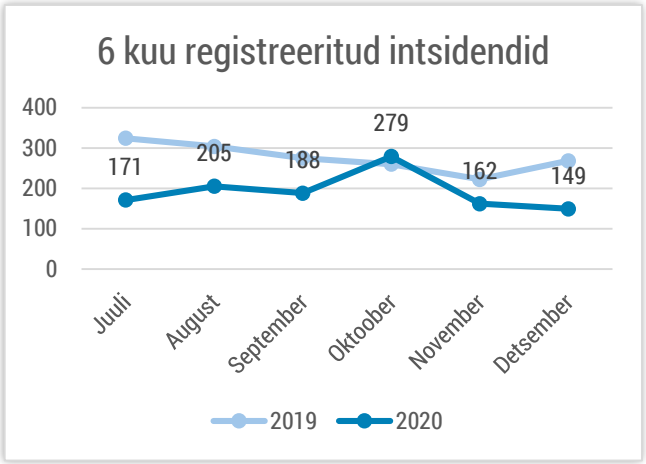
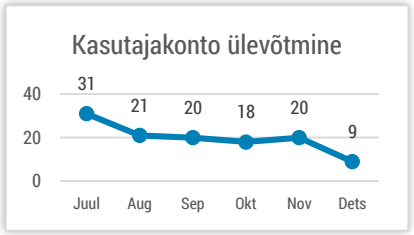
Olukord küberruumis – detsember 2020

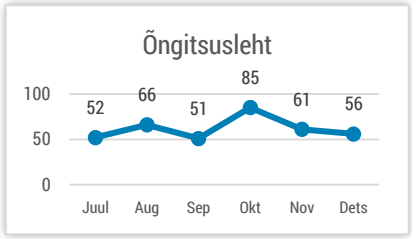
- Detsembris registreerisime 149 intsidenti.
- Maailmas sai enim tähelepanu IT-halduse tarkvaratootja Solarwinds tarneahelarünnak ja nende kaudu valitsuste ja suurettevõtete kompromiteerimine.
- Eestis jätkusid lunavaraintsidendid, õngitsused ja arvepettused.
- Aitasime tuvastada turvanõrkuse, mis andnuks võimaluse võtta kiirlaenu võõra inimese nimel.
- Toetasime Eesti väiksemate vee-ettevõtete küberturvalisuse taseme tõstmist.



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



Teated kontode ülevõtmisest langesid aasta lõpuks.



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

Olukord Eesti küberruumis

Detsembris avastati ülemaailmne tarneahelarünnak, kus tõenäoliselt Venemaalt pärit küberluurajad kompromiteerisid IT-halduse ja -monitoorimistarkvara Orion pakkuva USA ettevõtte Solarwinds. Kompromiteeritud tarkvarauuenduste abil saadi ligi tarkvara kasutavate asutuste IT-taristule. Mõjutatud on ligi 18 000 klienti, enamasti suurkliendid, nende seas mitmed USA ministeeriumid, Microsoft, Cisco ja FireEye. Ka Eestis on asutusi, kes nimetatud tarkvara kasutavad, kuid meile teadaolevalt rünnak neid mõjutanud ei ole.

Detsembris registreerisime hulga lühiajalisi katkestusi mobiil-ID töös. 1. detsembril oli häireid mobiil-ID töös Telia ja Elisa võrgus pooleteise tunni jooksul, 6. detsembril pea tunni vältel üle terve mobiil-ID taristu, 15. detsembril mitme tunni jooksul taas hulgal Telia klientidel, 28. detsembril jälle Elisa klientidel.

Detsembris teavitati meid kolmest lunavararünnakust: pihta said metallitööstuses, transpordisektoris ja ehitusmaterjalide valdkonnas tegutsevad ettevõtted. Kahel juhul saadi ligipääs Windowsi kaugtöölaua-protokolli (*Remote Desktop Protocol* ehk RDP) kaudu, kolmandal juhul teise kaugelt ligipääsetava ühenduse kaudu. Ettevõtted märkisid kahjudena süsteemide ja andmete taastamiseks kuluvat tööaega.

Detsembris saime taas hulga teateid õngitsuskirjadest. Jõulude eel, 18. detsembril hakkasid näiteks levima Omniva nimel saadetud kirjad, milles teatati, et adressaati ootab pakk, kuid selle eest on vaja tasuda. Kirjas oli link petturite kontrolli all olevale veebilehele, kuhu meelitati sisestama pangakaardi andmeid.23., 27. ja 30. detsembril levisid taas petukirjad, millega püüti välja petta SEB klientide internetipanga kasutajatunnuseid ja Smart-ID PIN-koode.

Augustist alates Eesti küberruumis levinud Emotet pahavara andis endast märku ka detsembris, saime teada enam kui poolesajast nakatumisest, millest teavitasime omakorda vastavaid internetiteenusepakkujaid.

Üks Tartu ettevõte teatas arvepettusest, mis jälgis tuntud valemit: petturid jälgisid ettevõte ja selle koostööpartneri vahelist e-kirjavahetust ning sekkusid sellese hetkel, kui jutt läks arve tasumisele. End tarnijana esitlenud petturid saatsid Tartu ettevõttele arve, mille palusid tasuda uuele pangakontole. Arvepettusega kaasnenud kahju on üle 3400 euro.

28. detsembri hommikul algas teenusetõkestusrünne ühe uudisteportaali vastu, mis kestis terve päeva. Leht ei kättesaadav olnud ajavahemikus 11:35 kuni 16:30. Rünnaku motiiv pole teada, ettevõte võttis kasutusele uue teenusepakkuja, et taolisi olukordi vältida.

Tegevused küberturvalisuse parandamisel Eestis

Juulis kirjutasime, kuidas eksperdid avastasid turvanõrkuse paarikümnel Eesti veebilehel, mis ei kontrollinud ID-kaardiga autentimisel sertifikaatide kehtivust ja allkirjastatust. **Detsembris avastasime, et ühel kiirlaenu pakkuva ettevõtte lehel on sarnane turvanõrkus, mis andis teoreetiliselt võimaluse võõra inimese nimel kiirlaenu võtta.** Andsime ettevõttele nõrkusest teada, misjärel nõrkus likvideeriti. Kiirlaenupakkuja hinnangul ei ole ühtegi märki, et turvanõrkust oleks ära kasutatud.

Korraldasime infopäeva kriitilise taristu kaitsjatele ehk siis Eestis elutähtsaid ja olulisi teenuseid pakkuvate asutuste infoturbejuhtidele ja -töötajatele. Varasemad infopäevad on keskendunud päevakajaliste teemade kõrval rohkem tehnilistele tähelepanekutele, kuid sel korral võeti tähelepanu alla riskianalüüside olulisus ning selgitati, kuidas neid teha nii, et need päriselt ka ettevõtet või asutust kriisis aitaksid.

2020. aastaga sai punkti Eesti väiksematele ja keskmise suurusega vee-ettevõtetele suunatud küberturvalisuse pilootprogramm, mille eesmärgiks oli ettevõtete küberturbe teadlikkuse ja -taseme tõstmine. Pool aastat kestnud programmis osales viis asutust, kellega vaadati üle nende küberturvalisuse tegevused lähtuvalt CIS20 meetmetest ning kellele koostati ka näidisdokumendid, mille abil saavad ettevõtted edaspidi paremini hinnata oma valmisolekut ning väljast tellitavaid it- ja küberturvalisuse teenuseid.

Detsembriga lõppes taas pikem küberintsidendist tingitud hädaolukorra riskianalüüsi ajakohastamise protsess. Hädaolukorra seaduse järgi on RIA-l kohustus regulaarselt uuendada riskianalüüsi ja hädaolukorra lahendamise plaani, sealhulgas planeerida ennetavaid tegevusi riskide maandamiseks. Ajakohastatud stsenaariumid aitavad meil kaitsta Eesti e-riiki, ette valmistuda olukordadeks, kus küberintsidendid võivad kasvada üleriigiliseks hädaolukorraks ning on sisendiks hädaolukorra lahendamise plaani ajakohastamise protsessile.

Rahvusvaheline keskkond

Detsembris avalikustas Euroopa Komisjon uue Euroopa Liidu küberstrateegia, uue võrgu- ja infosüsteemide turbe (NIS) direktiivi ettepaneku ning 5G turvalisuse rakendamise vahearuande. Uue NIS direktiivi lähenemine näeb ette rohkemate sektorite hõlmamist elutähtsate ja oluliste teenuste alla, mis tähendab, et küberturbe miinimumstandardeid peavad järgima hakkama muuhulgas sellised sektorid nagu postiteenused, ravimi- ja toidutööstus. Suuremat rõhku hakatakse panema tarneahela turvalisusele, kus elutähtsate teenuste osutajatele võivad kohalduda uued reeglid, mis kohustavad välistama riskantsete tootjate tooteid.

Kuu keskel leidis aset ülemaailmne tunniajane katkestus Google teenustes, kusjuures mõjutatud olid nii Google pilveteenused, Youtube voogedastusplatvorm, Gmail ning paljud teised nendest sõltuvad teenused. Google teatas, et juhtumi põhjustas viga keskses identiteedihaldussüsteemis.

Lunavararünnakud jätkusid – ohvriks langes muuhulgas maitse- ja lõhnaainete tootja Symrise, kelle klientide seas on ka Nestle, Unilever ja Coca-Cola. Ettevõte pidi enda töö pea täielikult seiskama, kuna krüpteeriti ligi 1000 nende seadet. Samuti tabas lunavararünnak tuntud USA poeketti Kmart-i ning Saksa üht suurimat meediamaja Funket. Lõuna-Korea jaekaubandusketilt varastati lunavara rünnaku järgselt väidetavalt ligi 2 miljoni kliendi krediitkaardi andmed.

Emoteti robotvõrgustik levis aasta lõpus uute lainetega üle maailma. Sarnaselt otsivad ka teiste pahavaraperekondade levitajad uusi trikke. Dridexi pahavara levitati jõuluootuses läbi Amazoni ja muude virtuaalsete kinkekaartide.

Detsembrikuus aset leidnud intsidentidest on märkimisväärsed ka mitmed riiklike asutuste (Soome parlament, Vietnami sertifitseerimisasutus) kompromiteerimised ja rahvusvaheliste organisatsioonide (Euroopa Inimõiguste Kohtu vastane rünnak tõenäoliselt seotud ühe konkreetse kohtuotsusega) tegevuse häirimised. Jätkus pahatahtlik tegevus ravimite ja vaktsiinidega tegelevate asutuste vastu, kus muu hulgas saadi ligipääs olulistele Euroopa Ravimiameti dokumentidele perioodil, mil kogu Euroopa ootas esimese COVID-19 vaktsiini heakskiitu.

Jätkuvad vaenulikud kübertegevused Iisraeli vastu, mis on laienenud ka viimase uutele partneritele nagu näiteks Iisraeli-Araabia Ühendemiraatide vaheliste diplomaatiliste sidemete sõlmimise tagajärjel sagenenud küberrünnakud Ühendemiraatide suunal.