

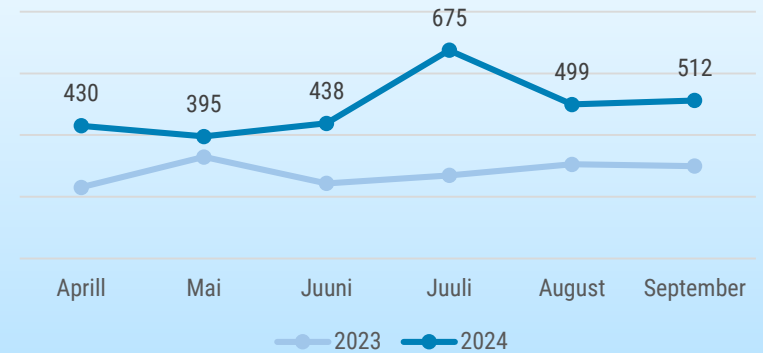


OLUKORD KÜBERRUUMIS

SEPTEMBER 2024

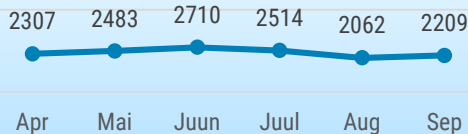
- Septembris **registreerisime 512 mõjuga intsidenti**, mis on viimase poole aasta keskmisest veidi kõrgem näitaja.
- Septembris **katkes mitmete oluliste teenuste töö**, näiteks esinesid tõrked Telia kõnesides ja Swedbanki teenuste töös. Nägime **LHV nimel saadetud õngitsuskirjade** levikut.
- Korraldame täiskasvanutele mõeldud **küberturvalisuse töötubasid**. Avaldasime uued lastele ja nende vanematele mõeldud eestikeelsed **juhendmaterjalid**.
- Eesti koos teiste riikidega andis välja **ühisavalduse** küberrünnete omistamiseks Vene sõjaväeluurele. Autorendifirma **Avis** langes küberrünnete ohvriks.

6 kuu registreeritud intsendidid



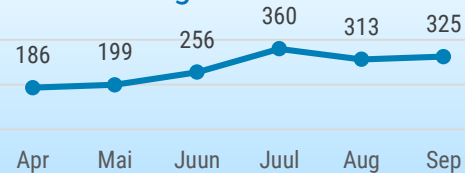
CERT-EE-le teavitatud intsendidid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.

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

Septembris katkes mitmete oluliste

teenuste töö. 5. septembril kell 10.56 ajal algasid torked Telia kõnesides. Üle Eesti polnud võimalik Telia võrgust välja helistada, mõjutatud olid nii lauatelefonid kui ka mobiilikõned. Kell 12.28 oli kõneside suures osas taastunud, kuid osadel klientidel võis probleeme esineda ka hiljem. Ligi tunni jooksul oli häiritud ka kõnede tegemine hädaabinumbri 112. Rikke põhjustas tarkvaraviga kõneside süsteemis.

7. septembril ajavahemikul 9.45 kuni 13.26 oli häireid ID-kaartide väljastamisel, kuna uute kaartide sertifikaate ei saanud muuta kehtivaks. Probleemi põhjustas Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) hooldustööde käigus tehtud seadistusviga.

16. septembril ajavahemikul 6.58 kuni 8.44 toimus laialtlevinud veebilehtede töö katkestus. Ligi kahe tunni jooksul ei avanenud mitmed olulised veebilehed, nende hulgas näiteks Riigi

autentimisteenus tara.ria.ee. Mõjutatud oli üle 200 erineva veebilehe ja probleemi põhjustas tehniline tõrge teenusetökestusrünnete vastast kaitset pakkuva ettevõtte Cloudflare andmekeskuses.

17. septembri varahommikul kell 4.35 tekkisid Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) tuumikvõrgu hooldustööde käigus torked andmesideühendusega, mistõttu katkesid SMITi teenused, sealhulgas hädaabiteadete süsteem, mida kasutab Häirekeskus 112 kõnede menetlemiseks. Enamus SMITi teenustest taastusid varem, kuid Häirekeskuse tavapärase töö taastus alles kella 8 paiku.

26. septembril ajavahemikel 15.28 kuni 19.09 ja 20.05 kuni 21.02 oli häireid Swedbanki kaardimaksetes ja internetipanga töös. Samal päeval esines tõrkeid ka ühe teise panga teenuste töös. Hetkel ei ole veel katkestuste põhjus teada.

Septembris levis näiliselt LHV panga

poolt saadetud õngitsuskiri, milles paluti kasutajatel oma andmeid uuendada. Kirja saatjaks oli kahtlane e-posti aadress, mis ei kuulu LHV pangale ja kirja sees oli link, mis suunas kasutaja oma pangakaardiandmeid sisestama. Kahjuks läksid paljud inimesed selle kirja õnge ja CERT-EE sai mitmeid teavitusi suurte rahasummade kaotuse kohta. Mõnel korral oli kaotatud summaks üle 10 000 euro. Tuletame meelde, et pank ei saada taolisi kirju ega palu andmeid uuendada tundmatu lingi kaudu. Kui pangas on vaja andmeid uuendada, siis saadetakse selle kohta teavitus internetipanga vahendusel ja andmete uuendamine toimub samas keskkonnas.



Tegevused küberturvalisuse parandamisel Eestis

Alates septembri lõpust korraldame üle Eesti 25 täiskasvanutele mõeldud tasuta töötuba, kus õpetatakse internetiga seotud ohte ära tundma ning oma arvuteid ja nutiseadmeid paremini kaitsma. Õpitoad on mõeldud eeskätt keskealistele ja vanematele inimestele (55+), aga oodatud on kõik huvilised. Osalejaid õpetatakse näiteks ära tundma õngitsuslehti, petukõnesid ja muid kuritegelikke skeeme. Õpitoad kestavad umbes kaks tundi ning toimuvad alates septembri lõpust kuni novembri alguseni üle Eesti kohalikes raamatukogudes ja sotsiaalasutustes. Täpsema info õpitubade toimumisaegadest ja -kohtadest leiad RIA [kodulehelt](#).

30. septembril jõudis eetrisse esimene episood „IT-vaatliku“ saatesarjast. Esimene osa keskendus õngitsustele ja pettustele ning vaataja saab teada, et kust saavad petturid meie andmed ja kuidas nad neid edasi kasutavad. Saade on ETV eetris 26 nädala jooksul,

mil kaetakse mitmed olulised küberturvalisuse teemad. Saated on järele vaatavad ERRi voogedastusplatvormil [Jupiter](#), ning moodustavad olulise osa 30.09 avapaugu saanud RIA igasügisest küberhügieenialasest [teavituskampaaniast](#), mis vältab oktoobri lõpuni.

Avaldasime RIA kodulehel uued algkoolieas lastele ja nende vanematele mõeldud eestikeelsed juhendmaterjalid, mis aitavad interneti kasutamisega seotud ohte ära tunda ja vältida. RIA välja antud [tööraamat](#) sobib 7–11-aastastele lastele ning tutvustab interneti ja nutiseadmete turvalisuse teemasid lastele arusaadaval ja huvipakkuval viisil, kasutades selleks ristsõnu, harjutusi ja mängu. Lapsevanematele mõeldud [abimaterjal](#) keskendub sellele, et kuidas kaitsta oma lapsi ja õpetada neile internetiga seotud ohte.

Nüüd on võimalik Kübertesti sooritada ka inglise keeles! Kübertest on RIA loodud e-õppe keskkond, mis katab kõik olulisemad küberhügieeni teemad ning aitab hoida töötajate küberturbeteadlikkust. Ootame Kübertestiga liituma kõiki asutusi ja ettevõtteid. Kui soovid hakata kasutama ingliskeelset kursust, kirjuta aadressile kybertest@kybertest.ee.

Septembris alustasime 9 uut järelevalvemenetlust, mille käigus kontrollime küberturvalisuse seaduse alusel kehtestatud nõuete täitmist. Menetluse eesmärgiks on kontrollida nii organisatsiooniliste, füüsiliste kui infotehniliste turvameetmete täitmist ettevõttes või asutuses. Kõrgendatud tähelepanu all on asutuse infoturbe- ja riskihaldusprotsesside toimimine ja E-ITS turvameetmete rakendamine. Lisaks tegime ka viis ettekirjutust neile, kes pole piisavalt turvameetmeid rakendanud.



Rahvusvaheline keskkond

USA, Ühendkuningriigid, Holland, Tšehhi, Eesti, Läti, Kanada, Austraalia, Ukraina ja Saksamaa andsid 5. septembril välja ühisavalduse, milles omistavad mitmete riikide vastu viimastel aastatel toime pandud küberründed Vene sõjaväeluure (GRU) üksusele „29155“. Riikide küberametkondade hinnangul on üksuse eesmärk küberluure, sabotaaž ja mainekahju tekitamine. Eestis pani üksus 2020. aastal toime küberrünnakuid (sealhulgas andmevarguseid) erinevate riigiasutuste vastu, samuti seostatakse seda üksust 2022. aastal Ukrainas toime pandud rünnetega, milles kasutati andmeid hävitavat pahavara WhisperGate.

Autorendifirma Avis langes augusti alguses küberründe ohvriks ja nüüdseks on selgunud, et lekkinud on vähemalt 300 000 kliendi isiklik informatsioon, sealhulgas krediitkaardiandmed ja

juhiloanumbrid. Peamiselt puudutab leke ettevõtte USA kliente, keda on sellest ka teavitatud. Arvestades, kui palju on Avisel kliente ning kui tundlikke andmeid nad säilitavad, on juhtum tekitanud pahameele ettevõtte ebapiisavate küberturbemeetmete osas.

Septembris sooritasid Ukraina häkkerid rünnaku asutuse Osnovanie vastu, mis sertifitseerib Venemaa antavaid digiallkirju. Ründajad näotustasid asutuse veebilehe, jättes sinna sõnumi, et “teie sertifikaadid on turvalistes kätes, müügituludega toetatakse Ukraina kaitseväge”. Osnovanie teate kohaselt oli tegemist vaid veebilehe näotustamisega, digiallkirjadega seotud infrastruktuur polevat kahjustada saanud. Samas veel mitu päeva hiljem oli leht maas ning Vene klientide sõnul ei olnud digiallkirjastamise teenused kättesaadavad. Rünnaku eest võttis vastutuse Ukraina sõjaväeluure

koostöös rühmitusega „BO team“ ning nende väitel õnnestus osa andmebaase hävitada ja osa andmeid varastada. Osnovanie kommertsdirektori Alexey Senchenkovi sõnul kasutati rünnakuks USA-s, Hollandis ja Eestis asuvaid servereid.

Europoli, Eurojusti ja üheksa riigi ühisoperatsiooni tulemusel likvideeriti krüpteeritud suhtluskeskkond Ghost, mida kasutasid organiseeritud kuritegelikud rühmitused üle maailma. Platvorm sobis kurjategijatele, kuna võimaldas anonüümset kasutamist, mitmeid krüpteerimisvõimalusi ja ka teenust, millega saadetud sõnumid haihtusid sihtmärgi seadmest teatud aja jooksul. Platvormil vahetati igapäevaselt tuhatkond sõnumit ja sel oli oluline roll globaalse narkokaubanduse ja rahapesu võimaldamises. Operatsiooni tulemusel arreteeriti 51 inimest, peamiselt Austraalias ja Iirimaaal.