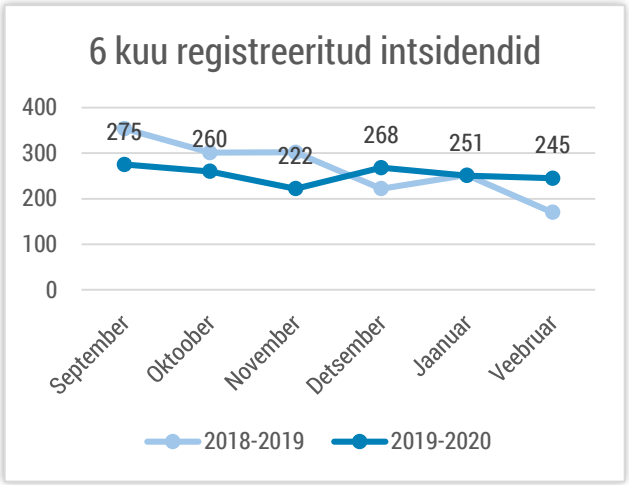
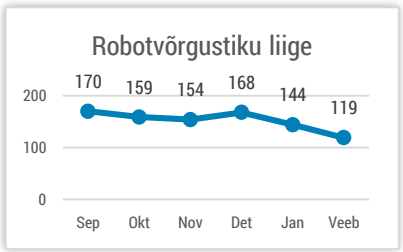
Olukord küberruumis – veebruar 2020

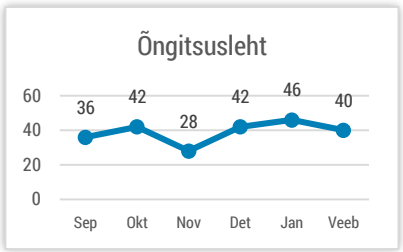
- Veebruaris registreerisime 245 intsidenti, mis on veidi vähem kui eelmise aasta keskmine tase.
- Mobiil-ID ja riigivõrk ei pääsenud tõrgeteta ka veebruaris.
- Küberkurjamid kasutavad maailmas pahavara levitamisel ära inimeste huvi COVID-19 viirust puudutava info vastu. (Eestisse jõudis trend märtsis.)
- 20 riiki, sealhulgas Eesti, omistasid eelmise aasta oktoobris Gruusia valitsusasutuste vastu suunatud rünnakute Venemaale.



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. Näha on nii kontoandmeid õngitsevaid, kui ka pangakontodele ligipääsu otsivaid lehti.

Olukord Eesti küberruumis

Veebruari iseloomustasid mitmed lühiajalised teenusekatkestused. 21. veebruari hommikul oli häiritud hinnanguliselt viiendik Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) teenustest, neist kriitilisim Häirekeskuse kõnejaotuse tarkvara Agent. Hädaabinumber 112 toimis siiski edasi, sest kõned suunati telefoniliinile. Probleemi põhjused on tuvastatud ning erinevad järeltegevused sarnase rikke kordumise ennetamiseks on planeeritud ja osaliselt juba ka teostatud.

3. veebruaril kell 19:43 kuni 20:34 oli taas häiritud Mobiil-ID kasutamine: probleeme oli Mobiil-ID ja ka ID-kaardiga e-teenustesse sisenemisel ning digitaalallkirja andmisel. ID-kaardi kasutus oli häiritud vaid neis e-teenustes, kus kasutatakse DigiDocService'i veebiteenust. **Mobiil-ID töös oli häireid ka 24. veebruaril, kuid seekord oli mõju väiksem.** Ajavahemikul 9:15 kuni 11:25 jäid vastuseta 25-30% Tele2 võrgus tehtud Mobiil-ID päringutest.

Veebruaris esines taas häireid avalikule sektorile andmesideteenust pakkuva riigivõrguga.
5. veebruaril oli tunni jooksul võrguühendus häiritud kolmandikul riigivõrgu Lõuna-Eesti klientidest, teiste seas jäid ühenduseta Tartu Vangla, Tartu kohtumaja ja Koidula piiripunkt. Sidekatkestused kimbutasid riigivõrgu kliente ka 20. veebruari öösel.

4. veebruaril tabas üht Eesti arhitektuuribürood lunavararünnak, mille käigus krüpteeriti arvutis olnud failid. Tõenäoliselt teostati rünnak läbi puudulikult turvatud kaugtöölaua protokolli, mis on üks levinumaid lunavara levitamise viisiks.

Veebruaris laekus meile mitmeid teateid pettustest, toome neist välja ühe. Kohtla-Järve elanik sai vigadest kubiseva e-kirja, milles lubati kanda tema arvele „annetusena“ ligi pool miljonit eurot. Enne seda aga paluti ohvril tasuda „maksud“. Esmalt kandis ohver petturitele 426 ja seejärel veel 1152 eurot, kuid lubatud „annetus“ jäi tulemata. RIA tuletab meelde, et kui miski tundub liiga hea, et olla tõsi, on tõenäoliselt tegu pettusega.

Tegevused küberturvalisuse parandamisel Eestis

RIA kaasabil valmis keskkriminaalpolitsei küberkuritegude büroo veebileht cyber.politsei.ee, mille kaudu saab edastada politseile infot ja teateid küberkuritegudest. Samuti saab lehelt nõu, kuidas tunda ära õngitsuskirju või taastada ligipääs isiklikele kontodele.

Jätkasime perearstide nõustamist infoturbe alal. Koostasime veebruaris ühe perearstikeskuse näitel infoturbe riskianalüüsi näidise, mida saavad edaspidi aluseks võtta ka teised perearstikeskused. Riskianalüüs on osa infoturbealasest dokumentatsioonist, mille koostamine muutub perearstidele 2022. aastast kohustuslikuks.

Veebruaris kogusime statistikat küberturvalisuse õppeplatvormide kasutamisest avalikus sektoris. Selgus, et viimase 13 kuu jooksul on RIA pakutava DigiTesti või mõne muu küberhügieeni testi läbinud 59% kõikide ministeeriumite teenistujatest. Kui lisada ka ministeeriumite haldusalade andmed, on testi läbinute osakaal peaaegu poole madalam. Meie soovitus on kehtestada ministeeriumite ja nende haldusalade teenistujatele küberhügieeni testi läbimise kohustus vähemalt kord aastas.

Lõpetasime järelvalvemenetlused kolme omavalitsuse suhtes, kuna puudused kõrvaldati tähtaegselt. Järelevalvetoimingutega seoses külastasime nelja omavalitsust ja lisaks käisime ühes linnavolikogus rääkimas infoturbe olemusest ja vajalikkusest.

Kohtusime transpordi- ja tervisesektori esindajatega, et hoida üksteist kursis küberruumis toimuva ning sektoripõhiste ohtude ja arengutega.

Rahvusvaheline keskkond

Küberdiplomaatias puudutasid kuu olulisemad arengud Gruusia vastu tehtud küberrünnakute omistamist Venemaale. Praeguseks on 20 riiki, sealhulgas Eesti, teinud avalduse, millega nähakse eelmise aasta oktoobris Gruusia valitsusasutuste vastu suunatud rünnakute taga Venemaad.

13. veebruaril teatas Austria välisminister, et jaanuaris avastatud luureinfo kogumise eesmärgiga korraldatud küberrünnaku tagajärjed on lõpuks likvideeritud. Ministeeriumi hinnangul pole võimalik täie kindlusega öelda, kes olid rünnaku taga. Austria meediaväljaanded, sealhulgas avalik-õiguslik raadiojaam ORF, on öelnud, et intsidendi taga on Venemaaga seotud rühmitus Turla.

Küberkurjategijaid jälgivad maailma arenguid ning kasutavad inimeste murelikkust enda kasuks ära. Teatatud on mitmest uue COVID-19 viirusega seonduvast pahavaralainest. Kuna praeguses kriisiolukorras saadavad riigiametid olulist teavet ka eesti.ee meiliaadressidele, tuleks olla eriti tähelepanelik ning teada, kuidas end pahavara eest kaitsta.

Veebruaris ilmusid mitmed ülevaatlikud aastaraamatud 2019. aasta intsidentide trendide analüüsi kohta. Näiteks Cisco rõhutab aasta ohtude ülevaates lunavara rünnakute ulatuslikku mõju: eelmine aasta olid ohvrite seas näiteks mitmed USA kohalikud omavalitsused ning kohtuekspertiisi pakkuv Ühendkuningriikide ettevõte. Veebruaris USAs toimunud ülemaailmsel RSA konverentsil rääkis lunavaratrendidest USA föderaalne juurdlusbüroo, kelle hinnangul on lunavararünnete ohvrid maksnud viimase kuue aasta jooksul rohkem kui 140 miljoni dollarit lunaraha.

Veebruaris teatas olulisest andmelekkest USA kaitseministeeriumi haldusalas, muu hulgas Valge Maja infoturbe eest vastutav agentuur Defense Information Systems Agency. Lekke ulatus ei ole lõpuni selge, kuid meediaväljaanne Forbes viitab kuni 200 000 mõjutatud isikule.

Veebruaris tuli päevavalgele, kuidas Saksa ja USA luureteenistused külma sõja ajal (ja tõenäoliselt veel ka 21. sajandi alguses) teiste riikide valitsuste järel luurasid. Selleks kasutati Šveitsi ettevõtet Crypto AG, mis müüs erinevatele riikidele krüpteerimismasinaid, mille koodi suutsid Saksa ja USA eriteenistused vaevata lahti harutada.