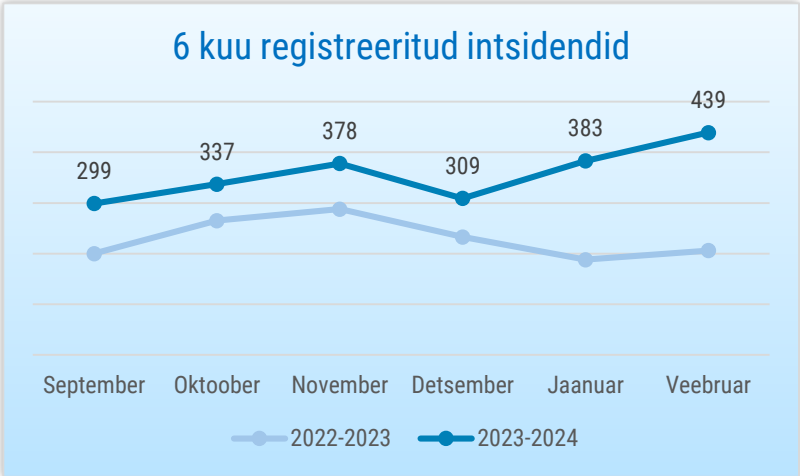
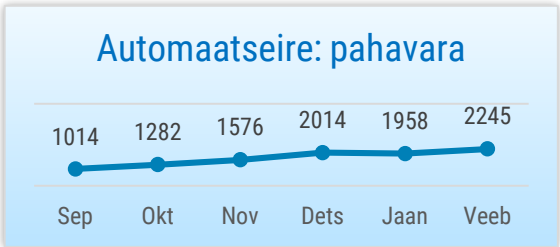
RIIGI INFOSÜSTEEMI AMET

OLUKORD KÜBERRUUMIS VEEBRUAR 2024

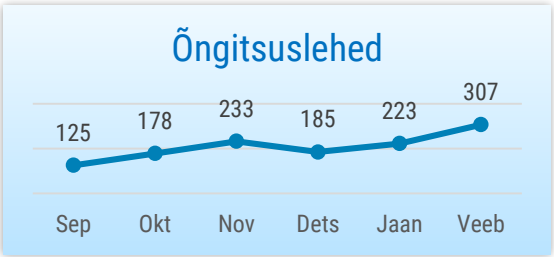
- Veebruaris registreerisime **439 mõjuga intsidenti**, mis on viimase poole aasta kõige kõrgem näitaja.
- Veebruaris tabasid mitmeid asutusi **küberintsidendid**. Lisaks saadeti ettevõtete nimel nii **õngitsus- kui ka pahavaraga kirju**.
- Avaldasime RIA **küberturvalisuse aastaraamatu**, milles võtame kokku eelmise aasta olulisemad küberintsidendid ja kirjeldame olukorda küberruumis.
- Jätkusid sõjategevusega seotud küberrünnad. **AnyDeski tootjat** tabas küberrünnak. Toimus mitu **tervishoiusektorit** mõjutavat intsidenti.



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

Veebruaris tabasid mitmeid asutusi küberintsidendid.

2. veebruaril teatas üks riigiasutus, et nende VPN-serverid on kompromiteeritud. Jaanuaris alanud rünnaku käigus kaardistati asutuse võrku ja võisid lekkida ka andmed. Praeguseks on kõik mõjutatud serverid suletud ja analüüsitakse rünnaku mõju. Rünnakuks kasutati Ivanti haavatavusi, mille kohta saab pikemalt lugeda siit.

Teine asutus uuendas failide majutuslahenduse tarkvara, kuid selle käigus tekkis viga ja süsteem tuli taastada varukoopiast. Taastamise käigus selgus, et varundus pole mõnda aega toiminud ning seetõttu pole võimalik kõiki andmeid taastada. Kui suur osa asutuse ja selle allasutuste andmetest kadunud on, ei ole veel selgunud.

10. veebruari hommikul ei olnud võimalik siseneda paljudesse Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) teenustesse, sealhulgas e-politseisse, kõnesalvestussüsteemi ega kaugtöö-lahendusse. Tõrgete põhjuseks oli rike SMITi tulemüüris.

16. veebruaril ei olnud umbes poole tunni jooksul kättesaadav Maksu- ja tolliameti tulude deklareerimise leht tuludeklaratsioon.emta.ee. Katkestus sattus just tuludeklaratsioonide esitamise perioodile ja selle põhjustas veebiserveri kettamahu täitumine.

22. veebruari ööl viis SK ID Solutions läbi korralisi hooldustöid. Selle käigus tekkis tõrge ning kehtivuskinnitusteenus andis ligi kümne tunni jooksul asutuse sertifikaatide (digitemplid, autentimis- ja krüpteerimissertifikaadid) kehtivuse kontrollimisel vastuseks “KEHTETU”. Seda juhul, kui kasutati SK vaba ligipääsuga kehtivuskinnitusteenust.

Veebruaris saadeti ettevõtete nimel nii õngitsus- kui ka pahavaraga kirju. 23. veebruari hommikul hakkasid paljude inimeste postkastidesse jõudma vigases eesti keeles kirjad, milles kutsuti üles domeeninime kehtivust pikendama. Kirjad saadeti näiliselt Zone Media OÜ nimel, neile oli lisatud võltsitud Zone’i veebilink ja prooviti kätte saada kasutajanimesid ning paroole. Kirjade saatjaks olid suvalised domeenid ja just seetõttu oli võimalik aru saada, et tegemist ei ole õige kirjaga.

Samal ajal levisid ka Tallinki nimel saadetud kirjad, mille manuses oli troojalase-tüüpi pahavaraga nakatunud fail. Kiri saadeti taas suvaliselt domeenilt ja väideti, et manuses on tellimus. Sellised kirjad tuleks edastada CERT-EE meeskonnale uurimiseks ning seejärel kiri kustutada. Väga oluline oluline on jälgida, milliselt aadressilt kiri saadeti ning tundmatu saatja korral manust mitte mingil juhul avada.

Tegevused küberturvalisuse parandamisel Eestis

Kuu alguses avaldasime RIA küberturvalisuse aastaraamatu, milles võtame kokku eelmise aasta olulisemad küberintsidendid ja kirjeldame olukorda küberruumis. Registreerisime mullu 3314 mõjuga küberintsidenti ehk 24 protsenti rohkem kui 2022. aastal: rekordtasemele tõusid nii poliitilise taustaga ummistusründed kui ka inimestelt ja ettevõtetelt raha varastamiseks mõeldud pettused. Värskest küberturvalisuse aastaraamatust saab lisaks eeltoodule lugeda veel Eesti tervishoidu tabanud tõsistest küberintsidentidest, ohtlike turvanõrkuste lainest, sündmustest rahvusvahelises küberruumis ja paljust muustki. Aastaraamatuga saad tutvuda siin.

Nii jaanuaris kui ka veebruaris tulid avalikuks mitmete laialdaselt kasutusel olevate tarkvaratoodete kriitilise mõjuga turvanõrkused. Näiteks teavitas CERT-EE meeskond ligi kahtsadat Fortineti toodete kasutajat nende võrgus olevatest seadmetest, mis võivad olla haavatavad FortiOSi kriitilise turvanõrkuse vastu. Soovitasime FortiOSi tarkvara uuendada esimesel võimalusel, kuna Fortineti seadmed ja nende haavatavused on olnud tihti ründajate sihtmärgiks.

Käisime Lasnamäe Linnaosa Valitsuses rääkimas küberhügieenist. RIA analüüsi- ja ennetusosakonna analüütikud tegid ülevaate internetis levivatest pettustest, kuidas neid ära tunda ja internetti turvaliselt kasutada. Tasuta internetiturvalisuse loengud viis läbi Lasnamäe linnaosa valitsus koostöös Tallinna keskraamatukogu, PPA ja RIAga. Loengutesarja peamine eesmärk oli tõsta eakate teadlikkust erinevatest petu- ja kelmusskeemidest.

22. veebruaril toimus järjekordne CyberMeetUp üritus Tallinnas Palo Alto klubis. Seekord tegid ettekanded kübervaldkonna iduettevõtted, kes osalevad küberkiirendi programmis. Kuna programm hakkab läbi saama, siis oli õige aeg teha kokkuvõtteid selle kohta, et millega on tegeletud ja milliseid probleeme lahendatud. Lisaks rääkis RIA ennetusjuht Kaisa Vooremäe värskest RIA küberturvalisuse aastaraamatust. Nii selle kui ka kõigi eelnevate ürituste salvestusi on võimalik järele vaadata RIA veebilehel.

Kuula ka taskuhäälingut "Olukorrast digiriigis", kus RIA analüüsi- ja ennetusosakonna juhataja Märt Hiietamm räägib uuest küberturvalisuse aastaraamatust, olukorrast Eesti küberruumis, RIA tegemistest küberturvalisuse parandamisel ning sellest, mida saavad inimesed ja ettevõtted enda kaitseks ise ära teha.

Rahvusvaheline keskkond

Veebruaris jätkusid samuti sõjategevusega seotud küberründed. Ukraina riikliku side- ja teabekaitseteenistuse (SSSCIP) sõnul murdsid Vene häkkerid sisse mitmesse populaarsesse Ukraina uudisteportaali ja levitasid nende kaudu sõjaga seotud valeinfot. Rünne mõjutas Ukraina üht loetuimat veebiväljaannet Ukrainska Pravda, ärilehte Liga.net, uudisteportaale Apostrophe ja Telegraf. Libauudis, mida levitati, puudutas Ukraina eriüksuse hävitamist Avdijivkas.

7. veebruaril avaldasid FBI, CISA ja NSA koos teiste Viie Silma luureliidu riikidega hoiatuse, mille kohaselt on Hiina riikliku taustaga häkkerite rühmitus Volt Typhoon juba aastaid imbunud USA kriitilise infrastruktuuri võrkudesse, näiteks side-, energia-, transpordi- ja veesektoris. Mõnedel juhtudel on saavutatud ligipääs vähemalt viis aastat tagasi. Agentuuride hinnangul pole selle eesmärk mitte küberluure, vaid eelpositsioneering hävituslike rünnete korraldamiseks tulevikus. Agentuurid on välja andnud ka tehnilise juhise, kuidas end Volt Typhoon ja teiste sarnaste tegutsemisviisidega rühmituste eest kaitsta.

Populaarset AnyDesk kaugjuurdepääsutarkvara arendav Saksa ettevõte teatas, et hiljutise küberründe käigus tungiti nende toodangukeskkonda. Lisaks on tõendeid ka andmelekkest – tuhandete AnyDeski klientide andmed (kontaktinfo, info sessioonide kohta, klienditunnused jm) on pandud tumeveebis müüki. Ehkki AnyDesk soovitas intsidendi järel kõikidel klientidel paroolid ära vahetada ja uuendada tarkvara, on osa tumeveebis müügis olevatest andmetest saadud pärast seda, kui intsident avalikuks tuli. AnyDeskil on üle maailma 170 000 klienti, nende hulgas Samsung, Siemens, ÜRO jpt.

Sel kuul toimus mitu tervishoiusektorit mõjutavat intsidenti. Lunavararünnak meditsiinisektori infosüsteemi vastu põhjustas Rumeenias olukorra, kus sada haiglat olid sunnitud oma süsteemid võrgust eemaldama. 25 haiglat on kinnitanud ka andmete krüpteerimist. Rünnakus kasutati Backmydata lunavara ja nõuti 3,5 bitcoini suurust lunaraha, oma nime rühmitus nõudekirjas ei avalikustanud. Ründe tõttu pidid haiglad töö ümber korraldama, retsepte ja haiguslugusid kirjutati käsitsi.

Küberrünnak häiris apteekide tööd üle kogu USA. Apteekidele tarkvara pakkuv Change Healthcare oli sunnitud küberrünnaku järel sulgema osa oma süsteemidest. See tähendas, et paljud apteegid üle kogu USA ei saanud näiteks kontrollida, kas patsientidel on ravikindlustus, kas neil on õigus retseptiravimitele ja soodustustele.