RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE JUULI 2018

Olukord Eesti küberruumis

Juulis registreerisime **296 intsidenti**, mida oli küll vähem kui juunis, kuid rohkem kui eelmisel aastal samal ajal. Üha enam näeme trendi nakatada infosüsteeme **krüptoraha kaevandamise** eesmärgil. Tegu on hetkel kindlasti ka ülemaailmse trendiga, mida kajastab näiteks ka Iisraeli küberturbeettevõtte Check Point värske raport.

Kuumalaine perioodil katkes Ida-Virumaal ühes 17 000 elanikuga linnaosas **automaatjuhtimissüsteemi rikke tõttu veevarustus.** Juhtimissüsteemi side katkemise tagajärjel seiskus veetöötlusjaam, mis katkestas omakorda veevarustuse. Antud juhtumi juures on oluline see, et polnud pööratud piisavat tähelepanu varulahendustele, mis oleks veevarustuse katkemise ära hoidnud.

Virumaal asuv tervisekeskus (5000 patsienti) langes lunavara ohvriks, mis tõi kaasa häired asutuse töös. Tervisekeskus ei omanud pärast intsidenti ülevaadet vastuvõtule tulevatest patsientidest, kuid inimeste vastuvõtt siiski ei katkenud ja digiretsepte oli võimalik väljastada. Krüpteeritud andmed õnnestus taastada nädala jooksul.

Tegevused küberjulgeoleku parandamisel Eestis

Juulikuus jõudis **kõigi inimeste arvutitesse uus ID-kaardi rakendus** DigiDoc 4, milles saab teha kõiki ID-kaardiga seotud toiminguid. Uue rakenduse saamiseks tuleb nõustuda arvuti pakutava uuendusega; sujuvama ülemineku jaoks jääb esialgu arvutitesse alles ka senine rakendus DigiDoc 3. DigiDoc 4 toob endaga kaasa erinevaid uuendusi paremaks kasutajakogemuseks – muudetud on kasutajaliidese disaini ja uuendatud kasutusloogikat ning nüüd saab kõiki ID-kaardi toiminguid teha ühes kasutajaliideses.

Eesti juhtimisel valmis valimisturvalisuse käsiraamat, mis on mõeldud valimiste korraldajatele ja nende küberturvalisuse eest vastutajatele. Kogumik koosneb praktilistest soovitustest ja tehnikatest küberturvalisuse tagamiseks kogu valimisprotsessi ulatuses alates kandidaatide registreerimisest kuni häälte kokkulugemise ja tööni erakondadega ning põhineb paljude ELi riikide parimal praktikal. Projekt sai alguse Eesti ELi Nõukogu eesistumise ajal ning selle valmimisele panustasid lisaks enam kui kahekümnele ELi liikmesriigile ka Euroopa Komisjon, Euroopa Info- ja Võrguturbeamet (ENISA) ja Euroopa Parlament.

Juulis andsime välja hoiatuse võrguseadmete vastu suunatud rünnakute eest. Rünnati Läti ettevõtte toodetud Mikrotiki võrguseadmeid, mida kasutatakse mitmel pool Eestis. Selle haavatavuse ärakasutamise kaudu on võimalik näiteks kuulata pealt võrguliiklust või varastada krediitkaardiandmeid. Haavatavuse tingis asjaolu, et seadmete tarkvara oli jäetud nende kasutajate poolt uuendamata.

Rahvusvaheline keskkond

Hiina küberluuregrupp ründas Kambodža valimisi. Varasemalt merendusvaldkonda rünnanud rühmitus on oma viimased rünnakud suunanud strateegiliselt oluliste riikide poliitiiliste süsteemide vastu. Kambodža on seni olnud üks Hiina toetajatest Lõuna-Hiina mere küsimuses.

Leedu riiklik küberjulgeoleku keskus (NCSC) andis välja avaliku soovituse mitte kasutada Yandex Taxi transpordiplatvormi, kuna tegemist on julgeolekuriskiga. Nimelt kogub Yandex Taxi kasutaja kohta enam andmeid, kui sarnased sõidujagamise platvormid ning Leedu kolleegide väitel toimub andmeedastus Venemaal paiknevatesse serveritesse. Ka Eesti ametkonnad soovitavad oma kommentaarides olla enda isikuandmete jagamisel valvsad ning pöörata tähelepanu, milliseid andmeid erinevaid rakendused kasutaja kohta koguvad.

Saksamaa nimetab siseturvalisuse ohte kirjeldavas raportis, et **küberrünnakuid informatsiooni infrastruktuuri** vastu kasutatakse ära kui standardset vahendit teostamaks küberluuret teiste riikide julgeolekuteenistuste poolt. Ohu alla on sattunud ka Saksamaa ettevõtted tänu tihedale konkurentsile maailmaturgudel.

USA kohus esitas kaheteistkümnele Venemaa luureohvitserile süüdistuse 2016. aasta presidendi valimistesse sekkumises. Süüdistuste kohaselt korraldati küberründeid Demokraatliku Partei ja valimiste korraldamisega seotud infosüsteemide vastu.

USA ja Lääne-Euroopa veebipoed on kandnud sel aastal pettuste tõttu ligi 19 miljardit dollarit kahju. Ohutudega võitlemiseks püütakse leida uusi lahendusi tehisintellektist. Ühe võimalusena proovitakse kasutada Blockchain tehnoloogiat, mida on juba edukalt rakendatud turvaliste maksete teostamisel.

NATO tippkohtumisel Brüsselis võeti vastu deklaratsioon, kus korrati üle lubadust tugevdada liikmesriikide kübervõimekust heidutamaks, kaitsmaks ning tõrjumaks küber- ja hübriidohte. Sealhulgas värskendati taas Küberkaitse kokkulepet (*Cyber Defence Pledge*), millega iga liikmesriik lubab arendada oma võimekust kriitilise informatsiooni infrastruktuuri kaitsmisel.