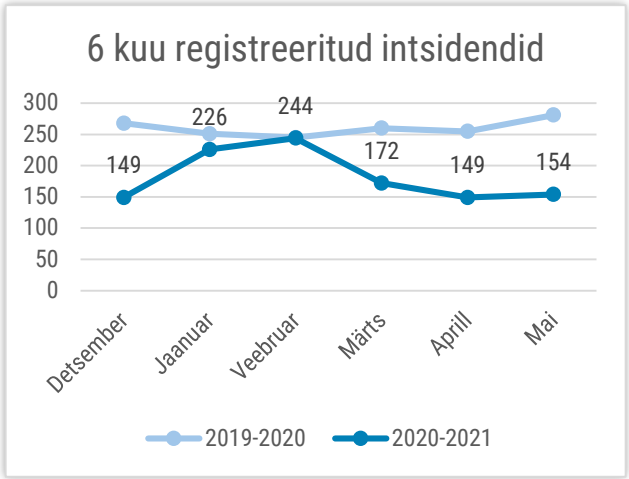
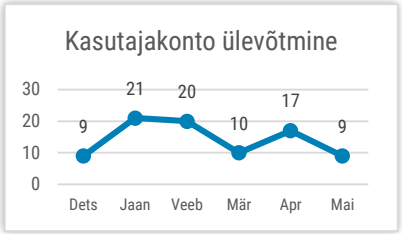
Olukord küberruumis – mai 2021

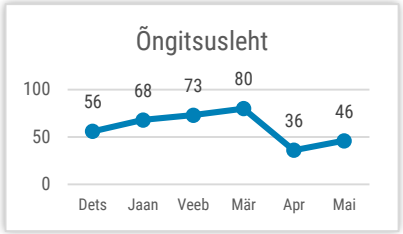
- Mais registreerisime 154 mõjuga intsidenti, mis on viimase aasta keskmisest madalam näitaja.
- ID-kaardi, Smart-ID ja Mobiil-ID teenusekatkestus mõjutas nii ID-väljastamist, kui ka teenuste kasutamist.
- Taas nägime IT-teenusepakkuja kompromiteerimist, mille tõttu jõuti ka klientide süsteemideni.
- Korraldasime Eesti telkodele õppuse Kübertorm, mis mängis kokku kaitseväe Kevadtormiga.
- Lunavara mõjutas USA kütuseturgu ning Iirimaa tervishoiusektorit.



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



Meilikontode ja sotsiaalmeedia-kontode ülevõtmine on jätkuvalt päevakajaline.



Mais tõusis taas õngitsuslehtede intsidentide hulk.

Olukord Eesti küberruumis

Eelmisel korral kirjutasime kuuülevaates juhtumist, kus IT-teenust pakkuva ettevõtte ründamise kaudu laienes lunavaraintsident teistesse asutustesse. Mais nägime sarnast tarneahelaintsidenti. Üks raamatupidamistarkvara ettevõte langes lunavararünnaku ohvriks ning ründajad said tema kaudu ligi ühele Läänemaa vallavalitsuse süsteemidele. Intsident demonstreerib globaalse lunavaraprobleemi taustal taas vajadust leppida IT-teenusepakkujatega kokku, kuidas viimased oma küberintsidentidest teavitama ja milliseid meetmeid enda kaitseks kasutama peaks.

21. mail katkes enam kui päevaks ID-kaardi, Smart-ID ja Mobiil-ID väljastamine. SK ID Solutionsi IT-taristu plaaniliste uuendustööde käigus peatus 21. mail öösel kõigepealt sertifitseerimisteenuse töö. Katkestuse tõttu ei saanud seetõttu PPA teenindused väljastada uusi ID-kaarte, elamisloakaarte ega digi-ID-d; mobiilioperaatorid ei saanud väljastada Mobiil-ID-d, samuti polnud võimalik registreerida Smart-ID kontosid. Lisaks eelnevale oli 21. mai hommikul kahe tunni jooksul häiritud Mobiil-ID kasutamine. ID-kaardi, elamisloakaardi ja digi-ID väljastus PPA teenindustes taastus samal päeval, kuid Mobiil-ID väljastamine ning Smart-ID registreerimine saadi täielikult töökorda alles 22. mai keskpäevaks.

4. mail teatas Tallinnas tegutsev hulgimüügiettevõtte lunavaraintsidendist, mille käigus krüpteeriti serveris olevad andmed, sealhulgas raamatupidamisdokumendid ja ka varukoopiad välisel kõvakettal.

Ühe Tallinna kooli vastu korraldati 24. mail lühiajaline ummistusrünne (DDoS). Muu hulgas kasutati rünnakus ka Eestis asuvaid seadmeid, näiteks turvanõrkustega ruutereid või avatud teenustega servereid. CERT-EE teavitas võrkude omanikke, kes suhtlesid seadmete omanikega või sulgesid vastava teenuse, mis võimaldas ründajatel rünnakut võimendada.

31. mail ei olnud andmebaasivea tõttu keset tööpäeva enam kui kahe ja poole tunni jooksul kättesaadav patsiendiportaal digilugu.ee. Patsiendiportaali tagava tervise infosüsteemi kesksüsteemi töö taastus täielikult alles keskööks.

Tegevused küberturvalisuse parandamisel Eestis

Oleme juba aastaid teavitanud Eesti telekommunikatsioonisettevõtteid, veebiteenuste majutajaid ja oma võrke haldavaid asutusi nendest nakatumistest ja haavatavustest, millest oma partneritelt teada saame. Kui info jõuab lõpptarbijani – seadme või süsteemi omanikuni – saab ta niimoodi paremini oma süsteeme kaitsta. Turvanõrkused seadmetes ja süsteemides ei pruugi mõjuda halvasti ainult seadme omanikele, vaid neid nõrkuseid saab ära kasutada ka teiste ründamiseks näiteks DDoS-iga.

Maikuus saime informatsiooni kahe sellise rünnaku kohta, milles osalesid teadmatult ka Eestis asuvad seadmed. Üks rünnakutest toimus Tallinna kooli vastu, teine ühe Euroopa Liidu liikmesriigi süsteemi vastu. Mõlemal puhul saime nimekirja IP-aadressidest ja teavitasime aadresside omanikke, et nemad omakorda teavitaksid seadmete omanikke või rakendaks ise vastavaid abinõusid. Teavituse tulemusena pole kurjategijatel võimalik enamikku neist seadmetest enam ära kasutada.

Korraldasime koos partneritega Eesti telekommunikatsiooni ettevõtetele õppuse Kübertorm, mis mängis kokku Kaitseväe suurõppusega Kevadtorm. Õppusel pidid Elisa, Tele2 ja Telia esindajad toime tulema sideteenuste häirimise ning küberrünnakute tõrjumisega. RIA ja teistest riigiasutustest pärit kübereksperdid olid abiks, et ründajad süsteemidest välja heita ning telkod harjutasid päriselt läbi, kuidas kriisiolukorras sideteenuse toimimine tagada.

Jätkame Eesti infoturbestandardi ehk E-ITSi rakendamise tutvustamise ja juurutamise tegevustega. Märtsis avalikkuse ette jõudnud E-ITS peaks pika üleminekuperioodi järel aastaks 2024 välja vahetama senise avaliku sektori infoturbestandardi ISKE. Maikuus jätkasime pilootprogrammi tegevustega kümnes asutuses ning õigusruumi korrastamisega E-ITSi kasutuselevõtmiseks.

Rahvusvaheline keskkond

Mais nägime taaskord lunavaraintsidentide mõju mastaapsust. DarkSide nimelise lunavarateenuse abil tehtud rünnaku tõttu suleti ajutiselt USA suurim naftatorustik Colonial Pipeline, mis ahelreaktsioonina põhjustas kütuse puudujäägi mitmes osariigis. DarkSide lunavara abil rünnati kuu jooksul ka mitmeid teisi suurettevõtteid, sealhulgas keemiahiidu Brenntag. CISA ning FBI kirjutasid juhendi vajalike tegevustega, mis aitavad kõnealust lunavara vältida.

Iirimaa tervisesektorit tabas Conti-nimelise lunavara rünnak, mille ohvriks on viimase aasta jooksul olnud muuhulgas 16 USA tervishoiuasutust. Iirimaa puhul oli intsident nii laiaulatuslik, et suurem osa riikliku tervisesüsteemi IT-süsteemidest tuli mitmeks päevaks seisatada. Vaid mõned päevad hiljem võeti sihtmärgiks Uus-Meremaa haiglasüsteem, kus süsteemide seiskumise tõttu tuli mitmeid operatsioone edasi lükata.

Lunavaraintsidentidest on vajalik ära mainida veel helitehnika tootja Bose juhtumi, mille tulemusel toimus andmeleke ning Prantsuse kindlustusettevõtet AXA tabanud lunavararünnaku vaid paar päeva pärast seda, kui ettevõte teatas, et lõpetab küberkindlustuse pakkumise – põhjuseks liiga suur lunavararünnakute tagajärjel tehtud kahjunõuete arv. Mais avalikustati, et USA kindlustuspakkuja CNA Financial Corporation maksis märtsis lausa 40 miljonit dollarit lunaraha.

Belgias teavitati maikuus kahest olulisest küberrünnakust riikliku taristu vastu, millest riigi siseministeeriumi vastu suunatud tegevus toimus juba kahe aasta jooksul ja avastati tänavu märtsis. Teine, maikuus aset leidnud teenustõkestusrünnak viis rivist välja märkimisväärse osa Belgia valitsuse internetivõrgust, mille tagajärjel toimus katkestusi lisaks föderaalvalitsusasutuste süsteemidele ka ülikoolide ja teadusasutuste töös ning paari tunni vältel polnud kättesaadav ka COVID-19 vaktsineerimisele registreerimise portaal.

Briti küberkeskus NCSC avaldas Venemaa Välisluureteenistuse (SVR) küberrünnakute metoodika ülevaate. SVR-i seostatakse mitmete ulatuslike rünnakutega COVID-19 vaktsiiniarendajate suunal ning neid nähakse ühe peamise SolarWindsi tarneahelarünnaku eestvedajana.

Interpol pidas ulatusliku politseioperatsiooni käigus kinni üle 500 küberkuritegevusega seotud inimest ning ühtlasi tühistas 83 miljoni dollari väärtuses väljamakseid kurjategijate kontodele.

Pärast viimastel kuudel toimunud Emoteti pahavaraga seotud teabevahetuse katsetust teavitas USA föderaalne juurdlusbüroo, et hakkab kompromiteeritud paroolide kohta korrapäraselt Have I Been Pwned veebisaidiga teavet jagama.