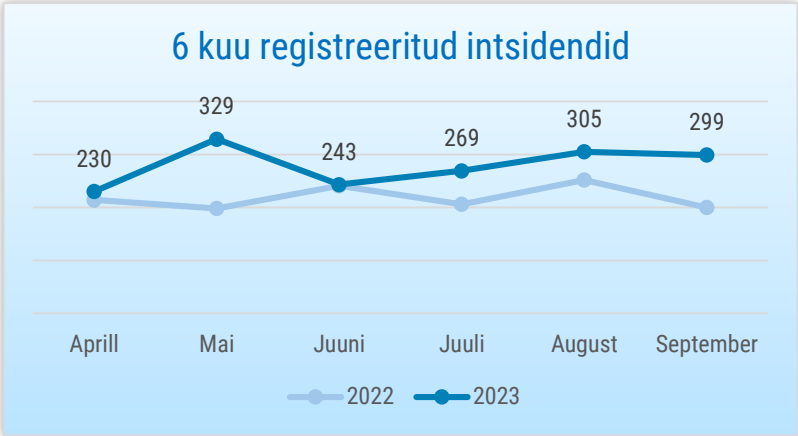
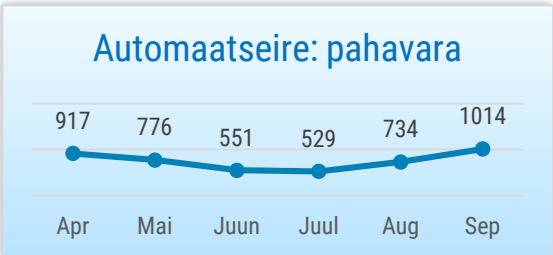
RIIGI INFOSÜSTEEMI AMET

OLUKORD KÜBERRUUMIS SEPTEMBER 2023

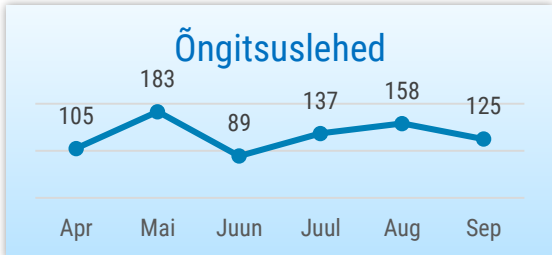
- Septembris registreerisime **299 mõjuga intsidenti**, mis on viimase poole aasta keskmisest veidi kõrgem näitaja.
- Septembri alguses toimus **ummistusrünnete kampaania**. Lisaks tõi kooli algus kaasa ka teenustõkestusründed haridusasutuste ja õppeinfosüsteemide vastu.Tarkvaravea tõttu jõudsid **tervise infosüsteemi valed andmed**.
- Kirjutasime **ohuhinnangu** jätkuvatest teenuse-tõkestusrünnetest ja veebilehtede näotustamisest.
- Vene riikliku taustaga küberrühmitused on **intensiivistanud ründeid** Ukraina õiguskaitseasutuste vastu.



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

Septembri alguses toimus ulatuslik ummistusrünnete kampaania, mille käigus rünnati paarikümmet kodulehte erinevates sektorites, kuid enamikele sihtmärkidest ei õnnestunud mõju avaldada. Kõige rohkem ründeid viidi läbi 4. septembril, mil rünnati näiteks Siseministeeriumi, NATO küberkaitsekeskuse CCDCOE, Kaitseuuringute keskuse, Eesti Raudtee, Tallinna Transpordiameti sõiduplaanide ja Eesti Energia kodulehti. Rünnete mõju oli väike, kuna tänaseks on enamik olulisi veebilehti võtnud kasutusele täiendavad kaitsemeetmed. Paar veebilehte olid lühiajaliselt maas ja lisaks õnnestus kolm veebilehte näotustada. Sarnaseid rünnakulaineid täheldati ka Lätis ja Leedus.

Lisaks tõi kooli algus kaasa ka teenustõkestusründed haridus-asutuste ja õppeinfosüsteemide vastu. 13. septembril viidi läbi DDoS rünnak ühe Harjumaal asuva kooli vastu, kuid ründel puudus mõju. 18. septembri hommikul rünnati infosüsteeme Moodle ja Tahvel, mille kasutamine oli ründe ajal häiritud. Endiselt arvame, et taoliste rünnete taga on samade koolide õpilased, kes ei soovi näiteks kontrolltööd teha. Enamasti toimuvad need koolitundide ajal ja on üsna väikese mõjuga, kuid vahel siiski õnnestub lühikeseks ajaks mõne infosüsteemi tööd häirida või kooli internetiühenduse kiirust vähendada.

Meditsiinitarkvara arendaja Medisofti vea tõttu jõudsid Perearst3 tarkvarast tervise infosüsteemi valed andmed. Veast teavitas perearst, kes avastas, et tema patsiendi epikriisil ehk haiguslool on teise isiku raviinfo. Medisofti andmeil mõjutas juhtum 45 perearstikeskust ja 672 epikriisi. Esimesed vigased epikriisid pärinevad juba 2019. aasta veebruarist. Samal päeval teavitas Terviseamet kiirabisid ja erakorralise meditsiini osakondi, et nad suhtuksid kriitiliselt Medisofti tarkvara kasutavate perearstikeskuste epikriisidesse, kuna neis võib esineda valesid andmeid, mis võivad põhjustada valesid raviotsuseid. Praeguseks on Medisoft vea tuvastanud ja parandanud ning uusi vigaseid epikriise juurde ei teki.

Kahjuks jätkuvad erinevad õngitsused, mille läbi inimesed kaotavad märkimisväärselt raha. Kõige enam nägime taas erinevate posti- ja kullerfirmade nimel saadetud õngitsuskirju ja -sõnumeid. Enamasti väidetakse neis, et saabumas on pakk ja suunatakse kasutaja tasuma näiteks tollimaksu või tarnekulu. Tihti on kirjas märgitud mõni väike summa, näiteks 1.99 eurot, kuid kui kasutaja sisestab õngitsuslehele oma pangakonto andmed, broneeritakse kaardilt juba oluliselt rohkem vahendeid.

Tegevused küberturvalisuse parandamisel Eestis

Kirjutasime ohuhinnangu jätkuvatest teenusetõkestus-rünnetest ja veebilehtede näotustamisest. Enamik ründeid olid mõjuta, ent ühe kindlustusseltsi ja ühe lennundussektori ettevõtte kodulehed olid ka lühiajaliselt häiritud. Lisaks DDoS-rünnetele, on CERT-EE-l teada vähemalt kolme veebilehe näotustamisest - toitlustusettevõte, muuseum ja logistikaettevõte. Näotustamine tähendab, et kasutatakse ära kodulehtede nõrkusi nagu nt vananenud tarkvara, murtakse lehele sisse ning kuvatakse teade eduka häkkimise kohta. Ohuhinnangus on toodud soovitused teenuste ja veebilehtede omanikele. Täpsemalt saad lugeda siit.

Riigi Infosüsteemi Ameti järelevalveosakonna juht Ilmar Toom rääkis oma osakonna tööst turvalise e-riigi blogis. RIA jälgib küberturvalisuse nõuete täitmist kogu avalikus sektoris ja elutähtsaid teenuseid pakkuvates ettevõtetes, et elekter ja vesi oleksid olemas ning inimeste andmed kaitstud. Intervjuust saab teada, mis juhtub, kui küberturvalisuse nõudeid ei täideta, milliseid vigu annaks lihtsa vaevaga vältida ning miks tuleb järelevalve asemel teha sageli hoopis selgitustööd. Lisaks saab teada, kuidas täpsemalt järelevalve töötab ja mis on selle eesmärgiks. Artiklis soovitatakse kasutusele võtta Eesti infoturbe-standard, mis on kõigile tasuta kättesaadav.

Koolitasime raamatukogutöötajaid küberturvalisuse teemadel programmis „Raamatukogu digiriigi nõustajana“. Koolitusel osales rohkem kui 100 raamatukogutöötajat üle Eesti ning selle eesmärgiks oli korrata üle küberturvalisuse põhimõtted. Koolitusele olid oodatud eelkõige raamatukogude teenindajad, kes oma igapäevatöös nõustavad kliente digiteenustega seotud küsimustes ja tegelevad nende digipädevuste arendamisega.

Teavitasime Microsoft Sharepointi serverite omanikke, kelle halduses on haavatavad seadmed. Turvanõrkus võimaldab ründajal veebiserveris Sharepointi kaudu õigustega manipuleerida, saada administraatori õigused ja seeläbi ohvri seade kompromiteerida. Soovitasime kõigil haavatavate seadmete haldajatel tarkvara uuendada esimesel võimalusel.

Septembris avaldasime RIA blogis taas ülevaateid olulistest turvanõrkustest. Septembris kirjutasime näiteks Androidi ja Apple’i seadmete olulistest turvauuendustest ning ka paljudest teistest laialdaselt kasutusel olevate seadmete turvapaikadest. Selleks, et olla kursis kõige olulisemate haavatavustega ja nõuannetega nende parandamiseks, soovitame lugeda RIA blogis regulaarselt ilmuvaid postitusi.

Rahvusvaheline keskkond

Ka sel kuul jätkusid sõjategevusega seotud küberründed. UK ja USA küberturbeagentuurid avalikustasid põhjaliku raporti uue pahavara Infamous Chisel kohta, millega GRU-ga seotud rühmitus Sandworm on rünnanud Ukraina kaitseväelaste kasutatavaid Android seadmeid. Pahavaraga üritati luua seadmetesse kaugligipääs ning saada ligi tundlikele andmetele, sealhulgas operatiivsele infole üksuste liikumise kohta. Ukraina julgeolekuteenistus SBU avastas ründekatsed augusti alguses ning koostöös Ukraina kaitseväega suudeti need blokeerida.

Ukraina CERT andis teada, et GRU-ga seostatud küberrühmitus üritas saada ligipääsu Ukraina energiasektori ettevõttesse. Selleks saadeti ettevõtte töötajatele hulgi õngitsuskirju, millega oli kaasas pahaloomuline link. Kui tavaliselt kasutatakse peibutisena pigem tööga seotud teemasid, siis seekord vihjas õngitsuskiri tüdrukutele ja kutsus üles klikkima lingil, et nende pilte vaadata. CERT-UA sõnul polnud ründekatse edukas, kuna ettevõtte küberturbespetsialist tuvastas selle kiiresti ning astus vajalikud sammud.

Vene riikliku taustaga küberrühmitused on intensiivistanud ründeid Ukraina õiguskaitseasutuste vastu (kohtud, prokurörid jm). Rünnete eesmärk on saada ligi infole ja tõenditele, mida Ukraina on kogunud Vene Föderatsiooni toime pandud sõjakuritegude kohta ning mille alusel on võimalik Vene kodanikke süüdi mõista.

Ekspertide hinnangul on Põhja-Korea riiklike sidemetega häkkerirühmitus Lazarus Grupp alates käesoleva aasta juunist varastanud erinevatelt platvormidelt (Atomic Wallet, CoinsPaid, Alphapo jt) ligi 240 miljoni dollari väärtuses krüptoraha ning neid kahtlustatakse ka 12. septembril aset leidnud varguses CoinEx kauplemisplatvormilt, mille kahju oli 31 miljonit dollarit. Küberrünnakute abil saadavaid finantsvahendeid kasutab Põhja-Korea muuhulgas oma relvastuse moderniseerimiseks.

USA kaitseministeerium avaldas kokkuvõtte 2023. aasta küberstrateegiast. Küberstrateegia avalik kokkuvõte käsitleb nii kaitse- kui ründeoperatsioone ning prioritiseerib koostööd liitlasriikidega ning vähem võimekate liitlaste võimearenduse toetamist.

USA küberturbeagentuur CISA koos FBI ja NSA ning Jaapani vastavate ametkondadega andsid välja hoiatuse Hiinaga seotud rühmituse BlackTech kohta. Nende hinnangul omab BlackTech tehnilist võimekust luua tagauks mitmetesse ruuteritesse, sh laialt kasutatavatesse CISCO ruuteritesse.