



# OLUKORD KÜBERRUUMIS

MÄRTS 2025

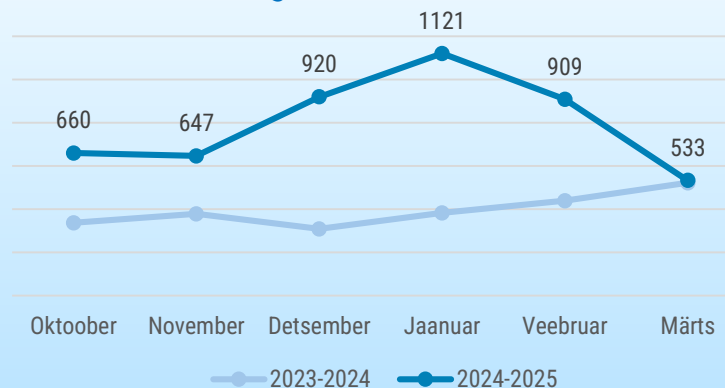
- Märtsis registreerisime **533 mõjuga intsidenti**, mis on viimase poole aasta kõige madalam näitaja.
- Eesti.ee rakenduse** töö katkes rohkem kui ööpäevaks. Paljude Eesti asutuste ja ettevõtete töötajate postkasti jõudsid näiliselt advokaadibüroode nimel saadetud **pahavara sisaldavad e-kirjad**.
- RIA küberturvalisuse keskuse juht Gert Auväärt osales CYBERCASTi taskuhäälingus. Kirjutasime RIA blogis **e- kirj vahetuse turvalisusest** ja Eesti **riiklikke e-teenuseid matkivatest õngitsusest** ning viimastel kuudel järsult kasvanud **petukõnedest**.
- USA kaitseminister andis korralduse panna kõik **Vene-suunalised küber- ja infooperatsioonid pausile**. Prantsusmaa **Sorbonne'i ülikooli** tabas lunavararünnak. Poola **kosmose-agentuur POLSA** andis teada neid tabanud küberrünnakust.

## Automaatseire: pahavara



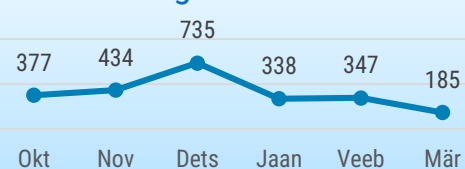
Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.

## 6 kuu registreeritud intsidendid



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

## Õngitsuslehed



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



# Olukord Eesti küberruumis

## Märtsis katkes mitmete oluliste teenuste töö.

Eesti.ee rakenduse töö katkes rohkem kui ööpäevaks. 28. veebruaril alates 13.54 kuni 1. märtsil 17.26 ei toimunud eesti.ee mobiilirakendus seadistusvea tõttu. Katkestus kestis nii pikalt puuduliku monitooringu tõttu.

3. märtsil ajavahemikul 8.24 kuni 9.53 oli häireid Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) sisselogimise (Active Directory ehk AD) teenuses. Seetõttu võis sisselogimine siseministeeriumi, politsei-ja piirivalveameti, häirekeskuse ja sisekaitseakadeemia süsteemidesse võtta minuteid või täielikult ebaõnnestuda. Rikke ajal ei toimunud ka Outlook ja e-kirju saata ei olnud võimalik. Katkestuse põhjustas viga AD kontrolleri töö, mis taastusid pärast nende taaskäivitamist.

10. märtsil ajavahemikul 18.52 kuni 19.13 oli häiritud Smart-ID kasutamine.

Tõrke põhjustas koormusjaoturi tarkvara rike, mis ei suutnud kõiki päringuid teenindada. Samal päeval ajavahemikul 17.21 kuni 17.47 toimus ummistusrünne Balti riikides tegutseva kommertspanga nimeserverite vastu. Selle tagajärjel oli häireid internetipanga, mobiilirakenduse ja välgmaksete töös.

Jätkusid teenusetõkestusründed CERT-EE nimeserverite vastu. Tänu kasutusel olevatele kaitsemeetmetele ei olnud neil rünnatel traditsiooniliselt mõju.

**Märtsis teavitati meid kahest lunavararündest, mille täpsemad asjaolud on uurimisel.** Kuna lunavararünnatel on tihti tõsised tagajärjed ja nende tulemusel võib organisatsiooni töö seisma jääda, siis tuleb meelde mõned viisid nende ennetamiseks. Kaugtöölauaühendus (RDP) ei tohiks olla internetis avalikult kättesaadav, vaid ühendus peaks olema lubatud kindlaksmääratud IP-aadressidelt. Lisaks tuleks kasutada

VPNi ehk virtuaalset privaattõrku ja kaheastmelist autentimist. Oluline on ka regulaarselt uuendada tagavarakoopiat ja hoida seda muust võrgust eraldi, näiteks välisel andmekandjal.

**Märtsis jõudsid paljude Eesti asutuste ja ettevõtete töötajate postkasti näiliselt advokaadibüroode nimel saadetud pahavara sisaldavad e-kirjad.** E-kirjas teatati autoriõiguse rikkumisest Eesti Televisioonile (ETV) kuuluvate video- ja audiofailide avaldamisest Facebookis. Kirjas väidetakse, et tõendid rikkumise kohta asuvad kirjale lisatud PDF-failis. Tegelikult on PDF-faili sees link, mille avamisel laetakse kasutaja seadmesse pahavara. Kirja saatjaks on enamasti märgitud mõne tuntud Eesti advokaadibüroo nimi, kuigi meili saatmiseks on kasutatud suvalist Gmaili aadressi.



# Tegevused küberturvalisuse parandamisel Eestis

RIA küberturvalisuse keskuse juht Gert Auväärt rääkis CYBERCASTi värskes episoodis, kuidas Eesti end küberohtude eest kaitseb ja mida igapäevaks saab teha, et digimaailmas turvalisemalt hakkama saada. Saates räägiti ka küberturvalisuse aastaraamatust ja sellest, et küberturvalisus mõjutab iga inimest ning ettevõtet.

RIA peadirektor Joonas Heiter andis [intervjuu Digigeeniuse portaalile, kus selgitati uue juhtimiskeskuse loomist ja senise CERT-EE seiretiimi töö ümberkorraldamist](#). Kogu muudatus viiakse ellu olemasoleva ressursi arvelt, ilma täiendavat eelarvet taotlemata. Selle käigus vaadatakse põhjalikult üle tööprotsessid ja uuendatakse kogu seireloogikat. RIA juhtimiskeskuse töö käivitamine on plaanis 2025. aasta esimesel poolaastal.

20. märtsil toimus Palo Alto klubis korra kuus toimuv CyberMeetUp. Sel korral tegid ettekanded Rain Nõmmsalu (CybExer Technologies), Jack Shis (NATO CCDCOE), Jesper Olsen (Palo Alto Networks) ja Teoh Chun Ping (Government Technology Agency of Singapore). Kõigil soovijatel on võimalik kas üritusele kohale tulla, vaadata seda otseülekanadena veebis või hiljem järele vaadata RIA kodulehel. Järgmine CyberMeetUp toimub 17. aprillil.

Avaldasime RIA [blogis e-kirjavahetuse turvalisuse ja usaldusvääruse tagamise soovitusel organisatsioonidele](#). Paljudes pettustes kasutatakse võltsitud e-kirju või organisatsiooni nimel tema partneritele läkitatud õngitsuskirju. Blogis kirjutame, kuidas meili- ja nimeserverit korrektselt seadistada, et e-kirjade võltsimise võimalust vähendada.

Kirjutasime RIA [blogis viimastel kuudel registreeritud petukõnedest, enamik neist jäljendasid Omnivat](#). Petturid väitsid, et nad on kullerid ning neil on vaja saadetis kohale tuua. Selleks paluti ohvril Smart-ID abil kinnitada kas paki saabumine või hoopis maksuametilt tulnud deklaratsioon.

Kirjutasime ka Eesti riiklikke e-teenuseid matkivatest [õngitsusest](#). Inimesi meelitatakse neile lehtedele peamiselt SMS-sõnumite kaudu, mis sisaldavad erinevad ettekäanded, miks peaks sõnumi saaja kaasasolevale veebingile vajutama. Uurisime RIA blogis lähemalt Transpordiameti nimel saadetud SMS-õngitsust ning jagasime soovitusi pettuste vältimiseks.

Märtsis olid ETV eetris ka uued IT-vaatliku saatesarja episoodid, kus rääkisime PIN-koodidest ja SMS-õngitsustest. Kõiki eetris olnud saateid saab igal ajal järele vaadata [Jupiteris](#).



# Rahvusvaheline keskkond

**USA kaitseminister Pete Hegseth andis USA küberväejuhatusele korralduse panna kõik Vene-suunalised küber- ja infooperatsioonid pausile, seoses Trumpi eesmärgiga saavutada kokkulepe Putiniga Ukraina sõja lõppemise asjus.** Ehkki selline praktika kõrgetasemeliste läbirääkimiste ajaks ei ole ebatavaline, on USA lähenemine Venemaale ja kannapööre senises välispoliitikas siiski olnud tervikuna paljude vaatlejate jaoks rabav. Paus ei puuduta küberluuret ega signaalluuret. Samas olevat ka USA küberturbeagentuuri CISA ohuanalüütikutele antud juhis keskenduda Vene ohu asemel teistele vaenlastele ning USA välisministeeriumi kõrge ametniku hiljuti ÜRO-s peetud küberohtude teemalises kõnes paistis silma, et Hiina ja Iraani kõrval Venemaad küberohuna enam ei mainitud.

**Prantsusmaa Sorbonne'i ülikooli tabas lunavararünnak, mille omistas endale**

**Funksec nimeline lunavararühmitus.**

Ründes kasutatud lunavaratüüp on asjatundjate hinnangul esimene loova tehisintellekti abil kirjutatud lunavara ning vaid mõned kuud tagasi esile kerkinud rühmitus Funksec just selliste kasutamise silma paistabki. Funkseci sihtmärkide ring on olnud võrdlemisi lai, hõlmates nii valitsus- ja kaitsektorit kui finantsasutusi, haridussektorit ja tehnoloogiasektorit. Rühmitusel on olnud ohvraid USA-s, Indias, Hispaanias ja Mongoolias.

**Poola kosmoseagentuur POLSA andis teada neid tabanud küberrünnakust ja infosüsteemi võrgust eemaldamisest.**

Ründe olemuse kohta ametlikku infot ei ole, aga ühe kosmoseagentuuri töötaja sõnul oli muuhulgas kompromiteeritud nende sisemine meilikeskond. Poola digitaliseerimisministri Krzysztof Gawkowski sõnul algatati uurimine ja riik annab endast parima, et sissetungija välja selgitada.

**Taani küberjulgeolekuagentuur avaldas ohuhinnangu, mille kohaselt on kasvanud küberluure oht Euroopa telekomiettevõtetele.** Küberrünnete oht Taani telekomisektori vastu **tõsteti** tasemele „kõrge“, seejuures on kõige kõrgem lunavararünnete ja küberkuritegevusega seotud rünnete oht.

**Ühendkuningriigi andmekaitseamet määras ettevõttele Advanced Computer Software Group 3,6 miljoni euro suuruse trahvi andmelekkete eest.**

Andmed varastati ettevõttelt 2022. aastal toimunud lunavararünde käigus, mille pani toime rühmitus LockBit. Advanced Computer Software Group pakub teenuseid muuhulgas riiklikule tervisekassale (National Health Service) ja teistele tervishoiuteenuste pakkujatele ning ründe tulemusel lekkisid ligikaudu 80 000 inimese andmed, sealhulgas umbes 900 koduhooldusel oleva patsiendi täpne aadress ja juhised, kuidas nende koju sisse saada.