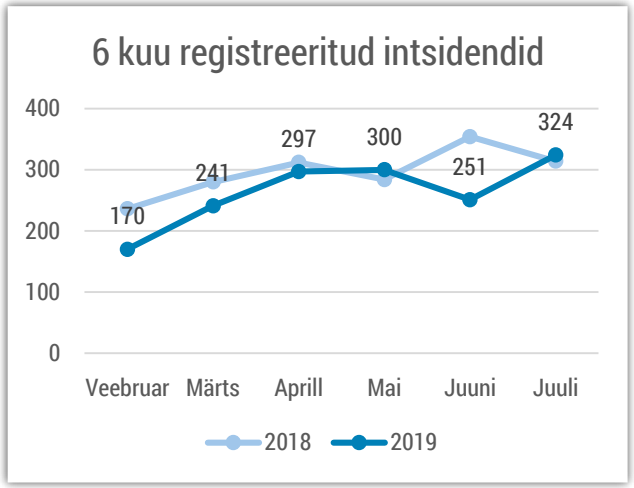
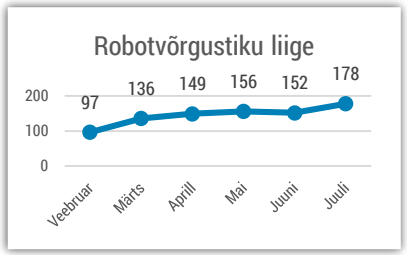
Olukord küberruumis – juuli 2019

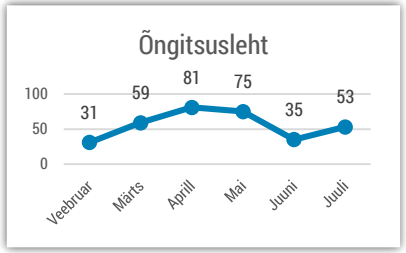
- Juulis registreerisime 324 intsidenti, mis on aasta keskmisest kõrgem, kuid samal tasemel kui mullu.
- Jätkuvad õngitsuskampaaniad, mille käigus püüavad kurjategijad meelitada inimesi sisestama oma Mobiil-ID või Smart-ID PIN koode.
- Kolme Eesti asutuse ja ettevõtte klientide andmed olid avalikult kättesaadavad.
- RIA ehitab üles võrgustiku Euroopa küberekspertidest.
- USA ja Suurbritannia määrasid mitmele ettevõttele andmelekete eest hiigeltrahvid.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtedega seotud intsidentide hulk juulis taas kasvas. Enamasti on tegu pankade lehekülgi imiteerivate lehtedega.

Olukord Eesti küberruumis

Juulist alates muutis isikutuvastamise teenuse Smart-ID pakkuja SK ID Solutions uute kontode loomist keerulisemaks, mistõttu kurjategijad ei saanud enam õngitsuslehtede kaudu ohvritele valekontosid luua. **Samas oleme teadlikud õngitsuskampaaniatest, kus ohvritel palutakse pangalehele sisenemise eesmärgil oma seadme Smart-ID või Mobiil-ID kaudu sisestada nii PIN 1 kui ka PIN 2 koodid.** Võltsitud lehele sisestatud kasutajatunnusega püüavad kurjategijad kohe siseneda õigesse internetipanka (ohver ootab samal ajal ja sisestab oma PIN 1) ning alustavad kohe ka maksekorraldust (mille jaoks on vaja sisestada PIN 2). Meile teadaolevalt on mitmed isikud saanud niimoodi rahalist kahju.

Taoliste intsidentide puhul tuletame meelde, et PIN 2 kood nii Smart-ID, ID-kaardi ja Mobiil-ID puhul on võrdsustatud isiku allkirjaga, mida näiteks pankadesse sisselogimiseks ei ole vaja sisestada.

Juuli lõpus teavitas SK ID Solutions veel ühest uuest petuskeemist, kus ohvritele helistatakse ja lubatakse talle mitme tuhande eurost tulu. Pettuse käigus luuakse kaugühendus ohvri arvutiga ja ja kasutades erinevaid autentimisvahendeid (sh ID-kaardi toel uue Smart-ID konto loomine) tehakse kliendi nimel maksekorraldusi.

Juuli esimeses pooles teavitati meid kolmest eraldiseisvast intsidendist, kus Eesti ettevõtete klientide andmed olid avalikult kättesaadavad. Bürootarbeid müüva veebipoe Charlot leheküljelt võis avalikult leida tuhandete klientide ees- ja perekonnanimed, meiliaadressid, e-poe konto algsed paroolid, aadressid ja isikukoodid. Tartus teavitati linna sellest, et vastavatud rattaringluse 20 000 kliendi andmed olid avalikult kättesaadavad (sealhulgas see, kust kuhu klient rattaga sõitis). Tanklakett Olerex teatas, et osade nende äriklientide andmed olid jäänud andmebaasi kolimise käigus puhverfaili kaudu avalikult internetis kättesaadavaks.

Meile teadaolevalt ei ole keegi (peale lekked avastanud isikute) neid andmeid endale salvestanud ega väärkasutanud ning andmetele ligipääs piirati kohe pärast andmelekkest teadaandmist. Kõigil kolmel juhul algatasime järelevalvemenetluse.

Tegevused küberturvalisuse parandamisel Eestis

Võitsime Euroopa Komisjoni hanke, millega hakkame rajama Euroopa Liidu riikide küberekspertide võrgustikku, mis hakkab koordineerima kõikide Euroopa Liidu poolt läbi viidavate küberturvalisuse projektide elluviimist kolmandates riikides. RIA poolt juhitavasse, algselt nelja aasta pikkusesse projekti on partneritena kaasatud Saksa välisministeerium, Soome küberturvalisuse keskus Traficom ning Luksemburgi küberturbekeskus Securitymadein.lu. Esmane ülesanne luua vajalikud andmebaasid, kaasata kübereksperdid ja käivitada koolitusprogrammid. Perioodi lõpuks soovime hõlmata vähemalt 500 eksperti ja 200 rahvusvahelist organisatsiooni üle Euroopa. Kaugem eesmärk on võrgustiku edasise kestvuse tagamine ning RIA juhtrolli säilitamine selles. Projekt on oluline nii Eesti maine kui ka ettevõtluse edendamise seisukohalt.

Jätkame järelevalvemenetlusi kohalike omavalitsuste suhtes, millest oleme rääkinud ka varasemates kuuülevaadetes ja meedias. Aasta algusest oleme algatanud menetlusi juba üle poolte omavalitsuste suhtes ning juulis jõudsime esimesed nendest juba ka lõpetada ilma ettekirjutusteta, kui menetluse käigus on puudujäägid kõrvaldatud.

Uuendasime küberintsidendist teavitamise vormi. Uuenduskuuri eesmärgiks on algselt teavitajat vähem koormata selliste küsimustega, millele tõenäoliselt intsidendi toimumisel alguses kohe vastust ei ole või millele saab vastata ainult väga kindlatel puhkudel. Uues teavitusvormis tuleb intsidendist teavitajal vastata ainult baasküsimustele, mis annaksid CERT-EE-le ülevaate, mis on juhtunud. Vajadusel saame teavitajaga eraldi suhelda ja leida vastused spetsiifilistematele küsimustele.

Meeldetuletuseks: riigiasutustel, kohalikel omavalitsustel, elutähtsate ja oluliste teenuste osutajatel ning digitaalsete teenuste osutajatel (nagu näiteks e-poe pidajatel) on küberturvalisuse seaduse kohaselt kohustus teavitada meid olulisest küberintsidendist viivitamata, kuid hiljemalt 24 tundi pärast intsidendist teada saamist.

Uuendasime ka ID-kaardi tarkvara, mille värske versioon toetab nüüd vaegnägijatele mõeldud ekraanilugereid. See võimaldab vaegnägijatel DigiDoc4s digiallkirja lisada ning valideerida allkirjastatud dokumente ning muuta ID-kaardi PIN-koode. Järgmistes tarkvaraversioonides jätkub funktsioonide lisamine ja täiustamine.

Rahvusvaheline keskkond

Ameerika ühendriikide konkurentsiamet FTC teatas kokkuleppest sotsiaalmeediahiiuga Facebook, mille järgi maksab ettevõte 4,5 miljardit eurot trahvi seoses isikuandmete lekkimisega Cambridge Analytica juhtumis ning muudab isikuandmete käitlemise protseduure. Vaid päev varem teatas USA väärtpaberite- ja börsi järelevalveamet SEC, et Facebook maksab 90 miljonit eurot trahvi veel selle eest, et ettevõte oli Cambridge Analytica juhtumi puhul avalikkust eksitanud. Juulikuus sai Facebook sama teema tõttu trahviotsuse ka Itaaliast.

Varasemate andmelekete tõttu said trahviotsused kätte ka teised ettevõtted. USAs peab üks kolmest suurest krediidivõimet hindavatest agentuuridest Equifax maksma 625 miljonit eurot trahvi 2017. aastal toimunud andmelekke tõttu. Ühendkuningriikide andmekaitseinspektsioon ICO teatas 200 miljoni eurosest trahvist Briti lennufirmale British Airways ning 108 miljonit eurosest trahvist Marriotti hotelliketile.

Ning andmelekked jätkuvad. USAs tegutsev suurpank Capital One andis märku, et üks isik suutis saada ligipääsu enam kui 100 miljoni kliendi andmetele. Häkker võeti ka vahi alla. Samas ei pea suure mõjuga leke olema massiivne – näiteks oli juulis märgata Magecartiks nimetatavate küberkurjategijate grupeeringute aktiivsemat tegutsemist, kes püüavad veebipoodidest krediitkaardi andmeid varastada.

Kasahstani valitsus nõuab oma kodanikelt (läbi interneti teenusepakkujate) oma arvutitesse ja nutiseadmetesse valitsuse juursertifikaadi installeerimist, mis lubab krüpteeritud internetiliiklust pealt kuulata. Ametnike sõnul on meede mõeldud kodanike kaitseks.

Veebiliikluse pealtkuulamise ja niiviisi kasutajaandmete varastamisega tegelevad ka erinevad riiklike seostega häkkerite grupid. Uurijad ettevõttest Cisco Talos uurijad paljastasid juba kevadel Lähis-Idas tegutseva grupeeringu, kes valitsusasutuste kasutajanimede ja paroolide varastamise nimel kompromiteerisid lausa interneti alustehnoloogiaks vajalikke nimeservereid ja sertifikaate. Grupeering pole avalikustamisest hoolimata oma tegevust tagasi tõmmanud.

Venemaal said häkkerid ligipääsu FSB-ga koostööd teinud arendusfirma Sytech andmetele ning varastasid 7,5 terabaiti ulatuses informatsiooni, sealhulgas tööriistad luureinfo kogumiseks ja Venemaa ülejäänud maailma internetist eraldamiseks.

The New York Times avalikustas, et Hiina piirivalve nõuab Xinjiangi piirkonda sisenejatelt ligipääsu nende nutitelefonidele ning lisab sinna nuhkvara islamiterrorismi piiramise ettekäändel. Hiina keskvõimu jõulist suhtumist isikuvabadustesse on näha ka meeleavaldustel Hong Kongis, kus aktivistid püüavad igatepidi riigipoolse jälgimise vastu võidelda.