RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE OKTOOBER 2016

Olukord Eesti küberruumis

Oktoobris jõudis RIA küberintsidentide süsteemi kokku 873 juhtumit, millest põhjalikumat tegelemist vajavaid intsidente oli 131. Avalikust sektorist pärines alla kolmandiku ning erasektorist kaks kolmandikku juhtumeist. Elutähtsaid teenuseid puudutavaid juhtumeid oli kokku 19, sealhulgas esines lühiajaliselt häireid ühe sideettevõtja kõnesideteenuses ning pankade kaardimaksete ning internetipanga töös.

Tegevused küberjulgeoleku parandamisel Eestis

Informeerisime riigiasutuste ja elutähtsate teenuste osutajate turvajuhte septembris internetti lekkinud DropBoxi kasutajakontode andmebaasi analüüsi leidudest ning teavitasime avalikkust riskidest, mis kaasnevad pilveteenuse kontode sidumisel tööaadressiga.

Teavitasime veebipoodide pidajaid Eestis laialt kasutatava e-poe veebiplatvormi Magento turvaveast, mis võimaldab varastada krediitkaardiandmeid. Ühtlasi juhendasime ettevõtjaid kasutatava tarkvara uuendamisel.

CERT-EE palub Joomla sisuhaldustarkvara ja Linuxi kasutajatel teha tarkvarauuendused oluliste turvanõrkuste parandamiseks. Juhendid nii Joomla kui Linuxi tarbeks on kättesaadavad RIA veebist.

Osalesime Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) korraldataval ELi suurimal küberkriisiõppusel Cyber Europe 2016. Õppusel harjutasid üle-euroopalisele küberkriisile reageerimist kõigi ELi liikmesriikide ning Norra ja Šveitsi eksperdid nii avalikust kui erasektorist. Eestist osalesid lisaks riigiasutustele ka Tallinna Lennujaam, sideettevõtjad ning Kaitseliidu küberkaitseüksus.

Seoses USAs asetleidnud küberrünnakutega (vt all) juhtisime tähelepanu vajadusele paremini turvata veebi ühendatud koduseadmeid.

Valik rahvusvahelisi teemasid

7. oktoobril teatasid USA riiklik luuredirektor ja sisejulgeolekuministeerium ühisavalduses, et peavad Vene Föderatsiooni valitsust vastutavaks Demokraatide Rahvuskomitee (DNC) infosüsteemidesse sissemurdmise ning rohkem kui 19 000 e-kirja varguse ja avaldamise eest, eesmärgiga mõjutada USA presidendivalimiste tulemusi. Seni ei ole teada, et valimiste hääletussüsteeme endid oleks kompromiteeritud, küll lekkisid mõnes osariigis valimisnimekirjad.

Kuu keskel sattus mastaapse teenusetõkestusründe (DDoS) ohvriks USA üks suurimaid domeeninimeteenuse (DNS) pakkujaid Dyn. Mitme tunni jooksul olid esmalt USA idarannikul, hiljem üle riigi ning ka Euroopas kättesaamatud üle tuhande veebilehe, nende seas sotsiaalvõrgustikud, meediaväljaanded ning e-kaubandus ja -teenused. Lõviosa DNS pakkuja vastu suunatud andmevoost pärines Mirai-nimelise pahavaraga nakatunud nn asjade interneti seadmetelt, milleks seekord enamjaolt veebikaamerad ja kodused videosalvestusseadmed. Ründed olid märkimisväärsed iseäranis nende sihtmärgi tõttu – suunatuna DNS-teenuse vastu, mis "tõlgib" sõnalised domeeninimed numbrilisteks IP-aadressideks, rünnati interneti baasarhitektuuri. Ekspertide hinnangul oli seekordse teenusetõkestusründe maht seninähtuist suurim, ulatudes tipphetkel kuni 1,2 terabitini sekundis. Asjade interneti seadmete üha laiem levik ning nende pea olematu turvalisus loovad eeldused taolise ründemustri kinnistumiseks.