

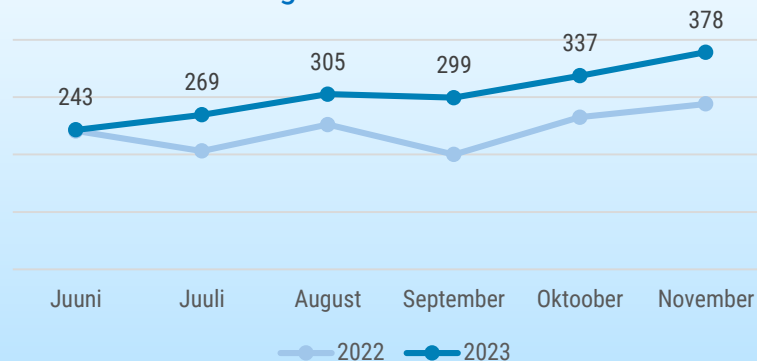


OLUKORD KÜBERRUUMIS

NOVEMBER 2023

- Novembris registreerisime **378 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja.
- Novembris katkes mitmel korral **Tervisekassa teenuste töö**. Lisaks oli sideteenuste katkemise tõttu häireid **Viljandi haigla töös**. Katlamajad sattusid **küberrünnaku ohvriks**.
- Novembris viisime läbi **küberõppuse**, kus osalesid riiklik küberreserv, Tele2 ja Elektrilevi.
- Lennukitootja **Boeing sattus küberrünnaku** alla. Jätkusid **sõjategevusega** seotud küberründed. Küberrünnak häiris ka **Ühendkuningriigi õigusasutuste tööd**.

6 kuu registreeritud intsidendid



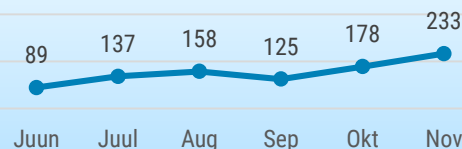
CERT-EE-le teavitatud intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.

Automaatseire: pahavara



Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.

Õngitsuslehed



Õngitsuslehed moodustavad jätkuvalt kõige suurema osa CERT-EE registreeritud intsidentidest.



Olukord Eesti küberruumis

Novembris katkes mitmel korral

Tervisekassa teenuste töö. 1.

novembril ajavahemikul 13.00 kuni 13.46 oli Digiretsepti töös häireid, mille põhjustasid tehnilised tõrked koostööpartneri süsteemides. Kaks päeva hiljem ehk 3. novembril katkes nii Digiretsepti kui ka teiste Tervisekassa põhiteenuste töö. Sel korral kestis katkestus kaks ja pool tundi ning teenuste töö taastus pärast süsteemide taaskäivitust. Ka 13. novembril ajavahemikel 9.34 kuni 10.08 ja 14.27 kuni 17.06 ei toimunud Digiretsept, kindlustatuse kontroll ega muud tervisekassa üle X-tee pakutavad teenused. Katkestuste põhjuseks oli serveri ülekoormus. Tervisekassa teenustes oli taas tõrkeid 20 novembril 13.30 kuni 15.35 – need küll toimisid, kuid tavapärasest aeglasemalt. 22. novembril ajavahemikul 5.45 kuni 8.20 ei toimunud taaskord mitmed Tervisekassa teenused.

Katkestuse põhjustas rike rakendus-tarkvaras, mille taaskäivitamise järel teenuste töö taastus.

Viljandi haigla töö oli häiritud sidekaabli füüsilise kahjustuse tõttu.

19. novembril tekkisid Viljandi Haigla peahoones ajutised sidekatkestused – mõjutatud oli nii andmeside- ja telefoniühendus. Intsidendi ajal olid tavapärased tööprotsessid häiritud, kuid patsientide ravikvaliteet ei olnud mõjutatud. Algselt arvati, et tegemist on võrguseadme rikkega, kuid hiljem selgus et viga on painutatud sidekaablis. 22. novembri õhtuks sai vigastatud kaabel terve vastu vahetatud ja tavapärane sideühendus taastatud.

30. novembril teavitas kaugkütte teenust osutav ettevõte, et langes küberrünnaku ohvriks, mille tõttu oli vähemalt kaheksa katlamaja juhtseadme töö katkenud. Mõjutatud katlamajad viidi üle käsijuhtimisele ja

ohtu sooja tootmisele ega edastamisele ei tekkinud. Tõenäoliselt ei õnnestu rikutud seadmete tööd taastada ja need tuleb välja vahetada. Rünnati kontrollereid, mis on toodetud Iisraelis. Sarnase ründe ohvriks langes meile teadaolevalt veel kaks Eesti ettevõtet, üks neist oli valla veevarustusega tegelev äriühing.

Jätakuvalt levivad erinevate postiteenusepakujate nimel saadetud õngitsuskirjad ja -sõnumid.

Sel kuul nägime taas Omniva nimel saadetud kirju, mis suunavad kasutajat õngitsuslehele enda pangakaardiandmeid sisestama. Kirjades kutsutakse üles kiirelt tegutsema ja väidetakse näiteks, et kui makset ei sooritata 24 tunni jooksul, siis tellimus tühistatakse. Omniva on varasemalt juhtinud tähelepanu, et nemad ei küsi kunagi kliendi pangakaardi andmeid ja soovivad üle kontrollida veebiaadress, kuhu kasutaja suunatakse.



Tegevused küberturvalisuse parandamisel Eestis

6.-9. novembrini toimus RIA eestvedamisel õppus, kus meie juhitud küberreservi kuuluvate IT- ja küberturvalisuse ekspertide ülesanne oli leida RIA töötajate poolt etendatud häkkerid Tele2 ja Elektrilevi IT-süsteemidest. Õppuse stsenaariumi järgi algas kriis Eestit laastanud tormist, mis põhjustas riigiüleseid elektri- ja sidekatkestusi. Kui tormikahjustused likvideeriti, kuid nii elektrivoolu kui sideteenuste töö ei taastunud, selgus et tuleb tõrjuda ka küberründeid. Appi tõttas riiklik küberreserv ehk maailmas ainulaadne IT- ja küberturvalisuse eksperte koondav meeskond, kuhu kuulub tänaseks juba ca 150 spetsialisti. RIA eesmärk on küberreservi kõiki liikmeid pidevalt koolitada ja treenida, et nad saaksid ise areneda ning neil oleks teadmisi ja oskusi, et riiki rünnaku korral aidata. Täpsemalt saab õppuse kohta lugeda [siit](#).

Uuendasime RIA kodulehel olevaid küberturbe soovitusi tippjuhtidele.

Soovitame muuhulgas palgata infoturbejuht ja tagada tema sõltumatus, lähtuda infoturbes standardist või parimast praktikast, planeerida vahendeid infoturbeks ja kasutada Kübertesti ettevõtte või asutuse küberhügieeni parendamiseks. Tutvuda tasub ka teiste asutustele ja ettevõtetele mõeldud nõuannetega, mis on koondatud meie [kodulehele](#) ja [IT-vaatliku veebi](#).

14. novembril toimus taas RIA CyberMeetUp üritus. Sel korral rääkis Eesti Interneti Sihtasutuse arendusjuht Timo Võhmar eelD-nimelisest teenusest, mille abil saavad ettevõtted vähendada bürokraatlikku koormust oma kasutajate identifitseerimisel. Lisaks tegid RIA analüüsi- ja ennetusosakonna analüütikud ülevaate viimasel ajal Eestit tabanud teenustõkestusrünnakute tagamaadest ja

tegijatest. Juba toimunud ürituste salvestusi on võimalik [järelle vaadata](#) RIA kodulehel.

Teavitasime sadakonda Wordpressi veebilehe omanikku nende halduses olevate kasutajakontode lekkimisest. Kuna kasutajatunnused ja paroolid olid internetis kättesaadavad, siis võib see kaasa tuua veebilehe kompromiteerimise ja sisu muutmise. Andsime nõu, kuidas edasi toimida ja taolist olukorda tulevikus vältida.

RIA analüüsi- ja ennetusosakonna analüütik Kaisa Vooremäe ja intsidentide käsitlemise osakonna infoturbe ekspert Joosep Sander Juhanson rääkisid Pärnu Postimehele antud intervjuus ettevõtetele suunatud küberrünnetest. Ettevõttele võib küberrünne kaasa tuua väga palju ebameeldivusi alates mainekahjust kuni töö seiskumise ja isegi pankrotini.



Rahvusvaheline keskkond

Jätkusid sõjategevusega seotud küberründed. Ukrainameelne küberrühmitus Ukrainian Cyber Alliance [andis teada](#), et neil õnnestus näotustada Vene kaardimaksete süsteemi Mir koduleht. Samuti väidavad häktivistid, et murdsid sisse Mir süsteemi ja varastasid sealt kasutajate andmeid, mida ettevõtte ise aga eitab. Mir kaardimaksete süsteem loodi 2014. aastal alternatiivina Visa ja Mastercardi omale ning selle osakaal Venemaal on tänaseks tõusnud pea pooleni kõikidest kaardimaksetest. Väljaspool Venemaad aktsepteerivad Mir makseid vaid üksikud riigid nagu Valgevene, Venezuela ja Kuuba.

Lennukitootja Boeing kinnitas novembri alguses, et küberründe tõttu on osaliselt häiritud nende globaalsed tarned ja teenused, ent lennukite turvalisust see ei mõjuta. Ehkki ettevõtte ei nimetanud ründajat ega andnud rohkem infot, on selle taga ilmselt Venemeelne lunavararühmitus,

mis mõni päev varem kinnitas Boeing'u ründamist. Rühmitus ähvardas, et kui ettevõtte lunavaranoõuet ei täida, avaldavad nad tundlikku infot, mis ründe käigus varastati.

Austraalia üht suurimat sadamate operaatorit DP World Australia [tabas novembri keskpaigas küberrünnak.](#) Ettevõtte teatel olid kompromiteeritud kriitilised süsteemid, mille kaudu koordineeritakse laevatransporti. Intsidendi ohjamiseks katkestas ettevõtte mõneks ajaks internetiühenduse ja tavapärase töö, mistõttu mitmes suures sadamas oli konteinerite logistika tugevalt häiritud ning tekkisid ummikud. Austraalia valitsus nimetas selle riikliku tähtsusega küberintsidendiks ja kaasas lahendamisse Austraalia küberjulgeolekukeskuse.

Taani kriitilise infrastruktuuri ettevõtete rahastatav SektorCERT [andis oma ülevaates teada, et](#)

aprillis ja mais toimus kolm suuremat ründelainet Taani energiaspektori vastu. Rünnetel ei õnnestunud kahju teha ja osa nendest võisid olla juhuslikud. Samas toob SektorCERT välja, et 11. mail toimus täpselt sihitud ja koordineeritud rünne 11 energiaettevõtte vastu, kasutades Zyxel tulemüüri haavatavust, mis oli jäänud ettevõtetele paikamata. Mai lõpus toimunud rünnete puhul viitab tehniline käekiri võimalikule seosele Venemeelse rühmitusega, mis on rünnanud ka Ukraina elektrivõrke.

Küberrünnak häiris ka Ühendkuningriigi õigusasutuste tööd. Notaritele, advokaadibüroodele ja teistele õigusasutustele IT-teenust pakkuv ettevõtte CTS sattus küberrünnaku alla, mistõttu oli häiritud hinnanguliselt 80 – 200 Ühendkuningriigi asutuse tavapärane töö. Näiteks ei saanud osad kliendid vormistada kinnisvara ostu- ja müügitehinguid.