



OLUKORD KÜBERRUUMIS

JAANUAR 2024

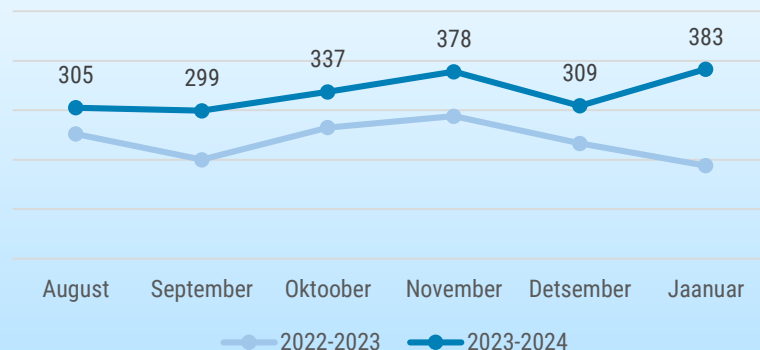
- Jaanuaris registreerisime **383 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja.
- Jaanuaris saadeti osad **peretoetuse ja vanemahüvitise** väljamaksed isikute vanadele pangakontodele. Tallinnas asuv ettevõtte langes **lunavararünnaku** ohvriks.
- Korraldasime IT-õpetajatele **küberturbekoolituse**, viisime läbi kriitilise infrastruktuuri küberkaitse **infopäeva** ja uuendasime **E-ITS portaali** ning Eesti infoturbe standardit.
- Jätkusid sõjategevusega seotud küberründed. Tietoevry Rootsis asuvat **andmekeskust tabas lunavararünnak**. Microsoft sattus küberründe ohvriks.

Automaatseire: pahavara



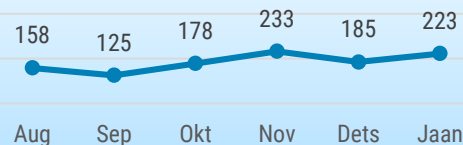
Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.

6 kuu registreeritud intsidendid



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

Õngitsuslehed



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



Olukord Eesti küberruumis

Jaauanaris registreerisime 17 mõjuga teenusetõkestusrõnnet. 2. jaauanaril toimus DDoS-rõnne Maksu- ja Tolliameti veebilehe emta.ee, 3. jaauanaril Rahvusraamatukogu ehk rara.ee vastu ning 7. jaauanaril Rahvusringhäälingu uudisteportaali err.ee vastu. Kõigi kolme lehe tõõs oli rõnnete tõttu lühiajalisi hääreid. 12. jaauanaril kuulutas ummistusrõnnetega tegelev rühmitus sihtmärkidena välja mitmeid Eesti veebilehti ja -teenuseid: tallinn.ee, evr.ee, pileet.ee, mnt.ee, nasdaqbaltic.com, app.energia.ee, nordica.ee, RMITi ja riigivõrgu nimeserverid. Nimeserverite ja Nordica lehe vastu tehtud ründed häärisid nende tõõd, teistel üritustel polnud mõju. Rõnnakute ajendina mainis rühmitus Eesti toetust Ukrainale. 22. jaauanaril tabasid teenuse-tõkestusrõnned RIA ja SMITi nimeservereid. Mõlema rõnnaku tõttu oli teenuste tõõs hääreid: mitmed SMITi ja RIA hallatavad lehed avanesid

tavapärasest aeglasemalt või sai kasutaja oodates veateate.

Sotsiaalkindlustusamet (SKA) saatis osad peretoetuse ja vanemahüvitise jaauanarikuised väljamaksed isikute vanadele pangakontodele. Viga mõjutas ligikaudu 1400 inimest, kes on vahetanud toetuse või hüvitise saamise kontot. Vea põhjustas osaliselt nii inimlik eksimus kui ka süsteemi tõõrge. SKA teavitas juhtunust mõjutatud isikuid, kelleni jõudis hüvitis tavapärasest hiljem, ja andmekaitse inspeksiooni.

18. jaauanaril langes Tallinnas tegutsev ettevõte lunavararõnnaku ohvriks. Rõnde käigus krõpteeriti ettevõte serveris olnud andmed, mille hulgas olid nii dokumendid kui ka majandustarkvara andmebaas. Esialgse info põhjal kasutati rõnnakuks nõõrgalt turvatud kaugtõõlaua rakendust (RDP). Osadest andmetest oli olemas varukoopia. Soovitame juhtumi

valguses lugeda RIA 2022. aastal koostatud [ohuhinnangut](#), kus kirjutame lunavararõnnakutest ja kaugtõõlaua protokollist.

Jaauanaris jätkusid Facebooki Marketplace'i pettused, mida kelmid on juba pikalt kasutanud raha teenimiseks. Skeem toimib enamasti jäõgmiselt: petis võtab ühendust inimesega, kes Facebookis midagi müüb ja väidab talle, et soovib kauba ära osta. Seejärel leitakse mingi põhjus, miks ostja ei saa ise kaubale jäõrgi tulla ja soovib kasutada kullerteenust. Müüjale väidetakse, et ta peab tehingu kinnitamiseks maksuma kohaletoometamise tasu või paki kindlustama ning suunatakse ta õõngitsuslehele oma pangakaardiandmeid sisestama. Enamasti kaotab pettuse ohver paarsada eurot, kuid eelmise aasta lõpus näõgime ka juhtumit, kus kahjusumma oli üle 10 000 euro.



Tegevused küberturvalisuse parandamisel Eestis

Korraldasime IT-õpetajatele küberturbe koolituse.

4. ja 5. jaanuaril toimus RIA teaduse ja arenduse koordineerimisosakonna (TAK) eestvedamisel kutsekoolide IT-erialade õpetajatele küberturbe koolitus Hands-on Hacking Essentials (HOHE). Koolituse viis läbi Clarified Security ning selle eesmärk oli tõsta kutsekoolide õpetajate teadmiste ja oskuste taset, et nad lõimiksid IT-erialasid õpetades küberturvalisuse küsimusi teadlikumalt muude teemadega. Koolitusel osalejate tagasiside oli väga positiivne ja saadi palju uusi teadmisi.

18. jaanuaril viisime läbi kriitilise infrastruktuuri küberkaitse infopäeva, mille sihtgrupiks on Eestis elutähtsat ja olulist teenust osutavate ja -korraldatavate asutuse esindajad. Teemade ring oli lai: rääkisime nii olukorrast küberruumis, õigusruumist kui ka küberkriiside korraldusest Eestist. Lisaks tegid

ettekandeid ka mitu elutähtsa teenuse osutajat. Infopäeval osales üle 100 huvilise nii riigiasutustest kui ka ettevõtetest.

Sel kuul tuli avalikuks mitu turvaviga, millest CERT-EE meeskond puudutatud isikuid teavitas. Näiteks jaanuari keskpaigas teavitasime kõiki asutusi ja ettevõtteid, kes meie monitooringu kohaselt kasutavad haavatavaid GitLabi versioone. Soovitame sellised teavitusi alati tõsiselt võtta ning neile kiirelt reageerida uuendades tarkvara. Paraku näeme tihti küberründeid, mis on õnnestunud läbi viia just paikamata tarkvara tõttu.

Uuendasime E-ITS portaali ning ühtlasi sai valmis ka Eesti infoturbe standardi 2023. aasta versioon. E-ITS on nõuete ja parimate praktikate kogum, mis aitab nii avalikul kui ka erasektoril tõsta oma infoturbe taset. Etalonturbe kataloogi lisandus üheksa

uut moodulit, eemaldasime kaks moodulit ja muutsime kokku 111 olemasolevat meedet. Portaalis paranes masinloetavus ja nüüd on võimalik ka võrrelda erinevate aastate versioonide muudatusi. Täpsemalt on muudatused kirjeldatud [siin](#).

25. jaanuaril korraldasime järjekordse RIA CyberMeetUp ürituse, kus sel korral oli kolm esinejat. Tanel Sepp, kes juhib Välisministeeriumi Digi- ja küberdiplomaatia osakonda, rääkis Tallinna Mehhanismist, mille eesmärk on võimendada riikide kübertoetust Ukrainale tsiviilvaldkonnas. Edgars Milgravis, Palo Alto Networksi Baltikumi ärijuht, tegi ülevaate kübermaailma ohtudest eelmisel ja käesoleval aastal. Viimasena rääkis Tartu Ülikooli teadur Vjatcheslav Antipenko IoT projektide juhtimisest ja nende seostest küberturvalisuse alastes uuringutes. Kõiki toimunud üritusi saab järele vaadata [siit](#).



Rahvusvaheline keskkond

Ka jaanuaris jätkusid sõjategevusega seotud küberründed.

Ukraina julgeolekuteenistuse (SBU) [teatel](#) murdsid Vene riikliku taustaga küberrühmitused sisse mitmetesse Kiievi elumajadel olevatesse turvakaameratesse. Hiljuti muudeti kahe kaamera vaatevälja ja kasutati neid Ukraina õhukaitse töö ja kriitilise taristu objektide jälgimiseks ning 2. jaanuaril Kiievi pihta läbi viidud raketi- ja droonirünnaku tõhusamaks sihitamiseks.

Jaanuari lõpus tabas küberrünnak Kiievis asuvat andmekeskust, millest olid mõjutatud mitmed kriitilist teenust pakkuvad riigiettevõtted:

nafta- ja gaasiettevõtte Naftogaz, riiklik postifirma Ukrposhta, transpordi turvalisusega tegelev amet DSBT ning riiklik raudtee-ettevõtte Ukrzaliznytsia. Ründe tõttu oli häireid teenustes ning kodulehed olid maas, Ukrzaliznytsia pidi katkestama rongipiletite müügi internetis. Pole

teada, kes oli ründe taga, ent kahtlustatakse Vene taustaga rühmitusi.

Beiruti lennujaama tabas küberrünnak, mille käigus kompromiteeriti lennuinfokraanid

ning kuvati seal Hezbollah ja Iraani vastaseid sõnumeid, süüdistades neid Liibanoni tirimises täiemahulisse sõjalisel konfliktis Iisraeliga. Ründe tõttu oli häiritud ka pagasi käitlemine. Sõnumi juures kuvati ühe kristliku äärmusrühmituse Soldiers of God logo, ent rühmitus ise eitab seotust rünnakuga.

Sel kuul tabasid ettevõtteid suure jõuga küberründed. 19. jaanuaril tabas [lunavararünnak](#) tarkvara- ja digiteenuste ettevõtet Tietoevry, täpsemalt selle Rootsis asuvat andmekeskust. Tietoevry on Põhjala-Baltikumi suurimaid IT-ettevõtteid, millel on üle maailma 24 000 töötajat, neist ligikaudu tuhat Balti riikides, sealhulgas Eestis. Ettevõtte sõnul oli

ründe mõju limiteeritud, ent selle tõttu siiski katkesid teenused mitmetele Rootsi klientidele. Rootsi suurim kinokett Filmstaden näiteks ei saanud müüa internetis pileteid, sarnaseid probleeme oli ka teistel ettevõtetel ning teenuste taastamine kestab veel. Ründe taga arvatakse olevat Akira rühmitus.

Microsoft andis teada, et avastas 12. jaanuaril oma süsteemist küberrünnaku jäljed.

Ründe taga arvatakse olevat Vene välisluurega seotud rühmitus. 2023 novembris olevat ohustajal õnnestunud kompromiteerida üks mitteaktiivne konto ning sealtna edasi liikuda osade töötajate, sealhulgas juhtkonna liikmete, postkastidesse. Hakeritel õnnestus varastada dokumente ja e-kirju ning nende algne huvi näis olevat rühmitust ennast puudutav info ja analüüs Microsofti poolt. Microsofti praegusel hinnangul ei pääsenud ründajad ligi kliendiinfole, AI arendustele ega algkoodile.