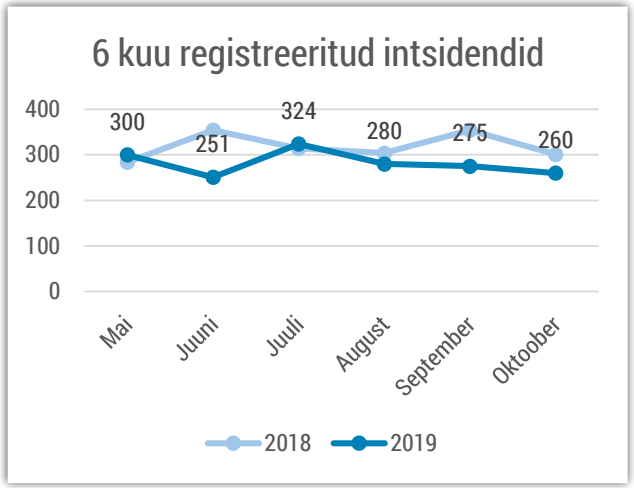
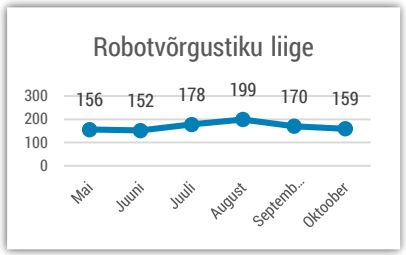
Olukord küberruumis – oktoober 2019

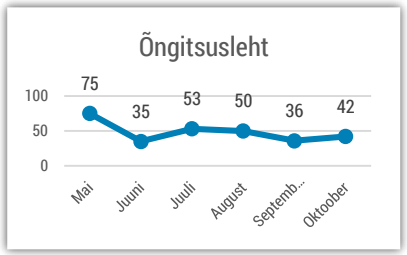
- Oktoobris registreerisime 260 intsidenti, mis on käesoleval aastal kuu keskmisel tasemel.
- Tarkvaravea tõttu olid kuue tunni jooksul häiritud infosüsteemid, mis sõltuvad rahvastikuregistrist kontrollitavatest aadressiandmetest.
- Jätkuvad õngitsuslained, mille kaudu on kompromiteeritud kontosid mitmes organisatsioonis.
- Algas küberhügieeni teavituskampaania „Ole IT-vaatlik!“
- Euroopa liidu liikmesriikide riskihinnangute kokkuvõte 5G tehnoloogia osas tehti avalikuks.



Intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede intsidentide hulk püsis oktoobris stabiilsena.

Olukord Eesti küberruumis

25. oktoobri päeval katkes tarkvaravea tõttu ligi kuueks tunniks rahvastikuregistri aadressiinfost sõltuvate infosüsteemide töö. Rahvastikuregistrit haldav Siseministeeriumi infotehnoloogia- ja arenduskeskus SMIT selgitas välja vea põhjuse, taastas andmed ja eemaldas intsidendi põhjustanud komponendid. Intsidendi tõttu ei töötanud sel ajal näiteks bussipiletiinfosüsteem Tallinnas ja Tartus, sündide ja surmade registreerimine, samuti sõidueksamitele registreerimine jne. Kuigi osaliselt olid häiritud ka mõne aadressikomponente vajava registri toimimine, siis näiteks äriregistri ja kinnistusraamatu teenuste osas Registrite ja Infosüsteemide Keskuse sõnul kasutajate jaoks probleeme ei esinenud. Nendes teenustes toimib aadressiväljade sisestamise lahendanud selliselt, et kui Rahvastikuregistrist aadressi väljundit automaatselt ei tule, küsib süsteem kasutajalt selle käsitsi täitmist.

Oktoobrikuud iseloomustas hulk meilikontode andmeid püüdvad õngitsuskampaaniaid ja nende tagajärjel ridamisi kompromiteeritud meilikontosid. Meile jõudis informatsiooni kompromiteeritud meilikontodest kahes Eesti suures ülikoolis, kahes suures haiglas, kütuseettevõttes, teehooldusfirmas ja veel mõnes asutuses. Enamasti avastati kompromiteerimine seetõttu, et kontodelt saadeti välja hulk uusi õngitsuskirju. Kontod kompromiteeriti aga mõne eelmise õngitsuskirjade laine tagajärjel, kus kasutaja oli oma parooli sisestanud võltsitud lehele. Mitmel puhul avastati tagajärgi likvideerides, et uute õngitsuskirjade väljasaatmise taustal püüti varjata seda, et kompromiteeritud meilikonto oli seadistatud saatma koopiaid kõigist kirjadest kolmandale osapoolele.

Sarnastest õngitsuskirjade lainetest oleme kirjutanud kuukokkuvõtetes nii oktoobris kui septembris. Taoliste meilikontode kompromiteerimise tagajärjel tuleks pigem eeldada, et kurjategijatel on ligipääs kogu kasutaja kirjakastile. Oleme varem näinud taoliste lekkinud postkastide kaudu hilisemat meilivestluste kaaperdamist, mille käigus üritati veel tükk aega hiljem välja petta lepingupartneritelt suuri rahasummasid. Välistada ei saa ka seda, et postkastide sisu üritatakse maha müüa.

27. oktoobril Lõuna-Eestit ja saari tabanud tormi tõttu katkes piirkonnas mitmel pool nii elektrivarustus ja selletõttu ka suures ulatuses andmeside. Muu hulgas katkes ka Riigivõrgu pakutud andmesideühendus, hoolimata sellest, et Riigivõrgu sidepunktid olid dubleeritud. Lisaks oli andmesidekatkestuse tõttu häiritud Luhamaa piiripunkti ületamine. Andmesidet ei olnud veel Lõuna-Eesti Haiglas, mitmes Võrumaa ja Põlvamaa koolis ja kohalikus omavalitsuses.

Tegevused küberturvalisuse parandamisel Eestis

Oktoobris tähistasime koos ülejäänud Euroopaga küberturvalisuse kuud. Tänavu algas küberturvalisuse kuuga meie viimase aja suurimaid kampaaniaid „Ole IT-vaatlik!“. IT-vaatliku kampaania põhiliseks eesmärgiks on pöörata tähelepanu parimatele praktikatele, kuidas küberruumis turvalisemalt käituda: näiteks paremad paroolid, tähelepanelikkus õngitsuskirjade osas, varundamine ja tarkvara uuendused.

Kuigi taolised küberhügieeni soovitused kehtivad küll kõigile, pöörame IT-vaatliku kampaania käigus eraldi tähelepanu vanemaealistele kodanikele. Seetõttu korraldasime näiteks töötubasid eakatele Tallinna keskraamatukogus ja rahvusraamatukogus. Kampaania kestab aasta lõpuni ning sellesisulisi reklaame ning teavitusi on võimalik näha nii avalikus ruumis, teles, raadios ja veebis.

Avalikkusele mõeldud ürituste kõrval jätkasime ka spetsiifilisemalt meie koostööpartneritele suunatud koolitustega. Nii toimusid küberhügieeni koolitused oktoobris Tallinna lastehaiglas (septembris koolitati nii Viljandi kui Valga haigla personali), samuti koolitused küberturvalisuse juhtimise ja ISKE rakendamise teemadel.

Jätkasime küberhügieeni koolituste korraldamist ka kohalikes omavalitsustes. Oktoobris külastasime Muhu, Tori, Kambja, Elva, Otepää, Nõo, Tõrva, Luunja ja Lääneranna valdu ning Haapsalu linna.

Kohalikud omavalitsused on olnud käesoleval aastal ka järelevalve fookuses (nagu oleme kirjutanud oma eelmiste kuude kokkuvõtetes). Oktoobri algatasime nende suunal taas kolm ning lõpetasime samuti kolm menetlust. Kui tavapäraselt oleme lõpetanud menetlused ilma ettekirjutusteta (menetluse käigus on puudujäägid heas koostöös kõrvaldatud), siis oktoobris olime sunnitud tegema ettekirjutuse puuduste kõrvaldamiseks ühele omavalitsusele.

Sügisel lõpetasime suvel alustatud järelevalvemenetluse kütusefirma Olerex andmelekke osas, kuna menetluse käigus selgitasime välja, et mõjutatud teenus ei olnud osaks elutähtsast teenusest, mille üle RIA järelevalvet teeb.

Rahvusvaheline keskkond

Euroopa Liidu liikmesriigid koos Euroopa Komisjoniga avaldasid 9. oktoobril riskianalüüsi 5G võrkude küberturvalisuse kohta. Liikmesriikide siseriiklikel analüüsidel põhinev riskihinnang tõi välja lisaks peamistele turvanõrkustele ja julgeolekuohtudele ka suurimad 5G võrkudega seonduvad väljakutsed, milleks nimetati turvastandardeid tõstvaid innovatsiooniarenguid ning teenusepakkujate muutuvat rolli. Kõige olulisemaks ohustajaks hinnatakse aruande kohaselt riike või riikliku toetusega ohustajat. Kõige tundlikumate varadena kirjeldati 5G võrgu põhikomponente (*core infrastructure*).

(Eestis peavad 5G võrkude riskide maandamiseks sideettevõtjad edaspidi kooskõlastama sidevõrkudes kasutatava tehnoloogia Tarbijakaitse ja Tehnilise Järelevalve Ametiga. Valmiv määrus nõuab, et elutähtsat teenust osutav sideettevõtjad peavad kasutama sidevõrgu projekteerimisel, ehitamisel ja hooldamisel riist- ja tarkvara, mille kasutamine ei kujuta ohtu riigi julgeolekule.)

Ligi 16 erinevat riiklikku ja rahvusvahelist spordi- ning antidopingu organisatsiooni langesid küberrünnakute ohvriks, mille taga oli Microsofti luureinfokeskuse andmetel Venemaa häkkerite grupp Strontium (tuntud ka APT 28 ja Fancy Bear nimede all), mis töötab paljude lääneriikide hinnangul Venemaa GRU luureteenistuse jaoks. Rühmitus on 2016. aastast korduvalt rünnanud Maailma Antidopingu Agentuuri (WADA) ning hiljutised sündmused leidsid aset vahetult enne WADA uut menetlust Venemaa dopinguskeemide kohta.

Venemaa suurima panga Sberbanki kliendid sattusid Venemaa läbi ajaloo ühe suurima andmelekke osaliseks, kui ligikaudu 60 miljoni krediitkaardi andmed paisati müüki tumeveebis. Kuna lekkinud teabe seas ei olnud CVV koode, suudeti rahalist kahju hoida minimaalsena. **Samuti paljastati tumeveebis müügiks olev hiiglaslik andmebaas 1,3 miljoni Indias registreeritud krediitkaardi ning nende detailidega.**

USA ja Ühendkuningriikide küberturvalisuse agentuurid NSA ja NCSC avalikustasid, et Venemaaga seostatud küberspionaažiga tegelev rühmitus Turla on suutnud üle võtta Iraaniga seostatud rünnakugrupi APT34 küberrünnakute taristu ning püüab neid imiteerides oma tegevuste jälgi peita.

Oktoobrikuus teatasid küberturvalisuse teenuseid pakkuvad ettevõtted (VPNi teenuste pakkuja NordVPN ja TorGuard ning viirustõrjeprogrammi tootja Avast), et nende teenustesse on sisse murtud. Avasti infoturbejuht sõnul oli rünne keerukas ja ründaja püüdis iga hinna eest end peita. Avast lükkas edasi ühe oma tarkvarauuenduse, et välistada võimalikku tarneahelarünnakut.