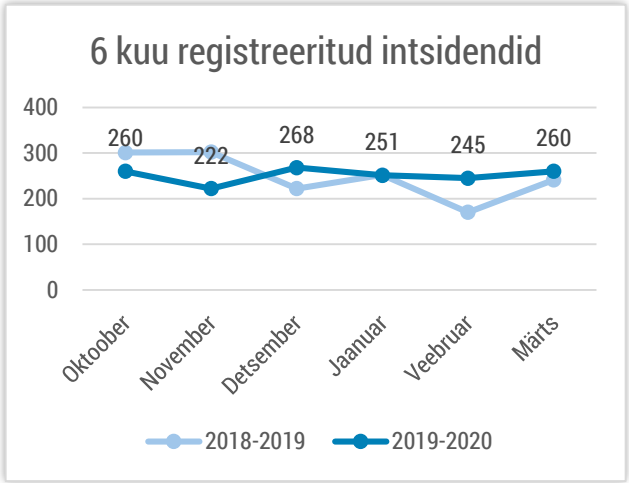
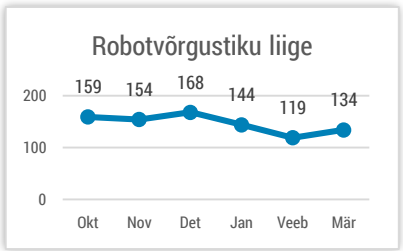
Olukord küberruumis – märts 2020

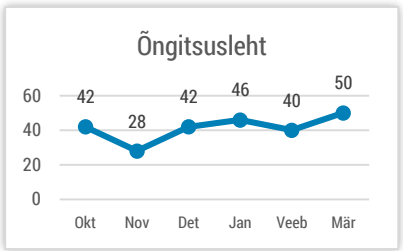
- Märgatud intsidentide hulk on stabiilne, märtsis registreerisime 260 mõjuga intsidenti.
- Eestis ja maailmas on erilise tähelepanu all koroonaviiruse infoküllust ära kasutavad skeemid.
- Eesti e-teenused on laias laastus hästi hakkama saanud suures mahus kaugtööle ja –õppele üleminekuga.
- Eestis on näha taas arvepettuseid ja palgaraha pettuseid.
- Gruusias lekkis andmebaas 5 miljoni inimese, sealhulgas surnud isikute isikuandmetega (riigis elab kokku 3,7 miljonit inimest).



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede hulk püsib kõrgel tasemel. Eelkõige on märgata kontoandmeid õngitsevaid lehti.

COVID-19 viiruse levikuga seotud intsidendid Eestis ja mujal

Märtsis jõudis Eestisse globaalne trend üritada nii pahavara levitamiseks kui õngitsusteks COVID-19 koroonaviiruse temaatikat ära kasutada.

10. märtsil saime teada, et inimestele saadetakse terviseameti poolt 8. märtsil saadetud ametlikku kirja kopeeriv libakiri, milles on link pahavarale. Lingile vajutamise järel avaneb pealtnäha tavaline ennetusplakat, kuid taustal paigaldatakse ohvri arvutisse pahavara, mis varastab brauserisse salvestatud paroolid ja pangakaartide andmed. Ehkki kirja pealkirjas („Tervis hoiuministeeriumi poolt heaks kiidetud teade COVID-19 viiruse levikus“) oli vigu, oli kiri vormistatud suhteliselt heas eesti keeles.

Viiruse tõkestamiseks kaugtööle üle läinud Eesti elanikke püüti veel mitmel viisil meelitada oma andmeid ja raha loovutama. Märtsi keskel teavitati meid petukõnedest, kus kurjategijad püüdsid arvuti turvasätete kontrollimise ettekäändel saada kaugligipääsu kasutaja arvutisse. Samuti oleme näinud õngitsuskirju, mis teavitavad justkui, et tööandja on lisanud kirja saaja uue virtuaalse keskkonna projektimeeskonda. Kui kasutaja kirjas olnud linkidel klõpsas, paigaldati tema arvutisse pahavara. Õngitsuskirjad matkivad ka maailma terviseorganisatsiooni WHO kirju.

COVID-19 intsidendid rahvusvaheliselt

Rahvusvahelises kontekstis annab sarnaselt Eestis toimuvale tooni COVID-19 pandeemiast tõuke saanud suundumuste ahel, kus nii pettused, küberründed kui ka valeinfo seostuvad üle maailma leviva viiruse mõjudega.

Eelnevalt välja toodud õngitsuste (peamiselt WHO-d matkiv, nagu ka Eestis), tegevjuhi- ja palgakontopettuste, võltsitud isikukaitsevahendite müügi juhtumeid on esinenud üle maailma. Kuna paljude riikide valitsused on kriisiolukorras elanikkonna teavitamiseks kasutanud SMS-e, siis on ka sõnumite kaudu levivate pettuste arv märgatavalt tõusnud – matkitakse nii valitsust kui ka pankasid.

Järsu kaugtööle ülemineku käigus populaarseks osutunud videokõnede platvormiks olevat Zoom keskkonda proovitakse järele teha „kloonidega“, mille kaudu laetakse seadmetesse pahavara. Samuti on kutsumata külalised videokõnedesse sisse murdnud ning seda tehes jaganud ebasündsaid sõnumeid või materjali ning kuulanud pealt konfidentsiaalseid vestlusi. Zoom on andnud märku, et pöörab avastatud nõrkustele hetkel rohkem tähelepanu.

Olukord Eesti küberruumis

Otseselt koroonaviiruse levikuga seotud intsidendid on eraldi alajaotuses

Märtsikuus läksid Eesti elanikud koroonaviiruse tõkestamiseks vajalike meetmete tõttu kiirendatud korras üle kodust töötamisele ja õppimisele. Üldjoontes on Eesti e-teenused koormuse tõusuga meie hinnangul adekvaatselt hakkama saanud. Ära tuleb märkida, et näiteks eKool andis märku ülekoormuse tõttu teenusekatkestusest vaid esimesel üleriigilisel kaugõppe päeval. Samuti teavitati meid Haigekassa e-teenustes (kindlustatuse kontroll, digiretsept jt) nii ülekoormusest kui ka seadistusvigadest lähtuvatest teenusekatkestustest 13.-20. märtsi vahel. Eriolukorra kehtestamise järgselt suurenes ravimite väljaost, mis omakorda põhjustas süsteemidele lisakoormust ja aeglustas teenuste toimimist. Aprilli alguses teostatud taristu arendustöö tulemusena on Haigekassa süsteemide koormustaluvus suurenenud ja teenuste aeglust enam ei esine. Haigekassa ja TEHIK on CERT-EE hinnangul andnud parima, et tagada intsidentide ajal süsteemi töö. Intsidentide ajal oli süsteem tavapärasest aeglasem, kuid siiski toimis.

Märtsi lõpus saime taas teateid palgaandmete petuskeemi katsetest. Skeem näeb välja selline, et näiliselt palgatöötajalt saabub personalijuhi või raamatupidaja aadressile kiri, mis palub edaspidi palgaraha kanda tavapärasest erinevale pangakontole. Selleks kasutatakse visuaalset pettust, näiteks asendatakse nimes mõni täht või muudetakse vaevumärgatavalt domeeni (ettevõte.ee vs ettveõte.ee). Samuti võidakse kasutada meilikonto puudulikku turvalisust ning teeseldakse ettevõtte töötaja aadressi, mida tavainimesel on keeruline märgata. Palgaandmete petuskeem hakkas maailmas levima sellisel moel umbes aasta tagasi, meieni jõudsid teated esimestest katsetest eesti keeles mullu augustis. Eriolukorra ja kaugelt töötamise kontekstis (näost-näkku suhtluse puudumisel) võivad taolised katsed osutuda lihtsamini edukaks.

Märtsis teavitati meid taaskord arvepettustest, mis päädisid ka rahalise kaotusega. Üks Eesti ettevõte, kelle äripartneri meilikonto oli kompromiteeritud, saatis valele arvele 15 000 eurot. Üks Eesti eraisik saatis 2600 eurot Norra teenuspakkujat teesklevale kurjategijale, kuid sai selle pankadega koostöös tagasi.

Märtsikuus teavitas üks elutähtsa teenuse pakkuja meid ühe turvanõrkuse kuritarvitamisest oma serveris, mille tõttu võinuks lekkida isikuandmeid. Märkasime, et olime tegelikult teavitanud ettevõtte teenusepakkujat antud turvanõrkusest juba varem meie automatiseeritud ohuteadete protseduuri kaudu. See tähendab, et turvanõrkuse oleks võinud juba ära parandada enne serveri kompromiteerimist. Pöörame sellele olukorrale tähelepanu ka oma kvartaliülevaates.

Tegevused küberturvalisuse parandamisel Eestis

Märtsis nõustasime Perearstide Seltsi, tervishoiutöötajaid ja haiglaid kaugtööle ülemineku, küberhügieeni reeglite ja digivõimekuse teemal. Seoses COVID-19 viiruse levikuga on tervishoiutöötajate koormus oluliselt tõusnud ning tekitanud vajaduse kaasata kiiresti lisapersonali, lisada töökohti ja luua täiendavaid kaugtöö võimalusi. Kuigi tervishoiutöötajate ülesanne on eelkõige osutada tervishoiuteenuseid, tuleb seejuures tähelepanu pöörata ka küberturvalisusele – aitasime leida selleks kõige sobivamaid lahendusi. Samuti nõustame Haigekassat põhjaliku riskianalüüsi koostamisel, mis on üks osa ettevalmistusest pilveteenuse edasiseks kasutuselevõtuks tervishoiusektoris.

Märtsis saime valmis kokkuvõtte tervishoiu vältimatu abi teenuse osutajate IT riskianalüüsidest. Võrreldes 2016. aastaga, kui viimati taolise kokkuvõtte tegime, on olukord tervishoiuvaldkonnas märgatavalt paranenud – teenuse osutajad on teadlikumad oma vastutusest süsteemi turvalisuse tagamisel ning paremini läbi mõelnud korralduslikud ja tehnilised abinõud riskide minimeerimiseks. Samas on palju tööd ka veel teha, näiteks sõltuvuste hindamisel teistest elutähtsatest teenustest ja välispartneritest, mõjude kaardistamisel jne.

Märtsis lõpetasime järelevalvemenetluse kahe omavalitsuse suhtes, kuna puudused kõrvaldati tähtaegselt. Tulime vastu mõnedele omavalitsustele, kes tegelevad kitsaskohtade kõrvaldamisega, ent palusid pikendada menetluse tähtaega seoses eriolukorraga. Ülejäänud menetlused jätkuvad tavapärases korras, ehkki kohal käimise asemel piirdume praegu suhtlusega telefoni ja kirja teel.

5.-6. märtsil toimus traditsiooniline iga-aastane tehnikute talvine teabepäev, mida kogukonnas tuntakse CERT@Voore nime all. Ligikaudu 140 tehnilist küberkaitse eksperti said CERT-EE-lt ülevaate uutest arengutest ja kasutatavatest tööriistadest, arutleti riigipilve, elektroonilise identiteedi ja muudel teemadel.

RIA koduleht on nüüd olemas ka vene keeles ja see täieneb pidevalt, et info RIA küberturvalisusega seotud tegemiste kohta oleks ka venekeelsele lugejaskonnale hõlpsasti leitav.

RIA blogis andsime märtsis näpunäiteid, kuidas turvaliselt kaugelt õppida ja töötada. **Samuti on võimalik tutvuda ülevaatega 2020. aasta esimese kvartali kohta** ja lugeda, millisteks hindame lähiajal küberturvalisuse trende.

Rahvusvaheline keskkond

Olukord maailmas on paljuski mõjutatud COVID-19 viiruse tõkestamise ja eriolukordade kontekstist, kuigi rünnakud ise on üsna tavapärased. Näiteks märtsi keskel toimunud rünnak Tšehhi Brno haigla vastu mõjutas oluliselt haigla tegevust, samas näiteks teenustõkestusrünnak USA terviseagentuuri vastu nende veebilehti maha ei võtnud. Rünnakuid haiglate suunas toimub üle maailma, nii Euroopa Liidu küberagentuur kui ka Microsoft on terviseasutustele kokku pannud juhendid, kuidas kõrgendatud ohuga toime tulla ja näiteks turvaliselt VPN-i kasutada.

Pahaloomuliste rünnete ohvriks on langenud ka teised kriisi ajal olulise tähtsusega teenused, sealhulgas toidukulleri teenus Saksamaal, mida tabas ulatuslik teenustõkestusrünnak. Samuti on küberründed puudutanud kohalikke omavalitsusi, mis kriisiolukorras suunavad oma tähelepanu akuutsete probleemide lahendamisse ning tihtipeale ei oma inimressurssi, et küberohtusid ennetada ega maandada.

Märtsis tabas Gruusiat ulatuslik andmeleke, mille põhjusel lekkisid pea viie miljoni inimese isikuandmed. Paljastatud andmed puudutasid endas nii inimeste nimesid, isikukoode kui ka koduseid aadresse ning telefoninumbreid. Lekkinud info seas oli ka üle miljoni surnud inimese andmed.

Märtsikuu ulatuslikuim andmeleke puudutas 538 miljonit Hiina sotsiaalmeediaplatvormi Weibo kasutajat, kelle andmed riputati pimeveebi müügiks. Kuna andmete seas leidus nimesid, sugu, asukohta ja pea pooltel juhtudel ka telefoninumbreid, aga mitte salasõnasid, siis kogu paketi hind oli vaid 250 dollarit.

Hiina on välja töötanud ja välja pakkunud uue interneti alusprotokolli, mis seab põhimõtteks kõigi seadmete ja IP-aadresside identifitseerimise ehk anonüümsete aadresside kadumise. Kriitikute hinnangul oleks see oht sõnavabadusele, ehk riigid saaksid niimoodi juurde meetmeid, et internetis toimuvat kontrollida.

Microsoft teatas märtsi alguses, et võttis üle 9 miljoni seadmega robotvõrgustiku nimega Necurs, mis viimase viie aasta jooksul on aidanud levitada pahavara, õngitsuskirju ja rämpsposti üle maailma. Seni oli Necursi puhul küll võimalik näha, millised seadmed on nakatunud, kuid märtsi algusest need robotvõrgustiku liikmed enam aktiivselt tegutse. *(Ka Eestis oleme pidevalt teavitanud teenusepakkujaid nende võrkudes olevatest Necursi robotvõrgustikuga liitunud seadmetest, mis moodustab märkimisväärse osa CERT-EE poolt registreeritud robotvõrgustiku intsidentidest. Need seadmed on jätkuvalt nakatunud, kuid ei ole enam teistele selle võrgustiku mõttes ohtlikud.)*