RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE AUGUST/SEPTEMBER 2017

Olukord Eesti küberruumis

Augustis registreeris CERT-EE 736 juhtumit, millest ligi kolmandik (259) olid infosüsteemide käideldavust, terviklust või konfidentsiaalsust mõjutanud küberintsidendid. Registreeritud sündmuste arvu poolest oli august selle aasta rahulikem kuu; intsidentide arv jäi siiski aasta keskmisele tasemele. Elutähtsa (uue hädaolukorra seaduse mõistes) ja teiste ühiskonnale oluliste teenuste osutajaid puudutanud intsidente oli 61.

Septembris tõusis juhtumite arv taas viimase poolaasta tavapärasele tasemele (816). Küberintsidente, millega kaasnes tegelik mõju, oli 225, sh kaheksa kõrge prioriteediga.Oluliste teenuste osutajatega seotud juhtumeid oli septembris 50. Tavapärasest kordades aktiivsem oli lunavara levik.

Augusti ja septembri kõige akuutsemaks küberturvalisuse sündmuseks oli kahtlemata **Eesti ID-kaardil kasutatavate kiipide võimalik turvanõrkus**, mille kohta RIAt teavitati 30. augustil. Turvariskist puudutatud kaartide suure arvu tõttu – ligi 750 000 ID-, elamisloa-, digi-ID ja e-residendi kaarti – oli võimaliku mõju väljaselgitamine ja riskide operatiivne maandamine ülioluline. Selge on, et ühe ID-kaardi murdmiseks vajalik ekspertteadmine ja ressurss on sedavõrd suured, et massiline identiteedivargus ei ole võimalik, ent pikemas perspektiivis ei saa üksikuid ründeid välistada. Tegemist on kõrge usaldusnõudega teenusega, mistõttu juhul, kui leiab kinnitust turvanõrkuse reaalse ärakasutamise võimalus, tuleb sulgeda kõik turvanõrkusest mõjutatud sertifikaadid.

Sellest tulenevalt on RIA koos partneritega augusti lõpust alates töötanud mitmel suunal: ID-kaardirakenduse konfiguratsiooni väljatöötamine, mille puhul kiibi turvanõrkus ei avalduks, uuest konfiguratsioonist tingitud muutuste sisse viimine teenustesse ning ühtlasi valmistumine suuremahuliseks ID-kaartide kauguuenduseks; valmistumine alternatiivsete autentimis- ja allkirjastamislahenduste (ennekõike mobiil-ID) rakendamiseks riigi ja erasektori e-teenustes; ning avalik riskihaldus eesmärgiga säilitada pikaajaline usaldus e-riigi vastu ja suunata mobiil-ID näol varulahenduse kasutuselevõttu. RIA soovitab kõigil omada e-teenuste kasutamiseks rohkem kui ühte eID lahendust – ID-kaardile lisaks näiteks ka mobiil-IDd.

RIAle teadaolevalt ei ole endiselt aset leidnud ühtki turvanõrkuse realse ärakasutamise juhtu. Kava kohaselt algab ID-kaardi uuendamine oktoobri lõpus ning kaarte saab uuendada kauguuendamise teel või PPA teenindusbüroodes 2018. aasta märtsi lõpuni. Uue aasta aprillist uuendamata kaartide sertifikaadid tühistatakse (see ei puuduta ID-kaarte, mis on välja antud enne 16. oktoobrit 2014, ega mobiil-IDd). RIA koos partneritega jälgib sündmuste arengut hoolikalt ning plaanitud ajakavas võib tulla ette muutusi, kui olukord seda nõuab.

Muudest sündmustest augustis ja septembris olid olulisemad:

Internetiteenuse pakkuja Levikom võrgurike 6.-7. augustil tõi ilmsiks, et paljud Eesti veebilehed sõltuvad toimimiseks teenusepakkuja välisühendustest, kuna kasutavad välisriigi serveris asuvaid komponente (käsujada, kirjatüüp, sisu jne). Ettevõtja välisühenduse tõrke tõttu olid klientidele kättesaamatud või loetamatud ka mõned riigiasutuste ja meediaväljaannete veebilehed.

Katkestuse puhuks loodud varulahendused rakenduvad eeskätt välisühenduse ulatusliku katkemise, mitte üksikut operaatorit puudutava teenustõrke puhuks. Probleeme ei olnud nt politsei.ee, 112.ee ja valimised.ee lehtedega.

Augustis-septembris on taas hoogustunud finantspettuste katsed, kus asutuste juhtide nimel saadetakse finantsjuhile tasumiseks libaarveid. Samuti levis Facebookis uus petuskeem libaloosiga Estonian Airi (sic!) ja Air Balticu lennupiletitele.

Tegevused küberjulgeoleku parandamisel Eestis

Augustis ja septembris jätkus töö küberturvalisuse seaduse eelnõu ettevalmistamiseks. Eelnõu on esitatud ministeeriumitevahelisele kooskõlastusringile, vastamise tähtajaga 24. oktoobril.

14.-15. septembril toimus RIA korraldatud ELi küberkonverents „Digitaalne ühisturg, ühine digitaalne turvalisus", kus Euroopa riikide partnerasutuste ja Euroopa komisjoni, ELi küberturbeagentuuri ENISA ja ettevõtjate esindajatega arutleti küberkuritegevuse, rahvusvahelise koostöö ja ELi küberturvalisuse initsiatiivide üle ELi värskelt avaldatud uues küberpaketis.

Septembrist sai RIA Euroopa ühtsete IT-turvastandarditega tegeleva organisatsiooni SOG-IS liikmeks, kuhu peale meie kuulub veel 13 Euroopa riiki. CERT-EEle omistati maailmas kuuenda riikliku küberüksusena Trusted Introducer sertifitseerimistunnistus, mis kinnitab CERT-EE intsidentide haldamise võimekust ning koostöö ja infovahetuse kvaliteeti. Mõlemad ühinemised on ühtlasi tunnustus Eesti kübervõimekuse kõrgest tasemest.

Avaldasime ka mitu hoiatust käimasolevate küberründekampaaniate kohta ja soovitused avalikus võrgus kättesaadavate seadmete kaitsmiseks.

Rahvusvaheline keskkond

Hiina on karmistanud internetitsensuuri oktoobris toimuva parteikongressi eel, kus kardetakse mitme tippjuhtkonna liikme erruminekuga seoses võimuvahetust. Aastaid rakendatud „suure Hiina tulemüüri" kõrval on nüüd keelatud ka krüpteeritud suhtluskanalite kasutamine (sarnane piirang jõustub k.a novembrist ka Venemaal) ja anonüümne kommenteerimine veebikeskkondades. Internetiteenuse pakkujatele ja andmekeskuste haldajatele korraldatakse kohustuslikku väljaõpet „kahjuliku sisuga" veebilehtede tuvastamiseks ning nende omanikest riigile teada andmiseks; sisse on seatud ööpäevaringne vihjetelefon, kuhu vastav info raporteerida. Hiina kolm suurimat internetiteenuse pakkujat on juba sattunud ametkondade uurimise alla seoses suutmatusega „kontrollida kasutajate üles laaditud illegaalset teavet".

Hiina loodeosa Xinjiangi provintsi uiguuri moslemitest elanikke sunnitakse „terrorismivastase meetmena" paigaldama oma nutiseadmetesse „Kodanikukaitse"-nimelist mobiilirakendust, mis võimaldab kasutaja internetiliiklust jälgida. Paigaldamata jätmine on karistatav ja politseil on õigus paigaldamist kontrollida.

Samal ajal on hüppeliselt kasvanud teenustõkestusründeid (DDoS) pakkuvate Hiina veebilehtede arv.

Üheks kübervaldkonna 2017. aasta peamiseks märksõnaks on kujunemas poliitilisi protsesse mõjutavad küberohud, iseäranis **valimiste küberturvalisus** laias mõttes. Ründed väljenduvad seejuures väga erinevalt – kampaaniaaegsetest teabeleketest kuni valimissüsteemide turvanõrkuste ärakasutamiseni. Augustis avalikustas Wikileaks (kolm kuud pärast Prantsusmaa presidendivalimisi) peaaegu 72 000 e-kirja ja Emmanuel Macroni valimiskampaaniaga seotud kirjavahetust ajavahemikust 2009. aastast kuni vahetult valimiseelsete päevadeni. Erinevalt 2015. aasta küberründest TV5 Monde'i vastu, on Prantsuse küberturbeagentuur ANSSI hoidunud teabevargust Vene luureteenistustega seostamast, viidates vaid, et dokumendivargus õnnestus tänu üsna lihtsakoelisele ründele.

Aafrika ühes demokraatlikumas riigis **Keenias** puhkesid üleriigilised rahutused pärast augusti alguses toimunud presidendivalimisi, kus opositsioonijuht süüdistas võimuparteid valimiskomisjoni keskserveris hääletamistulemuste manipuleerimises. Selle ja teiste rikkumiste tõttu tunnis-

tas kohus 1. septembril valimistulemused kehtetuks.

USAs valimisseadmeid ja -infosüsteeme haldav ettevõte laadis Amazoni pilveteenusesse kogu Chicago valimispiirkonna 1,8 miljoni valija registreerimisandmete varukoopiad, jättes juurdepääsu andmetele ekslikult avalikuks. Avastamise hetkeks oli teave olnud avalikkusele kättesaadav mitu kuud ning sisaldas lisaks valimisnimekirjadele ka infot ettevõtja turvaprotseduuride kohta ja töötajate parooliräsisid.

Poliitiliste protsesside kõrval on **riiklikku päritolu luuretegevus** aktuaalne ka tööstussihtmärkide suunal. Saksamaa vastuluureteenistus avaldas hoiatuse Venemaa, Hiina ja Iraani spionaaži kohta Saksamaa ettevõtete ja huvide vastu. Saksamaa tööstusassotsiatsiooni raporti kohaselt on koguni 53% Saksamaa ettevõtetest langenud majandusspionaaži ohvriks ning igal aastal põhjustab tööstusspionaaž ettevõtetele kahju üle 55 miljardi euro. Saksamaa ettevõtted ja riigiasutused välisluure tähelepanu all ka seoses 2017. aastal Saksamaal toimuvate G20 üritustega: augusti keskel sai teatavaks pahavarakampaania seoses G20 tippkohtumise ja jätkuüritustega Hamburgis.

Petya/NotPetya pakub ikka veel õpikunäiteid sellest, kui pikaajalise ja laialdase mõjuga võib olla tõsine küberintsident. Ravimifirmal Merck oli veel augusti alguses suuri probleeme ravimitootmise ja ravimiarenduse taastamisega täies mahus, häiritud oli ka mõnede turgude varustamine ravimitega. Sagedased lunavararünded valmistavad endiselt peavalu ka haiglatele: Šotimaa Glasgow haigla langes taas lunavara ohvriks pärast maikuist WannaCry kampaaniat, mis jättis puutumata vaid kolm piirkondlikku tervishoiukorraldajat viieteistkümnest. Omamoodi märgilisena väärib mainimist ka juhtum USAst, kus ligi pool miljonit patsienti kutsuti arsti juurde südamestimulaatori püsivara uuendama – selgunud turvanõrkus võimaldanuks ründajal seadme aku tühjendada või seadeid muuta.

Septembri alguses sai teatavaks maailma ühe suurima krediidihinnangu teenust pakkuva ettevõtte **Equifax andmeleke**, mis puudutas 145.5 miljoni USA elaniku (suurusjärgus ca pool USA rahvastikust) andmeid: sotsiaalkindlustusnumbreid, juhilubade ja krediitkaardiandmed, aadresse jmt. Lekkis ka firma Mehhiko, Ühendkuningriigi ja Kanada klientide andmeid. Paraku kujunes lahendusest probleemi osa nii ebaõnnestunud kommunikatsiooni kui korralduse tõttu. Ettevõte viivitas poolteist kuud, enne kui lekke klientidele teatavaks tegi; veebileht, mis võimaldas kliendil kontrollida, kas andmeleke teda puudutas, osutus vigaseks ja tagastas samale päringule erinevaid tulemusi. Võimalike identiteedivarguste tuvastamiseks pakkus Equifax klientidele üheaastast tasuta krediidimonitooringu teenust, ent sidus selle tingimusega, et klient loobuks edasistest nõuetest ettevõtte vastu. Samuti nõuti klientidelt esiotsa teenustasu kontodele juurdepääsu blokeerimise eest, mis võimaldaks väärkasutamist tõkestada. Mõlemast viimasest nõudest küll hiljem loobuti.

Lisaks klassikalisele õppetunnile küberturbesse investeerimise vajalikkusest juhtis Equifaxi juhtum tähelepanu ka kriisideks valmisoleku tähtsusele. Suurte teenusepakkujate epideemia mõõtmed võtnud andmelekked viitavad vajadusele turvalisemate isikutuvastusmeetodite järele teenustes, nagu seda on kaheastmelised autentimislahendused (sh Eesti ID-kaart ja mobiil-ID).

14.-20. septembril toimunud Vene-Valgevene sõjalise ühisõppuse **Zapad 2017** ajal täheldati Venemaa ja Hiina internetiaadressidelt lähtunud teenustõkestusründeid Soomes Ahvenamaa mobiilsidevõrgus; sarnaseid intsidente oli lisaks Soomele väidetavalt ka Ühendkuningriigis ja Hollandis. Eestis Zapadiga seoses teenustõkestusründeid ei täheldatud. Küll kinnistas Norra samal ajal Venemaalt lähtunud raadiohäireid, mis mõjutasid lennuliiklust, põhjustades GPS teenuse tõrkeid. Sarnaseid juhtumeid on tulnud ette ka varasemate Vene Föderatsiooni sõjaliste õppuste käigus ja ilmselt ei ole tegu taotlusliku ründe, vaid kõrvalmõjuga, mida mööndakse, ent ei püüta vältida.