RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE MAI 2017

Olukord Eesti küberruumis

Maikuu sündmuste arv Eesti küberruumis jäi aprilliga samale tasemele – registreeriti 795 juhtumit, millest küberturbeintsidendiga oli tegu 215 juhul. Avalikust sektorist pärinevate juhtumite osakaal jääb stabiilselt 20% piirimaile. Elutähtsa teenuse osutajaid puudutanud juhtumeid oli mais 51.

Stabiilsena on aasta algusest püsinud ka kõrge prioriteediga intsidentide igakuine osakaal (mais kokku 17); seevastu oli mais intsidentide pilt tavapärasest kirjum. Olulisemana võib välja tuua korduvaid teenusekatkestusi elektroonilise isikutuvastamise ja digiallkirjastamise teenuste kasutamises ID-kaardi ja mobiil-ID abil. 10. mail toimus teenustõkestusrünne Leedu SEB panga vastu, mille tagajärjel olid lühiajaliselt kättesaamatud kõigi kolme Balti riigi SEB panga kodulehed, samuti polnud võimalik internetipanga kasutamine.

Tegevused küberjulgeoleku parandamisel Eestis

Maikuuga jõudis lõpule küberturvalisuse koolitustesari eesistumisega seotud riigiametnikele. Kokku osales ligi 1200 ametnikku; saadud tagasiside hindas koolitused sisukaks, praktiliseks ja igapäevaselt vajalikuks. Osalenud asutused väljendasid huvi edasise koolituse vastu ka nutiseadmete turvalise kasutamise teemal.

Mai keskel avas RIA riigiasutustele kasutamiseks digitaalse õpikeskkonna digitest.ria.ee, kus saab testida ja täiendada teadmisi turvalisest käitumisest küberruumis. CybExer Technologies väljatöötatud digitest kasutab näidetena elulisi olukordi ja realistlikke stsenaariume, et parandada kasutajate teadlikkust. Tulevikus soovib RIA keskkonna teha kättesaadavaks ka koolidele.

24.-25. mail toimus RIAs kolme Balti riigi ja USA ekspertide kohtumine elutähtsa taristu kaitse teemadel, kus keskenduti energeetikavaldkonna sõltuvusele ning sellest tulenevate riskide haldamisele. Kohtumisel osalesid ka energiaettevõtjate esindajad.

Lisaks hoiatas CERT-EE kuu jooksul avalikkust mitmest ohtlikust tarkvarahaavatavusest ja pahavarakampaaniast. Kuu keskel toimunud üleilmse WannaCry lunavararünde ajal viisime läbi ulatusliku teavituskampaania, et selgitada ohu olemust ja anda juhiseid ohust hoidumiseks.

Rahvusvaheline keskkond

Kuu tähelepanuväärseim rahvusvaheline kübersündmus oli kahtluseta üleilmne **WannaCry** lunavararünne. Mai teisel nädalavahetusel loetud tundidega üle maailma levinud lunavara ohvrite seas oli Hispaania suurim telekommunikatsioonieettevõte Telefonica, ligi 40 Ühendkuningriigi raviasutust, Vene Föderatsiooni siseministeerium ning pangad, raudteejaamad, logistikafirmad ja olulised ettevõtted ligi 150 maailma riigis. Enim kahju kannatasid Euroopa ja Venemaa organisatsioonid. Ühendkuningriigis tühistati intsidendist tabatud haiglates operatsioonid ja suunati ümber kiirabibrigaade; Renault autotööstus oli sunnitud tootmise mõneks päevaks peatama. Ohvrite arvuks hinnatakse üle veerand miljoni. Ehkki ametlikku kinnitust pole, osutavad mitmed allikad võimalusele, et WannaCry rünne võis olla seotud Põhja-Korea häkkeritega.

WannaCry näol ei olnud tegemist sihitud ründega, ohvriks sattusid iganenud operatsioonisüsteemiga arvutid valimatult. Lunavara levik kasutas ära aprillis USA riikliku julgeolekuagentuuri NSA teabelekke järel teatavaks saanud sideprotokolli turvaviga vananenud Microsoft Windows operatsioonisüsteemides. Turvauuendus vea parandamiseks oli välja antud kaks kuud varem, ent uuendamata süsteemid (eeskätt Windows XP, mida Microsoft 2014. aastast enam ei toeta) jäid haavatavaks ning lunavara levis kiiresti, sest selle käivitumine toimus kasutajast sõltumatult.

WannaCry esmaversiooni levikule pandi mõne päevaga piir, ent järgnenud on mitu uut lainet ning võib eeldada, et avalikuks saanud turvanõrkusi kasutatakse ära edaspidigi. Lunavara vastu pakub kaitset vaid uuendatud tarkvara. Riskide maandamiseks on oluline teha kriitilistest andmetest varukoopiaid.

Eestis WannaCryl ohvreid ei olnud. Pahavara üritas rünnata paarikümmet süsteemi, ent aiakohase tarkvaraga seadmetes see ei käivitunud ja kahju ei tekkinud. Lisaks võttis CERT-EE ühendust potentsiaalselt ohustatud asutustega, et ohust teavitada ja juhendada süsteemide turvamisel, samuti avaldasime hoiatusi ja juhiseid avalikkusele. Kahju ärahoidmisel oli oluline roll ka RIA 2013. aastal korraldatud ennetaval teavituskampaanial Windows XP kasutamisest loobumiseks, mille järel vähenes selle osakaal Eestis alla 20%-ni operatsioonisüsteemidest. Lisaks oleme terve 2016. aasta pööranud erilist tähelepanu tervishoiusektori infoturbe parandamisele.

Küberturbeettevõtte NTT Security uuringu kohaselt on **riigivalitsemine** tõusnud finantsvaldkonna kõrval üleilmselt esimeseks küberrünnete sihtmärgiks. Ründeviiside seas on esikohal nn õngitsusründed, mida lisaks andmepüügile kasutatakse ka pahavara levitamiseks. Mai keskel teatas Rumeenia luureteenistus riigi välisministeeriumi ametnike vastu suunatud ja viimistletud õngitsusründest, kus NATO allikana esinedes saadeti ametnikele väidetavalt Süüria sündmusi käsitlev võltsitud dokument, mis sisaldas pahavara.

Vahetult **Prantsusmaa presidendivalimiste** teise vooru eel teatas Emmanuel Macroni kampaaniameeskond erakonna vastu korraldatud „massiivsest ja koordineeritud" küberründest, mille tagajärjel paisati anonüümses internetikeskkonnas avalikkuse ette suur hulk erakonna sisemist kirjavahetust ja dokumente. Andmeleke leidis aset vahetult enne valimiseelse poliitreklaami keelu jõustumist, mis ei võimaldanud dokumentide sisu ametlikult kommenteerida või aiakirjanduses kajastada ning jättis tõlgendamise ja vandenõuteooriate levitamise sotsiaalvõrgustike meelevalda. Nagu USA valimiste eel, kombineeriti lekitatud materiale ka nüüd väärinfoga, et külvata segadust ja kahtlusi.

Macroni kampaaniameeskond oli juba varem valimiskampaania käigus korduvalt viidanud erakonna juhtide e-postikontode vastu üritatud häkkimiskatsetele. Paar nädalat enne valimisi sai teatavaks Macroni erakonna En Marche'i nime järjendavate domeeninimede registreerimine, kust saadeti õngitsuskirju, saamaks ligipääsu erakonna võtmeisikute kontodele.

Prantsuse ja USA valimiste kogemusele toetudes on Saksamaa suurendanud riigi küberturbeagentuuri BSI rahastust ja lisanud ametikohti, samuti kavandatakse tugevdada BSI õiguslikku mandaati küberrünnetele reageerimiseks.

Mai lõpul tingis **British Airwaysi** mastaapne infosüsteemide rike ettevõtte lendude ärajäämise ja hilinemise kahe päeva vältel. Katkestus mõjutas tuhatkonda British Airwaysi lendu üle maailma ning tõi ettevõttele karmi kriitika IT-personali koondamise eest möödunud aasta lõpul, mistõttu nüüd jäädi hätta teenuste töö taastamisega.