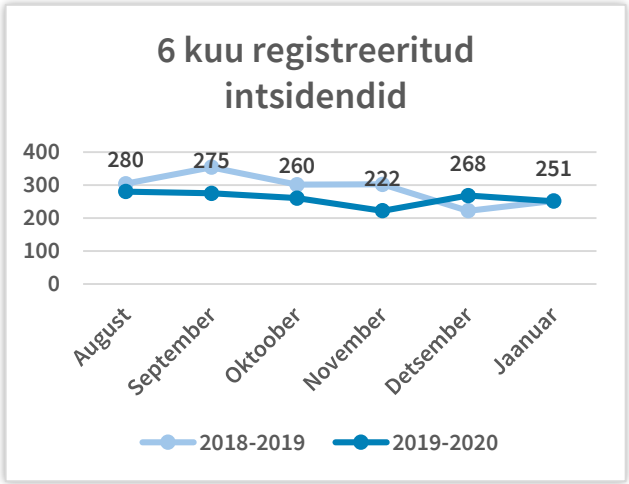
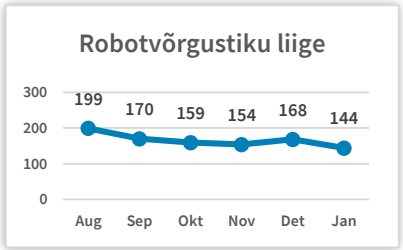
Olukord küberruumis – jaanuar 2020

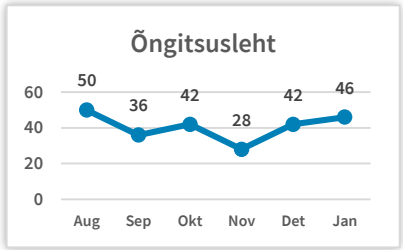
- Jaanuaris registreerisime 251 intsidenti, mis on umbes sama hulk, kui mullu keskmiselt.
- Nagu detsembris, katkes ka jaanuaris korduvalt digiretsepti ja kindlustatuse kontrolli teenus Haigekassa hooldustööde käigus.
- Finantspettused on arenemas, kurjategijad sihivad võltsarvetega suurte ettevõtete kliendibaasi.
- Kurjategijad suutsid kiirelt ära kasutada äsja avalikustatud turvanõrkusi tarkvaras ja seadmetes.
- Euroopa Liidus avaldati ühtne 5G riskide maandamise meetmete pakett.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede hulk hakkas tõusis taas jaanuarikuus. Taas paistsid silma internetipanku imiteerivad leheküljed.

Olukord Eesti küberruumis

Jaanuaris teavitas Haigekassa meid taaskord neljal korral (6., 9., 27. ja 30. jaanuaril) katkestustest digiretsepti ja kindlustatuse kontrolli teenustes. Sarnastest katkestustest kirjutasime ka detsembris ning nende põhjuseks on Haigekassa nimetanud osaliselt aegunud infosüsteemide ülevaatamist, korrastamist ja uuele baastaristule ülemineku ettevalmistamist. Pikim katkestus toimus 09.01 hommikul ja kestis 41 minutit, kokku olid digiretsepti ja kindlustatuse kontrolli teenused jaanuaris häiritud 1 tunni ja 40 minuti jooksul.

Jaanuaris jõudis meieni info kolmest finantspettuse katsest võltsarvete abil. Näiliselt Eesti ehitussektori, meditsiinisektori ja logistikasektori ettevõtete nimel saadeti koostööpartneritele ja klientidele laiali hulk võltsarveid, kus paluti raha kanda petturite pangakontole. Kahel juhul oli registreeritud ettevõttele sarnase nimega domeen, kolmandal juhul kasutasid petturid ära asjaolu, et ettevõtte enda meilidomeen ei olnud piisavalt hästi kaitstud väärkasutamise vastu. Tegemist on uuema petuskeemiga, mis võib tulevikus põhjustada märkimisväärset majanduslikku kahju, sest sihtmärgiks võib sattuda mõne ettevõtte kogu kliendibaas.

RIA on välja andnud juhendi (küll avalikule sektorile, kuid soovitame seda ka ettevõtetele), kuidas meilivahetust turvalisemaks muuta, kasutades väärkasutamise ennetamiseks korrektselt konfigureeritud SPF, DKIM ja DMARC protokolle.

Jaanuaris nägime ka ühte suuremat pahavara sisaldavate e-kirjade lainet, kus inimesed said e-kirja teemaga “HP ePrinti kasutaja skannitud dokument” ning lisatud manuse avades võis arvuti nakatuda pahavaraga, mis võimaldab kurjategijatel autoriseerimata kaugligipääsu arvutisse.

Jätkuvalt üritavad kurjategijad teenida hõlptulu ka lunavararünnakutega. Jaanuaris saime teada kuuest juhtumist, kus ettevõtte või eraisiku arvuti oli nakatatud andmeid krüpteeriva lunavaraga. Ühel juhul peatas lunavararünnak ühe tööstusettevõtte äritegevuse 36 tunniks, ettevõte ise hindas oma majanduskahjuks 17 000 eurot.

23. jaanuari pealelõunal oli ligikaudu pooleteist tunni jooksul häiritud riigivõrgu töö. Interneti põhivõrgu trassi plaanilise hoolduse käigus suunati riigivõrgu liiklus tagavaratrassile, mis aga ei tulnud koormusega toime. Seetõttu oli mõnede klientide andmesideühendus tavapärasest aeglasem.

Tegevused küberturvalisuse parandamisel Eestis

2019. teisel poolaastal otsustasime eestindada maailmas küberturvalisuse ekspertide kogukonna poolt kokku pandud turvameetmete kogumi nimega Center for Internet Security (edaspidi CIS) Controls. 20 meetmest koosnev turvameetmete kogumi 7. versioon on nüüd eesti keeles leitav RIA koduleheküljelt, inglisekeelne CIS koduleheküljelt. Center for Internet Security on USA küberturvalisuse agentuuriga CISA lähedalt koostööd tegev mittetulundusorganisatsioon, mis kogub parimate praktikate kirjeldused kokku valdkonnas töötavatelt ekspertidelt.

Oleme ette valmistamas uut infoturbe standardit nendele asutustele ja organisatsioonidele, kes hetkel peavad järgima ISKE baasturbemeetmeid. Uus regulatsioon peaks valmima aasta lõpuks. Jaanuaris korraldasime infopäeva nendele asutustele, kes uut standardit peaksid rakendama hakkama, et saada tagasisidet meetmete praktiliste nüansside kohta.

Jaanuaris jätkusid küberhügieeni koolitused kohalike omavalitsuste personalile, mida oleme süsteemselt korraldanud juba üle aasta. Veebruari alguseks jõudsime küberhügieeni koolituste sarjas sajanda koolituseni. Nendest 75 koolitust on toimunud kohalikus omavalitsuses, 9 Tallinna linnaosavalitsustes ja 16 koolides ning lasteaedades. Koolitussari on jõudnud kokku 3000-3500 osalejani. Kõige vähem oli kuulajaid Vormsil (4) ning kõige rohkem Saaremaal (enam kui 120).

Jaanuaris korraldasime järjekordse Suricata-4-All (S4A) koolituse kriitilise informatsiooni infrastruktuuri pakkujate infoturbepersonalile. S4A on RIA CERTi poolt välja töötatud võrguliikluse analüüsi vahendite pakendamise tarkvara, mille abil saame võimalikult kiiresti jagada oma klientidele meile teadaolevaid ründeindikaatoreid ja toetada asutusi pahaloomulise võrguliikluse avastamisel.

Jaanuari lõpus hoiatasime Eesti avalikkust detsembri keskel avaldatud kriitilise turvanõrkuse eest Microsofti internetibrauseris Internet Explorer, mis võimaldab selle kasutajate arvutisse pahavara saata.

Osaleme majandus- ja kommunikatsiooniministeeriumi ja Tallinna Tehnikaülikooli koolitusprogrammis, mille eesmärgiks on järgmise kolme aasta jooksul koolitada perearste ja –õdesid efektiivsemalt ja turvalisemalt digitaalseid lahendusi kasutama.

Rahvusvaheline keskkond

29. jaanuaril esitlesid Euroopa Komisjon ning liikmesriigid EL-i meetmepaketti 5G võrkude turvalisuse tagamiseks. Paketi eesmärgiks on luua üle-Euroopaline ühtne lähenemine 5G riskide küsimuses ning määratleda EL-i ja liikmesriikide rollid, õigused ja volitused. Töövahendit tuleks käsitada kui soovituslikku riskide maandamise vahendite paketti. EL-i ja Euroopa Komisjoni ülesandeks kujuneb välisinvesteeringute sõelumine, 5G tehnoloogiate arendamise võimekuse rahastamine ning 5G toodete sertifitseerimise süsteemi loomine.

(Eestil on kavas luua taoliste riskide maandamiseks protseduur sidevõrkudes kasutatava tehnoloogia kooskõlastamiseks. Selle eesmärgiga esitas väliskaubandus- ja infotehnoloogiaminister jaanuari lõpus eelnõu, millega lisanduks elektroonilise side seadusesse valitsusele volitus kehtestada vastav protseduur.)

Päev varem esitlemist teatasid Ühendkuningriigid, et annavad Hiina tehnoloogiagigandile piiratud ligipääsu 5G võrkude ehitamisele.

Jaanuari alguses avalikustas Austria, et nende välisministeerium on sattunud tõsise küberrünnaku alla, viidates riiklike seostega häkkerite tegevusele. Kompromiteeritud süsteemide taastamine ja rünnaku tõrjumine võttis pikemalt aega, Austria ajalehe Die Presse andmetel on rünnaku käekiri äratuntav Venemaa APT rühmituse Turla tegevusena.

Maailma suurimat valuutavahetajat ja reisitšekkide vahendajat Travelexi tabas uue aasta alguses lunavararünnak, mille käigus küsiti ettevõttelt üle 5 miljoni euro lunaraha. Teenuste taastamine on olnud aeganõudev ning ründajad – Sodinokibi nime all tuntud grupeering – ähvardas lunaraha mittemaksmise korral avalikustada Travelexi klientide andmed.

Lunavararünnakute puhul oleme sarnaseid nõudmisi näinud maailmas üha enam ning rünnakud on niimoodi ka muutunud, et enne failide krüpteerimist ohvrite andmed kätte saada. See annab lunavaraga opereerivatele kurjategijatele ka võimaluse nõuda raha nendelt organisatsioonidelt, kes muidu lunavararünnaku varukoopiate tõttu lihtsamini üle elaks.

Jaanuaris saime teada mitmetes laialdaselt kasutatavates tehnolahendustes. Turvanõrkusi avastati Microsofti eri toodetes, Wordpressi plug-in liidestes ning varem avastatud turvanõrkuste ärakasutamist Citrix serverites. Näiteks Hollandi küberturvalisuse keskus NCSC-NL soovitas ettevõtetel Citrixi süsteeme mitte kasutada, kuniks pole turvapaiku ja kui see on teenuste pakkumise kontekstis võimalik.

(Ka RIA teatas jaanuaris, et soovitab Microsofti veebibrauserit Internet Explorer mitte kasutada, kuni turvapaigad pole kättesaadavad.)