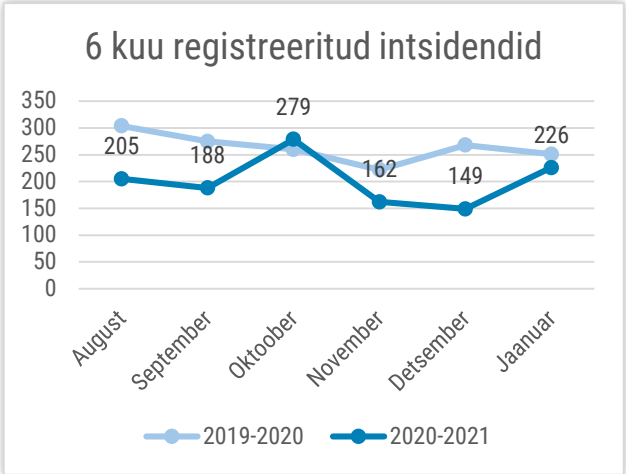
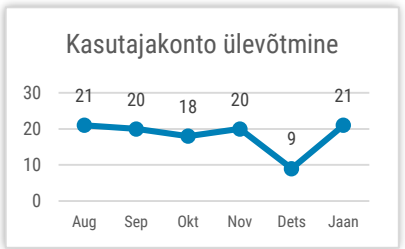
# Olukord küberruumis – jaanuar 2021

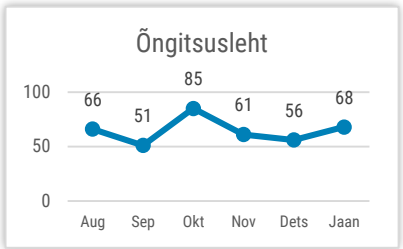
- Jaanuaris registreerisime 226 mõjuga intsidenti, mis on viimase kuue kuu keskmisest kõrgem
- Eesti finantsasutuste ja tehnoloogiaettevõtete suunas toimusid taas teenustõkestusründed, millega kaasnesid väljapressimiskirjad.
- CERT-EE sai uuesti kõrgeima taseme sertifikaadi.
- Uuendasime ID-kaardi brauserilaiendust, kus teadlased avastasid kriitilise vea.
- Europoli ja mitme riigi korrakaitsjate koostöö tulemusel võeti maha kurikuulus Emoteti pahavaravõrgustik.




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




*Jaanuaris saime taas rohkem teateid kontode ülevõtmisest.*




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

# Olukord Eesti küberruumis

**Jaanuaris täheldasime taas teenustõkestusrünnakuid Eestis tegutsevate pankade ja tehnoloogiafirmade suunas,** millega kaasnesid väljapressimiskirjad. Tegemist on kordusrünnetega. Samu ettevõtteid tabasid sarnased rünnakud ka sügisel ja ähvarduskirjades viidatakse nendele sügisestele rünnakutele ja öeldakse, et „me ei ole teilt makset kätte saanud“ ja „oleme nüüd tagasi, makske ära“ ning „kui te nüüdki ei maksa, tuleme varsti taas“. Sarnased ründed toimuvad ka teistes Euroopa riikides (CERT-EU andmetel vähemalt viies liikmesriigis) ning kaugemalgi. Sarnaselt Eestiga pööratakse tähelepanu samadele ettevõtetele, keda rünnati juba sügisel.

**Teenustõkestusrünnakust teatas 28. jaanuaril ka üks Eesti omavalitsus,** kus hommikul ja pärastlõunal oli koolide ja lasteaedade internetiühendus lühiajaliselt häiritud. Rünnak oli suunatud küll vaid ühe kooli vastu, kuid kuna kõik haridusasutused on ühtse tulemüüri taga, mõjutas rünnak ka teisi koole ja lasteaedu. Meile teadaolevalt ei ole rünnak seotud eelpoolmainitud väljapressimistega.

**18. ja 22. jaanuaril olid tarkvararikke ja administreerimisvea tõttu mitme tunni jooksul kättesaamatud sajad kuni tuhanded veebilehed.** 18. jaanuaril tabas rike veebimajutust pakkuva Zone Media võrguseadet, mille tagajärjel katkes paljude veebilehtede töö. 22. jaanuaril olid paari tunni jooksul tuhanded domeenid kättesaamatud teenusepakkuja tehtud administreerimisvea tõttu nimeserverite lahenduses. Intsidendid ei ole seotud.

**Jaanuari alguses katkesid korduvalt kas ühe või mitme teenusepakkuja juures autentimis- või allkirjastamisteenused.** 5. jaanuaril ajavahemikel 10:14-12:02 ja 17:13-17:33 esines tõrkeid kõigis SK ID Solutionsi pakutavates teenustes, sealhulgas ID-kaardi, Mobiil-ID ja Smart-ID väljastamine ning kasutamine ja kehtivuskinnitusteenused. Lisaks oli samal päeval lühiajaliselt häiritud Eesti ja Leedu Mobiil-ID kasutamine.

# Tegevused küberturvalisuse parandamisel Eestis

**1. jaanuaril 15. sünnipäeva tähistanud CERT-EE uuendas jaanuarikuus edukalt SIM3 standardile vastava kõrgeima taseme sertifikaati.** Esimest korda jõuti sertifikaadini 2017. aastal, kuid kuna see kehtib kolm aastat, siis 2020. aasta sügiseks oli vajalik selle uuendamine. SIM3 kordusaudit algas 2019. aasta lõpus, kuid protsess venis väliskeskkonna tegurite tõttu oodatust pikemaks. Kordusauditi raport sai heakskiidu 27. jaanuaril, mille tulemusena on CERT-EE jätkuvalt sertifitseeritud kõige kõrgemal tasemel.

Kvaliteeditunnistuse andis üle tuntud CERTide kogukond Trusted Introducer (TI). Sertifikaadi saamine eeldab kõrgete rahvusvaheliste nõuete täitmist. Hinnatakse dokumenteeritust, valmidust koostööks, töökorraldust, juhtumite käsitlemise efektiivsust ja professionaalsust, infovahetust jms, mis tagavad parema intsidentide lahendamise võimekuse ja küberturvalisuse tagamise.

**Jaanuari keskel sõlmisime majandus- ja kommunikatsiooniministeeriumi ja riigi valimisteenistusega (RVT) koostöölepingu,** et taaskord määrata kindlaks asutustevahelised ülesanded elektroonilise hääletamise korraldamiseks ja valimiste küberturvalisuse tagamiseks. Lepingu järgi toetame RVT-d eelkõige tehnilistes küsimustes, kõige tähtsam ülesanne on korraldada VIS3 ja sellega seotud veebide tehnilist arendamist, samuti valimisteks vajalike süsteemide majutus- ja haldamisteenust. RIA ülesandeks saab ka valimiste küberturvalisuse alaste teavitustegevuste korraldamine ning e-hääletamise edasiarenduste teostatavuse analüüsi tellimine.

**Jaanuari lõpus korraldasime koos Pangaliidu ja Eesti Pangaga lauaõppuse Eesti finantsasutustele,** kus mängiti läbi pankade vastu suunatud laiaulatusliku küberrünnaku lahendamine. Osalejad harjutasid koostööd rünnaku tõrjumisel ja selle tagajärgedega toimetulekul, samuti testiti erinevate reeglite ja protseduuride ajakohasust. Õppuse käigus tuvastati mitmeid kohti, kuidas oleks võimalik omavahelist koostööd ja kriisiolukorra juhtimist parandada.

**Uuendasime jaanuari lõpus ID-kaardi brauserilaiendust,** et parandada kriitiline viga, mille aitasid avastada Tartu Ülikooli teadlased. Detsembris teatas üks meie partnerasutus nõrkusest veebilehitseja pluginas ehk programmis, mida kasutatakse ID-kaardiga e-teenusesse digiallkirja andmiseks Chrome'i, FireFoxi, Safari, Internet Exploreri Edge'I ja Edge Chromiumi veebilehitsejas. Kurjategija saanuks pistikprogrammi nõrkust ära kasutada, kui ta kas võtab üle või omab veebilehte, kus saab ID-kaardiga autentida. Kui kasutaja logib ründaja kontrolli all olevasse portaali ID-kaardiga, siis ründaja saanuks kasutada autentimistoimingu infot, et kasutaja nimel sisse logida mõnda teise e-teenusesse ilma, et ta seda teaks.

# Rahvusvaheline keskkond

**Jaanuari lõpus teatasid mitme riigi õiguskaitse- ja julgeolekuasutused, et on edukalt ühisoperatsiooni tulemusel üle võtnud Emoteti pahavara levitanud taristu.** Emoteti laialdasest levikust oleme kirjutanud korduvalt oma ülevaadetes ning hoiatanud selle pahavara võimalike kahjude eest tulevikus. Operatsiooniga seoses jõudis Madalmaade politsei kätte nimekiri meiliaadressidest, mis on Emotetiga nakatunud (asutuse kodulehel saab kontrollida, kas e-mail on nakatunud). Nii töötati välja ka tööriist, mille abil on võimalik pahavara vahenditest eemaldada. Oleme meile teadaolevatest nakatumistest Eesti vastavatele teenusepakkujatele ja asutustele ka teada andnud.

**USA võimud ja küberkogukond laiemalt uurivad detsembris ilmsiks tulnud SolarWinds Orion intsidendi** tagamaid ning mõjusid. On tuvastatud mitmeid üksikasju, sealhulgas asjaolud, et kolmandik rünnaku ohvritest ei kasutanud SolarWindsi tarkvara ning et ründaja on kasutanud kompromiteeritud võrgustikus edasi liikumiseks mitut erinevat pahavara, millest SUPERNOVA nimeline võeti kasutusele alles paar nädalat pärast intsidendi avastamist. Küberturbe ettevõtte FireEye töötas välja tasuta tööriista, mille abil on võimalik sissemurdmisi tuvastada.

**Sarnaselt eelnevatele kuudele, sattusid lunavararünnakute ohvriks ettevõtted ning asutused paljudest eri valdkondadest.** Lunavararünnakust teatasid nii Ühendkuningriikide üks suuremaid riiklike teadusinstituute (UKRI) kui ka Šotimaa keskkonnakaitseagentuur (SEPA), kellest viimase puhul avalikustas kurjategija tuhandeid dokumente, kuna agentuur ei nõustunud lunaraha maksma. Lunavararünnaku poolt sai pihta ka järjekordne tehnoloogiakontsern Whirlpooli näol.

Jätkuvalt on küberkurjategijate sihtmärgiks ka tervisesektor, kus rünnak tabas Belgia CHwapi haiglat, mille 40 serverit krüpteeriti. USA ametiasutustel õnnestus kõrvaldada NetWalkeri lunavaraga seotud veebilehed.

**Nagu Eesti küberruumi puhul, on DDoS rünnete võimsamaks ja tihendamaks muutumine globaalne trend,** kus möödunud aasta jooksul tuvastati üle 10 miljoni hajusa ründe, ületades Netscouti andmete põhjal 2019. aasta juhtumeid 1,6 miljoniga.

**Jaanuaris teatati ka paljudest ulatusliku mõjuga andmeleketest:** lekitati 77 miljoni Nitro PDF kasutaja andmed, US Cellular klientide isikuandmed ning Uus-Meremaa keskpanga konfidentsiaalne teave. Kurjategijad on lekitanud ning moondanud möödunud kuude jooksul vaksiini välja töötamisega seotud varastatud andmeid, et tekitada inimestes umbusaldust Covid-19 vaktsiini vastu.