RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE SEPTEMBER 2016

Olukord Eesti küberruumis

Septembris käsitleti Eesti küberruumis kokku 610 juhtumit. Olulisema mõjuga juhtumiteks võib pidada petuskeemide laienemist avalikus sektoris, kus võltsitud e-kirjade ja nimede kaudu üritati raha välja petta. Säärastes skeemides üritati septembris senisest laiemalt kasutada avaliku sektori tippjuhtide ja isegi peaministri identiteete.

Lisaks nakatus septembris lunavaraga piiratud mahus ka üks elutähtsa teenuse osutaja Tallinnas. Suuremat kahju õnnestus vältida ja andmed taastati varukoopia abil.

Küberjulgeoleku parandamine Eestis

20.–22. septembrini osalesime Kaitseministeeriumi ja USA Euroopa Väejuhatuse EUCOM korraldatud rahvusvahelisel küberkaitseõppusel Baltic Ghost 2016, mille raames harjutati rahvusvahelist tegevust olulise mõjuga küberintsidentide korral, ennekõike USA ekspertide kaasamist Balti riikides toimuvate küberintsidentide lahendamisse. Õppuse siseriiklikus osas harjutati küberturvalisuse teenistuse koordineerimisel ka praktiliselt läbi Kaitseliidu küberkaitseüksuse kaasamist elutähtsa teenuse osutaja Elering abistamiseks küberintsidendi korral.

Viisime lõpule analüüsi selle kohta, kuidas suudavad infotehnoloogiast tulenevaid riske oma teenustele analüüsida elutähtsate teenuste osutajad ja neid korraldavad asutused. Olukord Eestis ei ole selles valdkonnas hea, kuna enamasti **ei suuda elutähtsate teenuste toimimisega seotud asutused Eestis IT-riske ning nende võimalikku mõju oma teenustele** veel piisavalt hinnata. Olukorra parandamiseks korraldame koolitusi IT-riskide analüüsimise oskuste parandamiseks. Septembris osales meie läbiviidud järjekordsel koolitusel 19 spetsialisti 12 asutusest.

Internetis sai kättesaadavaks Dropboxi pilveteenusest mõni aeg tagasi varastatud kasutajakontode andmebaas, mida oli kokku umbes 68 miljoni kasutaja kohta. Küberturvalisuse teenistus analüüsis neid andmeid ja leidis **suure hulga Eesti kõrgete riigiametnike** ja oluliste asutuste töötajate Dropboxi kontode infot, **kes olid kasutanud oma tööalaseid e-posti aadresse avalikku pilveteenusesse sisenemiseks** ja kes selle juures kasutasid mitmel puhul nõrga turvalisusega paroole. Seega sai selles andmekogus leidunud info abil rünnata nii inimeste ametialaseid kontosid kui nendega seotud asutusi ja kuna andmed varastati juba mõnda aega tagasi, võivad paroolid olla tänaseks lahti murtud ja konto üle võetud. Jätkame analüüsi ja informeerime asutuste turvajuhte leidudest.

Valik rahvusvahelisi teemasid

Yahoo teavitas u 500 miljoni kasutaja informatsiooni vargusest, mis sai alguse juba 2014. aastal ja on seni suurim ühte teenusepakkujat puudutav kasutajainfo vargus, mis hiljem on juhtumi uurijate sõnul jõudnud „riiki Ida-Euroopas“. Juhtumi hilisem analüüs on jõudnud ka selleni, et tegelik varastatud kontode arv Yahoost võib olla isegi rohkem kui miljard. Suurtest kasutajanumbritest olulisem on aga see, et nii täna kui tulevikus kasutavad inimesed endiselt samu paroole erinevate teenuste lõikes ja seega on jõutud ka järeldusele, et ohus on ka kõikide teiste paroole kasutavate meili- ja muude internetiteenuste kasutajainfo. Mis omakorda lihtsustab tuntavalt erinevat laadi küberkuritegevust ja ka erinevate sihitud rünnete läbiviimist.

Saksamaa küberturbeagentuur BSI teavitas augustis läbiviidud hästi sihitud kampaaniast, millega rünnati Saksamaa erakondi, eesmärgiga viia erakondade infosüsteemidesse nuhkimistarkvara. BSI president seostas rünnakuga Venemaad ja selle grupeeringut Sofacy (APT28), kelle eesmärk olevat õõnestada eelseisvaid valimisi, ja pakkus Saksa erakondadele vajadusel abi küberturvalisuse tõstmisel.

Uue ülemaailmse trendi ettekuulutajana toimusid septembris mõned väga suure mahuga teenusetõkestusründed, mis viidi läbi kasutades n-ö „asjade Interneti“ ehk erinevaid Interneti ühendatud seadmeid, mille turvalisus on nõrk ja mis võimaldavad neid seega samuti rünneteks ära kasutada.

USA ekspertide sõnul võib näha märke sellest, et mõned riigid võivad üritada teha ettevalmistusi Interneti kui terviku aluseks oleva taristu ründamiseks, eesmärgiga peatada kogu Interneti toimimine.

Ettevalmistused Eesti EL eesistumiseks 2017

Alustame alates novembrist 2016 küberohtude vältimise koolitusi eesistumisega seotud ametnikele ja töötajatele, keda on kokku umbes 1300.