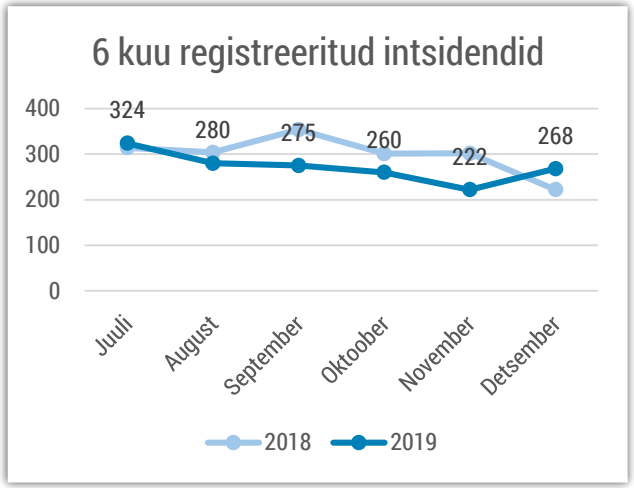
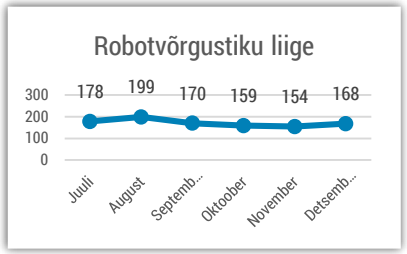
Olukord küberruumis – detsember 2019

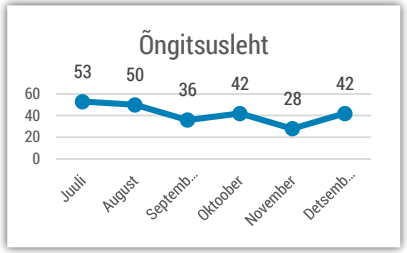
- Detsembris registreerisime 268 intsidenti, mis on aasta keskmisel tasemel.
- Eraldi paistsid Eesti küberruumis silma tervishoiusektoriga seotud intsidendid.
- Eesti perearstide küberturvalisuse tagamise kulud kajastuvad üldarstiabi teenuse rahastusmudelis.
- Detsembrist juhib RIA küberturvalisuse teenistust Lauri Aasmann.
- Lunavararünnakud on jätkuvalt suureks probleemiks üle maailma.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede hulk hakkas detsembris taas tõusma. Enim nägime kontoandmeid õngitsevaid lehekülgi.

Olukord Eesti küberruumis

Detsembris teavitas Haigekassa meid kolmel korral (5., 7., ja 30. detsembril) digiretsepti ja kindlustatuse kontrolli katkestusest. 5. ja 7. detsembri katkestused toimusid öösel või hilisõhtul, mistõttu nende mõju oli väiksem. 30. detsembril katkes digiretsepti teenus ja kindlustatuse kontroll pea pooleteiseks tunniks alates kella 16st pärastlõunal. 20. detsembri hommikul oli 4 tunni jooksul häiritud Digiloo ja Tervise Infosüsteemi kasutamine, sest süsteemirikke tõttu alustati öösel hooldustöödega.

Haigekassa on üle vaatamas ja uuendamas oma infosüsteeme, probleemide juurpõhjused peaks lahendama uus baastaristu ja tarkvarakihi korrastamine.

31. detsembri esimestest tundidest kuni tööpäeva lõpuni olid serveriruumi jahutussüsteemi katkestuse tõttu häiritud Ida-Tallinna Keskhaigla IT-teenused. Tegevuste dokumenteerimine toimus paberil. Kriitiliste andmekogude terviklikkus ei olnud ohus. Kuna oli lühendatud tööpäev ja plaanilisi vastuvõtte vähe, oli mõju ka väiksem võrreldes tavalise tööpäevaga.

Detsembris nägime taas õngitsuslehtedega seotud intsidentide tõusu. Jätkusid pangakontodele sissepääsu püüdvad õngitsuskampaaniad, kus meelitati ohvreid sisestama oma PIN1 ja PIN2 koode oma isiklikes seadmetes. Suurem osa detsembris nähtud õngitsuslehtedest aga püüdis meilikontode andmeid. Eraldi oli märgata haiglate ja tervishoiuasutuste kontoandmeid püüdvaid õngitsuskampaaniaid.

Kompromiteeritud meilikontode kaudu algatatud finantspettuste osas teavitati meid Eesti ettevõtete välispartnereid mõjutanud intsidentidest. Petturid, kes mõnda aega jälgisid ettevõtete omavahelist meilivestlust, sekkusid pärast Eesti ettevõtte arve saatmist välispartnerile ja saatsid omalt poolt järele kirja, kus paluvad arve teisele pangakontole maksta. Üks välisriigi ettevõte saatis niimoodi mitukümmend tuhat eurot valele pangakontole ühes Saksamaa pangas. Õnneks ei jäänud too ettevõte lõpuks oma rahast ilma, sest pank oli konto juba varem musta nimekirja kandnud.

Samuti saime teada ühest tegevjuhi petuskeemi ohvrist, kus ühe väikese ehitusettevõtte juhi nime matkides saadeti juhiabile e-kiri sooviga teha kiiresti ühele pangakontole ülekanne. Ettevõtte kahju oli 17 000 eurot.

Tegevused küberturvalisuse parandamisel Eestis

Detsembrist asus ametisse uue RIA peadirektori asetäitjana küberturvalisuse alal Lauri Aasmann. Aasmann tuli RIAsse NATO küberkaitse koostöökeskusest, kus juhtis sealset õigusteadlaste meeskonda. Varem on ta töötanud Swedbank ASis juristina ning Põhja Ringkonnaprokuratuuris ja Tallinna Prokuratuuris prokurörina, kus ta tegeles valgekraelise kuritegevuse ja küberkuritegude uurimisega.

3. detsembril sõlmisime Kaitseväe küberväejuhatusega koostööleppe, mille alusel lubame jagada vastastikku parimaid käitumistavasid ja ressursimahukaid tehnoloogiaid, osaleda koos õppustel ning ühtlustada küberintsidentide lahendamise protsesse.

Võtsime mullu eesmärgiks kontrollida seda, kuidas kohalikud omavalitsused täidavad neile kohustuslikke küberturvalisuse eeskirju. Seetõttu algatasime järelevalvemenetlused kõigi Eesti omavalitsuste suhtes ning enamikes käisid RIA eksperdid ka kohapealseid toiminguid tegemas. Aasta jooksul olime sunnitud tegema kolm ettekirjutust nõuete mittetäitmise kohta. Detsembris alustasime samuti kolm uut järelevalvemenetlust ja lõpetasime kolm menetlust, kuna puudused kõrvaldati tähtaegselt. Küberhügieeni koolitusi korraldasime detsembris veel viies omavalitsuses.

Detsembris lõppesid järjekordsed turvatestimised elutähtsat teenust osutavate ettevõtete juures, et aidata neil parandada oma infosüsteemide turvalisust ja riskide hindamist. RIA korraldab riigi jaoks elutähtsate ja oluliste teenuste osutajatele turvatestimisi 2012. aastast. 2019. aastal testiti infosüsteeme kaheksas ettevõttes ja asutuses (2018. aastal korraldati teste kuues asutuses).

Koostasime koos Haigekassa, TEHIKu ja Perearstide seltsiga „Baasturbe meetmed perearstidele“, millest perearstikeskused hakkavad lähtuma. Kulutused küberturvalisuse tagamisele kajastuvad nüüd ka perearstide rahastusmudelis ning nende nõuete täitmine on edaspidi üks perearstide kvaliteedisüsteemide indikaator. Perearstid peavad hakkama 2022. aastast jälgima küberturvalisuse seaduses sätestatud nõudeid. Küberturvalisuse kulutuste lisamine üldarstiabi teenuse rahastusmudelisse aitab neil selleks valmistuda.

Detsembriga jõudis lõpule küberturvalisuse kampaania “Ole IT-vaatlik”. Peamiselt vanemaealistele suunatud kampaania raames toimusid kolme kuu vältel praktilised infopäevad küberturvalisuse põhitõdedest üle terve Eesti.

Rahvusvaheline keskkond

Hiina kommunistliku partei keskkomitee on uuendanud oma suunist, mis nõuab Hiina valitsusasutustel loobuda välisriikides toodetud infotehnoloogiast, asendades seadmed ja tarkvara Hiinas valmistatud toodetega. Hiina valitsus on juba ammu sarnaseid plaane pidanud.

Venemaa teatas, et on edukalt katsetanud niinimetatud RuNeti toimimist ehk teisisõnu – on edukalt proovinud, kuidas Venemaad lahti ühendada rahvusvahelisest internetist. Venemaa ametnike sõnul on lahtiühendamise võimekus vajalik selleks, et kindlustada võrguühendused ka juhul, kui välisriigid püüavad Venemaal interneti toimimist takistada. Kriitikud näevad Venemaa plaanides aga head viisi, kuidas piirata sõna- ja internetivabadust.

Ameerika Ühendriikide merevägi ja maavägi keelasid oma sõduritel ja teistel töötajatel sotsiaalmeedia-platvormi TikTok kasutamise, viidates küberturvalisusele. Hiinas välja arendatud lühivideode jagamise platvorm on maailmas ülipopulaarne. USA seadusandjad on aga mures äpi omandisuhte pärast ja seetõttu on USAs TikToki suhtes tehtud ka julgeolekuanalüüsid.

Sarnase nimega äpp ToTok – populaarne suhtlusäpp eelkõige Araabia Ühendemiraatides, kus näiteks WhatsApp ja Skype on blokeeritud – eemaldati detsembris äpipoodidest, kui The New York Times paljastas, et Ühendemiraatide valitsus kasutas äppi kasutajate järel nuhkimiseks. (Jaanuari alguses jõudis ToTok Google Play Store'i tagasi.)

Iraani telekommunikatsiooniminister teatas kahel korral detsembris suuremahulistest küberrünnakutest.

Microsoft sai USA kohtust õiguse üle võtta 50 domeeni, mida Põhja-Koreaga seotud häkkerirühmitused kasutasid rünnakute läbiviimisel. Domeene kasutati õngitsuskirjade ja -lehtede haldamiseks.

Lõuna-Aafrika vabariigi ühe internetiteenusepakkuja Conor poolt pakutud veebifiltreerimissüsteemi kasutanud klientide kogu internetiliikluse andmed lekkisid avalikkusele. Sealhulgas oli võimalik avalikult näha, milliste sotsiaalmeediakasutajatega kliendid käisid näiteks pornolehekülgi külastamas. Mõjutatud kliente oli mitmetest Aafrika ja Lõuna-Ameerika riikidest.

Lunavararünnakutest teatati mitmel pool. Pihta said teiste hulgas mõned USA linnad (Pensacola, New Orleans), üks haiglavõrgustik, üks rannavalve sadamahoone, samuti Hollandis asuv Maastrichti ülikool. Kuna suuremad asutused on õppinud lunavara-rünnakutest taastuma, on eelmiste kuude jooksul üha enam kuulda ähvardusi, et lunaraha mittemaksmisel lubavad kurjategijad kõik andmed ka avalikustada.