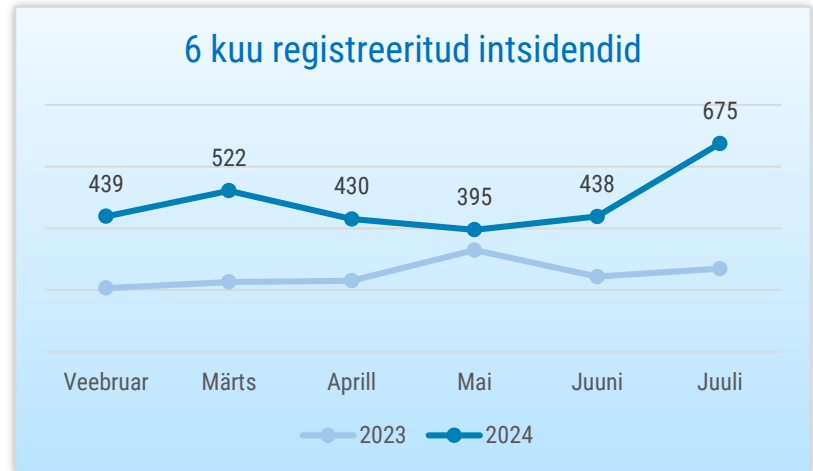




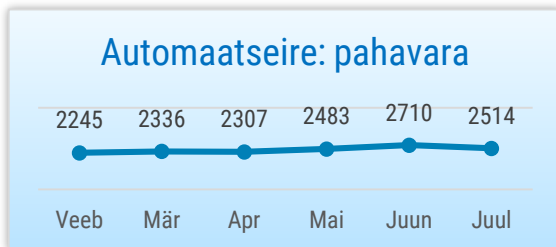
# OLUKORD KÜBERRUUMIS

JUULI 2024

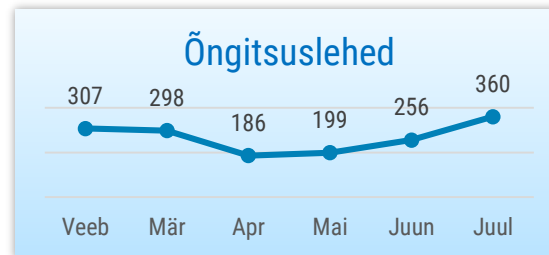
- Juulis registreerisime **675 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja.
- Üle poole registreeritud intsidentidest olid **õngitsuslehed**, mida kasutatakse aina enam inimestelt raha või kontoandmete välja petmisel.
- Aitasime koostada **riiklikku küberturvalisuse strateegiat** aastateks 2024-2030. Avaldasime uued **abimaterjalid**, mis teevad ettevõtetel infoturbe alustamise lihtsamaks.
- Jalgpalli EM Euro2024 tõi kaasa **küberrünnakuid**. NATO riigid loovad Belgiasse uue **küberkaitsekeskuse**.



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

**Mujal maailmas põhjustas suuri tõrkeid ja katkestusi CrowdStrike'i vigane tarkvarauuendus**, mis viis rivist välja 8,5 miljonit Windowsi seadet. Mõjutatud olid paljude riikide erinevad sektorid - lennundus, tervishoid, kaubandus, pangandus, meedia, kuid Eestis ei põhjustanud see olulisi tõrkeid. Siin ei ole CrowdStrike Falcon Sensor nimelt kuigi laialdaselt kasutusel. Meile teadaolevalt mõjutas see üht energiaettevõtet ja eraettevõtet. Esimeses olid mõne tunni jooksul häiritud ettevõttesiseseid teenused ja klienditeenindus, kuid mõju energiatootmisele polnud. CrowdStrike'i rike häiris ka Tallinna Lennujaamas Ryanairi lendudele registreerimist.

**Juulis oli mitmel korral tõrkeid erinevate Tervise ja Heaolu Infosüsteemide Keskuse (TEHIK) teenustega.** 1. juulil ajavahemikul 8.05 kuni 9.14 toimus katkestus Üleriigilise Digiregistratuuri veebilehe

digiregistratuur.ee töös. Tõrkeid põhjustas võrgukatkestus, mille järel teenuste töö ei taastunud koheselt. Ka digireseptide töös esines häireid. 6. juulil alates 8.30 olid osad retseptiravimid vale soodumääraga ning mõnesid retseptiravimeid ei saanud välja kirjutada. Intsidendi põhjustas vale andmestik ning see lahenes 8. juulil kell 14.18. 10. juulil ajavahemikul 14.29 kuni 14.47 polnud võimalik kasutada Tervisekassa põhiteenuseid (digiresept, ravikindlustatuse kontroll) üle x-tee. Põhjuseks oli java rakenduse tõrge, teenuste töö taastus peale selle taaskäivitamist. 17. juulil alates 22.04 kuni 18. juulil kell 15.14 oli taas probleeme veebilehe digiregistratuur.ee laadimisega. Probleemi põhjustas rakenduse mälu täitumine.

**Juulis levisid mitmed õngitsused.** Kõige enam nägime näiliselt politsei nimel saadetud ja Smart-ID kehtivuse

lõppemist väitvaid õngitsuskirju. Politsei nimel saadeti ka erinevate pealkirjadega e-kirju, milles väideti, et kirja saaja suhtes on käimas kohtumenetlus ja edastatakse kutse istungile. Kirja saatjaks oli märgitud Euroopa Politseiamet, Eesti Politsei või riiklik politsei direktoraat. Taolisi e-kirju on juba mitme aasta vältel massiliselt saadetud. Soovitame kirjaga kaasas olevat manust mitte avada ja kiri kustutada. Smart-ID kontoandmeid õngitsevas kirjas väideti, et kasutaja konto on peatatud ja selle taastamiseks tuleks oma identiteeti kinnitada. Kiri saadeti suvaliselt domeenilt, mis ei ole Smart-ID teenusega seotud ja kirjas oli link, mis suunas õngitsuslehele.

**29. juulil tabas Tartus tegutsevat väikeettevõtet lunavararünnak.** Selle käigus krüpteeris pahavara failid neljas arvutis. Ettevõtte tavapärane töö katkes ja juhtunu täpsemad asjaolud selgitamisel.



# Tegevused küberturvalisuse parandamisel Eestis

**Väikesed ja keskmise suurusega ettevõtted saavad kuni 2. septembrini taotleda toetust oma küberturvalisuse hindamiseks ja parandamiseks**, et hoida ära

küberrünnakute või tehniliste tõrgetega kaasnevat kahju. Toetuse suurus on kuni 60 000 eurot ja see jaguneb kaheks: ettevõtte küberturvalisuse hindamiseks saab küsida 10 000 ja arendustöödeks 50 000 eurot. Kübertoetuse taotlemise kohta saab lisainfot Ettevõtlaste ja Innovatsiooni Sihtasutuse [kodulehelt](#).

**Teavitasime võrguseadmete omanikke, kelle halduses on seadmeid, mis võivad olla haavatavad OpenSSH turvanõrkuse CVE-2024-6387 vastu**. Tegemist on haavatavusega, mille eduka ärakasutamise korral saab ründaja volitamata ligipääsu süsteemile. Soovitasime kõigil uuendada OpenSSH serveri rakenduse kõige uuemale versioonile, kus nimetatud turvaviga on paigatud. Teeme taolisi

teavitusi tihti ja soovitame neid kindlasti tõsiselt võtta, kuna tihti saavad ründajad ligipääsu just paikamata tarkvara kaudu.

**Majandus- ja Kommunikatsiooniministeriumil koostöös Riigi Infosüsteemi Ametiga valmis Eesti riiklik küberstrateegia aastateks 2024–2030 „Läbivalt IT-vaatlikum Eesti“**, milles nähakse peamise eesmärgina, et Eesti küberruum oleks turvaline, usaldusväärne ja küberohtudele vastupidav. Eesti küberturvalisuse strateegia kaardistab valdkonnas viimasel ajal toimunud muutused ja toob välja vajalikud töösuunad nendega kohanemiseks. Küberturvalisuse strateegiaga saab tutvuda [siin](#).

**RIA Analüüsi- ja ennetusosakonna ennetusjuht Kaisa Vooremäe käis Kuku Raadios rääkimas, et millised ohud meid küberruumis varitsevad ja kuidas end nende eest kaitsta**.

Tuletasime ka meelde, et kuidas õngitsuslehti ära tunda ja mis on virtuaalne privaatvõrk (VPN).

**Avaldasime uued abimaterjalid, mis teevad ettevõtetel infoturbe alustamise lihtsamaks**. Eesti infoturbestandardi (E-ITS) [stardimeetmed](#) on mõeldud eeskätt ettevõtetele, kes pole varem infoturbe süsteemselt tegelenud ega pea küberturvalisuse seaduse nõudeid täitma, aga soovivad oma äritegevust ja klientide andmeid paremini kaitsta. Värskest valminud infoturbe juhendmaterjalid aitavad ettevõtetel ja asutustel ära hoida nii küberrünnakute, andmelekete kui ka tehniliste probleemidega kaasnevat majanduslikku ja mainekahju.

**Kuula ka [taskuhäälingut](#) „Olukorrast digiriigis“**, kus RIA riikliku mobiilirakenduse talituse juhataja Greta Preast käis rääkimas Eesti äpi arenduse hetkeseisust, tehnilistest uuendustest ja edasistest plaanidest.



# Rahvusvaheline keskkond

**14. juunist 14. juulini väldanud jalgpalli Euroopa meistrivõistlused tõid kaasa mitmeid küberrünnakuid.** CyberInt raportist [selgus](#), et Euro2024 ajal hoogustusid küberründed Euroopa jalgpalliliidu UEFA liikmete vastu ning mitmetes tumeveebi foorumites pakutakse müügiks tuhandeid UEFA partnerite ja klientide kontoandmeid. Kuna paljud neist on registreeritud oma töömeiliaadressiga ja kasutavad ka samu parooli, on kaudselt ohustatud väga palju erinevaid ettevõtteid. Samuti toimusid DDoS ründeid mänge kajastavate meediakanalite vastu. Raportis tõdetakse, et küberrünnete arvu kasv seoses suurte spordisündmustega on muutunud tavapäraseks ning sama ennustatakse ka 26. juuli kuni 11. august toimuvate Pariisi olümpiamängude ajaks.

**Kevadel tabas LiveNation/ Ticketmaster meelelahutusettevõtte küberrünnak**, kus kurjategijatel õnnestus varastada andmebaas miljonite klientide isikuandmetega.

Andmebaas paisati tumeveebis müüki 500 000 dollari eest. Juulis aga [väitsid](#) kurjategijad, et nende valduses on ka Taylor Swifti käimasoleva kontserttuuri 166 000 pileti ribakoodid ning veel mitmete suurürituste (F1 formula, Stingi kontsert jpm) pileтите info, mille avaldamise ärahoidmiseks nõuti miljoneid dollareid. Ticketmaster omakorda kinnitas, et pileтите ribakoode uuendatakse regulaarselt ja varastatud piletid on seega kehtetud.

**NATO liikmesriigid loovad Belgiasse uue küberkaitsekeskuse.** Keskuse eesmärk on tõsta NATO võrkude turvalisuse taset, parandada olukorrateadlikkust ning küberruumi kaitset nii rahu, kriisi kui konflikti ajal. Keskuses hakkavad tööle sõjalised ja tsiviilekspertid NATO riikidest ning see hakkab andma infot NATO väeülematele küberruumi haavatavuste ja ohtude kohta.

**Juuli keskpaigas põhjustas CrowdStrike'i vigane uuendus**

**ülemaailmseid katkestusi Windowsi süsteemides**, mis mõjutas paljude organisatsioonide ja teenuste tööd. Antud viga põhjustas nn sinist ekraani mõjutatud Windowsi tööjaamades ja serverites, mistõttu olid häiritud ka paljud elutähtsate ja oluliste teenuste osutajad nagu lennujaamad, haiglad ja sadamad. 30. juulil korraldati Microsofti vastu DDoS-rünne, mille tõttu katkes mitmete teenuste (näiteks Outlook ja Azure) töö pea 10 tunniks.

**Ühendkuningriigi õiguskaitseorganid sulgesid ummistusrünnete tellimise platvormi DigitalStress.** See oli üks populaarsemaid teenusetõkestusrünnakute (DDoS) tellimise platvorme, mis võimaldas vähese tehnilise võimekusega inimestel küberkuritegusid toime panna. Ühendkuningriigi õiguskaitseorganite andmetel telliti DigitalStressi kaudu kümneid tuhandeid teenusetõkestusründeid nädalas.