

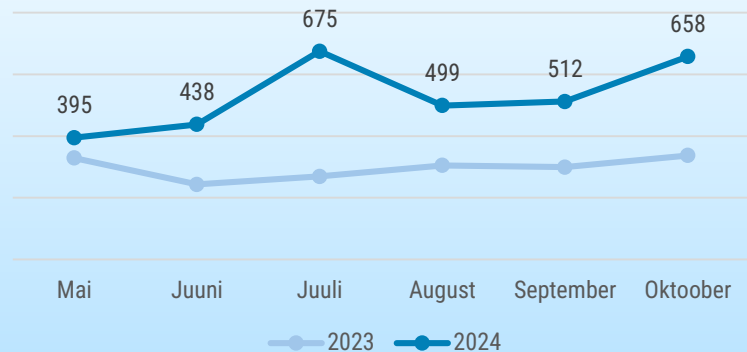


OLUKORD KÜBERRUUMIS

OKTOOBER 2024

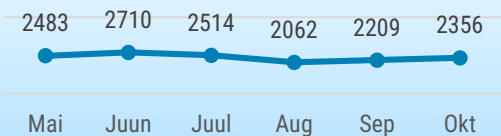
- Oktoobris **registreerisime 658 mõjuga intsidenti**, mis on viimase poole aasta keskmisest kõrgem näitaja.
- Kuu alguses **lekkisid** mõned eesti.ee rakenduse testimiseks soovi avaldanud inimese **meiliaadressid**. Teadmata isik sisenes **ERR-i failijagamisserverisse**.
- Oktoober on rahvusvaheline küberturvalisuse kuu ja korraldasime **küberohtude ennetamiseks teavituskampania**.
- Küberrünnak tabas **Prantsuse uudisteagentuuri** Agence France-Presse (AFP), USA üht suuremat vee-ettevõtet **American Water Works** ja **Iraani avaliku sektori asutusi**.

6 kuu registreeritud intsidendid



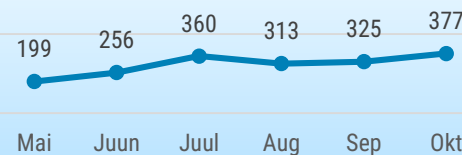
CERT-EE-le teavitatud intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.

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

Oktoober on juba aastaid küll küberturvalisuse kuu, kuid kahjuks ei möödunud see siiski intsidentideta. 2. oktoobril ajavahemikul 9.49 kuni 14.55 ei toiminud automaatne piirikontrolli süsteem ehk ABC-väravad, mida kasutatakse dokumendikontrolliks. Katkestuse tõttu oli häiritud Tallinna Lennujaama, Narva ja Saatses piiripunktide töö. Intsidendi põhjus pole teada, kuid praeguse seisuga ei kahtlustata rünnakut.

4. oktoobril lekkisid eesti.ee rakenduse testimiseks soovi avaldanud 350 inimese meiliaadressid. RIA arenduspartner saatis neile e-kirja, mille kõik adressaadid olid inimliku eksituse tõttu näha. Mõjutatud isikuid on juhtunust teavitatud.

7. oktoobril tuli katkestada 4. klasside vene keele tasemetöö, kuna selleks kasutatud eksamite infosüsteemi (EIS) töös tekkisid tõrked. Põhjuseks olid tehnilised tõrked – süsteemis ei töötanud helifail ja mõned kasutajad ei saanud infosüsteemi kasutada.

19. oktoobri õhtul sisenes teadmata isik Eesti Rahvusringhäälingu FTP-serverisse, mida kasutatakse failide vahetuseks koostööpartneritega. Kelm kustutas seal olnud failid ja laadis üles uued, mille hulgas oli ka pahavara. Ülevõetud konto kaitsmiseks kasutati nõrka parooli. Õnneks saadi kustutatud failid taastada, kuid soovitame juhtumi valguses üle vaadata paroolipoliitika ja võtta kasutusele kaheastmeline autentimine igal pool kus võimalik.

Alates 29. oktoobrist esines tõrkeid Krooning tanklate maksesüsteemis, mis broneerib klientide kontodelt suurema summa kui kütuse eest tasumiseks vajalik, kuid ei vabasta hiljem broneeringu jääki. Tanklaketile pakub makseteenust Soome ettevõtte Nets Finland, kellega koostöös probleemi lahendatakse. Krooning on lubanud ülebroneeritud summad klientidele esimesel võimalusel tagastada.

Oktoobris kaotasid paljud Eesti inimesed oma raha kelmidele. Selleks kasutati erinevaid viise, kuid enim nägime postiteenusepakujate nimel saadetud õngitsusi. Näiteks levisid erinevate kullerifirmade (DPD, DHL) nimel saadetud e-kirjad ja SMS-id, milles kutsuti üles oma aadressi uuendama või postitasu maksma. Mitmed inimesed sattusid taas Facebooki Marketplace'i pettuse ohvriks. Skeem toimib järgmiselt: petis võtab ühendust inimesega, kes Facebookis müüb ja väidab talle, et soovib kauba ära osta. Seejärel teatab ostja, et ei saa kaubale ise järele tulla ja pakub lahendusena kullerteenuse kasutamist. Müüjale väidetakse, et ta peab tehingu kinnitamiseks maksma kohaletoimetamise tasu või paki kindlustama ning ta suunatakse õngitsuslehele oma pangakaardiandmeid sisestama. Peale seda võetakse pangakaardilt maha vähemalt mitusada eurot, kuid tihti ulatuvad varastatud summad ka tuhandete eurodeni.



Tegevused küberturvalisuse parandamisel Eestis

9. oktoobril toimus RIA aasta-konverents, kus räägiti muuhulgas tehisintellektist, elektroonilise identiteedi (eID) tulevikust, E-ITSi rakendamisest, olukorrast küberruumis, Eesti uuest küberturvalisuse strateegiast, õigusruumist ja NIS2 seonduvatest muudatustest. Laval said sõna nii RIA töötajad kui ka head koostööpartnerid. Kohapeal osales umbes paarsada inimest, teist sama palju oli ürituse järgijaid veebis. Konverentsi saad järgi vaadata [siin](#).

17. oktoobril toimus selle hooaja esimene RIA CyberMeetUp. Avakõne pidas RIA peadirektor, seejärel tutvustasid oma ideid küberinkubaatori viis edukamat iduettevõtet ning lõpetuseks anti infot detsembri alguses toimuva küberfoorumi *CyberBazaar* kohta. Ürituse salvestust saab vaadata [siit](#). Järgmine RIA CyberMeetUp toimub 14. novembril.

Kuni kevadeni on esmaspäeva õhtuti

ETV eetris IT-vaatliku lühisaated küberturvalisusest. Oktoobrikuus võeti vaatluse alla õngitsuslehed, asjade internet, pahavara ja paroolid. Saated on järelvaadatavad [Jupiteris](#).

Oktoober on küberturvalisuse kuu ja korraldame küberohtude ennetamise teavituskampaania. Värsked küsitluse tulemused näitavad, et valdav osa Eesti elanikest järgib internetis vähemalt mõnda turvalise käitumise soovitusi, aga ligi kümme protsenti inimestest ei kasuta neist mitte ühtegi. Oleme oktoobris esinenud ka mitmetel erinevatel meediakanalitel. RIA ennetusjuht Kaisa Vooremäe selgitas 3. oktoobri [StarFMi](#) hommikuprogrammis Booking.com'i petuskeeme ja Kuku [raadios](#) internetipettustest hoidumist. Kuula ka „Pere ja kodu“ [taskuhäälingut](#), kus jagame küberturvalisuse nõuandeid lastele ja nende vanematele.

Kirjutasime RIA blogis, kuidas hallata turvaliselt ettevõtte sotsiaalmeediat.

Kuna üha suurem osa reklaamieelarvest suunatakse sotsiaalmeediakanalitesse ettevõtete nähtavuse tõstmiseks, siis on sellega suurenenud ka küberkurjategijate huvi valdkonna vastu. Seetõttu on tarvilik teadvustada riske ja ohte ning parandada selles osas ettevõtete teadlikkust. Kirjutasime [blogis](#) ka booking.com pettuste teemal – kuidas neid vältida ja mida RIA soovib silmas pidada.

Oktoobris ja novembris korraldame Tallinnas ja Tartus E-ITS kaasamiseminare. [Seminaridel](#) jagame E-ITSi rakendajatele praktilisi nõuandeid ja soovitusi, mis lihtsustavad standardi sisust arusaamist ja selle rakendamist.

Septembris ja oktoobris toimus RIA tellimisel kolm praktilist küberturbe koolitust arvutiõpetuse ja informaatika õpetajatele. Koolitused korraldati kolmel järjestikusel nädalal Tallinnas, Tartus ja Pärnus ning kokku osales neil ligi 70 õpetajat.



Rahvusvaheline keskkond

Oktoobri alguses [teatas Prantsuse uudisteagentuur Agence France-Presse \(AFP\)](#), et 27. septembril toimus nende vastu küberrünne. Intsident mõjutas AFP IT-süsteeme ning klientidele info edastamist. Agentuur kinnitas, et ülemaailmsete uudiste edastamist see ei puudutanud, kuid osad teenused olid mõjutatud. AFP tegi juhtunud asjaolude väljaselgitamiseks koostööd Prantsuse küberturbeagentuuriga (ANSSI).

Kuu alguses [tabas ka küberrünnak USA üht suuremat vee-ettevõtet American Water Works](#), mis pakub veevarustust ligikaudu 14 miljonile inimesele 14 eri osariigis. Rünnak ei mõjutanud veevarustust ega vee kvaliteeti, kuid lõi rivist välja ettevõtte arveldussüsteemi ning kliendiportaali. Ükski rühmitus ei ole seni ründe eest vastutust võtnud. Sagenevate rünnete ja puuduliku küberturvalisuse taseme tõttu on veesektor sel aastal olnud USA valitsuse eritähelpanu all.

12. oktoobril tabas ulatuslik [küberrünnak Iraani avaliku sektori asutusi, samuti kriitilisi sektoreid nagu tuumarajatised, kütusetransport ja sadamad](#). Ründe olemuse kohta pole seni infot, ent Iraani küberjulgeoleku ülemkogu endise kõrge ametniku sõnul varastati rünnete käigus ka tundlikku informatsiooni. Spekuleeritakse, et rünnete näol võis olla tegemist Israeli kättemaksuga Iraani raketirünnaku eest 1. oktoobril.

Ukraina kaitseministeerium [asutas eraldi operatiivse küberturbe osakonna CERT \(Computer Emergency Response Team\) riigi kaitseväge ja sõjaliste võrkude kaitseks](#). Ka varem oli kaitseministeeriumi haldusalas selleks eraldi meeskond, ent spetsiaalse struktuuriüksuse loomine laiendab selle volitusi ning aitab küberkaitset veelgi tõhustada, muuhulgas Venemaalt lähtuvate küberrünnete vastu. Loodud üksus hakkab koostööd tegema ka NATO riikidega.

Kaks vene häktivistide rühmitust [korraldasid oktoobri keskel ummistusrünnete kampaania Jaapani valitsusasutuste ja logistikaettevõtete vastu](#). Rünne oli ajendatud Jaapani hiljutisest otsusest tõsta oluliselt kaitsekulutusi ja osaleda sõjalistel õppustel USA ja teiste liitlastega. Küberettevõtte Netscout [raportist](#) selgub, et Jaapani võrkude vastu tehakse ligikaudu 2000 ummistusrünnet päevas.

Microsofti hiljutise [raporti kohaselt teevad Venemaa, Hiina ja Iraan küberoperatsioonides järjest rohkem koostööd kuritegelike rühmitustega](#). Juunis näiteks õnnestus kurjategijatel sisse murda mitmekümnesse Ukraina kaitseväelaste kasutuses olevasse seadmesse ja koguda Vene valitsusele huvipakkuvat infot. Microsofti hinnangul on piirid organiseeritud küberkuritegevuse ja riiklike ohustajate tegevuse vahel järjest enam hägustumas.