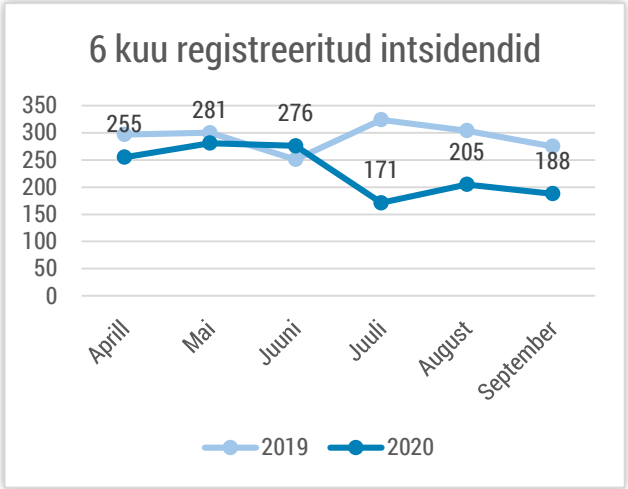
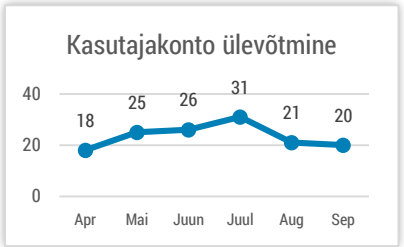
Olukord küberruumis – september 2020

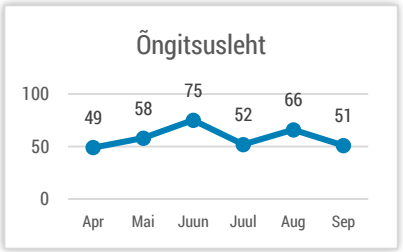
- Septembris registreerisime 188 intsidenti. Võrreldes mullusega madalam intsidentide hulk on seletatav kahe neutraliseeritud robotvõrgustiku intsidentide statistikast eemaldamisega alates juulist.
- Mitmed Eesti teenusepakkujad sattusid teenustõkestus-rünnaku alla, mille eesmärgiks oli välja pressida lunaraha.
- Emotet pahavara levib Eestis jätkuvalt.
- Septembris alustasime väikestele ettevõtetele mõeldud ennetuskampaaniaga „Ole IT-vaatlik!“.
- Saksamaal suri patsient, kellele Düsseldorfi haigla ei saanud lunavararünnaku tõttu õigeaegselt abi anda.



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



Teated kontode ülevõtmisest on aasta jooksul stabiliseerunud.



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

Olukord Eesti küberruumis

Septembris jõudis Eestisse taas väljapressimise eesmärgil tehtavate teenustõkestusrünnakute laine. Mitmes riigis ettevõtteid kimbutanud kurjategijad kasutavad hirmutamistaktikana ka laialt tuntud APT-de nimesid (Eestis näiteks Fancy Bear, mille all tuntakse ka Venemaa GRU APT rühmitust), et veenda ohvrit kindlasti lunaraha maksma. Esmalt saadetakse ettevõttele väljapressimiskiri, seejärel tehakse demonstratsioonrünnak (mõne tunni ulatuses) ja hoiatatakse, et kui lunaraha ei maksta, rünnatakse paari päeva pärast pikemalt. Sarnast skeemi kasutati ka 2017. aastal ja 2019. aastal.

Septembri rünnakutel on olnud Eestis reaalne mõju. 19. septembril toimus taoline teenusetõkestusrünne serveri- ja veebimajutusteenuse pakkuja Zone.ee vastu. Rünnaku tagajärjel ei suunanud Zone.ee nimeserverid kolmandikku .ee-lõpuga internetiaadressidest õigetesse serveritesse, mistõttu polnud paljud veebilehed kättesaadavad. Septembri lõpus toimusid lühiajalised näidisrünnakud Eesti finantsasutuste vastu, mistõttu olid nende teenused häiritud. Nimetatud intsidendid on mõjutanud ka andmesideteenuse pakkujaid, kelle taristut rünnakuteks kasutatakse.

Veel septembri keskel nägime tuttavat õngitsusskeemi, kus SMSide kaudu paluti uuendada Smart-ID profiili. Sõnumis olnud link viis ohvrid internetipankade õngitsuslehtedele, kus neilt üritati Smart-ID PIN koodide abil raha varastada. Taolisi rünnakuid Eesti inimeste vastu oleme näinud juba üle aasta. Septembri lõpus vahistas keskkriminaalpolitsei küberkuritegude üksus eduka rahvusvahelise politseioperatsiooni tulemusel rünnakutes kahtlustatavad kurjategijad Rumeenias.

Emoteti pahavara levis septembris taas mitme erineva lainega. Levimiseks kasutab pahavara nakatunud arvutist leitud meilipostkasti aadressiraamatut ja juba olemasolevaid kirjavahetusi, millele saadetakse justkui järgmine vastus, kuid sellele on lisatud pahavaraga manus. Emotet on pakub oma taristut teistele pahatahtlikele rühmitustele, kes võivad selle kaudu paigaldada nakatunud arvutitesse enda pahavara, eesmärgiga varastada andmeid või viia läbi lunavararünnakuid. Samal teemal vaata ka „Trendid ja tähelepanekud küberuumis – III kvartal 2020“.

29. septembril katkesid 2,5 tunniks Haigekassa e-teenused (sealhulgas digiretsept ja kindlustatuse kontroll) hooldustööde käigus tehtud seadistusvea tõttu.

Septembris teatati meile viiest erinevast lunavaraintsidendist. Ära märkimist väärib ühe Harjumaa perearstikeskuse süsteemide nakatumine, kuhu jõudmiseks kasutati tõenäoliselt kaugtöölaua (RDP) protokolli. Aitasime keskusel andmed taastada.

Tegevused küberturvalisuse parandamisel Eestis

Alustasime septembris väikeste ja keskmise suurusega ettevõtetele suunatud ennetuskampaaniat "Ole IT-vaatlik", mille eesmärk on juhtida tähelepanu levinumatele petuskeemidele ja anda nõu, kuidas end nende eest kaitsta. Eesti ettevõtted kaotavad aastas küberpettuste läbi üle miljoni euro, suurima mõjuga on arvepettused ja lunavararünnakud. Ehkki petturid sihivad nii suuremaid kui väiksemaid ettevõtteid, on probleem eriti terav väikeste, kuni 50 töötajaga ettevõtete jaoks, milliseid on Eestis valdav enamus. Lisaks teadlikkuse tõstmisele on kampaania eesmärk aidata väikeettevõtetel astuda esimesed sammud küberturvalisemate äriprotsesside suunas. Levinumatest petuskeemidest ja kuidas end ja oma ettevõtet nende eest kaitsta, saab lugeda siit.

Korraldasime koostöös Eesti Infoturbe Assotsiatsiooniga 10. septembril küberhommikusöögi – mitteametlikus õhkkonnas kohtumise info vahetamiseks riigisektori ja küberkogukonna vahel. Eelkõige väikeettevõtetele ja akadeemiale suunatud formaadi eesmärk on muuhulgas anda infot erinevatesse Euroopa Liidu projektidesse kaasumise võimaluste kohta. Kohtumisi on plaanis korraldada kolm kuni neli korda aastas ning nende toimumiskoht hakkab roteeruma osalevate asutuste vahel.

Jõudsime lõpule küberturbe arenguprogrammis osalevate vee-ettevõtete hindamisega nende vastavuse osas CIS20 küberturbe meetmete rakendamise nõuetele. Järgmise sammuna analüüsime koos ettevõtetega, milliste meetmete täiendamine annab kõige suuremat efekti ning kas ja milliseid rakendusi saab kasutusele võtta tegevuste automatiseerimiseks.

Kohtusime Lääne-Viru Omavalitsuste Liidu liikmetega, et tutvustada peagi valmivat Eesti infoturbestandardit ja anda ülevaade võimalustest ja piirangutest, mis seonduvad pilveteenuste laiema kasutuselevõtuga avalikus sektoris.

Rahvusvaheline keskkond

Lunavara rindel toimus möödunud kuul tihe tegevus, kui pihta said mitmed meditsiiniasutused ja koolid. Palju kajastust on saanud rünnak Düsseldorfi haigla vastu, mis võis reaalselt põhjustada ühe patsiendi surma. See rünnak on markantne, kuna ohver on teadaolevalt esimene mittesõjalise küberrünnaku põhjusel elu jätnud inimene.

USAs tabasid lunavararünnakud New Jersey'i ülikooli haiglat, tervishoiuettevõtet Universal Health Systems (sarnaselt Düsseldorfi juhtumile põhjustas patsientide ümber suunamist ning kirurgiliste operatsioonide edasi lükkamist). Nevada kooliringkonna esindajad järgisid ametivõimude soovitusi mitte maksta lunaraha, kuid see tõi kaasa õpilaste isikuandmete pimeveebis avaldamise küberkurjategija poolt. Lunavararünnak tabas ka suurt koolide võrku Washingtoni-Baltimore'i piirkonnas (Fairfaxis), videoedastustarkvara pakkujat ning kohalikele omavalitsustele teenust pakkuva tehnoloogiaettevõtet.

Septembris suurenes teenustõkestusrünnakute (DDoS) maht üle maailma – pihta said kaks reaalajas lennuinfo teenust pakkuvat ettevõtet, sealhulgas Flightradar24, Ungari suurim telekomiettevõte Magyar Telekom, meiliteenust pakkuv Saksa ettevõte Tutanota,

Küberründe ohvriks sattus järjekordne kellatootja Swatch Group, kes peatas IT-süsteemide töö rünnaku tõkestamiseks.

Ligi 2000 e-poodi, mis töötasid vananenud ning turvauuendusteta Magento platvormil, sattusid automatiseeritud rünnaku ohvriks, mis oli alates 2015. aastast omataolistest suurim.

Hispaania luureamet teatas, et Hiinaga seotud küberrühmitused on korraldanud mitmeid küberrünnakuid, mille tulemusel on varastatud Hispaania laborites arendatava koroonavaktsiini teavet.

Venemaaga seostatav küberrühmitus APT28 proovis NATO-ga seotud riike sihtida Zebrocy-nimelise pahavaraga, mida levitati läbi õngitsusmeilide, milles peitus pealtnäha NATO õppuste korraldamisega seonduvat materjal.

Valgevenes lekitasid häktivistid protestiks riigipea Aljaksandr Lukašenka repressioonide vastu ligi tuhande Valgevene politseiniku isikuandmed.