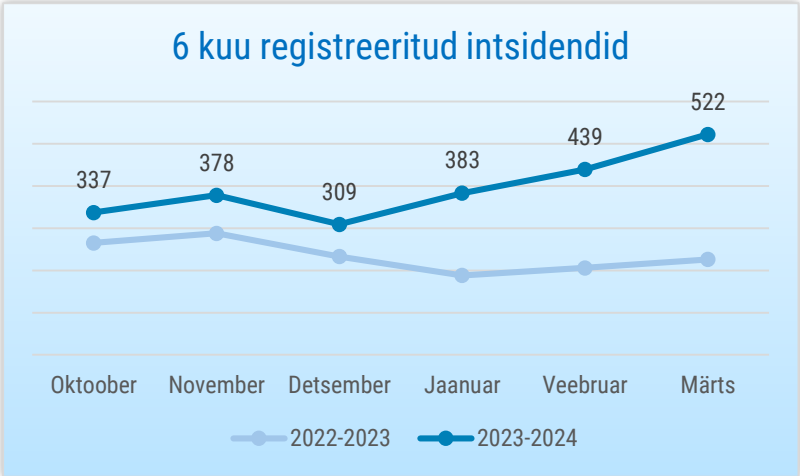
RIIGI INFOSÜSTEEMI AMET

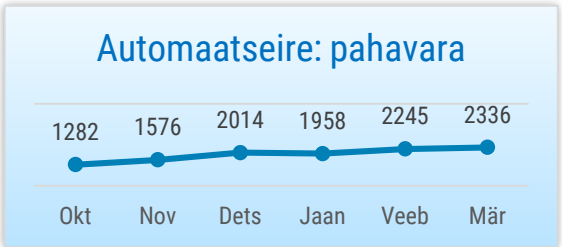
OLUKORD KÜBERRUUMIS

MÄRTS 2024

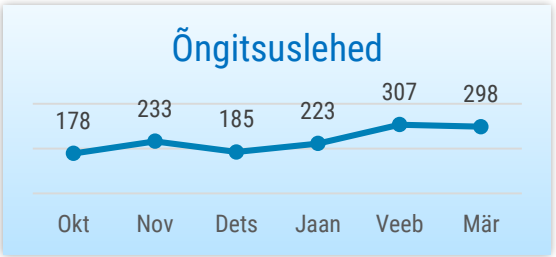
- Märtsis registreerisime **522 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja.
- 1. märtsil tabas sularahakäitlemisega tegelevat ettevõtet Hansab **küberintsident**. 9. märtsil viidi läbi **suurima mahuga ummistusrünne** Eesti avaliku sektori veebilehtede vastu.
- Tellisime **tehisintellekti ja masinõppe tehnoloogia riskide** ning nende leevendamise võimaluste uuringu. Avaldasime **küberturvalisuse aastaraamatu ingliskeelse** versiooni.
- Jätkusid sõjategevusega seotud küberründed. **Microsoft** tegeleb endiselt jaanuarikuus toimunud küberintsidendi tagajärgedega. **Prantsuse tööamet** sattus küberründe alla.



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

1.märtsil tabas küberrünnak sularahakäitlemise ja makseterminalidega tegelevat ettevõtet Hansab. Hansab täidab vastavalt pankade tellimustele Eestis Swedbanki, Luminori ja LHV pankade sularahaautomaate. Küberründe tõttu oli häiritud Hansabi mõnede IT-süsteemide töö, kuid kommertspankade teenused toimisid. Paljude teenuste tagamisel mindi üle nn käsijuhtimisele. Ettevõtte ühendas oma süsteemid välisvõrgust lahti kohe peale intsidendist teadasaamist ja asus välja selgitama täpsemaid asjaolusid.

9. märtsil viidi läbi suurima mahuga ummistusrünne Eesti avaliku sektori veebilehtede vastu. Sihtmärkideks olid veebilehed ttja.ee, airport.ee, mkm.ee, ria.ee, riigikogu.ee, siseministeerium.ee,transpordiamet.ee, transport.tallinn.ee, eesti.ee, id.ee, estonia.ee, president.ee, emta.ee, politsei.ee ja just.ee. Veidi rohkem kui nelja tunni jooksul tehti ligi kolm miljardit pahaloomulist päringut. Eelmine rekordiline rünne avaliku sektori vastu toimus 2022. aasta augustis, kui tehti 425 miljonit päringut veebilehe id.ee vastu. Kolme veebilehe töös oli kuni 15-minutilisi katkestusi, teistel rünnakutel polnud mõju. 10. märtsil järgnesid rünnakud CERT-EE lehtede report.cert.ee ja cuckoo.cert.ee vastu, mille töös oli paari tunni jooksul katkestusi.

18. märtsil ajavahemikul 00.06 kuni 9.26 **ei toiminud riiklikus autentimisteenuses TARA ega riigi SSO-teenuses (single-sign-on) ID-kaardiga autentimine.** Katkestuse põhjuseks oli sertifikaadi aegumine.

Kolmel korral esines häireid eesti.ee portaali töös. 14. märtsi õhtul ajavahemikul 18.57 kuni 19.11 esinenud tõrgete põhjuseks oli muudatuste käigus tehtud seadistusviga. 21. märtsil ei toiminud ligi kahe ja poole tunni jooksul osa riigiportaali eesti.ee teenustest. Katkestuse põhjuseks oli x-tee turvaserverite sertifikaatide vahetuse käigus tekkinud viga. 26. märtsil esines 2 tunni jooksul tõrkeid riigiportaali sisse logimisel, mille põhjust ei ole veel teada.

4. aprillil avalikustati andmeleke, mis puudutab Apotheka, Apotheka Beauty ja Pet City kliendikaardi omanikke. Jaanuaris sattus kurjategija(te) kätte andmebaasi varukoopia, kus hoiti andmeid aastatest 2014-2020. Lekkisid ligi 700 000 Apotheka, Apotheka Beauty ja PetCity kliendikaardi omaniku isikukoodi, üle 400 000 e-posti aadressi, ligi 60 000 koduaadressi ja umbes 30 000 telefoninumbrit. Samuti lekkisid 43 miljoni ostu andmed, kus on näha käsimüügiravimid ja muud apteegikaubad, nagu plaastrid või valuvaigistid. Ostetud retseptiravimite andmeid kurjategijad kätte ei saanud.

Tegevused küberturvalisuse parandamisel Eestis

CERT-EE juht Veikko Raasuke rääkis Geeniuse portaalile antud intervjuus sellest, et milline olukord on Eesti kübermaastikul ja milliste ülesannetega tema meeskond igapäevaselt tegeleb. Lisaks tuli juttu RIA poolt arendatavatest kaitsemeetmetest ja CERTi tulevikuplaanidest. Veikko annab muuhulgas nõu, kuidas toimida lunavararünde puhul ja tõdeb, et ründed lähevad aina sihitumaks. Intervjuus räägitakse ka programmist, millega Eesti digiriigist leitud turvanõrkuste avastamise ning sellest teavitamise eest makstakse headele häkkeritele raha.

Veebruaris avaldatud RIA küberturvalisuse aastaraamat on nüüd ka inglise keelde tõlgitud ja seda saad lugeda siit.

RIA Teaduse ja arenduse koordineerimisosakond tellis tehisintellekti ja masinõppe tehnoloogia riskide ning nende leevendamise võimaluste uuringu, mis võtab kokku erinevad AI/ML mudelid ja pakub välja, milliste küberturvalisuse riskidega peaks arvestama. Uuring on mõeldud kõigile, kes kavatsevad kasutusele võtta tehisintellekti ja masinõppe tehnoloogiaid. Cybernetica ASi analüüs kirjeldab tehisintellekti süsteemide hetkeseisu ja levitusmudeleid, aga ka kaasnevaid küberriske ja nende leevendusmeetmeid. Muu hulgas annab see ettevõtetele ka ülevaate 2024. aastal kehtivast õigusruumist tehisintellekti valdkonnas, sealhulgas Euroopa Liidu algatustest ja ettepanekutest.

21. märtsil toimus taas RIA CyberMeetUp. Aleksi Rantaniemi Soome riiklikust küberkaitsekeskusest (NCSC-FI) andis ülevaate Soomet varitsevatest küberohtudest. Laiema vaate regiooni ohtudest ja olukorrast andis Põhja-Euroopa Küberturvalisuse Ühenduse (NECC) juhatuse esimees Juha Remes. Rubriigis “Olukorrast küberruumis” astus lavale Austraalia kriitilise tehnoloogia ja kübervaldkonna saadik Brendan Dowling. Ettekannetele pani punkti TAKi ekspert-koordinaator Hendrik Pillmann, kes tutvustas RIA tellitud ning Cybernetica koostatud tehisintellekti ja masinõppe tehnoloogia riskide ja võimaluste uuringu tulemusi. Ettekandeid saab jälgida Facebookist otseülekandena või vaadata neid hiljem järele RIA veebilehelt.

Käisime Vikerraadio „Huvitaja“ saates rääkimas ummistusrünnetest – mida need endast kujutavad ja kuidas on võimalik kaitsta enda seadmeid, et neid küberkurjategijate poolt ära ei kasutataks.

Rahvusvaheline keskkond

Ukraina sõjaväeluure (GUR) teatel pääsesid nende häkkerid Vene kaitseministeeriumi serveritesse ning said sealt tundlikku infot – struktuuriüksuste ja personali kohta, Vene eriteenistuste korraldusi, juhiseid ja muid dokumente ning infot kasutatavate krüpteerimistarkvarade ning infoturbemeetmete kohta. Ukraina pressiteates on eraldi välja toodud Vene asekaitseminister Timur Vadimovich Ivanov, kelle dokumentidele õnnestus samuti ligi pääseda ning kellel olevat olnud suur roll operatsiooni õnnestumises.

Saksa kaitseministeerium oli sunnitud kinnitama, et märtsi alguses Vene meedias täismahus avaldatud vestlus Saksa õhuväe ülema ja teiste kõrgete ohvitseride vahel, kus arutati Ukraina abistamist, on ehtne. Sakslased ei kasutanud turvalist sidekanalit, vaid Cisco WebEx platvormi ning salvestuse edastasid meediale Vene eriteenistused. Saksa kaitseministri Boris Pistoriuse sõnul olevat kõne pealtkuulamine õnnestunud seetõttu, et üks ohvitser kasutas sisselogimiseks Singapuri hotellitoa ebaturvalist ühendust. Kuna Saksa ohvitserid arutasid ka brittide ja prantslaste relvatarneid Ukrainale ning kohapeal ukrainlastele pakutavat toetust, olid lekkeskandaalist häiritud ka Ühendkuningriigid ja Prantsusmaa.

Vene välisluurega seotud rühmitus APT29 on sihikule võtnud Saksamaa erakonnad. Selline fookuse muutus on tähelepanuväärne, kuna seni on ohustaja keskendunud peamistelt saatkondadele. Erakondade esindajatele saadetakse õngitsusmeile eesmärgiga nakatada süsteemid WineLoader pahavaraga, mis võimaldab häkkeritele kaugligipääsu loomist. Peibutisena on kasutatud Kristlik-Demokraatliku Liiduga seotud materjale.

Microsoft tegeleb endiselt jaanuaris toimunud ründe tagajärgedega. 8. märtsil avaldatud postitusest selgub, et rünnak oli seni arvatust tõsisem ning kestab siiani. Häkkerite rühmitus olevat ligi pääsenud ka Microsofti koodihoidlasse, sisemistesse süsteemidesse ning mõnedesse meilivestlustesse Microsofti ja klientide vahel, mistõttu võivad ohus olla ka ettevõtte mõned kliendid. Microsofti teatel kestab ründe ja selle mõju uurimine ning taolised väga võimekad riiklikud ohustajad on tinginud vajaduse ettevõttel veelgi rohkem investeerida küberturbesse.

Märtsi keskel teatas Prantsuse tööamet France Travail, et langes veebruaris küberründe ja selle käigus andmevarguse ohvriks. Andmevargus võib puudutada kuni 43 miljonit inimest ehk rohkem kui kahte kolmandikku Prantsusmaa elanikkonnast. Lekkinud on nimed, sotsiaalkindlustusnumbrid, aadressid. Andmevarguse tegelik maht ja ründe üksikasjad on uurimisel, praegu pole teada, kas tegu oli lunavararünde gа.