RIIGI INFOSÜSTEEMI AMET

# RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE DETSEMBER 2016

## Olukord Eesti küberruumis

Detsember oli CERT-EEle aktiivne ning sündmusi Eesti küberruumis leidis aset tublisti rohkem kui aasta vältel keskmiselt, mis peegeldab ka sarnast üleilmset tendentsi. 959st registreeritud juhtumist oli küberintsidente kokku 286, neist omakorda viis kõrge prioriteediga. Viimaste sekka liigitus kuu lõpul aset leidnud mobiil-ID ja DigiDoci tõrge, kui digitaalsetesse keskkondadesse sisenemine ja digiallkirjastamine olid viie tunni vältel häiritud. Elutähtsa teenuse osutajaid puudutavaid juhtumeid oli detsembris 33.

Ülekaalukas osa kuu kübersündmustest olid seotud **pahavara levitavate e-kirjade ja domeenidega**. Arvukalt teavitati meid õngitsuskirjadest, millega püüti teenusekasutajatelt kätte saada maksevahendite (enim PayPali) andmeid välismaistes ostukeskkondades. Läänemaailma pühade-eelset veebiostlemist silmas pidades on selline muster aastati korduv ning on ootuspärane, et see ei jäta puutumata ka Eesti internetikasutajaid; CERT-EE avaldas kasutajatele ka juhiseid vastavatest ohtudest hoidumiseks.

**Lunavara** osakaal on tervikuna vähenenud, ent muret teevad korduvad nakatumised samades asutustes. Sarnaste intsidentide kordumine viitab, et organisatsioonis ei teadvustata adekvaatselt arvutikasutajate tegevuses esinevaid riske ning nende mõju organisatsiooni osutatavatele teenusele. Selliste juhtumite vältimine on võimalik vaid nii IT eest vastutavate töötajate (arvutite turvaseadistused, varukoopiad) kui ka iga kasutaja teadliku ja vastutustundliku käitumise korral, mis nõuab lisaks tehnoloogilisele ka organisatsioonilist toetust.

## Tegevused küberjulgeoleku parandamisel Eestis

Detsembris toimus järjekordne avaliku sektori süsteemiadministraatoritele ja infoturbejuhtidele suunatud seminar **Admin@gov**, mille eesmärk oli kasvatada sihtgrupi infoturbeteadlikkust, jagada teavet aktuaalsetest teemadest ning toetada sihtgrupi-sisest infovahetust. Osalejate tagasiside oli väga positiivne ning on ilmne, et sellises formaadis üritusi tuleb jätkata.

Detsembris alustasime ka koostööd E-kaubanduse Liiduga, aitamaks neil parandada e-poodide turvalisust Eestis.

## Rahvusvaheline keskkond

**USA president Barack Obama** andis riigi luureametkondadele korralduse koostada ammendav uuring presidendivalimistega seotud küberrünnakute kohta. 29. detsembril teavitas Valge Maja ka sanktsioonide kehtestamisest Venemaa luureteenistuste ametnike ja Vene luurega seotud organisatsioonide suhtes ning diplomaatide USAst väljasaatmisest. Sanktsioonide loetelu pole lõplik ning USA kinnitusel jätkab riik meetmetega talle „sobival ajal ja kohas“, detaile lõpuni avamata.

Saksamaa ja Prantsusmaa möönavad, et sihitud rünnete sagenemine nende riikide ametiasutuste vastu annab alust oodata USAs toimunule sarnast mõjutustegevust ka **Euroopas eesseisvate valimiste eel**. Saksamaa sisejulgeolekuteenistus (Bundesamt für Verfassungsschutz, Bfv) avaldas kuu algul hoiatuse kasvavast ohust agressiivseks riigivastaseks küberspionaažiks ja –rünneteks.

**Ukraina elektrivõrku** tabas aastapäevad pärast laia rahvusvahelist kajastust leidnud 2015. detsembri intsidenti uus küberründest põhjustatud

katkestus. On oletatud, et kriitilise infrastruktuuri vastased küberründed Ukrainas viitavad Ukraina kasutamisele nö katsepõlluna, kus ründemeetodeid laiema kasutuse tarbeks testida ja viimistleda.

Rahvusvahelist pankadevahelist arveldussüsteemi haldav SWIFT hoiatab liikmesorganisatsioone jätkuvalt SWIFT liidese pankadepoolsete turvanõrkuste eest. Pärast veebruarikuist intsidenti, mille käigus kurjategijatel läks korda varastada Bangladeshi keskpanga kontodelt üle 100 miljoni USD väärtuses raha, on leidnud aset mitu sarnast juhtumit - SWIFTi väitel on ligi viiendik rünnetest osutunud edukaks. Viimati teatas Türgi kommertspank, et on sarnast skeemi kasutanud kurikaelte tõttu kandnud kahju kuni 4 miljoni USD väärtuses. Vene Föderatsiooni Keskpank kinnitas intsidendi toimumist, mille käigus võltsitud autentimisandmete abil varastati arvukatelt kontodelt kokku ca 2 miljardit rubla (31 miljonit eurot).
Sedamööda, kuidas laieneb **mobiilirakenduste** kasutusala, annavad mobiilseadmete ja -rakenduste turvanõrkused üha enam rahvusvahelist kõneainet. Risk puudutab nii eraelulist, ärilist kui ka riigi julgeolekut puudutavat teavet. Mobiilirakenduse Quest Diagnostics arendaja teatas 34 tuhande kasutaja terviseandmete (sh uuringutulemuste) lekkimisest kolmandale isikule; USA juhtiv küberturbeettevõte CrowdStrike avaldas raporti, millest ilmneb Ukraina suurtükiväe kasutatud Androidirakenduse manipuleerimine, mis tegi relvastuse paiknemise teabe vastasele kättesaadavaks.

## Muud olulist

Avaldasime RIA tellitud küberjulgeoleku õigusraamistiku analüüsi tulemused. Analüüsi koostanud advokaadibüroo Lextal hinnangul vajavad valdkonna regulatsioonid ulatuslikku ülevaatamist ja korrastamist, et selgelt määratleda RIA pädevus võrgu- ja infosüsteemide turvalisuse tagamisel ning korrastada eri seadusi mööda laiali paiknev mõisteaparaat ning ülesanded. Samuti tingib õigusraamistiku uuendamise vajaduse uus NIS direktiiv, mis tuleb Eesti õigusesse üle võtta 2018. aasta kevadeks.