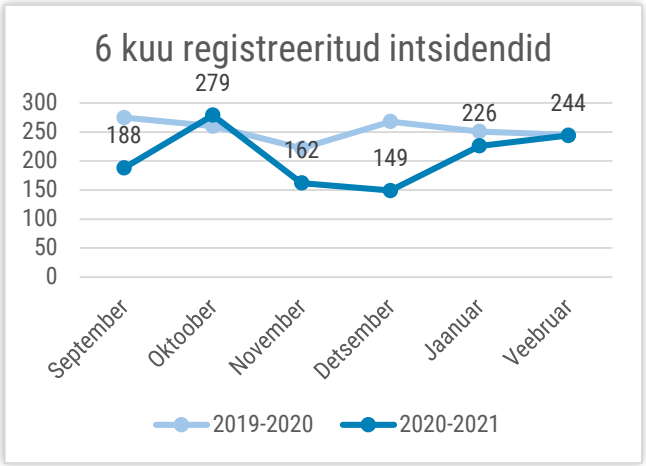
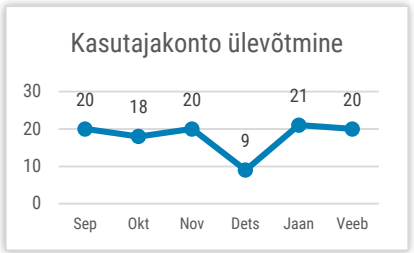
Olukord küberruumis – veebruar 2021

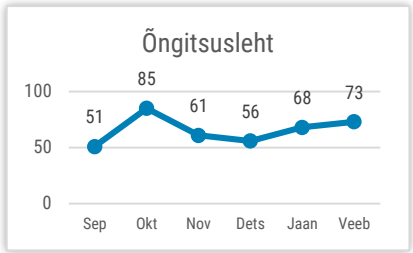
- Veebruaris registreerisime 244 mõjuga intsidenti, mis on umbes sama hulk nagu mullu, kuid viimase kuue kuu keskmisest kõrgem.
- Eesti ettevõtteid rünnati sarnasel viisil nagu mullu novembris kolme Eesti riigiasutust.
- Ühe Eesti ettevõtte tähelepanelike töötajate tõttu jäi ründaja ilma ligi miljonieurosest kuritegelikust tulust.
- Maailmas jätkus SolarWindsi tarneahelarünnaku tagajärgede likvideerimine ja mõjude tuvastamine.
- Kehva küberhügieeni tõttu sai ründaja ligi USAs Florida väikelinna veepuhastusjaama SCADA süsteemile.



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



Meilikontode ja sotsiaalmeedia-kontode ülevõtmine on jätkuvalt päevakajaline.



Õngitsuslehtede hulk on püsivalt kõrgel tasemel ja tõusutrendis. Eelkõige õngitsetakse kontoandmeid.

Olukord Eesti küberruumis

Veebruaris teavitati meid kahest olulisest intsidendist, kus kasutati sarnast käekirja nagu 2020. aasta sügisel majandus- ja kommunikatsiooniministeeriumi, välisministeeriumi ja TEHIKu kompromiteerimise puhul: ründajad skaneerisid avalikult kättesaadava teenusega veebiservereid, leidsid turvanõrkuseid, laadisid üles ründekoodi ja said autoriseerimata ligipääsu serveritele. Veebruaris teavitas meid kompromiteerimisest üks ettevõte, kes pakub pilveteenuseid ja tarkvara paljudele avaliku sektori asutusele (ministeeriumid ja kohalikud omavalitsused) ning teine, kes pakub samuti avaliku sektori asutustele kaugligipääsu teenuseid. Ettevõtted on oma teenused ära paiganud ja oma kliente teavitanud. Oleme omalt poolt tuletanud avaliku sektori infoturbejuhtidele meelde, et sellist ründemeetodit katsetatakse järjepidevalt. Lisaks on CERT-EE käsutuses ründajate peamiselt kasutatav automaattööriist, mille abil oleme pakkunud asutustele võimalust veebilehti üle skaneerida, et parandada need kohad, mis parandamist vajaks enne kui ründajad nõrkused avastavad.

1. veebruaril toimus kaheksa tunni jooksul ummistusrünne ühe Eestis toimetava panga suunal, mille tõttu oli häiritud internetipanga, kaardimaksete ja pangasiseste teenuste töö. Rünnaku eel saadeti taas väljapressimiskiri, kus nõuti lunaraha. Sarnastest rünnakutest kirjutasime ka jaanuarikuus.

Kohaliku e-poe Mineral Garden veebilehel olid avalikult ligipääsetavad ligikaudu viie tuhande isiku tellimuste andmed, nimed, telefoninumbrid, meiliaadressid ja muud isikuandmed. Poe andmelekkest kirjutati ka meedias. E-poe haldaja kinnitusel kõrvalised isikud kõnealuseid andmeid alla ei laadinud.

Päev enne vabariigi aastapäeva tabas lunavararünnak Harjumaal asuvat eakate hooldekodu serverit. Phobos lunavaraga krüpteeriti serveris olnud terviseandmed, abikutsungisüsteem ning majandustarkvara.

Veebruari keskel teavitas üks sporditeenuste pakkumisega tegelev ettevõte, et on langenud arvepettuse ohvriks. Petturil oli ligipääs kannatanu ja selle partnerite vahelisele kirjavahetusele, kuhu ta sobival hetkel sekkus ning muutis arvetel arvelduskonto numbrit. Kahjusumma pole teada.

Samuti saime teada untsu läinud arvepettuse katsest, kus ühe ehitusettevõtte töötajate tähelepanelikkus säästis neid suurest kaotusest. Ettevõtte üks meilikontodest oli kompromiteeritud ning ründajad jälgisid sellelt peetud meilivestlusi. Seejärel hakkasid nad suhtlema töötajaga ja ettevõtte raamatupidajaga ning üritasid suunata arvete maksmise Euroopa Liidust välja, Mehhikos asuvale arvele. Tähelepanelike töötajate tõttu jäid 900 000 euro ulatuses makseid tegemata.

Tegevused küberturvalisuse parandamisel Eestis

Nagu eelmises rubriigis mainitud, täheldasime taas tuttava käekirjaga rünnakuid, kus ründaja esimeseks sammuks oli ühe avalikult kättesaadava Acunetixi nimelise tööriistaga veebiserverite skaneerimine leidmaks turvanõrkusi. Seetõttu hakkasime veebruarist pakkuma avaliku sektori asutustele võimalust sama tööriistaga oma veebiteenused üle kontrollida ning leitud nõrkused parandada. Igale asutusele laekub skaneerimise järel põhjalik raport leidudest. Veebruarikuus kasutati seda võimalust pea sada korda ja pakume seda teenust avalikule sektorile ka edaspidi.

Lisaks avaliku sektori veebiteenustele tegeleme ka elutähtsaid teenuseid osutavate asutuste (ETO) üldise küberturvalisuse parandamisega. Korraldame tänavu turvatestid kaheksale elutähtsa teenuse osutajale, kes on selleks soovi avaldanud, et aidata parandada neil oma infosüsteemide turvalisust ja riskide hindamist. Veebruaris lõppes hange, millega valiti välja turvateste korraldavad ettevõtted. RIA korraldab riigi jaoks elutähtsate ja oluliste teenuste osutajatele turvatestimisi 2012. aastast.

Veebruaris valmis ja märtsi alguses avalikustati RIA koduleheküljel järjekordne krüptograafiauuring, mis on järg kuuele varasemale uuringule, mis viidi läbi aastatel 2011–2018. Tänavuse uuringu eesmärk on anda ülevaade krüptograafiliste vahendite kasutamise hetkeseisust ja heast tavast. Uuringust võib lugeda erinevatest levinud krüptograafilistest protokollidest ja nende kasutamise nüanssidest.

Eelmise aasta augustist alates alustasime järelevalvemenetlusi kõigi Eesti kriitilise tähtsusega andmekogude infoturbemeetmete rakendamise üle. Veebruaris lõpetasime neist menetlused viie – äriregistri, Riigi Teataja, E-toimiku, kinnistusraamatu ja riigikassa infosüsteemi – suhtes ettekirjutusi tegemata. Eestis on defineeritud kokku kümme kriitilise tähtsusega andmekogu. Korraldame nende suhtes järelevalvemenetlusi ennetavalt: selle asemel, et oodata järelevalvega puuduste ilmnemiseni, alustasime menetlusi eesmärgiga võimalikud puudused tuvastada enne, kui mõni intsident neid päriselt mõjutab.

Rahvusvaheline keskkond

Veebruaris jätkus üle maailma SolarWindsi tarneahelarünnaku tagajärgede tuvastamine ja paikamine. UK küberamet NCSC avaldas printsiibid, mida kriitiliste ahelate turvaliseks toimimiseks jälgima peaks. Rünnakust mõjutatud suurettevõtted Microsoft ja Fireeye kutsusid üles USA seadusandjaid panema paika kohustuslikke reegleid, kuidas ettevõtted peaksid oma küberintsidentidest teada andma.

Ameerika ühendriikides Florida osariigis 13 000 elanikuga Oldsmari linnas said kurjategijad ligipääsu veetöötlusjaama SCADA süsteemile, millega kontrolliti veepuhastuseks vajalike kemikaalide taset. Tõenäoliselt korduvkasutatava parooli tõttu sai ründaja ligipääsu Teamvieweri tarkvarale ning püüdis tõsta lubja sisaldust 100 korda. Kuna intsident juhtus tööajal ja teise töötaja nähes, oli kiiresti võimalik lubjatase ära muuta. Veetöötlusjaama hinnangul poleks kahjulik joogivesi jõudnud tarbijateni ka muude kaitsemeetmete tõttu.

Prantsuse küberasutus ANSSI avaldas veebruari keskel raporti kompromiteerimislaine kohta, kus kasutati sarnaseid tööriistu-taktikaid-protseduure, mida on seostatud varem Venemaa luureasutuse GRU üksusega, mida nimetatakse Sandwormiks. Kompromiteerimise sihtmärgiks olid IT-teenusepakkujad, eriti veebimajutuse pakkujad, kes kasutasid Prantsuse ettevõtte poolt pakutava IT-monitoorimistarkvara Centreon. Rünne algas 2017 ning ründes kasutati ära haavatavust teenusepakkujate poolt kasutatud Centreoni tarkvara vabavaralises vananenud versioonis, mida ei ole toetatud juba 5 aastat.

Veebruaris teatasid USA, Austraalia, Uus-Meremaa, Singapuri ja Ühendkuningriikide küberasutused koos, et paar kuud varem teatavaks tulnud Accelioni pilveteenuse failijagamisprotokolli turvanõrkust kasutatakse ära suurte ettevõtete kompromiteerimisel. Accelioni rünnaku ohvritena on mainitud Washingtoni osariiki, Uus-Meremaa suurpanka, Austraalia finantsjärelevalveasutust ja küberturbefirmat Qualys.

Lunavaratrendid on maailmas jätkuvalt murettekitavad. Veebruarikuu ühe nädala jooksul halvas Ryuki lunavaraga pihta saamine mitmed Prantsusmaa regionaalhaiglad, mis olid ajutiselt võimelised vaid piiratud mahus tööd jätkama. Lunavararünnaku ohvriks langes ka Kanada lennukitootja Bombardier, kes oli tõenäoliselt üks mitmekümnest ettevõttest, kelle võrkudesse tungiti Accellioni turvanõrkuse tagajärjel.

Jätkuvalt on kõrgelt hinnas COVID-19 uurimisega seotud teave – Oxfordi ülikooli vastavat laborit tabas küberrünnak ning Põhja-Korea päritoluga ründajad üritasid sisse murda Pfizeri arvutisüsteemidesse koroonavaktsiini info varastamiseks.