

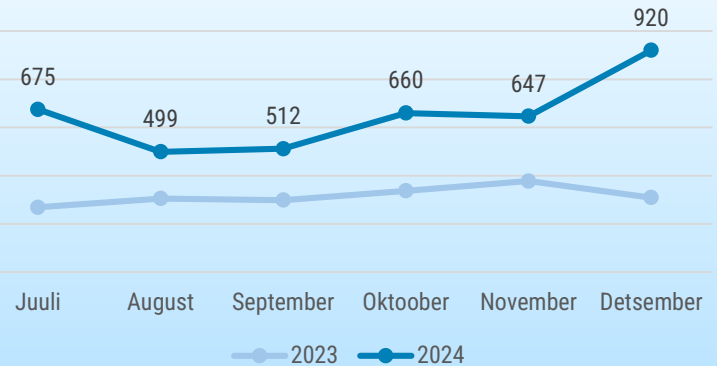


OLUKORD KÜBERRUUMIS

DETSEMBER 2024

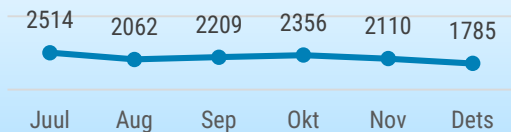
- Detsembris registreerisime **920 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja. Suurema osa registreeritud intsidentidest moodustasid õngitsuslehed.
- Detsembris tabas **haridusvaldkonna ettevõtet lunavararünnak** ja ühel riigiasutusel olid jäänud lahkunud töötajate kontod aktiivseks. Detsembris jätkusid ka **LHV nimel saadetud õngitsused**.
- Avaldasime uuendatud **ennetusportaali IT-vaatlik** ja uue **eesti.ee mobiilirakenduse**.
- Ukraina justiitsministeeriumit tabas ulatuslik **küberrünnak**, mille tulemusel olid mitmed avalikud teenused kättesaamatud. USA plaanib keelata julgeolekuriskide tõttu Hiina tootja **TP-Link ruuterid**.

6 kuu registreeritud intsidendid



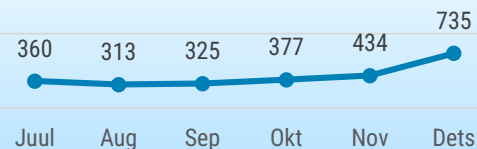
CERT-EE-le teavitatud intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.

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

Detsembris registreerisime möödunud aasta kõige suurem arvu intsidente.

2. detsembril langes haridusvaldkonnas tegutsev ettevõtte lunavararünnaku ohvriks. Selle käigus krüpteeris ründaja ettevõtte andmed Amazoni pilvekeskkonnas ning nõudis nende taastamise eest lunaraha. Tegemist polnud isikuandmete ega ärikriitiliste andmetega ja ettevõtte leppis nende kadumisega. Rünnaku tegi võimalikuks liiga suurte õigustega konto.

9. detsembri varahommikust ei saanud Tartu linnaliinibussides osta pileteid, samuti ei toiminud busside ees ja küljel liininumbrit näitavad elektroonilised tablood ega peatuste infokraanid. Katkestuse põhjustas kettaruumi täitumine Tartu ühistranspordile teenust pakkuva ettevõtte Ridango süsteemides. Kell 10.30 said tõrked kõrvaldatud.

10. detsembril ajavahemikul 10.38 kuni

11.04 toimus teenusetõkestusrünne Eestis tegutseva kommertsponga vastu. Sel ajavahemikul oli lühiajalisi häireid rünnatud panga teenustes.

16. detsembril ajavahemikul 14.07 kuni 15.09 ei toiminud Smart-IDga autentimine ega allkirjastamine. Tegemist oli tehnilise tõrkega, mis tekkis planeeritud muudatuse teostamise järgselt.

CERT-EE sai novembris teavituse, et ühe riigiasutuse mitmekümnel ametist lahkunud töötajal olid alles jäänud asutuse meilikontod, kuhu neil oli endiselt ka ligipääs. Aktiivsed olid ka osad endiste töötajate administraatoriõigustega kontod. Juhtunu mõju ja asjaolud on selgitamisel.

Detsembris jätkusid ka erinevad pettused. Meid teavitati taas paljudest juhtumitest, kus inimesed sattusid LHV õngitsuskirja ohvriks. Kirjades palutakse enda andmeid uuendada ja

inimesele tundub, et ta siseneb panga veebilehele, kuid tegelikult on petised loonud pangale väga sarnase keskkonna. Sarnased kirjad olid liikvel ka novembrikuus. Tuletame taas meelde, et pank ei küsi andmeid e-maili teel ega palu sisse logida kahtlastele domeenidele.

Meid teavitati ka juhtumist, kus laps avas TikToki QR-koodiga lingi ja selle kaudu sai perekond rahalist kahju.

Peale QR-koodi skaneerimist avanes kasutajale pealtnäha usaldusväärne telefonimängu kujundusega leht, kus paluti kinnitada tasuta mängulisa saamise soov. Peale nupule vajutamist hakati lapse telefonist saatma massiliselt sõnumeid välismaa numbritele. Paari minuti jooksul saadeti üle 160 sõnumi, kuid õnneks ei olnud sel korral rahaline kaotus siiski väga suur. Soovitame olla QR-koodides olevate linkide suhtes väga tähelepanelik ning kahtluse korral neid mitte avada.



Tegevused küberturvalisuse parandamisel Eestis

Novembri lõpus toimus RIA eestvedamisel [suurõppus](#), kus harjutati riigi IT-majade, muude asutuste ja küberreservi koostööd kriiside lahendamisel. Õppuse stsenaariumi järgi avastati justiitsvaldkonna infosüsteemis anomaaliad, mistõttu peatati ajutiselt kinnipeetavate vabastamine. Hiljem selgus, et tegemist oli küberrünnakuga ning lekkinud oli ka väga tundlikke andmeid. Põhjuste uurimiseks ja teenuste võimalikult kiireks taastamiseks kutsuti appi ka RIA hallatava küberreservi tehnilised eksperdid. Lisaks pidid riigiasutused tegelema ohtralt leviva valeinfo tõrjumisega. Seetõttu kaasati õppusele ka mitmete riigiasutuste avalike suhete spetsialistid ja valitsuse kommunikatsioonikeskuse reservliikmed.

[Detsembri alguses toimus Riias innovatsioonifoorum CyberBazaar 2024, mis korraldati Eesti, Läti ja](#)

[Leedu riiklike küberturvalisuse keskuste koostöös](#). Ettekanded toimusid kolmel temaatilisel laval: tehnoloogia, teadus ja äriarendus. Kokku esines ligi 50 asjatundjat Baltikumist ja kaugemalt. Samuti oli üles seatud EXPO ala, mis võimaldas tutvuda uusimate teenuste ja tehnoloogiatega ning otsida koostööpartnereid. Foorumi raames leidis Läti Ülikoolis aset tudengitele mõeldud häkaton, kus võisteldi kolmes kategoorias: küberturvalisus valitsemistasandil, küberinnovatsioon ning küberalase teadlikkuse kasv.

[11. detsembril nägi ilmavalgust uuendatud ennetusportaal IT-vaatlik](#): uuenduskuuri läbisid nii veebikeskkonna välimus, struktuur kui ka sisu. Lisaks põhjalikult uuendatud eraisikutele mõeldud juhenditele leiab sealt ka palju muud huvitavat, näiteks küberkaitse lühikursuse, õppevideod ja meie põnevad raadio- ja telesaated. Olulise täiendusena sai leht juurde

rubriigi „Levinud pettused“, kus tutvustatakse Eestis populaarseid petuskeeme, et neid ära tunda ja kahju vältida. Mine ja tutvu uuendatud [IT-vaatlikuga](#).

[RIA avaldas detsembri alguses uue eesti.ee mobiilirakenduse, mis toob riigiteenused otse taskusse](#). Uus Eesti äpp aitab kõigil mugavalt ja turvaliselt riigiga suhelda – kasutada riiklike teenuseid, vaadata oma andmeid ja tulevikus kasutada ka erasektori teenuseid. Täna on juba kasutusel ligi 50 teenust, kuid tulevikus on neid veelgi lisandumas. Mobiilirakendusse on arendatud ka isikusamasuse tõendamise lahendus, kuid juriidiliselt saab isikut tõendavaid dokumente (ID-kaart ja pass) rakenduses kasutada isikusamasuse tõendamiseks alles pärast seaduse muudatuse jõustumist.



Rahvusvaheline keskkond

Rumeenia konstitutsioonikohus tühistas maa presidendivalimiste esimese vooru tulemused, kuna riigi luureteenistuste andmetel oli Venemaa korraldanud koordineeritud mõjutuskampaania TikTokis paremärmuslasest kandidaadi Calin Georgescu toetuseks. Seni suhteliselt tundmatu Georgescu võitis esimese vooru ning lubas muuhulgas lõpetada Rumeenia toetuse Ukrainale. Rumeenia luureteenistuse raportist selgub ka, et valimiste taristu vastu tehti rohkem kui 85 000 küberrünnet. Ründed täitsid erinevaid eesmärke: ligipääsu hankimine taristule ning selle kompromiteerimine, valimistega seotud info muutmine ja ligipääsetavuse takistamine.

Iraani ohustaja on sihikule võtnud SCADA tööstusseadmed USA-s ja Iisraelis. Küberturbe-ettevõtte Claroty eksperdid andsid välja [raporti](#) spetsiaalselt asjade interneti (IoT) ja tööstusseadmete jaoks välja töötatud

pahavara IOCONTROL kohta. Iraani sidemetega rühmitus CyberAv3ngers sihib selle pahavaraga erinevaid kodu- ja tööstusseadmeid USA-s ning Iisraelis, sealhulgas turvakaameraid, ruutereid, tule müüre, tööstusautomaatika juhtpaneele jne. Samuti on sihikul tanklates kasutatavad seadmed ning rühmituse enda väitel on neil viimase aasta jooksul õnnestunud kompromiteerida 200 tanklat USA-s ja Iisraelis.

Ukraina justiitsministeeriumi andmebaase tabas ulatuslik küberrünnak, mille tulemusel olid mitmed avalikud teenused (abieluavalduse sisse andmine, sünnitõendi väljastamine, auto registreerimine jne) umbes kaks nädalat kättesaamatud. Ründe tõttu tuli sulgeda ka mitukümmend Diia äpi teenust, mis ei saanud vajalike andmebaasidega ühendust. Ukraina valitsus teatas reedel, et esialgse hinnangu kohaselt ei ole andmeid

lekkinud ega kustutatud. Ründe taga arvatakse olevat Vene sõjaväeluurega seotud häkkerite rühmitus ning tegemist on viimase aja suurima ründega Ukraina kriitiliste andmekogude vastu.

USA plaanib järgmisel aastal keelata julgeolekuriskide tõttu Hiina tootja TP-Link ruuterid, mida seostatakse Hiina häkkerite küberrünnakutega. CISA hallatavas aktiivselt ära kasutatavate turvanõrkuste kataloogis on praegu ära toodud kaks TP-Link seadmete turvanõrkust, mida on siiski vähem, kui mitmete suurte lääne tootjate seadmetes. Analüütikute hinnangul on TP-Link keelustamise plaani taga eelkõige mure TP-Link ruuterite suure, umbes 65% turuosa üle väike-ettevõtete ja erakasutajate seas ning tulevikus materialiseeruda võivad riskid, mis on seotud TP-Link sidemetega Hiina valitsusega.