

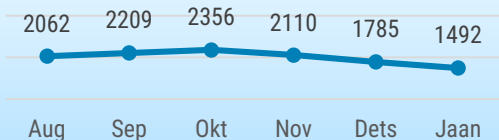


OLUKORD KÜBERRUUMIS

JAANUAR 2025

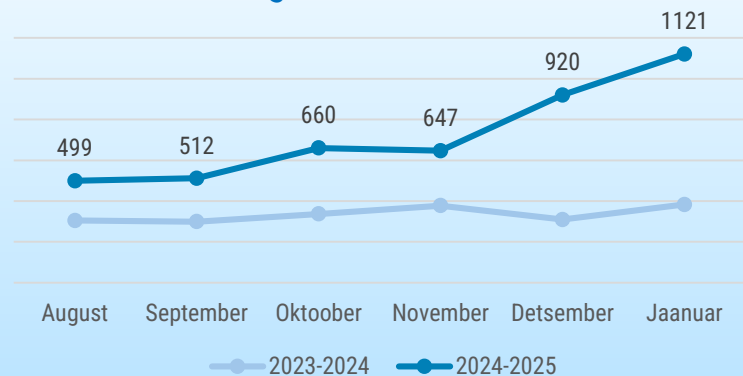
- Jaanuaris **registreerisime 1121 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja.
- Kahe riigiasutuse seadmed kompromiteeriti **Ivanti turvanõrkuse** kaudu. Jaanuaris levisid **näiliselt Maksuja Tollimeti nimel** saadetud e-kirjad ja sõnumid.
- Avaldasime **küberturvalisuse aastaraamatu**. Kirjutasime RIA blogis mitmetest laialdaselt kasutusel olevatest tarkvaradest, mille **tugi lõppeb sel aastal**. ETV eetris olid uued osad **saatesarjast „IT-vaatlik“**.
- Saksamaa lennujaamade piirikontrollisüsteemi tabas **ulatuslik IT-katkestus**. Ühendkuningriigi **domeeniregistr**it tabas küberrünnak. Itaalia andmekaitseamet blokeeris Hiina päritolu **DeepSeek** tehisarurakenduse kasutamise Itaalias.

Automaatseire: pahavara



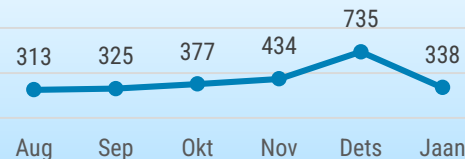
Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.

6 kuu registreeritud intsendid



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

Õngitsuslehed



Õngitsuslehed moodustavad jätkuvalt suurema osa CERT-EE registreeritud intsidentidest. Alates selle aasta jaanuarist registreerime lisaks petulehti, mistõttu on õngitsuslehtede arv vähenenud.



Olukord Eesti küberruumis

Jaнварis toimus taas katkestusi mitmete oluliste teenuste töös.

2. jaanuaril ajavahemikul 13.30 kuni 15.58 ei toiminud automaatne piirikontrollisüsteem ehk ABC-väravad Narva ja Saatse piiripunktis ning Tallinna lennujaamas. Katkestuse põhjustas sertifikaadi aegumine.

8. jaanuaril ajavahemikul 11.18 kuni 13.15 ei saanud SIRENE (Supplementary Information Request at the National Entry) süsteemis, mida Politsei- ja Piirivalveamet kasutab infovahetuseks, seadistusvea tõttu sõnumeid muuta ega salvestada.

3. jaanuari õhtul ja 4. jaanuari hommikul tabas ummistusrünne Eestis tegutsevat kommertsbanka. Rünna tõttu oli lühiajalisi katkestusi selle internetipanga töös.

Jaanuari alguses selgus, et kahe riigiasutuse VPN-seadmed, mis kasutavad Ivanti Connect Secure tarkvara, on kompromiteeritud.

Rünna jaoks kasutati 8. jaanuaril avalikustatud kriitilist haavatavust tähisega CVE-2025-0282, mis võimaldab ohvri süsteemis käivitada pahaloomulist koodi. Kompromiteerimise üks tunnustest on süsteemi logide edastuse katkemine. Kahjuks on ka varasemalt õnnestunud Eesti riigiasutuste seadmetesse ligipääs saada just Ivanti turvanõrkuste kaudu. Tuletame siinkohal meelde, et paikamata turvanõrkused on üks põhilisi edu toovaid ründevektoreid.

31. jaanuaril ajavahemikul 8.00 kuni 9.45 esines tõrkeid Tervisekassa retseptide loetelu teenuses üle x-tee. Intsidendi põhjus ei ole veel teada, kuid selle lahendas arenduse tagasisivõtmine.

Sel kuul jätkusid ummistusründed erinevate asutuste nimeserverite vastu. Löögi all olid CERT-EE, RIA, EENet.ee ja Välisministeeriumi nimeserverid. Tänu kaitsemeetmetele polnud neil rünnetel mõju.

Jaнварis levisid näiliselt Maksu- ja Tollimeti nimel saadetud e-kirjad ja sõnumid, milles väideti, et inimest ootab aastane maksutagastus.

Juhtumi puhul oli eriline see, et saaja suunati linki avama QR-koodi kaudu. Kuna tihtilugu avavad QR-koodi skannerid lingi automaatselt ja kasutajale ei näidata domeeni eelvaadet, siis kasutaja ei pruugi aru saada et tegemist on kahtlase lingiga. Loe ka lisaks EMTA [juhust](#), et kuidas ära tunda petukirju ja -sõnumeid. Meile teadaolevalt ei olnud see pettus õnnestunud ja inimesed said aru, et tegemist ei ole õige kirjaga. Kahjuks ei saa sama öelda jätkuvate LHV panga nimel saadetud öngitsuskirjade kohta, milles palutakse kiirelt andmeid uuendada. Näeme, et endiselt langetakse LHV nimel saadetud öngitsuskirjade ohvriks.



Tegevused küberturvalisuse parandamisel Eestis

Avaldasime küberturvalisuse aastaraamatu, kus kirjutame kõigest olulisest, mis toimus küberruumis möödunud aastal. Näiteks selgub aastaraamatus, et eelmisel aastal toimus Eestis 6515 mõjuga küberintsidenti ehk umbes kaks korda rohkem kui 2023. aastal. Ligi kaks kolmandikku neist olid erinevad õngitsused, kuid ka näiteks pettuste arv kasvas. Lisaks Eestis toimuvale tegime ülevaate ka mujal maailmas toimunud, sealhulgas Hiina ambitsioonidest küberruumis.

2025. aastal lõppeb mitmel olulisel tarkvaral tootjapoole tugi, sealhulgas turvauuenduste väljastamine. Suurimat mõju avaldab nii eraisikutele kui ka ettevõtetele ning asutustele Microsoft Windows 10 Enterprise, Education, Home ja Pro versioonide ametliku toe lõpp 14. oktoobril 2025. Kirjutasime RIA [blogis](#) mitmetest laialdaselt kasutusel olevatest tarkvaradest, mille tugi lõppeb sel

aastal. Kirjutame ka regulaarselt blogis igal nädalal olulisematest turvanõrkustest. Tarkvarades olevad turvauugud on üks ründajate lemmiksihtmärk, mille kaudu saadakse esmane ligipääs organisatsiooni süsteemidele. Soovitame RIA turvanõrkuste [postitusi](#) igal nädalal lugeda.

Nii detsembris kui ka jaanuaris olid ETV eetris uued osad saatesarjast „IT-vaatlik“. Saadetes rääkisime näiteks laste turvalisest internetikasutamisest, kontode ülevõtmisest, sotsiaalmeedia ja nutitelefonide turvalisest kasutamisest, pettuste ohvriks langemisest ning Eestis levinud küberintsidentidest ja pettustest. Kõik saated on vaadatavad [ERRi Arhiivis](#).

16. jaanuaril toimus selle aasta esimene RIA CyberMeetUp, mida saab järgi vaadata [siin](#). Sel korral tegid ettekanded Jürgen Erm (NEVERHACK Estonia), Raimundas Matulevičius (Tartu Ülikool), Rain Ottis (Taltech),

Triin Toimetaja (PwC) ja Johannes Kadak (ECSC Estonia). Aasta esimene CyberMeetUp tegi külastajate rekordi – kohale tuli 70 inimest ja lisaks kuulasid paljud seda ka veebis. Järgmine üritus toimub juba 13. veebruaril.

Avaldasime RIA ennetusportaalis „IT-vaatlik“ artikli investeerimispettuste kohta. Kuna viimasel ajal on erinevate investeerimispettuste hulk teinud Eestis märkimisväärse kasvu, siis on oluline neid ära tunda ja teadlik olla. Politsei- ja Piirivalveameti andmete alusel kaotasid Eesti inimesed 2024. aastal ainuüksi investeerimiskelmustega üle 4,8 miljoni euro. Investeerimispettuse korral pakutakse ohvrile pealtnäha väga head raha paigutamise võimalust, lubatakse madala riskiga või riskivaba investeringut ning garanteeritud tootlust. Tutvu pettusele tüüpiliste ohumärkidega ja konkreetse näitega IT-vaatliku [portaalis](#).



Rahvusvaheline keskkond

3. jaanuaril tabas Saksamaa lennujaamade piirikontrollisüsteemi ulatuslik IT-katkestus, mis põhjustas pikki järjekordi Schengeni väliste piiriületuste puhul. Mitmetes suurtes lennujaamades tuli piirijärjekorras oodata vähemalt kaks tundi ning lennujaama ülerahvastatuse vältimiseks hoiti osasid reisijaid pikemalt lennukis. IT-katkestuse põhjust ei ole avaldatud.

Ühendkuningriigi domeeniregister Nominet avalikustas jaanuari alguses avastatud küberintsidendi, kus ründajad kasutasid ära Ivanti VPN tarkvara nullpäeva turvanõrkust. Seda turvaviga on ära kasutatud alates detsembri keskpaigast ja üldiselt seostatakse neid ründeid Hiina riikliku taustaga ohustajatega. Nominet haldab üle 11 miljoni .uk domeeninime ning pakkus kuni eelmise aasta septembrini UK küberturvalisuse keskusele nimeserveri kaitseteenust.

Ukraina vabatahtlik häkkerirühmitus Ukrainian Cyber Alliance tungis Vene telekomiettevõtte Nodex võrku, varastas sealt andmeid ja hävitas süsteeme. Nodex kinnitas samal päeval sotsiaalmeedia postituses, et on langenud hävitusliku küberründe ohvriks ning püüavad süsteeme varukoopiatest taastada. Võrguandmeid vaatlev organisatsioon NetBlocks tuvastas Nodexi võrgus nii tavatelefon- kui mobiilside katkemise. Ka Vene telekomijärevalveamet Roskomnadzor kinnitas laiaulatuslikke sidekatkestusi peamiselt Moskva regioonis, ent ei maininud konkreetset sideoperaatorit ega katkestuste põhjust.

Jaanuari teisel poolel jõustus USA-s seadus, mis keelustas TikTok rakenduse kasutamise kõikidel kasutajatel, kuniks see ei ole eraldatud Hiina ettevõttest ByteDance. TikTok lakkaski töötamast ja seda ei olnud võimalik rakenduspoodidest alla

laadida. Paus kestis aga vaid umbes 14 tundi, sest juba järgmisel hommikul kirjutas ametisse asuv president Trump oma sotsiaalmeediaplatvormil, et kavatseb selle seaduse pausile panna ja anda 90 päeva ajapikendust TikTokile kohaliku ostja leidmiseks, et 170 miljonit ameeriklast saaks populaarset rakendust edasi kasutada.

Itaalia andmekaitseamet Garante blokeeris Hiina päritolu DeepSeek tehisarurakenduse kasutamise Itaalias. Garante põhjendab otsust sellega, et ei saanud ettevõttelt adekvaatseid vastuseid selle kohta, milliseid isikuandmeid ja millise regulatsiooni alusel rakenduse abil Itaalia kasutajatelt kogutakse ning kas need andmed talletatakse Hiinas. DeepSeekiga seotud ettevõtted Hangzhou DeepSeek AI ja Beijing DeepSeek AI olevat päringule vastanud, et nad ei tegutse Itaalias ja seega ei kohaldu neile Euroopa Liidu seadused.