RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE JUUNI 2017

Olukord Eesti küberruumis

Eesti küberruumis registreeriti juunis poolsada juhtumit rohkem kui mais. 845 juhtumist olid 262 küberturbeintsidendid, millel oli mõju andmete terviklusele, käideldavusele või konfidentsiaalsusele. Võrreldes aasta varasemaga on juhtumite ja intsidentide arv kasvanud. Seda võib osaliselt põhjendada kasutajate ohuteadlikkuse kasvuga, sest osatakse märgata turvariske ja neist teada anda. Ka on CERT-EE intensiivistanud monitooringutegevusi, mistõttu potentsiaalseid probleeme märgatakse suurema tõenäosusega varem.

Avaliku sektoriga oli juunis 2017 seotud 108 juhtumit ning elutähtsa teenuse osutajaid puudutanud juhtumeid oli juunis kokku 43. Enamik juhtumitest olid seotud teenusekatkestuste või veebilehtede kompromiteerimistega. Kaks juhtumit puudutas elektroonilise isikutuvastamise ja digiallkirja teenuseid, sh esines lühiajalisi tõrkeid Telia võrgus mobiil-ID kasutamisel.

Kuu lõpus tegi üle maailma kahju ulatuslik pahavarakampaania Petya/NotPetya, mis levis Ukraina ettevõtte poolt pakutava raamatupidamistarkvara MeDoC kaudu. Kuigi pahavara käitus pealtnäha nagu lunavara, on ta tehniliselt keerukam ning eesmärgiks oli andmete jäädavalt kasutamatuks muutmine. See tähendab, et andmed krüpteeriti ja dekrüpteerimine ei olnudki ette nähtud ega võimalik.

Arvatakse, et rünnak oli suunatud Ukraina asutuste ja suurettevõtete vastu. Esimesed nakatumised toimusid Ukrainas, kus teadaolevalt oli kokku üle 12 500 ohvri. Teateid nakatumistest laekus 64 riigist, sealhulgas Eesti erasektorist. Kõik teadaolevad Petya/NotPetya ohvrid Eestis nakatusid läbi ettevõtte või kontserni rahvusvahelise arvutivõrgu.

Kuni 1. juulini oli võimalik uuendada IDkaardi sertifikaate, mis väljastati enne 2014. aasta oktoobrit. Juuli algusega oli uuendatud kaarte kokku 107 512, uuendamata ca 400 000. Uuendamata jätmisel piirab Google'i veebilehitseja Chrome e-teenustele ligipääsu, muu mõju võib avalduda hiljem.

Tegevused küberjulgeoleku parandamisel Eestis

Küberturvalisus ja laiemalt digitaalse ühisturu teemad läbivad Eesti EL-i eesistumist. Kõrgenenud rahvusvaheline tähelepanu ning Eestis toimuvad sündmused suurendavad ka poliitiliselt motiveeritud küberrünnete tõenäosust.

Selle kevade küberründed on veelkord rõhutanud vajadust parandada Euroopa Liidu kui terviku suutlikkust tegeleda laiaulatuslike küberintsidentidega. Eesti eestvedamisel keskendutakse muuhulgas raamistiku loomisele, et Euroopa Liit saaks vajadusel kasutada oma poliitilisi ja majanduslikke hoobasid (sh sanktsioonide kehtestamine) küberrünnetele vastamiseks. Sellise mehhanismi loomine töötaks heidutusena, mis tagaks kogu ühenduse küberjulgeolekut senisest tõhusamalt.

RIA on märkimisväärselt kaasatud ka eesistumise korraldamisesse. EL2017 turvalisuse tagamisel arvestatakse teiste kõrval ka küberruumi ohtudega.

Kuu alguses hoiatas CERT-EE avalikkust õngitsuskirjade ja uue lunavaraga nakatumise laine eest. Sealhulgas tuletati taaskord meelde infoturbemeetmete rakendamise olulisust ja toodi välja näitlikustav nimekiri meetmetest, millega ennetada pahavaraga nakatumist.

Rahvusvaheline keskkond

Üha enam on sagenenud madala profiiliga ründed, mis püüavad vältida seiresüsteemide radarile jäämist. Juuni lõpus tehti sisselogimiskatseid Ühendkuningriigi parlamendi liikmete ja töötajate e-postisüsteemidesse. Metoodiliselt prooviti läbi levinumaid paroole sagedusega, mis ei lukustaks rünnatavat kontot, st rünne ei olnud kergelt tuvastatav.

Ründe tulemusena saadi ligipääs ca 90 kontole, millede puhul oli kasutatud nõrku paroole. E-posti ründele järgnesid õngitsuskatsed telefoni teel, kus helistaja esines Windowsi töötajana. Eesmärgiks oli teada saada parlamendi töötajate kasutajanimesid ja paroole, kuid edutult.

Kahe ründekatse vahel ei ole kinnitatud seost ning mõlemad on sarnased ka Eestis esinenud kampaaniatele.

Küberruumil on oluline roll rahvusvaheliste suhete tasakaalus. Katari riikliku uudisagentuuri *Qatar News Agency* kompromiteeritud võrgu kaudu süüdistati riiki terrorismi toetamises ja rahastamises. Avaldatud valeuudise tagajärjena teavitasid mitmed Lähis-Ida riigid Katariga sidemete katkestamisest ning olukord regioonis pingestus. FBI ja teised luureagentuurid on mitteametlikult omistanud ründe Venemaal asuvatele küberkurjategijatele, kelle võisid palgata teised Lähis-Ida riigid.

Tööstuslikud juhtimissüsteemid pole pahavarast puutumatud. Keerulist pahavara on võimalik kasutada erinevates tööstusjuhtimis-süsteemides olenemata riigist ja sektorist ning üha enam on ründeid suunatud kergelt haavatavatele tsiviiltaristule, sealhulgas elutähtsatele teenustele. Erilises fookuses on energeetika. Näiteks rünnati spetsiaalse pahavaraga 2016. aasta detsembris Kiievi (Ukraina) kõrgepinge alajaama juhtimissüsteemi põhjustades ulatusliku elektrikatkestuse ning aasta varem jättis rünnak levivõrgu vastu Ukrainas elektrita 30 alajaama ja umbkaudu veerand miljonit majapidamist.

Sel suvel kirjutab ajaleht Washington Post, et "Vene valitsuse häkkerid" on sisse tunginud energeetikaettevõtete ärivõrkudesse. Ajalehega rääkinud USA valitsusallikate sõnul on ohvriks olnud energiaettevõtted (sh tuumaenergeetikas tegutsevad), kelle võrke on kaardistatud. Selline tegutsemine võib olla märk suurema rünnaku korraldamise eeltööst.

Ajalehe andmetel on see esimene kord, kui "vene valitsuse häkkerid" on teadaolevalt jõudnud Ameerika tuumaenergeetika ettevõtete võrkudesse. Kasutajanimesid ja salasõnu varastades sai ründaja ligi ärivõrkudele (nt personalihaldus), kuid ei ole tõendeid, et ründajad oleks ligi pääsenud elektritootmise põhisüsteemidele, mis oleks ohustanud avalikkust.

Ilmselt on sektor olnud ründajate kõrgendatud tähelepanu all juba mõnda aega. USA energeetikaettevõtete vastased ründed näitavad veelkord, et tsiviilkasutuses olevate elutähtsate süsteemide häkkimine rahuajal ei ole vastase jaoks tabu.