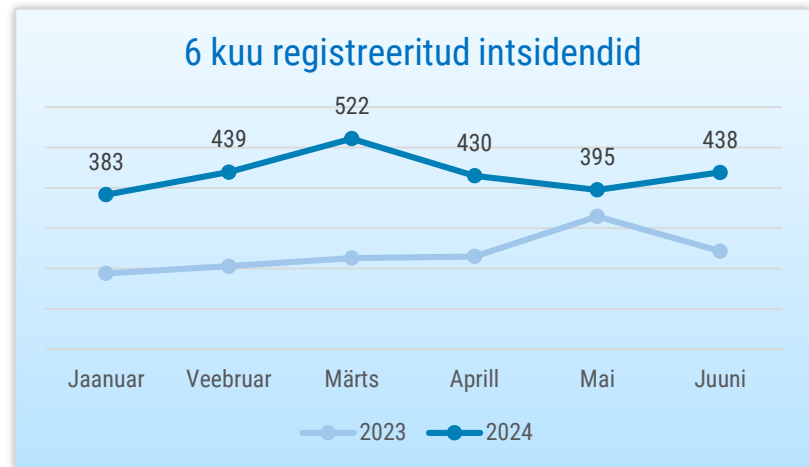




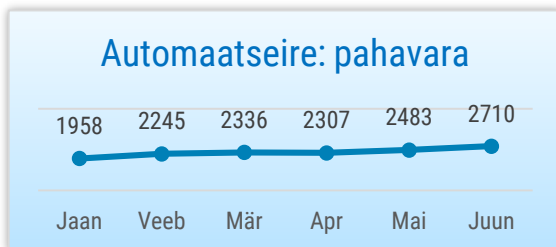
# OLUKORD KÜBERRUUMIS

JUUNI 2024

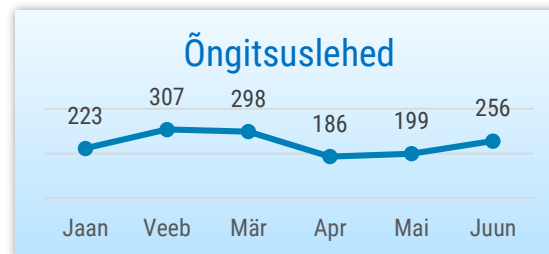
- Juunis registreerisime 438 mõjuga intsidenti, mis on viimase poole aasta keskmisest veidi kõrgem näitaja.
- Juunis esines tõrkeid **TEHIKu** teenuste töös ja **autentimisteenuste** kasutamisel. Tallinna Tervishoiu Kõrgkooli serveris olevad andmed krüpteeriti.
- Aitasime tagada Euroopa Parlamendi **valimiste e-hääletamise** valmisolekut, turvalisust ja tehnilist tuge. **Kübertest**i uus 2024. aasta versioon sai valmis.
- Ligi tuhande Euroopa ja Ühendkuningriigi poliitiku andmed olid kättesaadavad **tumeveebis**. Clevelandi linn sattus **küberründe** ohvriks.



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



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



Õngitsuslehed moodustavad jätkuvalt kõige suurema osa CERT-EE registreeritud intsidentidest.



# Olukord Eesti küberruumis

**Eestis 3. juunist 9. juunini läbi viidud Euroopa Parlamendi valimiste vaates oli olukord küberruumis üldiselt väga rahulik, kuid kahjuks nägime siiski teatud tehnilisi tõrkeid.**

3. juunil ehk e-hääletamise esimesel päeval oli veebilehitsejate Chrome ja Firefox kasutajatel probleeme valijarakenduse alla laadimisega valimised.ee lehelt. Nimelt pidasid veebibrauserid rakenduse faili algselt pahavaraks. Samuti ei toiminud valimisperioodi alguses valimiste veebilehel külastajate operatsioonisüsteemi tuvastamine, mistõttu pakuti mõnedele kasutajatele alla laadimiseks vale operatsioonisüsteemi jaoks loodud tarkvara.

**Juunis nägime mitmeid teenusekatkestusi.** 4. juunil kell 7.47 kuni 14.50 katkesid võrguseadme tarkvararikke tõttu pooleks päevaks TEHIKu teenused. Avalikest teenustest ei toiminud pikalt Sotsiaalkindlustus-ameti iseteenindusportaal.

Keskpäevaks taastati süsteemide töö, kuid umbes kell 13.30 katkes see taas. Mõjutatud olid kõik TEHIKu teenused, sh telefonid, meilid, veebilehed ja infosüsteemid. Häiritud olid ka kiirabibrigaadid, kuid mitte reageerimise osas ja häirekeskuse töö oli tagatud. Tervisekassa põhiteenuste töös oli katkestus 28. juunil ajavahemikul 11.34 kuni 11.55, põhjuseks teenusepakkuja tulemüüri tõrge.

**11. juunil alates 22.35 kuni 12. juunil kella 00.10 oli tõrkeid Eesti ja Leedu Mobiil-ID töös.** Seetõttu esines probleeme Mobiil-IDga internetipankadesse ja teistesse e-teenustesse sisenemisel ning digitaalallkirja andmisel. 20. juuni hommikul toimus DDoS-rünne Smart-ID teenuse vastu, mille tulemusel oli selle toimimine kõigis Balti riikides ligi kahe tunni vältel häiritud. Rünnak kordus 21. juuni hommikul, mis põhjustas samuti Smart-ID teenuse katkestusi.

Mitmel korral – 18. juunil ajavahemikul 21.15 kuni 22.00, 19. juunil 21.45 kuni

22.20 ja 20. juunil 4.01 kuni 4.09 – **esines tõrkeid hädaabi teadete menetlemise infosüsteemi (SOS2) töös.** Kasutajad ei saanud süsteemi sisse logida ja esines ka muid häired. Tõrkeid põhjustas andmebaasi vale seadistus.

**4. juuni varahommikul krüpteeriti Tallinna Tervishoiu Kõrgkooli serveris olnud andmed** kokku ligikaudu 1,5 TB mahus. Serveris hoiti ülikooli töötajate ning tudengite faile. Intsident mõjutas kooli enam kui 200 töötajat, tudengeid ning failiserveri teisi kasutajaid. 5. juuniks olid teenused varunduse abil taastatud.

**18. juunil avastas Moodle'i õppekeskkonna haldaja haridus- ja teadusministeerium, et nende juures majutatavasse TalTechi Moodle'sse on sisse tungitud.** Ründajad kaardistasid sisevõrku ja proovisid ligipääsu saada ka teistele võrgus paiknevatele arvutitele. Ründe täpsemad asjaolud on veel uurimisel.



# Tegevused küberturvalisuse parandamisel Eestis

## Aitasime tagada Euroopa Parlamendi valimiste, sh e-hääletamise valmisolekut, turvalisust ja tehnilist tuge.

Valimisnädal leidis aset 3. juunist kuni 9. juunini ning kogu valimiste perioodil oli RIA kõrgendatud valmisolekus (oranž, Charlie). Sel korral otsustas e-hääletamise kasuks enam kui 153 000 inimest ehk 41.5% kõigist valijatest. Tehniliselt sujusid nii e-hääletamine kui valimiste infosüsteemi töö suuremate probleemideta ning olukord küberruumis oli väga rahulik.

**13. juunil toimus hooaja viimane RIA CyberMeetUp üritus.** Sel korral oli meie poolt laval Joosep Sander Juhanson (infoturbe ekspert, CERT-EE), kes tegi ülevaate olukorrast küberruumis. Vanemveebel Kristo Pals (Eesti Kaitsevägi) rääkis küberajateenistusest Eesti Kaitseväes. Lisaks tegid ülevaate küberkindlustusest ning selle õiguslikust ja praktilisest vaatest

Rainer Ratnik (vandeadvokaat, WIDEN) ja Helen Evert (kindlustusmaakler, IIZI). Nii juunikuu kui ka kõigi eelnevate ürituste salvestusi saab järgi vaadata RIA [kodulehel](#).

**Avaldasime Digiriigi Akadeemias kursuse väljastellimisest (tarneahelast).** E-kursus "E-ITSi abiga turvaline väljastellimine" aitab mõista ja rakendada väljastellimise parimaid praktikaid, et tagada organisatsiooni andmete kaitse ja teenuste järjepidev kvaliteet. Digiriigi Akadeemia on eelkõige avaliku sektori e-kursuste ja digiteadmiste õppeplatvorm, kuid koolitusi võivad läbida kõik huvilised. Kursused on kõigile tasuta ja neid saab läbida endale sobivas kohas ning sobival ajal.

**Kübertesti uus, 2024. aasta versioon sai valmis.** Ka sel aastal koosneb Kübertest kahest osast: kursus põhitõdede kinnistamiseks ja seejärel

teadmisi kontrollida aitav test. Kursusel katame kõik olulisemad küberhügieeniga seonduvad teemad – paroolide turvalisus, pahavara levimine, õngitsuskirjade äratundmine, mä lupulcade ja muude andmekandjate kasutamine, turvaline kaugtöö ja palju muud. Sel aastal oleme koolitusele lisanud ka õppevideod, mis katavad kõik olulisemad teemad ja muudavad koolituse läbimise huvitavamaks. Kübertesti kasutamine on jätkuvalt kõigile soovijatele tasuta ja liitumise kohta saad rohkem infot [siit](#).

**Korraldame ka sel aastal küberturbehuvilistele tüdrukutele Kehtnas suvelaagri.** Rahvusvaheline küberturbe laager CyberWizards toimub 29. juulist 3. augustini ning sinna on oodatud 13–16-aastased tüdrukud, kellele meeldib lahendada põnevaid ülesanded ja võtta vastu väljakutseid. Täpsema info laagri kohta leiad RIA [veebilehelt](#).



# Rahvusvaheline keskkond

## **Ka juunis jätkusid Ukrainas toimuva sõjategevusega seotud küberründed.**

CERT-UA [teavitas](#), et Ukraina riigiteenistujaid ja kaitseväelasi, aga ka kaitsetööstusettevõtete töötajaid sihitakse aktiivselt pahavarakampaaniaga, mis levib Signali sõnumirakenduse kaudu. Enamasti käib nakatumine nii, et ohvrile saadetakse sõnum koos lingi või failiga ja parooliga selle avamiseks. Avamisel käivitub pahavara, mis võimaldab ründajal seadme oma kontrolli alla võtta. Usutavuse tõstmiseks võidakse kasutada ohvri kontaktilistis olevat, juba varem kompromiteeritud kontot.

## **Kuu alguses tuli avalikuks, et ligi tuhande Euroopa ja Ühendkuningriigi poliitiku andmed olid kättesaadavad [tumeveebis](#).**

Tehnoloogiaettevõtete Proton ja Constella Intelligence raportist selgub, et tumeveebis on müügiks ligikaudu tuhande Euroopa ja Ühendkuningriigi

poliitiku isikuandmed: meiliaadressid, sünniajad, paljudel juhtudel ka salasõnad. Kõige rohkem on saadaval Briti parlamendiliikmete andmeid, järgnevad Euroopa Parlamendi ja Prantsuse parlamendi liikmed. Andmetest tuli välja, et mitmel juhul oli kasutatud ametlikke meiliaadresse erinevatesse keskkondadesse kasutajakonto registreerimiseks, mõnel juhul ka näiteks tutvumisportaalides.

## **3. juunil [tabas](#) lunavararünnak patoloogia- ja**

## **diagnostikateenusepakkujat**

**Synnovis**, millel on partnerlus mitmete Londoni suurte haiglatega. Haiglate töö on seetõttu häiritud, intsident mõjutab peamiselt vereülekannete ja vere kiiranalüüside tegemist. Palju operatsioone on tulnud edasi lükata ning korralisi vastuvõtte tühistada. Ründe taga arvatakse olevat Qilin-nimeline Vene lunavararühmitus.

## **Juuni keskpaigas [teatas](#) Clevelandi linnavalitsus, et on langenud küberründe ohvriks ning paljud**

avalikud teenused on seetõttu võrgust eemaldatud. Intsidendi uurimise ajal töötab linnavalitsus väiksema võimekusega ja ehkki hädaabi ja kriitilised kommunaalteenused toimusid, olid siiski paljud teenused pikalt rivist väljas. Küberründed on ka varem Ameerika kohalikke omavalitsusi häirinud, kuid 400 000 elanikuga Cleveland on seni suurim linn, mis on pidanud paljud teenused ajutiselt sulgema.

## **Ühendriikides [otsustati](#) alates 20. juulist täielikult keelata Vene päritolu küberturbeettevõtte [Kaspersky.Labs toodete müük USA klientidele](#).**

Keelu põhjuseks on Kaspersky.Labsi sidemed Vene valitsusega ning võimalus, et viimane võib survestada ettevõtet jagama andmeid USA klientide kohta, mis aitaksid USA-vastaste küberoperatsioonide planeerimisel. Kaspersky praeguste klientide hulgas on mh USA kriitilise infrastruktuuri ettevõtteid ja kohalikke omavalitsusi.