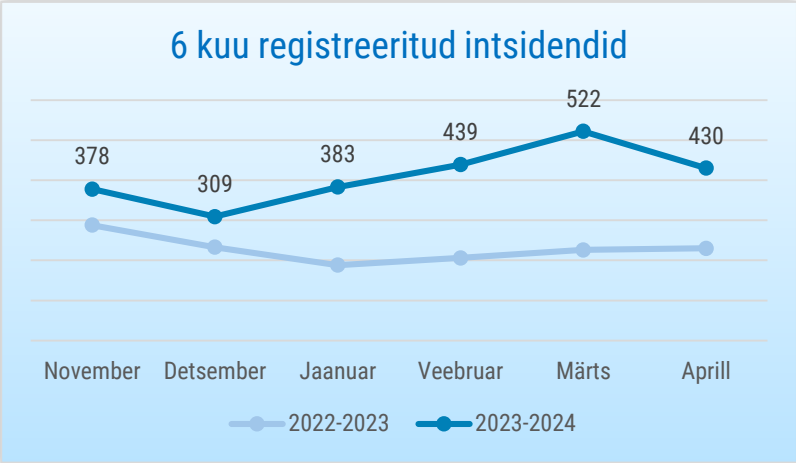
RIIGI INFOSÜSTEEMI AMET

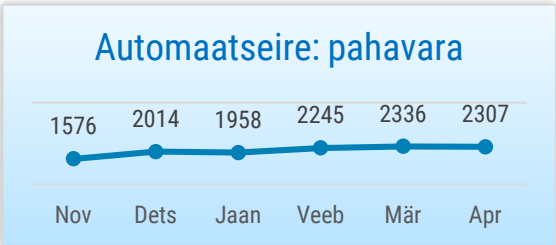
OLUKORD KÜBERRUUMIS

APRILL 2024

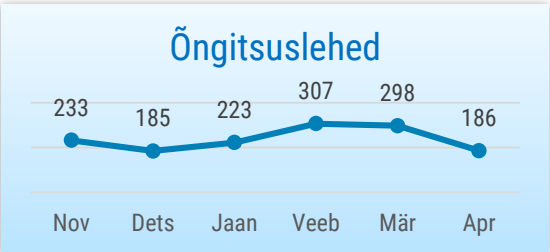
- Aprillis **registreerisime 430 mõjuga intsidenti**, mis on viimase poole aasta keskmisest veidi kõrgem näitaja.
- Aprillis esines tõrkeid nii **eksamite Infosüsteemi** kasutamisel kui **digiallkirjastamisel**.
- Aprillis viisime läbi E-**ITS kaasamisseminarid**, kus jagasime rakendajatele praktilisi nõuandeid. RIA ja Tehnopoli **küberkiirendis** startis kaheksa iduettevõtet.
- Jätkusid sõjategevusega seotud küberründed. USA küberagentuur **CISA langes küberründe** ohvriks. Rahvusvahelise politseioperatsiooni tulemusel suleti üks suurimaid **õngitsuskelmide kasutatavaid platvorme.**



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

Aprillis oli mitmel korral probleeme eksamite infosüsteemiga. 6. aprillil toimusid Tallinna ja Harjumaa riigigümnaasiumides sisseastumiskatsed, kuid tõrgete tõttu eksamite infosüsteemise (EIS) katkestati testide tegemine ja nende tulemusi ei arvestata. Haridusministeeriumi riigikoolide pidamise juhi Raivo Trummali sõnul oli tõrgete põhjuseks süsteemi ülekoormus. 10. aprillil sai CERT-EE lisaks teavituse, et eksamite infosüsteemi GitHubi lehel on avalikult kättesaadavad 539 inimese isikuandmed. Need lisati sinna seitse aastat varem ja olid märgitud testandmetena, kuid lähemal uurimisel selgus, et tegu oli päris isikuandmetega. Praeguseks on andmed eemaldatud ning haridus- ja noorteamet kinnitanud, et teavitab rikkumisest andmekaitse inspektsiooni.

Sel kuul oli ka mitmel korral tõrkeid digiallkirjastamisega. 12. aprillil ajavahemikul 9.53 kuni 10.57 ei toiminud digiallkirjastamine DigiDoc rakenduses. Katkestuse põhjustas SK ID Solutionsi poolt tehtud sertifikaatide uuendamine. 15. aprill alates 20.32 kuni 16. aprill 8.30 oli tõrkeid DigiDoc rakenduse uuendamisega Windowsi seadmetel. Kasutajatele, kes üritasid sel ajavahemikul rakendust uuendada, kuvati veateade ja Microsoft Defender ei lubanud tarkvara käivitada. Intsidendi põhjustas inimlik eksimus: installer.id.ee lehele laeti üles fail, millel puudus allkiri.

9. aprilli pärastlõunal polnud umbes nelja tunni jooksul kättesaadav andmejälgija – teenus, mille abil saab riigiportaalis eesti.ee vaadata oma andmete kohta tehtud päringuid. Katkestuse põhjustas rakenduse uuendamise käigus tekkinud viga.

26. aprillil ajavahemikul 11.40 kuni 16.33 toimus üleriigiline teenusekatkestus perearstide infosüsteemi töös. Katkestuse tõttu oli häiritud retseptide väljastamine, haiguslehtede alustamine ja lõpetamine ning vastuvõtuaja registreerimine. Katkestuse põhjustas Medisoft AS peaserveri voolukatkestus.

Aprillis nägime ka mõjuga ummistusründeid. 20. ja 21. aprillil sooritati kolm teenusetõkestusrünnet Tallinna Sadama veebilehe ts.ee vastu. Selle töös oli rünnakute tõttu mõneminutilisi katkestusi. 24. aprillil ajavahemikus 9.13 kuni 9.57 ning 10.47 kuni 11.45 ei olnud Tallinna Tööstushariduskeskuse internetiühendus kasutatav. Katkestuse põhjustas küberrünne, millega koormati üle kooli internetiühenduseks kasutatav juurdepääsukanal.

Tegevused küberturvalisuse parandamisel Eestis

Aprillis viisime läbi järjekordsed E-ITS kaasamisseminarid, kus jagame E-ITSi rakendajatele praktilisi nõuandeid ja soovitusi, mis lihtsustavad standardi sisust arusaamist ja standardi rakendamist. Esinejate hulgas on ka Eesti infoturbestandardi rakendajad, kes räägivad oma kogemust selle rakendamisel. Kui soovid ka osaleda, siis hoia silm peal E-ITS portaalis oleval sündmuste infol.

18. aprillil toimus ka traditsiooniks saanud RIA CyberMeetUp. Sel korral said sõna kolonelleitnant Urmet Tomp (NATO CCDCOE) ja Dr Adrian Venables (Taltech), kes andsid eksklusiivse ülevaate peatselt toimuvast rahvusvahelisest küberkaitseõppusest Locked Shields, mida korraldab NATO Küberkaitse Kompetentsikeskus. Arne Ansper (Cybernetica AS) tutvustas postkvantkrüptograafiale pühendatud konverentsi ning teema olulisust. Märt Hiietamm (RIA) tegi ülevaate olukorrast küberruumis. Nii seda kui ka eelmisi üritusi saab järele RIA veebilehelt.

Tehnopoli ja RIA küberkiirendis startis kaheksa iduettevõtet. Küberkiirendi eesmärk on tuua küberturvalisuse valdkonda uusi tooteid ja ettevõtteid, mis looksid kasu ka teistele ettevõtetele. Kiirendisse pääsenud tiimid saavad oma ideede arendamiseks tipptasemel nõu ja kuni 48 000 eurot toetust. Täpsemat infot leiad küberkiirendi teises vooru ja selles osalevate ettevõtete kohta siit.

Viisime läbi küberturvalisuse ja -hügieeni koolituse Valgamaa raamatukogude töötajatele. Rääkisime, kuidas arvutit ja internetti turvalisemalt kasutada ning millised petuskeemid ning õngitsused meid ohustavad.

Käisime Raadio 2 saates „R2 päev“ rääkimas küberrünnakute suurenevast hulgast. Kaisa Vooremäe RIA analüüsi- ja ennetusosakonnast selgitas, et milliseid õngitsusi ja pettusi proovivad kelmid internetis läbi viia ning kuidas neid ära tunda.

RIA peadirektori asetäitja Gert Auväärt ning Info- ja Kommunikatsioonitehnoloogia Liidu juhatuse liige Lauri Almann arutlesid MKM-i veebisaates "Strateegia Akadeemia" küberturvalisuse valdkonna hetkeolukorrast, peamistest väljakutsetest nii riigis kui ka erasektoris ning valdkonna strateegilistest suundumustest. Saate vaatajad saavad teada, millise hinde annavad külalised Eesti küberturvalisuse olukorrale ning kas riik, aga ka iga kodanik võib ikka rahuliku südamega öösel magada.

Rahvusvaheline keskkond

Ka aprillis jätkusid sõjategevusega seotud küberründed. Väidetavalt õnnestus Ukraina julgeoleku-teenistusega (SBU) seotud rühmitusel Blackjack edukalt rünnata ja hävitada andmekeskus, mida kasutab Vene sõjatööstus ja energia- ning telekommunikatsioonisektor. Andmekeskus kuulus pilveteenusepakkujale OwenCloud.ru, mida kasutavad muuhulgas Gazprom, Rosneft. Rostelecom ning ka mitmed metallurgiaettevõtted. Ründe käigus hävitati 300 terabaiti andmeid ning see olevat vastutasu Ukraina andmekeskuse ründe eest jaanuaris. Lisaks on sama rühmitus nüüd sihikule võtnud Moskva kanalisatsioon-isüsteemi haldava ettevõtte Moskollector, mille töö olevat seetõttu häiritud.

CERT-UA andmetel viis Venemaa häkkerirühmitus 2024. aasta märtsis läbi rünnakud umbes 20 Ukraina energia-, vee- ja küttetarnija info- ja sidesüsteemide häirimiseks. CERT-UA reageeris küberrünnakutele, eemaldades pahavara ning tugevdades turvameetmeid.

Jaanuaris langes USA küberturbeagentuur CISA küberründe ohvriks, mille käigus õnnestus kurjategijatel kompromiteerida kaks CISA infosüsteemi. Rünne viidi läbi Ivanti turvanõrkuse kaudu, mida kuritarvitati kogu maailmas (sh Eestis) ning mille kohta andis agentuur veebruaris välja ka hoiatuse. Nüüd aprillis kinnitas CISA esindaja, et andmevargust rünnete käigus ei ole tuvastatud. Samas oli üks rünnatud infosüsteem CISA hallatav keemilise julgeoleku hindamise portaal ning sealtkaudu võis kurjategijatele siiski teatavaks saada tundlikke andmeid.

Rahvusvahelise politseioperatsiooni tulemusel, kus osales ka Eesti, suleti üks suurimaid õngitsuskelmide kasutatavaid platvorme LabHost ja üle maailma peeti kinni 37 kahtlustatavat. Ligikaudu kümme neist tegid õngitsuspettusi Eesti suunal, peamiselt Eesti pankade keskkondi imiteerides. Rahvusvahelise uurimise käigus tuvastati vähemalt 66 000 veebilehte, mida ligi 10 000 kurjategijat kasutas kannatanute andmete või raha välja petmiseks. Üle maailma sai selle platvormi kaudu pettustes kannatada üle miljoni inimese.

Cannes'is asuv haigla teatas 16. aprillil, et on langenud küberründe ohvriks ja seetõttu sunnitud minema ajutiselt üle paberile ja pliiatsile ning lükkama edasi pea kolmandiku plaanilisi operatsioone. Ründe üksikasju avaldatud ei ole, samuti ei ole seni ükski lunavararühmitus võtnud vastutust ega kuuldavasti esitanud ka lunarahanõuet. Haigla märgib oma teadaandes, et oli just mõni kuu tagasi teinud õppuse taolise intsidendiga toimetulekuks, mistõttu nende üleminek tavapärasest erinevale režiimile läks võrdlemisi sujuvalt.