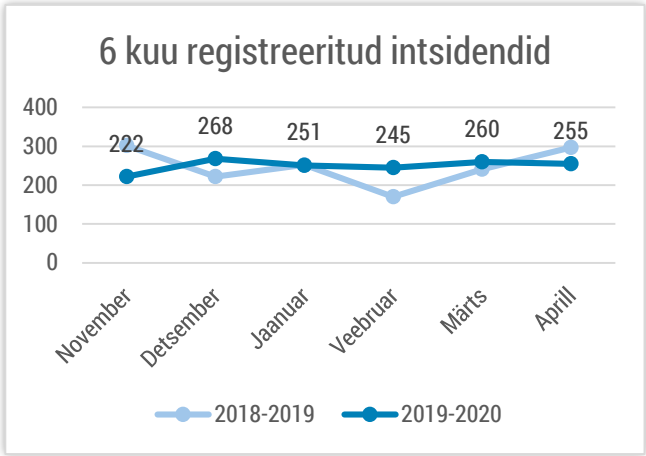
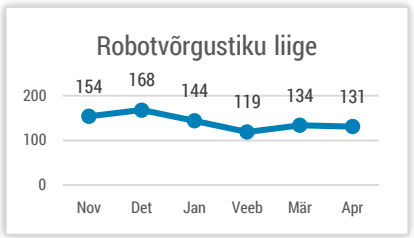
Olukord küberruumis – aprill 2020

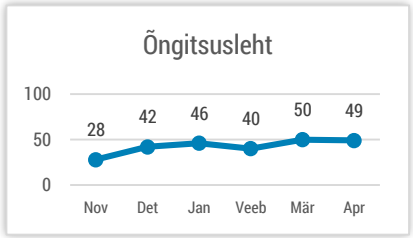
- Märgatud intsidentide hulk on stabiilne, aprillis anti meile märku 255st mõjuga intsidendist.
- Koroonaviirus domineerib uudistes ja õngitsuskirjades, kuid ei ole olulisel määral muutnud ohupilti.
- Eesti e-teenuste kättesaadavust mõjutasid eri mahuga teenustõkestusrünnakud ja rünnakukatsed.
- Korraldasime teavituskampaania „Ole eriolukorras eriti IT-vaatlik“ ning avaldasime aastaraamatu.
- Maailmas kaugtöö jaoks vajalikke suhtlusplatvorme kimbutavad olulise mõjuga turvanõrkused.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede hulk on taas kasvama hakanud. Eelkõige on märgata kontoandmeid õngitsevaid lehti.

COVID-19 viiruse levikuga seotud intsidendid Eestis ja mujal

Esialgsel hinnangul ei ole pandeemia oluliselt mõjutanud intsidentide hulka Eestis, kuigi viiruse temaatikat on kasutatud õngitsuskirjades ja petukirjades peibutisena.

Näiteks aprilli algul saime teada, et mõne avaliku sektori asutuse töötajate postkastidesse saabusid pahavara sisaldavad ingliskeelsed e-kirjad, mis näiliselt tulid Maailma Tervishoiuorganisatsioonilt. Kirja teemareal oli „Re: CF and FDA covid-19 certificate test kits", sisus ingliskeelne lühend FYI ja manuses pahavara-fail nimega „CF and FDA covid-19 certificate test kits.img". Samuti jõudis aprilli lõpus ühe riigiasutuse üldaadressile aprillis ingliskeelne e-kiri teemareaga „COVID-19 pandemic outbreak", kus öeldi, et tulenevalt COVID-19 pandeemiast tuleb e-posti turvalisuse tagamiseks rakendada erimeetmeid, kuid milles leitud link viis kontoandmeid küsivale õngitsuslehele. Viiruseteemalisi õngitsuskirju on aprillis saanud ka üks spordialaliit, viirust mainitakse logistikafirmadele saadetud õngitsuskirjades jne. Info nakatumistest või kompromiteerimistest puudub.

COVID-19 intsidendid rahvusvaheliselt

Maailmas on viirusega seonduvad ohud kõrgendatud tähelepanu all, kuid sarnaselt Eestiga pole viirus ega eriolukorrad ohupilti väga palju muutnud. Näiteks jätkuvad lunavararünnakud, kus kurjategijad on otsustanud lunaraha mitte maksvate ohvrite andmed lekitada internetti – küll aga on ohvrite hulgas ka näiteks COVID-19 vastu vaktsiinide välja töötamisega seotud ettevõte. Samuti on tavapärane küberspionaaž tervishoiu ja teadusasutuste vastu, kuid **USA föderaalne juurdlusbüroo (FBI) hoiatas, et on näinud küberspionaaži, kus sihtmärgiks on justnimelt need asutused, kes on avalikult teatanud osalemisest COVID-19 vaktsiini loomises.**

Küberspionaaž jätkub ka poliitilistel eesmärkidel. FireEye teatas, et Vietnamiga seostatud häkkerite grupeering OceanLotus või APT32 on üritanud kompromiteerida Hiina kriisireguleerimisministeeriumi ja Wuhani omavalitsuse töötajate e-maili kontosid.

Tšehhi küberturvalisuse büroo NUKIB andis kõrgetasemelise hoiatuse 16. aprillil, kus hoiatas tervishoiuasutuste ründamise eest. Hoiatuses nähtud indikaatorid andsid märku, et tegemist on juba varem nähtud pahavaraga, kuid mis võib kõrgendatud tervishoiukriisis siiski märkimisväärset kahju tekitada. Päev hiljem teatas Ostravas asuv ülikooli haigla, et tõkestas rünnaku ühele nende serveritest. Tšehhide hoiatusega liitusid poliitilisel tasandil mitmed liitlased, sealhulgas USA ja ka Eesti. Tšehhi eksperdid hindavad, et rünnakute taga võivad olla riiklike seostega rühmitused.

Olukord Eesti küberruumis

Otseselt koroonaviiruse levikuga seotud intsidendid on eraldi alajaotuses

Aprillis toimus mitmeid DDoS ehk teenustõkestusrünnakuid, mis mõjutasid reaalselt ka Eesti e-teenuste kättesaadavust hoolimata sellest, et taoliste rünnakute vastu on võimalik tehniliste kaitsemeetmetega võidelda. 3. ja 4. aprillil tabasid DDoS rünnakud rämpsposti ja pahavara vastu võitleva Spamhause'i teenust, mille üht koopiat majutavad CERT-EE/riigivõrk. Riigivõrgus rakendatud kaitsemeetmete tagajärjel lakkas töötamast vananenud võrguseade, mistõttu oli 4. aprillil ajavahemikus vähemalt poole tunni jooksul ühendusprobleeme osadel riigivõrgu klientidel. Teiste seas oli häiritud Digiretsepti töö.

Alates 18. aprillist nägime sarnase käekirjaga teenustõkestusrünnakuid järgmiste e-teenuste vastu: eesti.ee, id.ee, emta.ee, elron.ee ja elisa.ee. Osa rünnakut võimendanud seadmetest olid meile teadaolevalt turvanõrkustega, kuid uuendamata tarkvaraga Mikrotik ruuterid, mis asusid üle maailma (sh Eestis). Osa nimetatud teenustest oli lühiajaliselt ka häiritud, kuid mitte kõik.

Samuti anti meile märku teenustõkestusrünnakutest digitaalset päevikulahendust pakkuva eKool.eu vastu ning elektroonilist identiteeti pakkuva SK ID Solutions teenuste vastu. 22. aprillil oli häiritud Luminor panga kodulehe kättesaadavus ühe Leedu teenusepakkujale tehtud DDoS rünnaku tagajärjel.

Küberintsidendid jätkusid ka tervishoiusektoris. Ühe väiksema perearstikeskuse server nakatati aprilli alguses lunavaraga ning failide taastamiskatse käigus selgus, et regulaarne varundamine ei toiminud. Turvanõrkuse tõttu patsiendiportaalis kompromiteeriti aprilli keskel Ida-Tallinna Keskhaigla server. Arendaja sulges turvanõrkuse parandamiseni patsiendiportaali. Kuna eriolukorra tõttu on sellel praegu vähe kasutajaid, oli patsiendiportaali sulgemise mõju väike. Meile teadaolevalt ei olnud kummalgi juhul spetsiifiliselt sihitud tervishoiuteenust pakkuvaid asutusi.

Tegevused küberturvalisuse parandamisel Eestis

Korraldasime teavituskampaania "Ole eriolukorras eriti IT-vaatlik" jätkuna eelmisel aastal toimunud IT-vaatliku kampaaniale. Eriolukorra meetmete tõttu läks suur osa Eesti elanikkonnast kiirkorras üle kaugtööle ja koduõppele, kasutades selleks kõikvõimalikke tehnilisi vahendeid ja platvorme. Kampaania raames andsime nõu, kuidas küberturvaliselt kodus töötada ja õppida ning mitte langeda eriolukorda ära kasutada püüdvate petuskeemide ja küberkuritegude ohvriks.

Nõuanded e-õppe ohtude vältimiseks ning kaugtöö turvalisuse suurendamiseks, aga ka üldised küberhügieeni põhimõtted on hõlpsasti leitavad aadressil itvaatlik.ee.

Juba jaanuarikuus teatasime, et oleme teinud eesti keeles kättesaadavaks rahvusvaheliselt tunnustatud küberturvalisuse meetmete kogumi „CIS 20 Controls". Aprillist saab eestikeelset tõlget alla laadida ka Center For Internet Security ametlikul kodulehel.

Avaldasime aprillis ka CIS 20 meetmetele tugineva kuuest peatükist koosneva lühijuhendi *(PDF)*, kuidas parandada küberturvalisust väikestes ja keskmise suurusega ettevõtetes. Selle alusel sündisid kuus videoklippi, kus BCS Koolituse ekspert selgitab lihtsas keeles, kuidas ettevõtet tasuta või soodsate tööriistadega küberohtude eest kaitsta.

Aprillis saatsime kolmele kohalikule omavalitsusele ettekirjutuse hoiatused ning tulime vastu kümne omavalitsuse taotlusele pikendada puuduste kõrvaldamise tähtaegu seoses eriolukorraga.

Aprillis avaldatud RIA aastaraamatust saab lugeda, kuidas 2019. aasta oli Eesti küberruumis õngitsuste aasta, sest kasutajate andmete õngitsemiste ja selleks loodud veebilehtede arv kahekordistus. Mullu sai CERT-EE pea 25 000 teavitust küberjuhtumitest, nendest rohkem kui 3000 olid sellised, mille tõttu oli häiritud teabe või süsteemide konfidentsiaalsus, terviklus või kättesaadavus.

Aastaraamat kajastab ka RIA osakondade tänaseid ja eesootavaid töid – lugeda saab riigivõrgu, DigiDoc4 tarkvara, e-hääletamise, kriitilise info taristu kaitsmise ja CERT-EE tegemiste kohta. Lähiajal saavad RIA kodulehel kättesaadavaks ka aastaraamatu inglise- ja venekeelsed tõlked.

Rahvusvaheline keskkond

Otseselt koroonaviiruse levikuga seotud intsidendid on eraldi alajaotuses

Aprillis ilmnesid mitmed olulise mõjuga turvanõrkused. Apple'i toodetes leiti meililahenduses turvanõrkused, mis annavad võimaluse pelgalt meili avades kompromiteerida ohvri telefon. (Apple väitis hiljem, et kasutajaid kompromiteeritud ei ole.) Microsofti Teams rakenduses avastati turvanõrkus, kus pelgalt ühe GIF-faili vaatamise kaudu võinuks kurjategija organisatsiooni Teams'i kontod üle võtta. Plahvatuslikult kasvanud videokoosolekuplatvormi Zoom turvanõrkuse tõttu võinuks lekkida ettevõtte töötajate nimekiri.

Paljud riigid on eriolukorra tõttu kiirkorras välja töötanud mehhanismid toetamaks ettevõtteid ning see on endaga kaasa toonud teatud turvanõrkused. Saksamaa Nordheini-Vestfaalia liidumaa on praegusel hinnangul kaotanud juba kümneid miljoneid eurosid, kuna kurjategijad lõid ametlikku formulari matkivad võltsveebilehed, mille kaudu umbkaudu 3500 inimese taotluste eest kandis liidumaa raha hoopis petturitele.

Maailma Terviseorganisatsioon WHO on teatanud, et küberrünnete arv nende vastu on kasvanud viiekordselt võrreldes eelmise aasta sama perioodiga. Sellega seoses teavitati ka intsidendist, kus lekkisid 450 töötaja kasutajakonto kasutajanimed ja paroolid.

Üle maailma oli märgata rünnakuid erinevate kriitiliste sektorite suunas. Küberturvalisuse ettevõtte ESET on leidnud oma uurimises, et San Franscisco lennujaama tabanud küberründe taga on Venemaaga seostatav rühmitus Energetic Bear. Iisraeli ametivõimud teatasid, et küberrünnaku ohvriks langes veesektor – seekord küll oluliste kahjudeta. Aserbaidžaan koges pahaloomulist tegevust tuuleenergia tootmise süsteemide vastu.

Jätkuvalt saame teatada mitmetest suuremahulistest andmeleketest, mis mõjutasid ka laste isikuandmeid. Kasutajahalduse pärandsüsteemi nõrkuse tõttu kaaperdati ligi 160 000 Nintendo kasutajakontot, lekkis ka 23 miljoni Kanada lastemängude veebilehe kasutaja andmed. Järjekordsest andmelekkest teavitas Marrioti hotellikett – seekord on mõjutatud 5,2 miljoni kliendi andmed. Küberkurjategijad paiskasid pimeveebi müüki andmebaasi 267 miljoni enamasti Facebooki kasutaja andmetega. Leke puudutas peamiselt kasutajaid Ameerika Ühendriikidest, ent ei sisaldanud paroole.