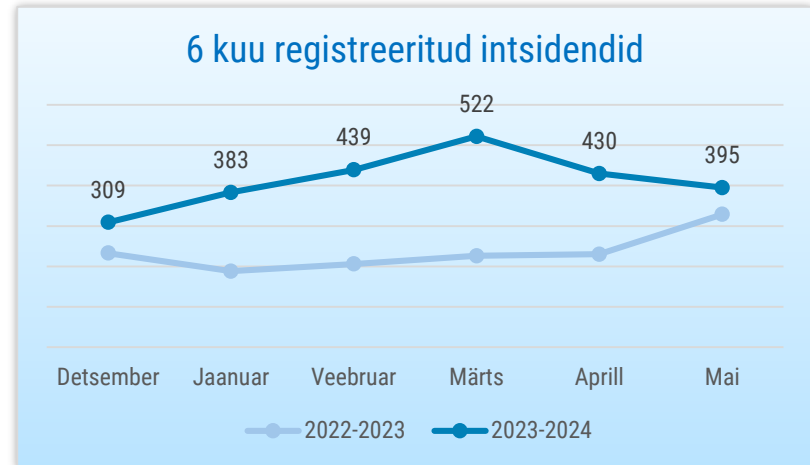




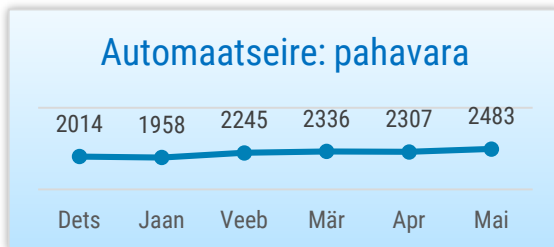
OLUKORD KÜBERRUUMIS

MAI 2024

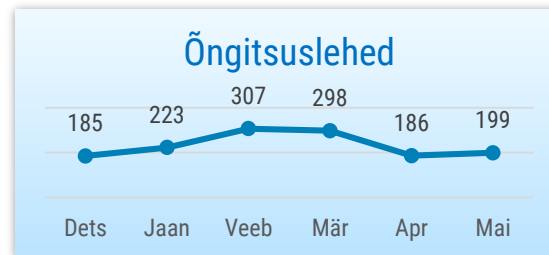
- Mais registreerisime 395 mõjuga intsidenti, mis on viimase poole aasta keskmisest veidi madalam näitaja.
- Mais esines tõrkeid autentimisteenuste kasutamisel ja ühistranspordi piletimüügi-süsteemide töös.
- Läbisime edukalt Eesti infoturbestandardi põhiauditi. Aitasime tagada e-valimiste turvalisust.
- Jätkusid sõjategevusega seotud küberründed. Helsingi linnavalitsuse haridusosakonda tabas küberrünnak. Ühendkuningriigi kaitseministeeriumi andmed lekkisid.



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

Mais esines mitmel korral tõrkeid autentimisteenuste kasutamisel. 10. mail ajavahemikul 14.00 kuni 22.30 ei toimunud Smart-ID registreerimine alaealistele. 14. mail ennelõunal oli umbes tunni jooksul SEB teenuste kasutamisel häireid Smart-ID ja ka Mobiil-ID töös, viimane tõrkus tunnikese ka 15. mai hommikul. Taas oli probleeme 18. mai öösel, kui toimus lühiajaline katkestus Tele2 Mobiil-ID teenustes. CERT-EE'le ei ole nimetatud katkestuste põhjused seni teada. 20. mail tõrkusid nii Telia kui ka Elisa Mobiil-ID teenused. Telia Mobiil-ID teenuse töös oli häireid ajavahemikul 8.01 kuni 9.55 ning nende põhjuseks oli administreerimisviga. Samal päeval ajavahemikul 13.07 kuni 13.26 tekkis katkestus Elisa Mobiil-ID teenuses, selle põhjustas seadme viga.

2. mai hommikul tabas Ida-Tallinna Keskhaigla Ravi tänava ja Magdaleena üksusi elektrikatkestus. Haigla lülitus üle generaatoritele,

millest üks ei toiminud ootuspäraselt ja selle tulemusel jäi osa Ravi tänaval asuvatest osakondadest vooluta. Nende hulgas olid ka üks serveriruum ja peamine sidesõlm. Intsidendi tõttu oli Ida-Tallinna Keskhaigla patsiendiportaal iPatsient neli tundi kättesaamatu.

Paaril korral esines probleeme ühistranspordi piletimüügisüsteemidega. 7. mail ajavahemikul 6.30 kuni 7.34 ei olnud Elroni piletimüügisüsteem elron.pilet.ee kättesaadav. Ridango sõnul ei olnud katkestuse põhjuseks rünnak, vaid riistvaraline tõrge. Kaugbussiliinidele pileтите müümiseks kasutatav veebileht tpilet.ee ei olnud kättesaadav 25.mail ajavahemikul 2.00 kuni 9.07. Katkestuse põhjustas tehniline tõrge tarkvaras.

14. mail ajavahemikul 20.50 kuni 21.35 **polnud võimalik Elisa TV kaudu vaadata ETV reaajas pilti.** Katkestuse põhjustas DRM (Digital

rights management) seadme rike.

24. mail ajavahemikul 20.13 kuni 22.10 oli tõrkeid tervisekassa pakutavates Digiretsepti ja kindlustatuse kontrolli teenuses. Need taastusid pärast rakenduse taaskäivitust, kuid intsidendi tekkimise põhjusest ei ole CERT-EE meeskonda seni informeeritud.

Endiselt levivad erinevate kullerifirmade nimel saadetud õngitsussõnumid. Viimasel ajal oleme rohkem näinud sõnumeid, kus väidetakse, et pakki ei saa kohale toimetada puuduva või vale aadressi tõttu. Kasutaja suunatakse seejärel õngitsuslehele oma pangakaardi-andmeid sisestama. Sel moel õnnestus Eesti inimestelt maikuu jooksul välja petta erinevaid summasid alates paarikümnest kuni mitme tuhande euron. Soovitame sellist sõnumit saades vähimagi kahtluse korral kullerifirmasse helistada ja üle kontrollida, kas tegemist on õige sõnumiga.



Tegevused küberturvalisuse parandamisel Eestis

Aprilli lõpus läbis RIA edukalt uue Eesti infoturbestandardi (E-ITS) rakendamise põhiauditi, mis kinnitas, et ameti tegevuste kaitseks vajalikud infoturbemeetmed on meil edukalt rakendatud. E-ITS koostati RIA tellimusel mitme aasta vältel ning seda peavad järgima kõik avalikke ülesandeid täitvad organisatsioonid. RIA alustas ise E-ITSi rakendamisega 2022. aasta kevadel ja tegevustele kulus enne auditi ligikaudu poolteist aastat. E-ITSi rakendamine on sarnaselt infoturbe tagamisele järjepidev tegevus, sest muutuvad nii organisatsiooni protsessid, varad kui küberriskid. Lisaks uueneb igal sügisel ka infoturbestandard. Enda kogemust infoturbestandardi järgimisel ja rakendamisel on RIA jaganud nii teiste E-ITSi rakendajatega, kellelt saadi häid mõtteid, kui ka rahvusvaheliste partneritega. Ka edaspidi tutvustatakse valminud infoturbemeetmete rakendusplaani kõigile, kes soovivad meie kogemusest õppida.

16. mail toimus igakuine üritus RIA CyberMeetUp. Olukorrast küberruumis tegi ülevaate Peeter Marvet (PPA), Talis Pähn (CR14) rääkis avatud küberharjutusväljast (Open Cyber Range) ning Tiina Pau (RIA) tutvustas noorte suvelaagrit CyberWizards 2024. Lisaks tegid ettekanded ka külalised välismaalt – Daniela Bularda (ECCC, Rumeenia) rääkis rahvusvahelisest vaates küberturvalisuse valdkonna arengu toetamisest ja Antonin Dufka ning Jan Kvapil (Masaryk ülikool, Tšehhi) lävikrüptograafia platvormist MeeSign. Nii seda kui ka eelmisi üritusi saab järele RIA [veebilehelt](#).

Oleme juba pikemat aega teinud ettevalmistusi, et tagada e-hääletamise valmisolek, turvalisus ja tehniline tugi. Euroopa Parlamendi valimised toimuvad juba 9.juunil. E-hääletamine algas 3. juunil kell 9.00 ja kestab ööpäevaringselt kuni 8. juunil kell 20.00. Lisaks korraldame ka üleriigilise kampaaniat, mis kutsub

inimesi üles turvaliselt hääletama, sealhulgas oma e-häält nutiseadmega kontrollima. Vaata rohkem infot [siit](#).

Käisime taskuhäälingus „Olukorrast digiriigis“ rääkimas e-valimistest.

Valimiste infosüsteemide arenduse osakonnajuhataja Alo Einla tegi ülevaate RIA panusest valimiste korraldamisel, muu hulgas tuli juttu ka e-valimiste turvalisusest. Podcastist saab teada, miks saab e-hääletamist usaldada, kui mitu kontrollkihti on süsteemil peal ja millal võiksime saada valida oma mobiiltelefonide kaudu. Kuula podcasti [siit](#).

Tellisime Tartu Ülikoolilt uuringu, mis aitab Eesti ettevõtetel tootmist turvaliselt automatiseerida. Tartu Ülikooli teadlased uurisid Eesti tööstusettevõtetes tootmise automatiseerimisega kaasnevaid riske ja nende maandamise võimalusi. Uuringuga saad tutvuda [siin](#).



Rahvusvaheline keskkond

Ka mais jätkusid Venemaa sõjategevusega seotud küberründed.

CERT-UA [teatas](#)

Ukraina sõjaväelaste nutitelefonide ja teiste mobiilseadmete vastu saagenenud rünnakutest, mille taga on Vene sõjaväeluurega GRU seotud häkkerid. Rünnakutes matkiti populaarseid rakendusi nagu Kropyva, mis tegelikult sisaldasid nuhkvara. Pahavara levitati ka sõnumirakenduste Signal ja Telegram kaudu. Ründajad reageerisid kiiresti kaitsemeetmetele ja otsisid viise neist möödaminemiseks.

2. mail teatas Helsingi linnavalitsus, et nende haridusosakonda on tabanud küberrünnak ja ulatuslik andmeleke.

Leke avastati paar päeva varem, 30. aprillil. Ründajad kasutasid tõenäoliselt ära kriitilist turvanõrkust kaugtöölaua haldusliideses ning neil õnnestus toime panna suuremahuline andmevargus. Andmete täpne koosseis on veel selgitamisel, kuid kindlasti oli nende hulgas tuhandete laste ja noorte isikuandmed,

sealhulgas tundlikud terviseandmed ning samuti nende täiskasvanute andmed, kes olid viimastel aastatel kasutanud linna pakutavaid täiendõppevõimalusi.

Mai esimesel nädalal sai teatavaks, et UK kaitseministeeriumi

kasutatava palgaarvestustarkvara kaudu lekkisid rohkem kui 225 000

Ühendkuningriigi kaitseväge

tegevteenistuja, veterani ja reservisti isikuandmed. Andmete seas olid näiteks nimed ja pangakonto andmed. BBC andmetel on palgaarvestustarkvara pakkuja Shared Services Connected Ltd ning antud juhtum toob taaskord esile vajaduse paremini maandada väliste teenusepakujatega kaasnevaid riske, eriti kaitsesektoris.

Euroopa Politseiameti Europol kinnitas, et nende EPE (Europol Platform for Experts) portaali kompromiteeriti ja sellega seotud andmeleket uuritakse.

Ründajate sõnul said nad Europolist süsteemidest ametkondlikuks kasutuseks mõeldud dokumente, mis sisaldavad salajast infot. EPE on online-platvorm, kus politseiametnikud jagavad teadmisi, parimaid praktikaid ja mitteisikustatud andmeid kiritegevuse kohta.

Blackbasta lunavararühmitus avalikustas oma TOR-lehel ründe USA ühe suurima kütusetarnija Atlas Oil vastu. Rühmitus väitis olevat muuhulgas varastanud 730 gigabaiti andmeid, mille hulgas on peamiselt ettevõtte töötajate isikuandmed, mõned näited on tumeveebis ka avalikustatud. Ettevõtte ise pole siiani rünnet kinnitanud.

Nädal enne Euroopa Parlamendi valimisi Saksamaal tabas küberrünnak Ursula von der Leyeni konservatiivset erakonda (CDU). Erakonna esindaja ei avaldanud detaile ründe kohta, ent kinnitas, et nad olid sunnitud osa IT-süsteemidest võrgust eemaldama.