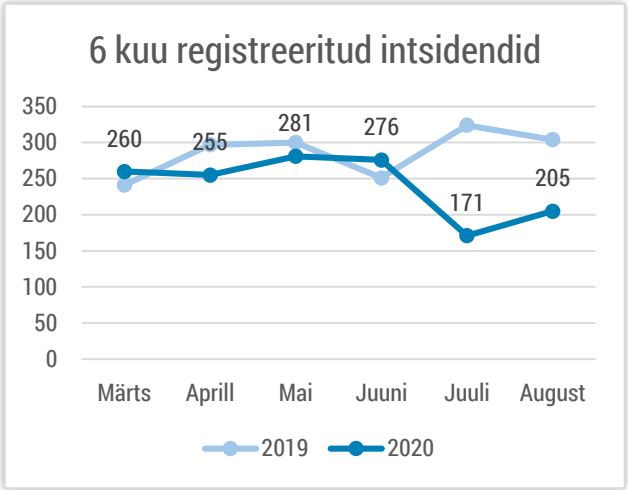
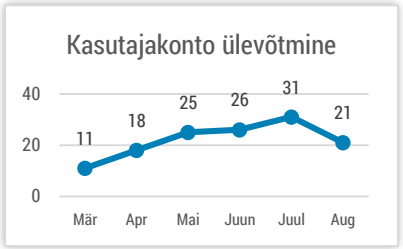
Olukord küberruumis – august 2020

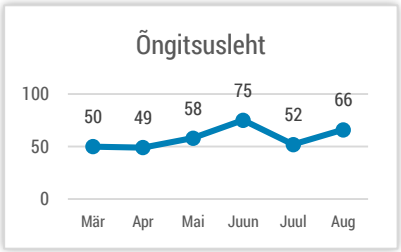
- Augustis registreerisime 205 intsidenti. Keskmisest madalam näitaja on seletatav kahe robotvõrgustiku intsidentide statistikast eemaldamisega alates juulist.
- Maailmas taas aktiveerunud Emotet pahavara jõudis ka Eestisse ning nakatas hulga arvuteid.
- Üle pika aja levitati Eestis laiaulatuslikult koroonaviiruse-teemalisi e-kirju, mille manuses oli pahavara.
- Alustasime järelevalvemenetlusi kõigi Eesti kriitilise tähtsusega andmekogude infoturbemeetmete üle.
- USA ja Hiina vastuolud mõjutavad digitaalseid rakendusi.



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



Aasta algusest oleme hakanud saama üha enam teateid kasutajakontode ülevõtmisest.



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

Olukord Eesti küberruumis

Juulis maailmas taas aktiveerunud Emotet pahavaravõrgustik jõudis augustis suuremas mahus Eesti küberruumi. Kokku saime augustikuus teada umbes sajakonnast nakatumisest, kuid eelkõige jõudsid meieni need kompromiteeritud kontod, mille kaudu püüdis pahavara end edasi levitada. See tähendab, et intsidendi mõju ei pruugi olla praegu veel nähtav ning oht võib realiseeruda alles mõne aja pärast, kui taristu omanikud aru saavad, milliste organisatsioonide seadmetesse neil ligipääs olemas on ja mida selle ligipääsuga teha.

Pahavara levitatakse üldiselt e-kirjadele lisatud dokumentide kaudu, kasutades juba kompromiteeritud kontodelt leitud meilivestlusi. Tuttavalt inimeselt tuleb sageli senisele kirjavahetusele jätkuks e-kiri, mille küljes on manus ja lakooniline teade, näiteks ingliskeelne „Please confirm". Manus on näiliselt tavaline Wordi fail, mille avamisel on näha, et teatud makrosisu on keelatud. Selle lubamiseks peab tegema veel ühe kliki (inglise keeles „Enable Content", eesti keeles „Luba sisu"). Klikkides kas lubamise nupule või pildile, nakatub arvuti pahavaraga, kusjuures kasutaja nakatumist ei märka.

Nakatumise järel pakub Emotet teenust teistele pahatahtlikele rühmitustele, kes võivad Emoteti taristut kasutada oma pahavara arvutisse saatmiseks eesmärgiga varastada sealt andmeid või nakatada arvuti hiljem näiteks faile krüpteeriva lunavaraga.

Augusti keskel levitati ulatuslikult pahavara kirjadega, mille söödaks oli kasutatud koroonaviiruse temaatikat. Pealkirjaga "Covid-19 kaitsevahendite tasuta levitamine (Eesti Vabariik Terviseamet)" kirjade saatjaks kuvati Terviseamet ja saatja aadressiks covid-19@terviseamet.ee. Kirjas lubati jagada tasuta näomaske ja muid kaitsevahendeid, nende saamiseks paluti täita kirja manuses olnud vorm, mis osutus tegelikult troojalaseks, mis varastab kasutajanimesid, paroole ja pangakaardi andmeid.

Augustis jätkusid õngitsuskatsed internetipankade klientide vastu. Seni eelkõige SEB panka imiteerivate lehekülgede kõrval oli augustis taas näha ka teiste pankade, Coopi ja LHV kliente püüdvaid õngitsuskatseid.

Tegevused küberturvalisuse parandamisel Eestis

Viimasel augustikuu nädalal korraldasime koos Clarified Securityga ning Euroopa Regionaalarengu Fondi rahastusel Eesti energeetikasektori elutähtsat teenust osutavatele ettevõtetele koolitus-õppuse KüberSärts. Õppuse eesmärgiks oli ettevõtete IT-spetsialistide isikliku ja meeskondadena hakkamasaamise proovilepanek päriselust inspireeritud ja reaalajas läbiviidavate intensiivsete küberrünnete tingimustes, et suurendada energiasektori vastupanuvõimet küberintsidentide korral. Kahepäevasele õppusele eelnes põhjalik väljaõpe eriala ekspertide poolt.

Augustist alates alustame järelevalvemenetlusi kõigi Eesti kriitilise tähtsusega andmekogude infoturbemeetmete rakendamise üle. Tegemist on ennetava lähenemisega: selle asemel, et oodata järelevalvega puuduste ilmnemiseni, alustame menetlust eesmärgiga võimalikud puudused tuvastada enne, kui mõni intsident neid päriselt mõjutab. Eestis on defineeritud kokku kümme kriitilise tähtsusega andmekogu: e-toimik, kinnistusraamat, äriregister, Riigi Teataja infosüsteem, maakataster, riigikassa infosüsteem, maksukohustuslaste register, rahvastikuregister, isikut tõendavate dokumentide register ja riiklik pensionikindlustuse register.

Augusti alguses kirjutas peadirektor Margus Noormaa alla vastastikkuse mõistmise ja koostöö kokkuleppe Eesti Infoturbe Assotsiatsiooni (EISA) juhi Oliver Väärtnõuga. Muu hulgas lepiti kokku, kuidas saame koostöös koordineerida Eesti küberturbe-ettevõtete teadus- ja arendustegevusi erinevates teadusprojektides ja panustada küberturvalisuse ennetustegevustesse.

Augusti keskel toimunud Arvamusfestivalil rääkisime kaasa laste ja nutiseadmete, vanemaealiste digioskuste, erivajadustega inimeste e-teenuste ja elanikkonna vananemise teemadel.

Rahvusvaheline keskkond

Augusti alguses kirjutas USA president Donald Trump alla korraldusele, millega andis populaarse sotsiaalmeediaplatvormi TikTok omanikule, Hiina firmale Bytedance'ile ülesande müüa maha oma tegevus Ameerika ühendriikides septembri keskpaigaks või arvestada rakenduse keelamisega USA kasutajatele. Sarnane keelamishoiatus tuli Hiinas populaarse vestlusäpi WeChat omaniku Tencent'i suunas.

Rahvusvahelise koostöö tulemusel tuvastatud mitmeid Põhja-Koreaga seotud küberrünnakuid ning petuskeeme, mille tõttu soovib USA Justiitsministeerium kurjategijate krüptovaluuta konfiskeerida. Põhja-Korea küberkurjategijate peamiseks sihtmärgiks on jätkuvalt pangandussektor. Ühendkuningriikide küberturbeettevõte Clearskysec on oma analüüsis pikemalt lahti seletanud Põhja-Korea ründevektorid ning kirjutisest selgub, et 2019. õnnestus riikliku taustaga rühmituse Lazarus rünnak lisraeli kaitsetööstusettevõtte vastu.

Hiina jätkab geopoliitiliste konfliktide käigus küberoperatsioonide läbiviimist ning seekord kahtlustab Taiwan Hiina riikliku taustaga ohustajaid kümne valitsusasutuse meilikonto ründamises.

Iraaniga seostatud APT35 (Charming Kitten) üritas ajakirjanikena esinedes saata pahavara kaitsetööstuses ja valitsussektoris töötavatele sihtmärkidele, et saada ligipääsu tundlikule infole.

USAs vahistati vene turist, kes pakkus autotootja Tesla Nevadas asuva tehase töötajale miljon dollarit, et ta enda ettevõtte süsteemidesse pahavara ringlusesse laseks. Ettevõttel läks õnneks, kuna töötaja otsustas kiire rikastumise asemel juhtumist ametivõimudele teatada.

Emotet pahavara, mis otsapidi ka Eestisse jõudis, levis augustis laialt ka mujal maailmas. Maailmas tõmbab see jätkuvalt küberturvalisuse-institutsioonide tähelepanu.

Juulikuus toimunud laiaulatuslik lunavararünnak Garmini pihta halvas ettevõtte seadmete töö mitmeks päevaks ning süsteemide töö taastati täies mahus alles augusti alguseks. Kuigi sellest saadi teada palju aega hiljem, tabas umbes samal ajal lunavararünnak tehnoloogiafirmat Konica Minoltat.

Möödunud kuul avastati andmebaas, kuhu oli eri sotsiaalmeediakanalitest kokku koondatud 235 miljoni inimese kasutajaprofiilide teave, mida üks ettevõtte kasutas turunduslikel eesmärkidel. Puudutatud olid nii Instagrami, TikToki ja Youtube'i kasutajad, kuigi kõikidel nendel veebisaitidel on kasutajaandmete kogumine kolmandatesse andmekogudesse kasutajatingimustega keelatud.