



RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE NOVEMBER 2016

Olukord Eesti küberruumis

Novembrikuu 747st CERT-EE teavituste süsteemi laekunud küberjuhtumist kvalifitseerus intsidentiks pea iga kaheksas (96).

Kõrge prioriteediga juhtumeid leidis aset 12, nende seas kaks mobiil-ID teenusekatkestust ning tööpäeva väldanud tõrked Digiresepti töös. Suurima osa kuu jooksul toimunud intsidentidest põhjustasid erinevad õngitsusmeetodid, millega üritati kasutajatelt kätte saada välismaiste teenusepakkujate kasutajaandmeid, samuti kuulusid olulisemate intsidentide sekka eespool mainitud teenusekatkestused. Ülejäänute (pahavara, turva- ja administreerimisvead, lunavara jt) esinemissagedus jäi üksikjuhtumite tasemele.

Tegevused küberjulgeoleku parandamisel Eestis

16. novembril korraldas Kaitseliidu küberkaitseüksus (KKÜ) koostöös RIAga Tallinnas küberkaitsekonverentsi, mille teema oli küberkriisideks valmisolek ja nende tõhus lahendamine. Sadakonnale konverentsist osavõtnule tutvustati valdkonna pakilisemaid probleeme ja otsiti ühiselt lahendusi.

25. novembril toimus RIA eestvedamisel kriitilise informatsiooni infrastruktuuri (KII) kaitse infopäev, millest võttis osa üle 70 spetsialisti riigiasutustest ja elutähtsate teenuste osutajate juurdest. Tutvustasime küberturvalisuse tagamise praktikaid nii RIA kui ETO vaatest, samuti andsime ülevaate RIA tellitud kübervaldkonna õigusanalüüsi tulemustest.

Lisaks toimus tavapärase teavitustöö meedias, sotsiaalvõrgustikes ja vahetutel kohtumistel, nt tutvustasime CERT-EE tegevust Põltsamaa Ühiskõhvikus küberkaitse õppesuuna õpilastele. Osalesime ka NATO Cyber Coalition õppusel.

Valik rahvusvahelisi teemasid

Novembrikuusse jagus üle ilma mitmeid näiteid elutähtsate teenuste mõjutatud küberintsidentidest. Muu hulgas olid kolm [Kirde-Inglismaa haiglat](#) arvuti viirusest tingitud intsidentide tõttu sunnitud mitme päeva vältel ära jätma plaanilised operatsioonid, arstivisiidid ja diagnostilised toimingud. Ühendkuningriigi Tesco pank külmutas [veebipõhised tehingud](#) pärast ligi 40 000 klienti mõjutatud küberrünnet; ligi [neljandikult](#) neist varastati kontodelt ründe käigus raha. Enamik panga kliente kasutab lihtsat paroolipõhist autentimist; kaheastmelise autentimise võimalus on küll olemas, ent klientidele soovituslik. Soomes [Lappeenranta](#) löi teenustööstusrühne kombineerituna tarkvaraveaga mõneks päevaks rivist välja kohaliku keskküttesüsteemi. USA San Francisco linna [ühistranspordisüsteemi](#) ning sellega seotud IKT vahendite ulatusliku lunavaraga nakatumise tõttu oli linn sunnitud piletimüügisüsteemi nädalavahetuseks sulgema ning pakuma reisijaile tasuta sõitu.

Mirai robotvõrk on jätkuvalt aktiivne. Kuu alguses sattus koordineeritud teenustööstusrühne alla Libeeria internetiteenuse osutaja, kes varustab pääsuga interneti kuni 15% riigi elanikkonnast. Rünnete kestus jäi lühiajaliseks, ent [muretekitav](#) oli nende tavatu maht ning asjaolu, et mõjutatud oli merealune ACE (Africa Coast to

Europe) valguskaabel, mida riik jagab kokku 22 Aafrika läänerranniku ning Euroopa riigiga. Novembri lõpus põhjustas sama Mirai pahavara Saksamaa suurima telekommunikatsioonifirma Deutsche Telekom'i võrgus [internetiruuterite](#) turvanõrkust ära kasutades tõrke, mis võttis interneti- ja telefoniühenduse üle 900 000 sellise seadme kasutajalt.

Saksamaa liidukantsler Angela Merkel [hoiatas](#) Venemaa võimaliku sekkumise eest Saksamaa 2017. aasta üldvalimistesse küberrünnete ja desinformatsiooni abil, sarnaselt USA 2016. aasta presidendivalimiste mõjutamiskatsetega. USA riikliku julgeolekuagentuuri (NSA) juht on uuesti [kinnitanud](#) luureorganisatsiooni veendumust, et küberrünnete näol oli tegemist välisriigi teadliku ja eesmärgistatud tegevusega valimiste mõjutamiseks. USA presidendiks valitud Donald Trumpi [kandidaat riikliku julgeolekunõuniku kohale](#) on väljendanud seisukohta, et USA peab parandama oma tehnoloogilist üleolekut ja arendama küber-

ründevoimekust.

[NATO ja EL](#) leppisid kokku praktilise koostöö tihendamises küberkaitse infovahetuse ning väljaõppe ja õppuste vallas. Soome teatas NATO-ELi ühise hübriidohtudele keskenduva oivakeskuse [asutamisest](#).

Ühendkuningriigi uus [jälitustegevuse seadus](#) (Investigatory Powers Act) annab ametkondadele laialdased õigused internetiliikluse jälgimiseks ning juurdepääsuks kasutaja andmetele, mh võimaldades nõuda teenuseosutajatelt [krüpteeringu kõrvaldamist](#) või tagauksi teenustes. Ehkki seadus sisaldab läbipaistvus- ja järelevalvemehhanisme jälitusametkondade tegevuse üle, on uus seadus saanud laialdase [kriitika osaliseks](#). Eesti seisukohalt on tugev krüptograafia oluline riigi e-teenuste usaldusväärsuse garant, mistõttu Eesti [ei toeta](#) riigi e-teenustesse tagauste loomist.