RIIGI INFOSÜSTEEMI AMET

# RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE OKTOOBER/NOVEMBER 2017

## Olukord Eesti küberruumis

**Oktoober** oli Eesti küberruumis registreeritud sündmuste (871) poolest viimase poolaasta aktiivseim kuu, ka küberturbeintsidentide hulk (299 ehk üle kolmandiku) ületas tuntavalt aasta keskmist taset. Kõrge prioriteediga intsidente oli seevastu vaid kaks ja ühiskondlikult oluliste (sh elutähtsate) teenuse osutajaid puudutanud intsidente 36. Intsidentidest veidi alla poole põhjustas kõikvõimalik pahavara; endiselt suur oli ka lunavara osakaal (ca kolmandik ehk 96).

Olulisemate intsidentide seas väärivad märkimist valvekaameratesse sissemurdmised neljas Harjumaa omavalitsuses. Rünneteks kasutati ära kaamerate lappimata turvaauke ning asjaolu, et ligipääs seadmetele oli piiramata. Intsidendi kordumise järel võttis üks valdadest ühendust CERT-EE-ga. RIA edastas hoiatuse teistele omavalitsustele, avaliku sektori infoturbejuhtidele ja elutähtsate teenuste osutajatele ning andis suunised turvanõrkuse kõrvaldamiseks.

**Novembris** registreeriti 894 juhtumit, millest küberturbeintsidente oli 224. Erasektorist pärineb stabiilne 85% juhtumitest; ühiskondlikult oluliste teenuste osutajaid puudutavaid intsidente oli novembris 34 ning kõrge prioriteediga juhtumeid 6. Oluliselt on vähenenud lunavara- ja tõusnud õngitsemisjuhtumite arv.

30. oktoobril avaldati teadusartiklis mh Eesti **ID-kaardi turvakiipe** puudutava haavatavuse (ROCA) detailne kirjeldus. Lisaks vähemalt 10 riigi digitaalsetele isikutunnistustele puudutas sama haavatavus mh Lenovo, HP, Toshiba, Fujitsu arvutite turvamooduleid (millele Microsoft andis välja ajutise turvapaiga); VPN juurdepääsu, e-posti turbe ning kriitiliste turvaoperatsioonide jaoks kasutatavaid krüptovahendeid ja osa kiibiga maksekaartidest. Infineon on maailma juhtivaid turvakiipide tootjaid ja müüdud kiipide arv ulatub nende väitel miljarditesse. Konkreetse turvaveaga kiipe on toodetud alates aastast 2012.

Uuendatud ohuhinnangust tulenevalt peatas Eesti 3. novembri südaööst turvanõrkusega ID-kaartide sertifikaatide kehtivuse. Selleks hetkeks olid laialdaselt kasutatavad era- ja avaliku sektori e-teenused valmis uuendatud sertifikaatide kasutuseks, ent arendused olid tehtud ajaga võidu joostes ega töötanud veatult; eriti meditsiiniasutuste valmidus oli väga kõikuv. Sertifikaatide kauguuenduslahenduse töökindlus oli stabiliseerunud, ent uuendatud oli vähem kui 6% kõigist turvanõrkusega ID-kaartidest ning alternatiivlahendus mID näol oli olemas vaid veerandil aktiivsetest kasutajatest. ID-kaardi juhtumi esmased õppetunnid viitavad vajadusele arvestada riskiplaneerimisel kogu eID ökosüsteemiga, kuivõrd lisaks autentimis- ja allkirjastamisteenuse enese toimepidevusele sõltub juhtumi ühiskondlik mõju samavõrra ka teenusepakkujate suutlikkusest tagada sõltuvate teenuste kättesaadavus ning toimiva eID lahenduse olemasolust võimalikult paljudel, kelle tavapärane töö- ja elukorraldus digitaalsetele teenustele juurdepääsust sõltub.

Teistest puudutatud riikidest on sama turvanõrkusega kaardid praeguseks sulgenud Slovakkia (ca 300 000) ja Hispaania (60 miljonit) vastavalt

31. oktoobril ja 2. novembril (lisaks varasemale Austria juhtumile, mille seos sama juhtumiga selgus hiljem). Veel viies ELi riigis on sama haavatavus teadaolevalt mõjutanud usaldusteenuse pakkujaid väiksemas ulatuses; osades neist on mõju ja edasised sammud veel hindamisel.

Novembri lõpus ületas uuendatud ID-kaartide hulk 300 000 piiri, neist 233 000 oli kasutanud kauguuendust. Septembri algusest novembri lõpuni lisandus üle 20 000 uue mID kasutaja. mID kasutuse osakaal alternatiivide seas on võrreldes septembri alguse 33% tasemega tõusnud 39%ni. Autentimis- ja digiallkirjastamise teenuste kasutusmahud pärast sertifikaatide peatamist vähenenud pole ja e-residentide osas on aset leidnud väike kasv.

## Tegevused küberjulgeoleku parandamisel Eestis

Oktoobris toimunud KOV volikogude valimiste küberturvalisuse tagamisel oli RIA-l seekord varasemast suurem roll: RIA osales konsultandina arenduses, vastutas turvatestimise läbiviimise eest, viis läbi riskianalüüse ja -hinnanguid ning pakkus tehnilist intsidendiseiret. Ühtegi intsidenti, mis võinuks mõjutada valimiste korraldamist või häälte lugemist, aset ei leidnud. E-hääletamise kasutusaktiivsus jäi üldjoontes samaks, mis viimastel kordadel (üle 30%), ning ID-kaardiga seonduv eelistusi valimisviisi osas seega ei mõjutanud.

Oktoobris toimus CERT-EE traditsiooniline Abuse@ee teabeseminar intsidentidele reageerimisest ja süsteemide turvalisest administreerimisest, samuti korraldati novembris koolitus intsidendihalduritele. Oktoobris tähistati ka üle-euroopalist küberturvalisuse kuud, mille eesmärgiks juhtida tähelepanu turvalisele digikäitumisele. RIA oli üks küberturvalisuse kuu eestvedajatest Eestis ning meie töötajad esinesid ettekannetega üritustel, külastasid loengutega koole ja osalesid töötubades.

Punkti sai Eesti poolt sel aastal EU TAIEX programmi raames pakutud kübertoetus Ukrainale avaliku ja erasektori koostööd puudutavates teemades. Sarja lõppüritusena korraldas RIA küberturvalisuse teenistus Ukraina ekspertidele novembris seminari, kuhu kaasas ekspertidena ka kolleege välisriikide partnerasutustest.

Koostöös Kaitseministeeriumi ja kaitseväega osales RIA Eestis toimunud NATO Cyber Coalition küberõppusel ja pakkus tuge selle läbiviimisel.

Lisaks korraldasime koostöös Rahvusvahelise Kaitseuuringute Keskusega riigikaitse erikursuse küberekspertidele, millest võtsid osa eksperdid nii eraõiguslikest (elutähtsate teenuste osutajad) kui ka riigiasutustest.

## Rahvusvaheline keskkond

Rahvusvahelises küberturvalisuse meediakäsitluses annavad üha enam tooni riiklikku päritolu küberründed, seda just kaasneva olulise mõju, mastaapsuse ja väljapaistvate sihtmärkide tõttu.

Küberturbefirma FireEye raporti kohaselt on sel sügisel täheldatud **Põhja-Korea** küberspionaaži aktiveerumist USA energiaettevõtete vastu. Siiani nähtu piirdub õngitsusrünnetega ning pole märke, et Põhja-Korea oleks seni suuteline leidma ligipääsu tööstusjuhtimisseadmetele või neid manipuleerima. Elutähtsatest teenustest on just energiasektor viimastel aastatel peamisi küberrünnete sihtmärke, ning FireEye väitel on neil andmeid vähemalt viie riigi toetatud rühmituste kohta, kes selles valdkonnas tegutsevad.

Oktoobris sai teatavaks Lõuna-Korea kaitseministeeriumi mulluse andmelekke ulatus – Põhja-Korea toimepandud andmevargus hõlmas ligi 235 GB salastatud dokumente, sh USA ja Lõuna-Korea operatiivplaane Põhja-Korea tuuma- ja raketisihtmärkide ründamiseks. Seoses sellega, et kuu alguses avati riigi teine interneti välisühendus (pakkujaks Venemaa telekomiettevõte), kasvab ekspertide mure Põhja-Korea suureneva küberründevõimekuse üle. Selle sagedaks sihtmärgiks on olnud finantssektor ning ka Euroopa pangad pole jäänud puutumata. Ühtlasi esinesid nii Ühendkuningriigi valitsus kui Microsofti president avaldustega, milles süüdistasid Põhja-Koread kevadises WannaCry lunavaralaines. Teadupärast kasutas WannaCry ära just Microsofti

toodete lekkinud turvaauke, ning Ühendkuningriigi tervishoiusüsteem oli üks kampaania suurimaid ohvreid.

Lisandub teavet Zapadi õppuse eel ja ajal toimunud **Vene Föderatsiooni** küberrünnete kohta. Läti mobiilsidevõrke suve lõpul tabanud seitsmetunnise katkestuse põhjustajaks on tõenäoliselt Venemaa, kinnitas Läti Seimi julgeolekukomitee asejuht. NATO liitlaste kaitseväe- ja valitsusametnikud on kinnitanud Venemaa katseid häkkida Balti riikides ja Poolas paiknevate väeüksuste liikmete isiklike mobiiltelefone, et hankida teavet üksuste suuruse ja operatsioonide kohta ning kaitseväelaste moraali õõnestada.

USAs pakub taas palju kõneainet Venemaa väidetav teabevargus USA riiklikust julgeolekuagentuurist (NSA), kus Kaspersky Labi viirustõrjetarkvara kaudu varastati salastatud teavet USA kübervõimekuse kohta. Teave lekkis NSA töötaja koduarvutist ning kujutas endast väidetavalt küberrünneteks kasutatavat pahavara. See, et seadmest leitud pahavaranäidised edastatakse viirustõrje tootjale analüüsiks ja viirustõrje ajakohastamiseks, on valdkonna tavapärane praktika. Kaspersky on väidetele teravalt reageerinud ja kinnitab endiselt, et ei tee luurekoostööd VF ametkondadega. Eksperdid näevad probleemi, et poliitilise kõmu otsimise taustal jääb tähelepanuta küberhügieeni ja turvaprotseduuride järgimise olulisus.

Oktoobri lõpus toimunud Tšehhi **parlamendivalimiste** tulemusi kajastavate veebilehti tabasid teenustõkestusründed (DDoS). Valimiskomisjon kinnitab, et katkestus ei puudutanud häältelugemise ja edastamise infosüsteeme ega mõjutanud hääletustulemust. Siiski on juhtunu näiteks sellest, kuidas valimiste küberriskidega tuleb arvestada kõigil riikidel, sõltumata e-hääletamise võimaluse olemasolust või selle puudumisest.

Aasta viimases kvartalis on sagenenud **lunavararünded**. Eeskätt Venemaad ja Ukrainat tabas oktoobri lõpus taas ulatuslik, Bad Rabbitiks nimetatud lunavaralaine. Pahavara „käekirjas" on mitu sarnasust suvise Petya/NotPetya lunavaraga, ent ohvrite arvu ja mõjuala poolest jäi selle levik suvisest piiratumaks. Lunavara jagati nt Venemaa Interfaxi ja Fontanka uudisteagentuuride kompromiteeritud veebilehtede kaudu, mh kannatasid lunavara tõttu kahju Odessa lennujaam, Kiievi metroo ning Ukraina taristuministeerium ja riiklik lennuliiklusteenindus. Vähemal arvul nakatumisi oli veel vähemalt viies riigis, sh Bulgaarias ja Saksamaal, ning mõned ohvriks langenud organisatsioonidest teatasid ulatuslikest häiretest asutuste töös. Lisaks suurematele kampaaniatele nagu WannaCry, Petya/NotPetya ja BadRabbit on arvukaid lunavaravariante käibel pidevalt – nt küberturbeettevõte Symantec on viimase 1,5 aasta jooksul loendanud ligi 130 erinevat „lunavaraperekonda". Uudised tervishoiu- ja haridusasutuste, avaliku halduse, ühiskonnaoluliste teenuste ja tööstusettevõtete lunavaraintsidentide kohta on muutunud iganädalaseks rutiiniks.

Rootsis põhjustasid DDoS-ründed transpordiameti infosüsteemide vastu oktoobri lõpus mõnetunnise katkestuse ja päev läbi kestnud tõrkeid liiklusregistri ning asutusesiseste infosüsteemide töös. Pooleks tunniks oli häiritud ka lähirongiliiklus. Novembris said ründajad juurdepääsu 24 Rootsi linnas edastatava eraraadiojaama programmiedastussüsteemile, mille tagajärjel mängiti eetris hommikuprogrammi ajal pool tundi terrorismipropagandat sisaldavat muusikat.