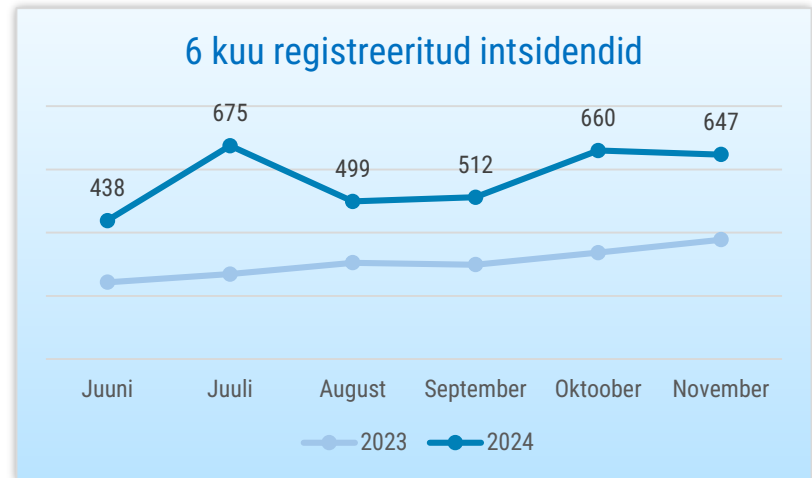




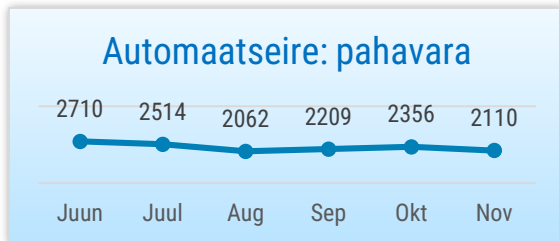
OLUKORD KÜBERRUUMIS

NOVEMBER 2024

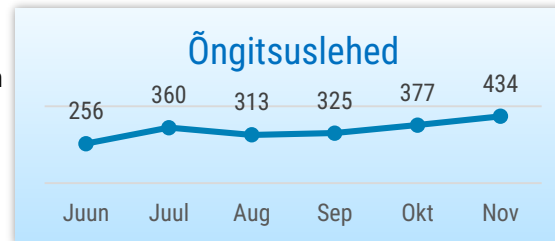
- Novembris registreerisime **647 mõjuga intsidenti**, mis on viimase poole aasta keskmisest kõrgem näitaja.
- Novembris tabas **hambaravikliinikut lunavararünnak** ja neli ettevõtet langes **arvepettuse** ohvriks.
- Viisime läbi **küberturvalisuse linnalaagri kodutütardele** ja alustasime **E-ITS töötubade** sarjaga. Kirjutasime RIA blogis AI rakenduste kasutamisest ründekoodi kirjutamisel ja turvaliselt e-poodides ostlemisest.
- Küberrünnak tabas nii **Washingtoni kohtute** infosüsteeme kui ka **Lõuna-Korea** valitsuse ja erasektoriga seotud veebilehti.



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

Novembris registreerisime taas mitmeid olulisi teenuseid mõjutanud intsidente.

1. novembril tabas üht hambaravikliinikut lunavararünnak, mille käigus krüpteeriti serveris olnud andmed. Kliinikul ei olnud toimivat varukoopiat ja andmeid taastada ei olnud võimalik. CERT-EE meeskond viis läbi analüüsi ning selgitas välja, et rünnak sai alguse avatud kaugtöölaua (RDP) ühenduse kaudu, mille parool oli liiga lihtne. Soovitame juhtumi valguses vaadata üle nii kaugtöölaua protokollid ligipääsud kui ka paroolide poliitika, et sarnast olukorda vältida.

Alates 3. novembrist kuni 5. novembrini esinesid torked Pärnu haigla infosüsteemis, mida kasutatakse andmevahetuseks (nt röntgenpiltide edastamiseks). Probleeme põhjustas üks moodul, mille taaskäivitamine aitas ajutiselt süsteemi tööd stabiliseerida, kuid peagi viga kordus. Intsidendi lahendamiseks tuli tarkvaras teha parandus. Torked häirisid haigla

tavapäraseid tööprotsesse, täpsemalt oli häiritud radioloogiliste uuringute tellimine.

17. novembril tabas ummistusrünne Tarbijakaitse ja Tehnilise Järelevalve Ameti veebilehte tjja.ee. Selle kõrvalmõjuna oli seitsme minuti jooksul katkestusi veel 18 veebilehe töös, mida haldab RMIT: sh siseministerium.ee, kliimaministerium.ee, emta.ee, cert.ee ja ti.ee. Nii oktoobris kui ka novembris on aktiivselt rünnatud CERT-EE ja RIA nimeserverid, kuid üldjuhul neil rünnatel mõju ei ole.

22. novembril ajavahemikul 10.16 kuni 10.56 ei toiminud ID-kaardiga allkirjastamine ega autentimine. Katkestuse põhjustas tõrge SK ID Solutionsi pakutavas kehtivuskinnitusteenuses, mis võimaldab teha reaajas päringuid sertifikaatide staatuse kohta. Katkestuse põhjustas hoolduse käigus tehtud seadistusviga.

Novembris teavitati meid neljast õnnestunud arvepettusest.

elja intsidendi peale kokku kaotasid Eesti ettevõtted ligi 300 000 eurot. Arvepettuse käigus saadetakse asutusele või ettevõttele tema koostööpartneri nimel arve, milles on vaid pangakonto ära muudetud. Petturid on selleks hetkeks juba mõnda aega jälginud kahe osapoole omavahelist suhtlust ja sekkuvad sobival hetkel, saates enda koostatud arve. Tihti peale ei ärata see kahtlust ja arve makstakse ilma pikemalt mõtlemata ära. Pettus tuleb tavaliselt välja siis, kui koostööpartner hakkab uurima, et kuhu oodatud makse jääb. Sel kuul toimunud esimeses juhtumis olidki petturid kahe osapoole omavahelist suhtlust pikemat aega jälginud. Teises aga saadeti muudetud kontonumbriga arve ettevõtte üldmeilile tasumiseks. Loe RIA [blogist](#) ka soovitusi, et mida tuleks teha arvepettuse ohvriks langemise vältimiseks.



Tegevused küberturvalisuse parandamisel Eestis

Novembri keskpaigas kogunesid Harju, Rapla ja Tallinna kodutütred küberturvalisuse linnalaagrisse, kus tutvustati küberturbe ekspertide tööd ja eetilist häkkimist ning õpiti end küberohtude eest kaitsma. Laagrit alustati küberhügieeni teemadega ning liiguti järk-järgult edasi tehnilisemate küsimuste juurde. Muu hulgas räägiti turvalistest paroolidest, uuriti failide metaandmeid ja testimise tööriista FlipperZero võimalusi, skaneeriti võrku ning tungiti ühe turvamata veebilehe administraatori vaatesse. Tegemist oli juba neljanda linnalaagriga, mis on toimunud RIA ja kodutütarde koostöös.

Kirjutasime RIA blogis, kuidas häkkerid on hakanud kasutama ründekoodi kirjutamiseks tehisintellekti (AI) rakendusi. See annab üha rohkem võimalusi tehniliselt madalama tasemega häkkeritele, kes võivad osavate päringutega luua siiski rünneteks sobiva pahavara. Tagantjärele on välja tulnud, et 2023.

aasta lõpus Eesti katlamajade ja pumbajaamade vastu korraldatud rünnakutes kasutati samuti tehisaru abil loodud koodi.

Seoses nn Musta Reedega ja ka pühadeperioodi lähenemisega jagasime blogis soovitusi, kuidas turvaliselt jõuluoste teha ja mitte pettuse ohvriks langeda. Ostlemisel tasub tähelepanu pöörata veebipoe sisule ning vajadusel selle osas tausta juurde uurida. Samuti tasub ettevaatlik olla maksesüsteemide kasutamisel ja oma andmete kergekäelise jagamise osas. Loe ka meie [blogist](#) viimasel ajal levinud arvepettusest ja tutvu soovitustega, kuidas mitte sarnase skeemi ohvriks sattuda.

Novembrikuus tulid ETV eetrisse uued osad saatesarjast „IT-vaatlik“. Teemadest olid vaatluse all küberkurjategijad, petukõned, andmete varundamine ja internetiostud. Kõik saated on vaadatavad [ERRi Arhiivis](#).

14. novembril toimus järjekordne RIA CyberMeetUp, mida saab järgi vaadata siin. Seekordne üritus toimus koostöös Eesti-Tšehhi ühisprojektiga [CHES Cyber-Security Excellence Hub](#). Õhtu jooksul esinesid ettekandega RITi, (ISC)² Estonia Chapteri, Masaryki Ülikooli ja Cybernetica esindajad. Järgmine CyberMeetUp toimub 11. detsembril. Lisainfo RIA [Facebooki](#) ja [LinkedIni](#) lehel vastava sündmuse all.

21. novembril leidis aset KOVidele, nende hallatavatele ja riigi haridusasutustele E-ITSi praktilisi rakendamismõimalusi tutvustava töötubade sarja avauüritus. Esimene töötuba oli suunatud asutuse juhtidele. Järgneval kolmel korral tutvustatakse äriprotsesside ja varade kaardistamist, rakendusplaani väljatöötamist (sh moodulite ja meetmete modelleerimine) ja E-ITSi alusel loodavate dokumentide koostamist. Kogu ürituste sarja on kaasatud 60 asutust, üle 180 osaleja ja 15 esinejat RIAst. Kõiki RIA sündmusi näed [siit](#).



Rahvusvaheline keskkond

Novembri alguses tabas küberrünnak Washingtoni kohtute infosüsteeme, mille tõttu oli kohtute töö osaliselt häiritud ning mitmed veebilehed ja teenused olid kättesaamatud.

Mõnedes kohtuhoonetes tuli ka istungeid edasi lükata. Infot selle kohta, kes võis olla ründe taga, ei ole avalikustatud ning kohtute esindaja sõnul ei ole põhjust arvata, et tegemist oli sihitud ründega.

FBI ja CISA uurimismenetlus kinnitab, et sügisel ilmsiks tulnud mitme USA telekomiettevõtte kompromiteerimise käigus õnnestus Hiina taustaga häkkeritel saada ligipääs mõnede USA valitsusametnike ja tipp-poliitikute seadmetesse, varastada neist andmeid ja jälgida vestlusi. Samuti olevat häkkerid varastanud infot, mis on seotud USA õiguskaitseorganite menetlustoimingutega. CISA ja FBI [ühisavalduse](#) kohaselt on see osa laiaulatuslikust küberluure-kampaaniast, mille taga on Hiina riikliku taustaga ohustajad.

Lõuna-Korea teatas novembris intensiivsetest ummistusrünnete lainetest valitsusega seotud veebilehtede ja erasektori vastu.

Rünnete taga on Kremli-meelsed häktivistid ja nende tegevus ajendatud Lõuna-Korea otsusest jälgida Põhja-Korea üksuste osalust Ukraina sõjas. Lõuna-Korea info kohaselt on rohkem kui 10 000 Põhja-Korea võitlejat saadetud Ukrainasse Venemaa eest sõdima, samuti osalevad nad sõjategevuses Kurskis. Infot on kinnitanud ka Ukraina ning Ameerika Ühendriigid. Lõuna-Korea presidendi kantselei teate kohaselt on Vene häktivistid ka varem Lõuna-Korea veebilehti rünnanud, ent seoses arengutega Ukrainas on see muutunud palju intensiivsemaks. Ehkki mõned veebilehed on rünnete tõttu olnud lühiajaliselt maas, on nende mõju üldiselt olnud väike.

Prantsusmaal õnnestus häkkeritel kompromiteerida MediBoard tarkvara

kliendikonto ning sealtkaudu varastada vähemalt ühe haigla patsientide terviseandmed.

MediBoardi pakkuv ettevõtte Softway Medical Group tunnistas konto kompromiteerimist, ent kinnitas, et see ei olnud seotud tarkvara turvanõrkuse ega ka seadistusveaga, vaid tõenäoliselt kliendikonto pääsuõiguste kuritarvitamisega. Intsidendi põhjuseks sai ilmsiks pärast seda, kui häkkerid panid müüki ühe haigla andmebaasi ligi 760 000 patsiendi kohta ning väitsid omavat MediBoard platvormi kaudu ligipääsu veel mitme teise haigla patsientide terviseandmetele, raviarvetele ning broneerimissüsteemile.

Kuu lõpus tabas Ühendkuningriigi mitmeid haiglaid haldavat sihtasutust küberrünnak, mistõttu tuli ära jätta plaanilisi vastuvõtte ja protseduure. Intsidendi ohjamiseks eemaldati osa IT-süsteeme võrgust ning mindi üle paberile ja pliitsile. Erakorralise meditsiini teenused jäid toimima.