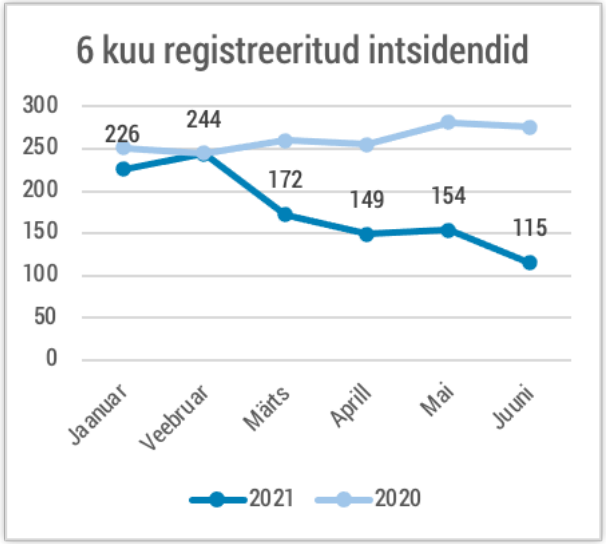
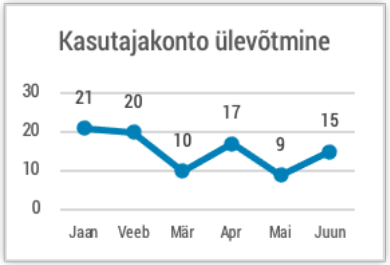
Olukord küberruumis – juuni 2021

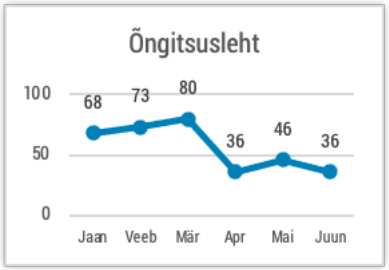
- Juunis registreerisime 115 intsidenti, mis on viimase 12 kuu keskmisest madalam näitaja.
- Õppeaasta lõpp ja eksamiteperiood tõi tavapärasest rohkem rünnakuid haridusasutuste vastu.
- Infoturbemeetmed aitasid ära hoida arvepettust, mille kahju ulatunuks mitme miljoni euroni.
- Korraldasime RIA küberturvalisuse teenistuse infopäeva.
- Eesti kerkis ITU küberturbe indeksis kolmandale kohale.
- Jätkuvad suure mõjuga lunavararünnakud.



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



Keskmisel iga paari päeva tagant saame teate e-posti vvõi sotsiaalmeedia-konto ülevõtmisest.



Õngitsuslehtede hulk on vähenenud: juunis registreerisime neid poole vähem kui veebruaris ja märtsis.

Olukord Eesti küberruumis

Juunis teavitati meid arvepettuse katsest, mille õnnestumise korral oleks kahju ulatunud mitme miljoni euroni. Kurjategijad hakkasid jälgima ühe Eesti suurettevõtte meilivahetust Poolas asuva koostööpartneriga, sobival hetkel võtsid nad meilivestluse üle ning palusid muuta arvel olevat kontonumbrit. Õnneks kasutas Eesti ettevõte tõhusat meilifiltrisüsteemi, mille abil jõuti pettusekatsele kiiresti jälile ning ühtegi ülekannet libaarvete alusel ei tehtud. Kuna ettevõtte enda meilisüsteemis sisse murdmise jälgi ei tuvastatud, on alust arvata, et kurjategijatel õnnestus kompromiteerida Poola koostööpartneri meiliserver. Oleme kirjutanud arvepettustest ka mitmeid kordi varem ning Eesti ettevõtted on nende läbi ka reaalselt kahju kannatanud; seekordne juhtum on aga hea näide, kuidas küberturbemeetmete rakendamine ennast ära tasub.

Tavapärasest rohkem oli intsidente haridusasutustega – ilmselt on siin seos õppeaasta lõpu ja eksamite perioodiga. 7. juunil nakatusid ühes Lääne-Eestis asuvas gümnaasiumis mõned arvutiklassi arvutid lunavaraga ning 9. juunil tehti neljakümneminutiline teenusetõkestusrünnak ühele Harjumaa gümnaasiumile. Kummalgi intsidendil suurt mõju ei olnud ning võib oletada, et nende taga oli mõni sama kooli õpilane.

Kuu lõpus üritati Eesti Maaülikooli matkiva kirjaga levitada pahavara – eestikeelne kiri oli näiliselt saadetud Maaülikooli nimelt ning kutsus osalema hankes, mille tingimused olevat juurde lisatud failis. Tegelikult sisaldas lisatud manus trooja pahavara. Kirja saajate hulgas oli nii riigiasutusi, eraettevõtteid kui ka eraisikuid. Üldjuhul läksid need rämpsposti kausta ning meile teadaolevalt nakatumisi ei olnud.

Kolmel korral oli tülikaid tõrkeid pangateenuste kasutamisel: 11. juunil jäid üheks tööpäevaks toppama ühe kommertspanga rahaülekanded Balti riikides, päev hiljem esines kolme tunni jooksul probleeme teise panga maksetega ning 16. juuni pärastlõunal oli pooleteist tunni jooksul häireid sama panga maksekaartide kasutamisel. Ühelgi juhul ei olnud probleemide põhjustajaks küberrünnak, vaid tegemist oli süsteemi tõrgetega.

Tegevused küberturvalisuse parandamisel Eestis

Juuni alguses korraldasime oma partneritele RIA küberturvalisuse teenistuse infopäeva. Cyber Security in Estonia 2021 nime kandval üritusel kõnelesime andmetest, elektroonilise identiteedi suundadest, e-valimistest, kriitilise taristu kaitsest ja rahvusvaheliste projektide arengust. Meie tegemistest huvitusid küberasutused ja -eksperdid nii Euroopast kui ka USAst. Infopäeva ettekandeid saad vaadata ja kuulata RIA YouTube'i kanalil.

Korraldasime koos Clarified Securityga üle pika aja nn küberhommikusöögi, kus riigi ja erasektori kübervaldkonna eksperdid said vabas vormis päevakajalisi küberteemasid arutada. Jutuks tulid muutused Euroopa Liidu õigusloomes, Eesti uus infoturbestandard E-ITS ja olukord küberruumis. Taoline kohtumise formaat sai alguse projektist Interreg Cyber.

Avaldasime DigiTesti uue õppemooduli, mis keskendub kaugtööga kaasnevatele riskidele. DigiTest on interaktiivne e-õppe keskkond, mille eesmärk on tõsta ja hoida avaliku sektori töötajate küberturbe-teadlikkust. Praeguseks on DigiTesti läbinud üle 16 tuhande inimese. See asub aadressil digitest.ria.ee ja on kättesaadav riigivõrgus.

Tuletasime elutähtsa ja olulise teenuse osutajatele meelde, et oma partneritega sõlmitud lepingutes tasub ära märkida, et partner peab oma infoturbeintsidentidest neile teada andma. See võimaldab kiiremini reageerida ning vajadusel lekkinud kasutajakontod või ohtu sattunud juurdepääsud sulgeda.

Rahvusvaheline keskkond

Ajal, mil maailma poliitiliste liidrite tippkohtumistel on turvaline küberruum üha kesksemaks teemaks, näeme jätkuvat **laialdase mõjuga lunavararünnakuid.**

Juuni märkimisväärsematest lunavaraintsidentidest väärivad mainimist maailma ühe suurima lihatootja JBS juhtum, kus ettevõtte maksis REvil rühmitusele süsteemide dekrüpteerimise eest 11 miljonit dollarit. Tehnoloogiaettevõtted ADATA ja Fujifilm said pihta lunavaraga, kuid keeldusid lunavara maksmast. Jätkuvalt on sihikul meditsiinisektor, seekord kahe UF Health Florida haigla ja Brasiilia suurima meditsiinidiagnostika ettevõtte Grupo Fleuryi näol. Taas toimus laiaulatuslik intsident Belgias, kus Liege'i linna IT-süsteemide töö katkes lunavararünnaku tõttu. Ukrainas arreteeriti peamiselt suuri ettevõtteid sihtinud Clopi lunavararühmituse liikmed. Juuli esimestel päevadel algas tarkvarafirmat Kaseya tabanud laiaulatuslik lunavararünnak, mida kajastame põhjalikumalt järgmises kuuülevaates.

Jätkub detsembris avalikustatud SolarWindsi intsidendi uurimine. On selgunud, et ohvriks langes teiste seas ka Taani keskpank, mille süsteemides liiguti ringi tõenäoliselt mitmeid kuid. Analüüsi käigus on ilmnenud, et SolarWindsi rünnakuga seotud rühmitus kasutas klientide ründamiseks Microsofti kasutajatoe süsteeme.

Vene telekanalit tabas Vladimir Putini esinemise ajal teenusetõkestusrünnak. Venemaad süüdistatakse hiljutistes küberrünnakutes Poola poliitikute vastu, kus kompromiteeritud isiklikelt meilikontodelt lekitati tundlikku teavet.

Lõuna-Korea ettevõtete vastu toime pandud pahavararünnaku taga oli Põhja-Korea riiklike sidemetega Andarieli-nimeline rühmitus, mille peamine eesmärk on teenida finantstulu. Sellele lisaks kasutas Põhja-Korea ära VPNi turvanõrkust, et murda sisse Lõuna-Korea aatomienergiauuringute instituuti.

Hispaania töö- ja sotsiaalmajanduse ministeeriumit tabas küberrünnak, mis on viimase paari kuu jooksul juba teine suure mõjuga intsident nende haldusalas. Interpol sulges taaskord tuhandeid veebilehti, mis tegutsesid illegaalselt ravimite müügiga.

Eesti kerkis Rahvusvahelise Telekommunikatsiooni Liidu (ITU) uues küberturbe indeksis kolmandale kohale.