RIIGI INFOSÜSTEEMI AMET

RIIGI INFOSÜSTEEMI AMETI KÜBERTURVALISUSE TEENISTUSE 2015. AASTA KOKKUVÕTE

2016

Sisukord

Eessõna

Riigi Infosüsteemi Ameti küberturvalisuse teenistuse (KTT) 2015. aasta aruannet on meeldiv sisse juhatada tõdemusega, et Eesti jaoks möödus aasta taas ilma suuremaid tagajärgi tekitanud intsidentideta. Eesti küberjulgeolek sünnib ettevõtete ja riigi igapäevases koostöös ning see koostöö on andnud häid tulemusi.

Küberturvalisuse valdkond areneb aga väga kiiresti ning riskikeskkond muutub pidevalt. Iga päev toob kaasa uudiseid uute haavatavate valdkondade ja ründeohtude kohta. Ometi pole nendega seotud riskide maandamiseks enamasti vaja mitte uute ja kallite süsteemide ostmist, vaid piisab ka andmeturbe aluspõhimõtete järgimisest. Möödunud aasta näitas, et elutähtsad teenused võivad sattuda katkemise ohtu ka nii lihtsa tegevuse tõttu nagu lunavararünne. Lohakus ja hoolimatus infosüsteemide elementaarse turvalisuse tagamisel (ehk varukoopiate tegemise ja õiguste korraliku halduse puhul) võib kaasa tuua ettevõtte või asutuse kõigi andmete hävimise, mida eelmisel aastal siiski juhtus.

Möödunud aasta näitas taas, kui ohtlik on kübervahendite kasutamine relvana. Jõululaupäeval Ukraina elektrivõrkudes ulatusliku katkestuse põhjustanud küberrünne tuletas maailmale meelde, et küberründed pole sugugi virtuaalsed, vaid põhjustavad vägagi käegakatsutavaid tagajärgi. Tänapäevase elukorralduse kahjustamine kübervahenditega on küllalt lihtne ja efektiivne ning kahjuks järjest kättesaadavam ka näiteks terroristide jaoks.

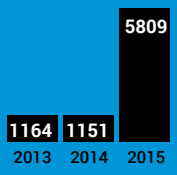
Euroopa riikide ees seisvate julgeolekuväljakutsete seas on seega olulisel kohal ka küberjulgeolek ning on astutud esimesed sammud senisest palju tihedama koostöö suunas. Euroopa Liidu info- ja võrguturbedirektiivi eesseisev rakendamine toob kaasa tihedama koostöö ja infovahetuse mitte ainult liikmesriikide, vaid ka era- ja riigisektori vahel. Just viimane on väga oluline, sest kübervaldkond sõltub täielikult just erasektori rajatud taristust ja teenustest. Eestis on koostöösse panustatud palju: oleme üks vähestest riikidest maailmas, kes aitab oma kriitilistel ettevõtetel riske hinnata ja infosüsteeme testida, korraldame õppusi, oleme siiani olnud edukad ka küberturvalisuse arendamisega tegelevate kogukondade loomisel ja toetamisel. Inimeste teadlikkuse tõstmine küberohtudest ning tehnoloogiaga toimetulekuks vajalike oskuste ja teadmiste arendamine on järjest enam kujunenud küberjulgeoleku tagamise võtmeküsimusteks. Tehnoloogia ei tekita ju ise riske – need tekivad tehnoloogia vääral, mitte-eesmärgipärasel kasutamisel. Mida teadlikumad oleme tehnoloogia võimalustest, seda paremini suudame ohtusid ette näha ja kahjulikke tagajärgi ära hoida.

Turvalist jätkuvat aastat!

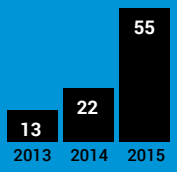
Toomas Vaks
Riigi Infosüsteemi Ameti peadirektori asetäitja küberturvalisuse alal

2015. aasta Eesti küberturvalisuses

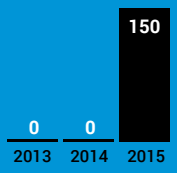
Eestis tervikuna:



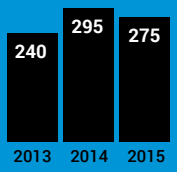
5809
Käsitletud juhtumit



55
Teenusetõkestusrünnet

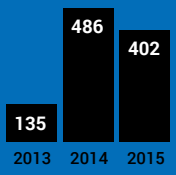


150
Krüptolunavara juhtumit



275
Näotustamise juhtumit

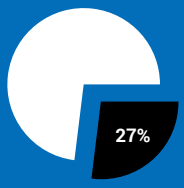
Riigiasutustes:



402
Riigiasutuste poolt raporteeritud intsidenti

Levinumad põhjused:

- rünne
- tarkvaraviga
- välise teenusepakkuja viga
- administraatori viga



27%
Raporteeritud intsidentidest olid kõrge kriitilisusega
(20 % aastal 2014)

420 000 ID-kaarti vajab uut sertifikaati

vajalik ID-kaardi turvalisuse tõstmiseks ja toimimise tagamiseks

SHA-1 murdumise tõenäosus on liiga suur

Google, Microsoft, Mozilla peavad ebaturvaliseks

KüberSiil 2015 - suurim küberõppus Eesti ajaloos

Õppused - CONEX, Locked Shields, Cyber Coalition, Cyber Europe

Küberjulgeoleku õiguslik raamistik vajab lihtsustamist

Küberjulgeoleku korraldus on täna kirjas enam kui kümnes õigusaktis

Sissejuhatus

Eesti paistab kõrgelt arenenud riikide hulgas kindlasti silma suure hulga hästi toimivate digitaalsete teenuste poolest, millega kodanikud on harjunud ja mille toimimist võtame kõik ilmselt loomuliku osana meie igapäevasest elust. Ühtlasi tähendab see riigi suurt sõltuvust digiteenuste toimimisest, mistõttu on küberturvalisus väga oluline osa meie julgeolekust.

Eestis on küberjulgeoleku tagamine üles ehitatud viisil, et iga asutus või kriitilise teenuse osutaja vastutab oma infosüsteemide turvalisuse ja teenuste toimimise eest ise. Elutähtsate teenuste osutajad ja riigiasutused on kohustatud teavitama Riigi Infosüsteemi Ametit (edaspidi RIA) teenuseid mõjutanud intsidentidest ning vastavalt soovitustele rakendama infosüsteemides sobilikke infoturbemeetmeid.

RIA ülesanded küberturvalisuse tagamisel on koguda infot ja analüüsida Eesti küberruumis toimuvaid intsidente, parandada valmisolekut küberrünnetega toimetulekuks, seada standardid infoturbe rakendamiseks ja teha järelevalvet nende rakendamise üle, keskendudes selle juures ennekõike elutähtsate teenuste küberturvalisuse tagamisele. Järgmistel lehekülgedel teeme kokkuvõtteid möödunud aastast Eesti küberturvalisuses ning selgitame mitmeid ees ootavaid väljakutseid.

Mis meid ohustab?

Tänapäevasele julgeolekule on omane sõjategevus ilma sõda kuulutamata ehk hübriidsõda, millega Eesti peab oma geopoliitilise asukoha tõttu pidevalt arvestama. Küberruum on hübriidsõjas eesmärkide saavutamiseks ideaalne lahinguväli, sest lisaks võimalusele mugavalt oma jälgi peita saab selle kaudu külvata ebastabiilsust või saavutada traditsioonilisele sõjategevusele omaseid eesmärke. Võrreldes teiste kõrgelt arenenud riikidega, on Eesti suhtes küberründeid kasutades võimalik saavutada eesmärke palju kiiremini, sest Eesti riigi toimimine ja rahva sõltuvus digitaalsete teenuste toimimisest on väga suur ning kasvab pidevalt.

Sellegipoolest ei saa nõustuda ajakirjanduses ilmunud väidetega, justkui võrduks juurdepääs arvutile tänapäeval relva omamisega. Ohud lähtuvad siiski konkreetsete inimeste tahtlikust tegevusest, mitte tehnoloogiast iseeneses.

Olulisemateks küberohtudeks tuleks Eesti jaoks pidada:

1. küberkuritegevust selle kõikides avaldumisvormides. Globaalne organiseeritud küberkuritegevus ohustab igaüht ning võib kergesti muutuda ka ohuks riiklikule julgeolekule. Heaks näiteks on juhud, kus lunavara muudab kasutamiskõlbmatuks elutähtsate teenuste osutajate infosüsteemid.

2. küberspionaaži, info lekitamist ja infoturbe põhimõtete rikkumist, mis toob või võib tuua kaasa usalduse kadumise infosüsteemide ning digitaalsete teenuste vastu. Ulatuslikud teabelekked ning infosüsteemide töö katkestused on mitmes riigis toonud kaasa ulatusliku usalduse kao ning on seadnud kahtluse alla riikide ja ettevõtete võimekuse kaitsta oma kodanike või klientide infot.

3. kübervahendite kasutamist relvastatud konflikti osana. Ukrainas 2015. aastal juhtunu tuletab meile valusalt meelde, kui haavatav on tänapäeva ühiskond rünnete vastu, kus kübervahendeid kasutades häiritakse tööstusseadmete juhtimissüsteeme, segades nende tööd või muutes need kasutamiskõlbmatuks.

4. asjaolu, et ohtude realiseerumisel mängib enamasti olulist rolli infosüsteemide kasutajate teadmatus, oskamatus või puudulik turvateadlikkus. Inimlik lohakus või teadmatus on enamiku tõsiste intsidentide peamine põhjus.

Eestil pole võimalik ignoreerida asjaolu, et meie kõrval paikneb agressiivset retoorikat viljelev Venemaa, kes arendab pidevalt oma küberründevõimeid ning kelle jaoks on teiste riikide vastane tegevus küberruumis pelk vahend mõjuvõimu suurendamiseks ja oma eesmärkide saavutamiseks. Oleme juba harjunud sellega, et Eesti võrke ja infosüsteeme kaardistatakse ning mõõdetakse regulaarselt, mille käigus kogutav info võib olla vajalik igasuguse suurema Eesti-vastase tegevuse planeerimisel. Lisaks Venemaale ei saa me ohte analüüsides ära unustada ka vajadust arvestada terroristide ja vaenulike küberaktivistidega. Asjaolu, et Daesh eksponeerib Eesti lippu oma vaenlaste nimistus, peaks meid mõtlema panema ning sundima arvestama võimalusega, et Eesti-vastaste küberrünnete algatajateks võivad olla ka seni füüsilisi rünnakuid eelistanud terroristid.

Oleme juba harjunud sellega, et Eesti võrke ja infosüsteeme kaardistatakse ning mõõdetakse regulaarselt, mille käigus kogutav info võib olla vajalik igasuguse suurema Eesti-vastase tegevuse planeerimisel.

Küberruumis on üha raskem vahet teha kurjategijatel, keda motiveerib isiklik kasu, ja naaberriigi eriteenistustel, kes soovivad Eesti vastu korraldada hübriidsõda riiklike eesmärkide saavutamiseks. Küberkurjategijate koostöö Eesti suhtes vaenulike eriteenistustega on igapäevane ja mõlemale poolele kasulik. See muudab Eesti jaoks olukorra järjest keerukamaks, kuna selgeid vastuseid peaaegu ei ole. Enam ei saa kindel olla, kas Eesti elutähtsa infosüsteemi vastu justkui rahalise kasu eesmärgil suunatud rünnak pole tegelikult kurjategijatelt tellitud mingi hoopis muu kriteeriumi alusel.

Küberruumis on üha raskem vahet teha kurjategijatel, keda motiveerib isiklik kasu, ja naaberriigi eriteenistustel, kes soovivad Eesti vastu korraldada hübriidsõda riiklike eesmärkide saavutamiseks.

2015. aasta on näidanud, et suures plaanis ohustab Eesti küberjulgeolekut ka suutmatus juba tuntud ohtudest piisavalt kiiresti järeldusi teha ning viia sisse muutusi oma infosüsteemides. Eelmist aastat Eesti küberjulgeolekus iseloomustas – ning ühtlasi suurendas käsitletud intsidentide hulka – küberjulgeoleku vaatevinklist mulluste ja tunamulluste haavatavuste ärakasutamine, sest avalikult publitseeritud turvahoiatused ja RIA avaldatud teavitused või käsitlused ajakirjanduses olid infosüsteemi omanikel jäänud märkamata. 2015. aasta põhilise õppetunnina on ohtude vältimiseks vaja viia turvahoiatused kiiremini kogu Eesti IT-spetsialistideni viisil, et neile ka reageeritakse.

Elutähtsad teenused

98% elutähtsate teenuste osutajatest on tunnetanud oma (äri)tegevuse otsest sõltuvust IT-süsteemide toimimisest. Sellesse tõdemusse peab riik tõsiselt suhtuma. Tulenevalt küberjulgeoleku strateegiast on RIA KTT üks olulisemaid ülesandeid suurendada elutähtsate teenuste osutajate teadlikkust küberriskidest ja parandada nende valmisolekut riskidega toime tulla.

Elutähtsate teenuste toimimist võivad mõjutada või halvata ka lihtsakoelised pahavara-kampaaniad, mille siht ei olnud nende teenuste häirimine.

2015. aasta näitas, et elutähtsate teenuste toimimist võivad mõjutada või halvata ka lihtsakoelised pahavarakampaaniad, mille siht ei olnud nende teenuste häirimine.

Aasta lõpus toimusid Ukrainas küberründed elektrisüsteemide vastu – asjaolu, millest ka Eesti peab tegema üsna tõsiseid järeldusi. Tegu on järjekordse näitega, kuidas kübervahendite abil on võimalik saavutada otseseid füüsilisi tagajärgi ja oluliselt mõjutada inimeste igapäevaelu. Ukraina juhtumi peamine õppetund on asjaolu, et infoturbemeetmete rakendamisega on tegelikult võimalik sääraseid ründeid kas üldse ära hoida või siis nende tagajärgi oluliselt vähendada. Kuigi Eesti elutähtsate teenuste osutajad on Ukraina kolleegidest palju paremini valmistunud, ei saa Eesti üheski mõttes loorberitele puhkama jääda. Oleme Ukraina juhtumi õppetunde arvestanud ja plaanime tegevusi elutähtsate teenuste küberturvalisuse suurendamiseks.

Kehtiva seaduse kohaselt on Eestis 46 elutähtsat teenust, mis on hädavajalikud ühiskonna toimimise, tervishoiu, turvalisuse ning inimeste majandusliku ja sotsiaalse heaolu korraldamiseks. Neid teenuseid osutab nii riigi- kui erasektoris kokku enam kui 140 asutust ja firmat, kes kõik on kohustatud asetleidnud turvaintsidentidest RIAt informeerima.

2015. aastal korraldasime mitmesuguseid koolitusi nende asutuste ja firmade enam kui 120 spetsialistile. Jätkame koolitustegevusega 2016. aastal: kavas on 14 koolitust. Eelmisel aastal osalesid mitmed elutähtsate teenuste osutajad ka RIA korraldatud üleriigilisel küberõppusel, mida käsitleme allpool.

Eesti on ainus riik Euroopas, kes testib ise elutähtsate teenuste IT-süsteemide turvalisust. 2015. aastal testis RIA kolme elutähtsa teenuse osutaja IT-süsteeme: üritasime tuvastada, kas ja kuidas on potentsiaalsel ründajal võimalik saavutada ligipääs asutuse kriitilistele infosüsteemidele. Sellist testimist jätkame ka tänavu.

Oluline väljakutse elutähtsate teenuste toimepidevuse tagamisel on teenuseosutajate vahelised ristsõltuvused. Eelmisel aastal haldasime mitut olulist turvaintsidenti, mis puudutasid just elutähtsa teenuse sõltuvusi teistest teenusepakkujatest. Seetõttu korraldame 2016. aastal elutähtsate teenuste osutamist mõjutavate tegurite välja selgitamise uuringu, et suurendada riigi teadlikkust oluliste elutähtsate teenuste infotehnoloogilistest rist- ja välissõltuvustest.

Tagamaks, et ühegi elutähtsa teenuse osutamine Eestis küberriskide reali-

seerumise tõttu ei katke, on vaja ka ekspertide omavaheline tihe infovahetus. Infovahetuse hõlbustamiseks toimuvad regulaarselt infopäevad ja valdkondlikke küberturvalisuse eksperte koondava komisjoni koosolekud. 2015. aastal osalesid mitmed elutähtsate teenuste osutajad küberõppusel KüberSIIL 2015. Tänavu korraldame ekspertidele valmisoleku tõstmiseks ka mitu koolitust. Elutähtsaid teenuseid osutavate asutuste infoturbespetsialistidel ja juhtidel tasub alati pöörduda RIA KTT poole, olgu põhjuseks kas infovajadus, nende poolt tuvastatud küberriskid või ettepanekud meie ühise tegevuse parandamiseks.

Turvaintsidentide käsitlemine

RIA KTT toimib ka rahvusliku ja riikliku küberturvalisuse intsidentide lahendamise meeskonna (CERT) ülesannetes ning on CERT/CSIRT võrgustikes rahvusvaheline kontaktpunkt. CERT/CSIRT organisatsioone eksisteerib üle maailma, omavahel tehakse tihedat koostööd, jagatakse informatsiooni küberintsidentide kohta ning teavitatakse partnereid ja avalikkust küberohtudest.

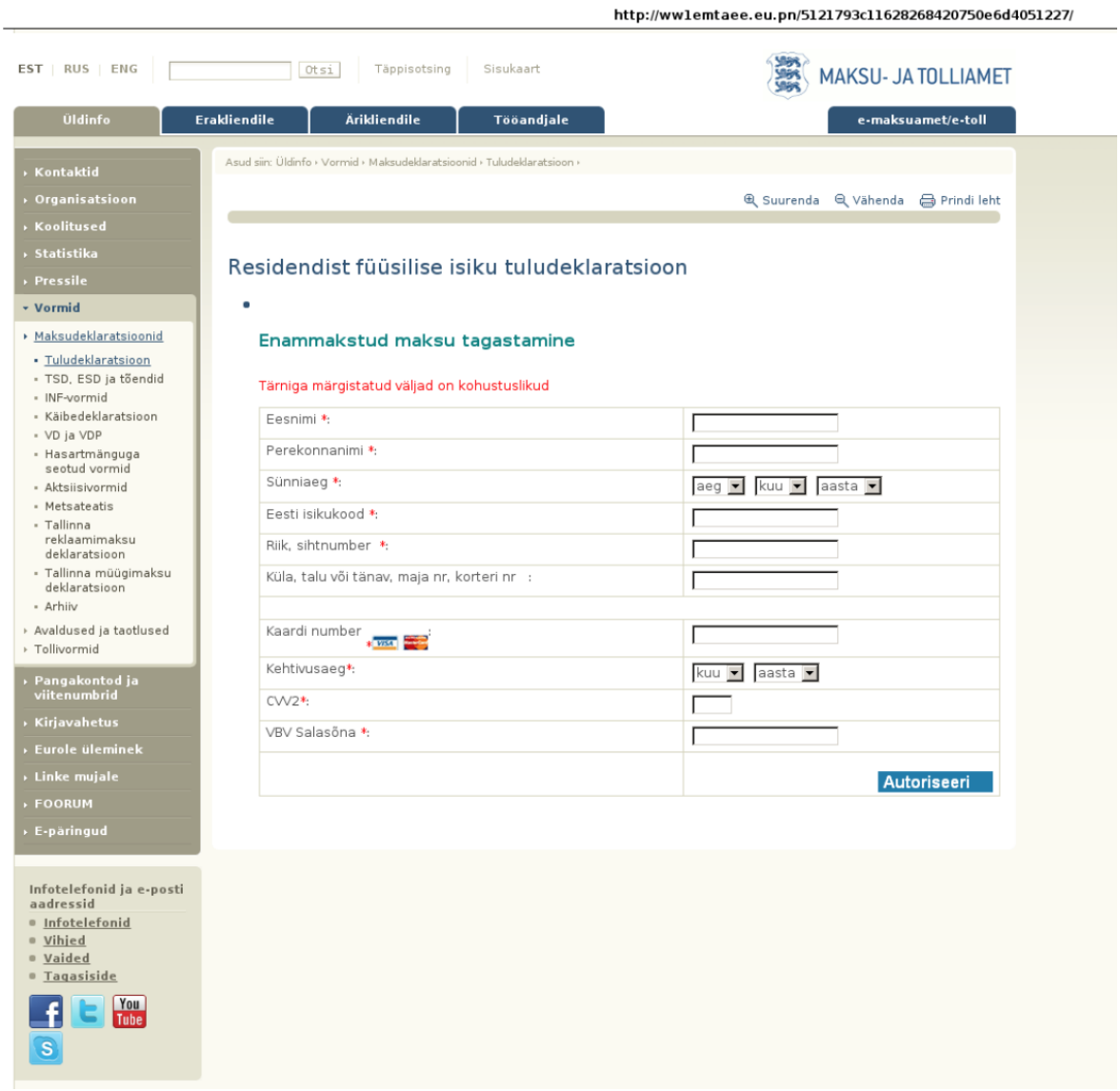
Küberturvalisuse teenistuse intsidentide käsitlemise osakond (CERT-EE) tuvastab, jälgib ja lahendab Eesti arvutivõrkudes toimuvaid turvaintsidente, teavitab ohtudest ja korraldab intsidentide seiret. Tänavu jaanuaris tähistas CERT-EE 10. aastapäeva.

Alates 2015. aasta suvest toimub Eesti küberruumi ööpäevaringne mehitatud seire, samuti võtsime kasutusele senisest paremad seire- ja monitooringulahendused. Tegevus küberruumis on pidev ja pole ühelgi moel piiratud Eesti ajavööndiga. Tänu ööpäev läbi tehtavale seirele oleme ennetanud ja avastanud palju rohkem küberintsidente kui varasematel aastatel ning nendele ka reageerinud.

Tänu ööpäev läbi tehtavale seirele oleme ennetanud ja avastanud palju rohkem küberintsidente kui varasematel aastatel ning nendele ka reageerinud.

Ööpäev läbi tehtava seire edukuse hea näide on möödunud aasta lõpus tuvastatud Maksu- ja Tolliameti (EMTA) võltsitud kodulehe operatiivne sulgemine. Petulehe abil püüti kätte saada kasutajate krediitkaartide andmeid.

Olgugi et ründajad olid plaaninud koguda pahaaimamatute inimeste krediitkaardiandmeid nädalavahetusel, mil vastutavad ametnikud tööpostil ei viibinud, tuvastas CERT-EE hästi koostatud võltslehe reede õhtul ja see suleti poolteist tundi pärast lehe avalikuks tegemist. EMTA teavitas RIAt võimalikust andmete õngitsemise ründest esmaspäeva hommikul, uue töönädala alguses. Olgugi et kurjategijad olid ründe planeerinud töövälisele ajale ja suutsid piiratud aja vältel meelitada pahaaimamatuid arvutikasutajaid krediitkaardi andmeid võltsitud lehele sisestama, õnnestus rünnak peatada just tänu küberruumi pidevale monitoorimisele enne, kui keegi selle tõttu teadaolevalt kahju kandis.



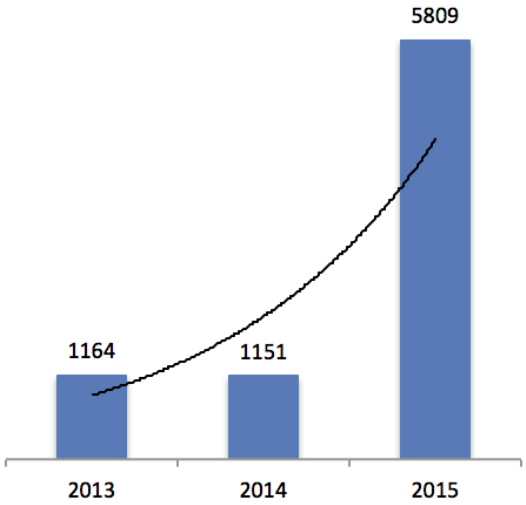
EMTA võltsitud kodulehe näidis.

Oluliselt keerukamad ja tunduvalt suuremat mõju avaldanud juhtumid olid 2015. aastal väljapressimise eesmärgil sooritatud pahavararünded ehk lunavara juhtumid. Lunavara krüpteerib kasutaja arvutis ja võimalusel ka arvutiga ühendatud salvestusseadmetel olevad andmed ehk muudab need kasutajale loetamatuks. Andmete taasavamiseks tarviliku krüptovõtme eest nõutakse lunaraha maksmist virtuaalses valuutas ehk *bitcoin*'ides. Juhul kui lunaraha ei maksta, jäävad andmed üldjuhul kasutuskõlbmatuks. 2015. aastal teavitati meid 150 säärasest juhtumist.

Eriti palju esines lunavara juhtumeid 2015. aasta viimase kahe kuu jooksul: neli korda enam kui eelnenud kümne kuu jooksul. Tüüpiliselt krüpteeriti andmed tavakasutajate kõvaketastel, kuid oli juhtumeid, kus andmed krüpteeriti serverite jagatud ketastel. Lunavaraga nakatumist pole järjest kavalamaks muutuvate kurjategijate tõttu võimalik täielikult ära hoida.

Lunavaraga nakatunud arvuti ekraanipilt.

RIA küberturvalisuse teenistuse spetsialistid analüüsivad kannatada saanud süsteemidest leitud pahavara näidiseid alati ning tuvastavad ja sulgevad nende levitamise kanalid. Lunavarajuhtumite analüüs 2015. aastal näitab ebaproportsionaalselt suurt kahjukannatajate arvu riigiasutuste ja elutähtsate teenuste osutajate seas, mis teatud juhtudel viitab ka ilmselt nende vastu suunatud rünnetele.



CERT-EE registreeritud infoturbe sündmused.

2015. aasta peamine järeldus on see, et lunavaraga nakatumist on raske täielikult ära hoida isegi kõige parema infoturbe korral. Lunavara tekitatavat kah-

ju aitab vähendada infosüsteemides olevatest andmetest varukoopiate tegemine. Kahju ulatust vähendab kindlasti ka see, kui infosüsteemides on kasu tajaõigused hästi määratletud ja kontrollitud. Ning loomulikult aitab kõikide küberrünnete vastu ka üldine turvateadlik käitumine.

Lunavara tekitatavat kahju aitab vähendada infosüsteemides olevatest andmetest varukoopiate tegemine.

Eelmisel aastal käsitletud juhtumid kinnitasid taas Eestis tehtud uuringute tulemusi: teoreetilised teadmised küberohtude vältimise kohta on üsna suurel hulgal Eesti arvutikasutajatest, samas praktikasse need teadmised sageli ei jõua. Enamasti põhjustab ohtliku käitumise inimlik laiskus või uudishimu.

Turvalisust tõstvad tegevused (paroolide regulaarne vahetamine, andmete varundamine seadmest välja, tarkvara uuendamine) ei tundu olulisena ning tundmatult aadressilt pärineva, vigases eesti keeles e-kirja manus avatakse enamasti pelgast uudishimust.

Lisaks pahavara abil tehtud rünnetele toimus möödunud aastal väljapressimise eesmärgil ka mitmeid teenusetõkestusründeid (DDoS). Juhtumid on üsna sarnased: asutus või ettevõte langeb esmalt lühikese teenusetõkestusründe ohvriks, seejärel saadetakse asutuse kontaktaadressile e-kiri: juhul kui teatud aja jooksul ei kanta üle lunaraha, järgneb tunduvalt suuremas mahus ja pikema kestusega rünne. Võib eeldada, et ründajad on üldjuhul teinud eeltööd, arvutades firma käibe või asutuse eeldatava kahju juhuks, kui ohver ei ole võimeline oma klientidele teenuseid osutama. Pole avalikku infot, et Eestis oleks teenusetõkestusrünnete vältimiseks kunagi lunaraha makstud.

Olgugi et 2015. aastal tegelesime väga palju rahalise kasu eesmärgil sooritatud küberrünnetega, ei saa unustada ka riikide jätkuvat huvi Eesti arvutivõrkude vastu. Tuvastame Eesti küberruumis regulaarselt nii teenusetõkestusründeid kui ka võrkude kaardistamisi, mille taga on suure tõenäosusega välisriigid. Teenusetõkestusrünnete tuvastamine ja haldamine on RIA küberturvalisuse teenistuse jaoks tavapärane ülesanne. Möödunud aastal registreerisime keskmiselt ühe teenusetõkestusründe nädalas. Võime eeldada, et paljudel juhtudel on sel viisil testitud asutuste suutlikkust rünnetega toime tulla. Teenusetõkestusrünnete puhul on märgata ka rünnete kestuse pikenemist. Enamikus teenusetõkestusrünnetes kasutatakse pahavaraga nakatatud kodu- või kontoriarvuteid, mis on liidetud nii-öelda robotvõrgustikuks ehk botnetiks, kusjuures enamasti pole arvutikasutajad teadlikudki, et nende arvutit kasutatakse mõne kolmanda isiku ründamiseks.

Olenemata sellest, kas kannatanu on teenusepakkuja või lõpptarbija, tuleb küberkuritegevuse tõttu kahju saamisel alati teavitada politseid.

Olenemata sellest, kas kannatanu on teenusepakkuja või lõpptarbija, tuleb küberkuritegevuse tõttu kahju saamisel alati teavitada politseid. RIA KTT ja keskkriminaalpolitsei küberkuritegude büroo teevad küll tihedat koostööd, kuid küberkuriteo kohta saab avalduse politseisse anda ikkagi vaid kuriteoohver ise.

Toimunud küberkuritegudest palume politseid teavitada aadressil **cybercrime@politsei.ee**.

Õppused

2015. aastal korraldasime õppusi ise ning ühtlasi osalesime mitmel riigisisesel ja rahvusvahelisel (küber)õppusel. Kõige olulisemad olid meie korraldatud üleriigiline küberõppus KüberSIIL 2015 septembris ning aprillis korraldatud küberõppus üleriigilise kriisiõppuse CONEX 2015 raames. Lisaks koordineerisime Eesti osalust NATO küberõppusel Cyber Coalition 2015 ning Euroopa Liidu õppusel Cyber Europe 2015.

CONEX 2015 raames korraldasime koostöös siseministeeriumiga küberõppuse majandus- ja kommunikatsiooniministeeriumi ning valitsemisalade asutuste juhtkondadele. Majandus- ja taristuministri juhitud laua-õppusel käsitleti ulatusliku küberintsidendi lahendamise strateegilisi tahke. Õppuse stsenaarium sisaldas ID-kaardi taristu, riigi ja eraõiguslike asutuste hallatava andmesidevõrgu, rahvastikuregistri ja e-residentide ning elutähtsate teenuste (energeetika ja laevaliikluse korraldamine) vastaseid küberründe ning andmelekkeid. Õppuse järelduste alusel täiendati valitsuse tegevuskava.

Õppusel osalenud asutuste vahel oli hädaolukorra lahendamisel hea koostöö.

2015. aasta sügisel korraldasime üleriigilise küberõppuse KüberSIIL 2015. Õppuse peamine eesmärk oli harjutada ulatusliku küberintsidendi lahendamise plaani rakendamist. Sealhulgas hädaolukorra lahendamisel osalevate asutuste kohustusi ja õigusi, partnerite kaasamist, valmisolekut, teabevahetuse korraldamist ja RIA-siseseid protseduure. Hädaolukorra lahendamist harjutati juhtstaapides nii operatiivsel kui ka strateegilisel tasandil. Kuigi tegemist ei olnud tehnilise õppusega, harjutati selle käigus hädaolukorra lahendamise korraldust asutuste koostöös praktiliselt ja reaalajas.

KüberSIIL 2015 oli Eesti seni suurim küberõppus. Sellest võttis osa 21 asutust (sh julgeoleku- ja korrakaitseasutused, riiklikud ja eraõiguslikud elutähtsate teenuste osutajad), õppusega oli seotud üle saja inimese.

Nii KüberSIIL 2015 kui ka CONEX küberõppus näitasid, et:

1. õppusel osalenud asutuste vahel oli hädaolukorra lahendamisel hea koostöö, tööprotseduurid informatsiooni vahetamiseks ja ühtse olukorrapildi tekitamiseks toimisid. Osalenud asutustel oli hea teadmine ja ülevaade oma rollist ning enda ülesandeid suudeti täita.

2. küberjulgeoleku tagamine vajab seadusandjalt siiski senisest selgemat reguleerimist eraldi seaduse kujul, mis suurendaks õigusselgust ja määratleks vastutuse küberjulgeoleku tagamisel riigis laiemalt.

3. õigusaktides on vaja sätestada ID-kaardi toimimisega seotud asutuste rollid ja ülesanded üheselt ning arusaadavalt.

4. riigi digitaalse usaldusteenuse ja baastaristu intsidentide mõjud tuleb täpselt välja selgitada ning kirjeldada protseduur nende lahendamiseks.

Küberjulgeoleku õiguslik raamistik

Küberjulgeoleku tagamise õiguslik raamistik Eestis vajab täiustamist.

Küberjulgeoleku tagamise õiguslik raamistik Eestis vajab täiustamist.

Õppuse KüberSIIL 2015 õppetunnid, hädaolukorra seaduse muutmine ja Euroopa Liidus heaks kiidetud võrgu- ja infoturbe direktiiv (NIS) kinnitasid 2015. aastal vajadust selge ja tänapäevaseid olusid arvesse võtva küberturvalisuse seaduse järele.

Lisaks ei arvesta praegu kehtiv avaliku teabe seadus piisavalt tehnoloogia arengusuundadega ning seega takistab uute tehnoloogiate kasutusele võtmist ja Eesti digitaalset arengut.

Siseministeerium on välja töötanud uue hädaolukorra seaduse (HOS) eelnõu, millega muudetakse elutähtsate teenuste valdkonda selgemaks. Sellel muutusel on oluline mõju küberjulgeoleku tagamise korraldusele Eestis.

Uus hädaolukorra seadus ei käsitle enam elutähtsana teenuseid, mis on küll vajalikud ja harjumuspärased inimeste igapäevaeluks, kuid mille toimimine hädaolukorras tagatakse vaid võimaluse korral, kuivõrd need ei ole suunatud elanikkonna esmavajaduste rahuldamisele kriisi ajal (näiteks lennujaamad). Samuti ei reguleeri uus hädaolukorra seadus teenuseid, millest sõltub riigi enda toimimine (näiteks valitsuse töö tagamine). Seega tekib terve rida teenuseid, mida uus hädaolukorra seadus ei reguleeri, kuid mille võimalik mittetoimimine mõjutaks otseselt riigi julgeolekut (näiteks ka raudtee, lennujaamad). Vastavalt riskianalüüsidele on need teenused suuresti sõltuvad IT-süsteemide toimimisest, mistõttu tuleb teenuse toimimise tagamiseks rakendada infoturbemeetmeid. Vastav kohustus peaks tulevikus tulenema valdkondlikest seadustest (näiteks raudteeseadus). Praegu on küberjulgeoleku korraldus jaotunud enam kui kümne õigusakti vahel ja muudatuste tulemusena lisandub sääraseid õigusakte veel vähemalt neli, misläbi muutub küberjulgeoleku tagamise õiguslik raamistik tulevikus veelgi keerulisemaks.

Eesti digitaalse arengu jätkumiseks on tehnoloogialahenduste pidev uuendamine möödapääsmatu. Seetõttu on riigil vaja kasutusele võtta muu hulgas ka pilvetehnoloogiaid ja -lahendusi, mida käsitleb 2015. aasta septembris valitsuse heaks kiidetud kontseptsioon.

Eesti infoühiskonna järjepidevuse toetamiseks kavandatav Eesti riigipilv on hübriidpilv, mis kätkeb endas riigiasutustele osutatavat privaatpilveteenust, erasektori hallatavaid avalikke pilvi ja välisriikides paiknevaid andmesaatkondi.

Lisaks pilvelahenduste arendamisele tuleb tähelepanu pöörata ka õiguslikule raamistikule. Kehtiv andmekogusid ja andmetöötlust reguleeriv õiguslik raamistik pärineb ajast, mil pilvandmetöötlus ei olnud veel nii levinud. Avaliku teabe seaduse kohaselt on riigi ja kohalike omavalitsuste andmekogudele seatud kohustus rakendada ühe kindlustava süsteemina infosüsteemide tur-

vameetmete süsteemi, mis eeldab aga auditeerimist ja järelevalve võimaldamist. Nimetatud kohustuste täitmine muutub väljaspool Eestit paiknevate pilvelahenduste kasutamisel võimatuks. Seetõttu tuleb välja töötada regulatsioon, mis võimaldaks ja toetaks pilvandmetöötlust ning erinevate pilvelahenduste kasutamist.

2015. aasta lõpus kiitis Euroopa Liidu Nõukogu heaks võrgu- ja infoturbe direktiivi (NIS). Tegemist on olulise ja uudse Euroopa Liidu õigusaktiga, mis esmakordselt korraldab liikmesriikides elutähtsate teenuste osutamist ning liikmesriikide CERTide operatiivkoostööd intsidentide korral. Direktiivi tulemusel peaks paranema küberintsidentide ennetamine, avastamine ja neile reageerimine ning liikmesriigid peaksid üksteist põhjalikumalt teavitama suurt mõju omavatest küberintsidentidest või -rünnetest. Direktiiv jõustub eeldavalt 2016. aasta esimeses pooles. Direktiivi jõustumisel tuleb Eestil see enda seadustesse üle võtta.

Eesti kehtiva õiguse kontekstis on selleks kaks võimalust: esiteks võib üle vaadata ja täiendada tervet hulka valdkondlikke seadusi, sealhulgas eelmainitud hädaolukorra seadust. Sellise lahenduse korral tuleb lisaks välja töötada ka eraldiseisev õigusakt, sest mõningaid direktiivist tulenevaid nõudeid ei ole ilmselt võimalik olemasolevate valdkondlike seaduste täiendamise kaudu üle võtta. Tegu oleks töömahuka lahendusega, mis õigusselgust pigem ei suurendaks.

Õigusselguse vaatevinklist on eelistatud lahendus töötada välja üks terviklik ja kompaktne küberjulgeolekut reguleeriv seadus.

Teine ja õigusselguse vaatevinklist eelistatud lahendus oleks töötada välja üks terviklik ja kompaktne küberjulgeolekut reguleeriv seadus, mis aitaks lisaks võrgu- ja infoturbedirektiivi nõuete ülevõtmisele tagada Eestis ka tõhusa küberjulgeolekukorralduse.

Uuringud

Küberjulgeoleku tagamise lahutamatu osa on tihe koostöö teadusmaailmaga. Sellest lähtuvalt korraldame igal aastal uuringuid, mis puudutavad tehnoloogia arengut ja selle võimalikke mõjusid küberjulgeolekule Eestis. 2015. aastal rakendasime uuringutega kogutud teadmise otseselt Eesti e-riigi turvalisuse tõstmise teenistusse.

Eesti e-riigi toimimine sõltub suures osas teenuste usaldusväärsusest, mis eeldab tugevate krüptograafiliste vahendite kasutamist. 2015. aastal tellisime juba kolmandat korda uuringu, mille eesmärk oli välja selgitada, kas mõni krüptograafiline algoritm ja nende teostus on murdumisohus. Eesti jaoks on oluline lõpetada murdumisohus algoritmide kasutamine enne, kui seda meie riigi või kodanike vastu ära kasutatakse.

2014. ja 2015. aasta massilised infoturbeintsidendid (HeartBleed, Shellshock) näitasid, et peamine probleem ei seisne mitte krüptoalgoritmide matemaatilises tugevuses, vaid praktilise rakenduse nüanssides. Lähtuvalt uuringu tulemustest alustati 2015. aastal muutusi ID-kaardi turvalisuse tõstmi-

seks. Üldine soovitus on arvestada uute lahenduste projekteerimisel juba eos vajadusega krüptograafilisi algoritme aeg-ajalt uuendada. Seega peaks nende algoritmide ja turvalahenduste kasutamine olema võimalikult paindlik ja vajadusel kiiresti ümberhäälestatav.

2015. aasta uuring käsitles lisaks algoritmidele ka kontaktivabade kiipkaartide ja mobiiliplatvormide turvalisust. Kontaktivabade kaartide puhul toimub andmeside üle potentsiaalselt ebaturvalise raadiokanali (NFC). Mobiilseadmete puhul on probleemiks kasutaja privaatvõtmete kaitse. Kui loobuda võtmete hoidmisest kiibil, pole privaatvõtmetele praegustes mobiilseadmetes head alternatiivset säilituskohta.

Üks võimalus oleks nii-öelda usaldatav täitmiskeskkond (*TEE – Trusted Execution Environment*), kuid see alles hakkab eri tootjate seadmetesse jõudma, mistõttu on pakutavat turvataset veel vara hinnata. Uuringu tulemused on olnud sisendiks kontaktivaba ID-kaardi planeerimisel Eestis ning neid peaksid tulevaste lahenduste arendamisel ja haldamisel arvesse võtma ka Eesti riigiasutused ja ettevõtted.

Viimased aastad on aina rohkem esile toonud kriitikat riigi kasutatavate infotehnoloogiliste lahenduste kohta. Oponendid pole rahul, et riiklike andmekogude hoidmist pilveteenustes peetakse ebaturvaliseks, kui paljud erasektori ettevõtted hoiavad samal ajal klientide andmeid pilves. Olgugi et pilvelahendusi peetakse odavamaks, kiiremaks ja töökindlamaks, pole sääraste kasutamine kooskõlas Eesti praeguste seadustega ning riiklike andmekogude säilitamist teiste riikide territooriumil võib pidada põhimõtteliselt ebaturvaliseks.

Kodanike poolt riigile usaldatud andmete puhul on väga oluline teada, kus need andmed asuvad, kellel on nendele ligipääs ja kui hästi on need kaitstud erinevate rünnete eest.

Kodanike poolt riigile usaldatud andmete puhul on väga oluline teada, kus need andmed asuvad, kellel on nendele ligipääs ja kui hästi on need kaitstud rünnete eest.

Pilve kommertslahendusi kasutades ei saa olla veendunud, millises riigis, millises andmekeskuses meie andmed asuvad või millise serveri administraatoril on mingil ajahetkel nendele võimalik ligi pääseda. Samal ajal on pilveteenuste järjest laiem kasutamine loomulik osa tehnoloogia arengust ning 2015. aastal alustasime põhjalikku juriidilist ja tehnilist analüüsi, mille valmimine täpsustaks Eesti riigiasutuste võimalusi pilveteenuseid siiski kasutada.

Selle tulemusel koostame Eesti riigiasutustele sobiliku juhendmaterjali, mis vastaks järgmistele küsimustele:

- milliseid andmeid ja mis tingimustel tohib pilves hoida ja käidelda ning milliste pilveteenuste pakkujate lahendusi oleks turvaline kasutada;

- milliste nõuetega peab arvestama ja milliseid turvameetmeid tuleb rakendada pilveteenuse tellimisel.

2015. aastal veendusime, et pilvetehnoloogiate kasutamisega kaasnevaid õiguslikke küsimusi ja andmete pilves töötlemisega kaasnevaid terviklust ja konfidentsiaalsust puudutavaid riske tuleb põhjalikult analüüsida ning töötada välja piisavad turvameetmed riskide minimeerimiseks. 2016. aastal valmib täiendav riigipilve õiguslik analüüs, mis keskendub eelnevalt kirjeldatud eesmärkidele.

Muudatused ID-kaardi kasutamisel

2015. aastal mõjutas Eesti küberturvalisust oluliselt vajadus teha muutusi Eestis välja antud ID-kaartide juures. 2015. aasta keskpaigas selgus, et suurel hulgal Eestis välja antud ID-kaartidel on isiku tuvastamiseks kasutusel sellised sertifikaadid, mille tunnustamise plaanivad suuremad tarkvaratootjad lõpetada või on juba lõpetanud. Seetõttu tekkis oht, et teatud kuupäeva möödumisel pole võimalik kaarte elektroonilistes kanalites isikutuvastamiseks kasutada. Otsest turvaohtu standardile mittevastavusest ei tulene ning kasutajate privaatsus või konfidentsiaalsus kannatada ei saa.

ID-kaartidel võetakse kasutusele tugevam krüptograafia.

Umbes 420 000 aktiivsel kaardil (isikutunnistused, elamisloakaardid ja digi-IDd, sh e-residentide digi-IDd) on digitaalseks isikutuvastamiseks vajalik sertifikaat, mille kuju ei vasta standardile. Seetõttu ei saa garanteerida, et nende kaartide kasutamine digitaalseks isikutuvastamiseks ja allkirjastamiseks elektroonilistes keskkondades on jätkusuutlik.

Seni polnud standardile mittevastavus ilmsiks tulnud, sest vastavad kontrollmehhanismid on laiatarbetarkvaras enamasti suhteliselt leebed. 2014. aasta massiliste turvaprobleemide tulemusena hakkasid suuremad tarkvaratootjad 2015. aastal kontrollmehhanisme karmistama. Esimesena andis muudatustest teada 2015. aasta suvel Google, kelle veebilehitsejat Chrome kasutab Eestis hinnanguliselt enam kui pool internetikasutajatest.

Tagamaks Eesti ID-kaardi sertifikaatide jätkuv vastavus tunnustatud standarditele, alustati 2015. aastal Politsei- ja Piirivalveameti (PPA) ning RIA koostöös ettevalmistusi ID-kaardi sertifikaatide vahetamiseks.

Senine praktika eeldas, et ID-kaardi sertifikaatide vahetamiseks tuleb külastada PPA teenindusbürood. Selline lahendus ei sobi aga olukorras, kus korraga tuleb vahetada suure hulga kaartide sertifikaadid, mille omanikest osa on füüsiliselt välisriikides asuvad e-residendid. Seetõttu otsustati 2015. aastal taastada võimalus vahetada isikutuvastuse kiipkaardil paiknevad sertifikaadid kauguuenduse teel. Mõjutatud kaartide omanikud saavad alates märtsist 2016 uuenduse iseseisvalt läbi viia, kasutades selleks ID-kaardi haldusvahendit.

Koos kauguuendusega alustati 2015. aastal PPA ja RIA koostöös ka väljasta-

tud ID-kaartide turvalisuse tõstmist, et tagada kaartide kestev jätkusuutlikkus. Enamik käibivatest ID-kaartidest kasutab autentimise ja digiallkirjastamise sertifikaate, mille signeerimiseks väljastamise hetkel pruugiti SHA-1 räsialgoritmi. Niisuguseid ID-kaarte on ligikaudu miljon ja need on väljastatud enne 01.03.2016.

Arvutusvõimsuse kasvades muutuvad varasemad krüptograafilised algoritmid (nagu SHA-1) haavatavaks, sest hästi rahastatud ründajatel tekib võimalus neid murda. Esialgu on tegemist küll vaid teoreetilise haavatavusega, kuid pikemas perspektiivis oleks ohustatud avaliku võtme infrastruktuur, mis tavakasutaja jaoks tagab inimese turvalise tuvastamise ID-kaardi, mobiil-ID või digi-ID abil. Selleks, et ohu realiseerumist ennetada, tuleb vananevad krüptograafilised algoritmid asendada tugevamatega. See tähendab tavakasutaja jaoks vajadust asendada ID-kaardi kiibil olevad sertifikaadid sellistega, mis põhinevad tugevamal krüptograafial (SHA-2).

Tarkvaratootjad on võtnud kindla suuna lõpetada SHA-1 räsifunktsiooni toetamine, sest selle n-ö murdmise tõenäosus on muutumas liiga suureks. Asjaolu, et arvutusvõimsuse kasvades ning krüptoanalüütiliste teadmiste täiustudes muutuvad vanemad krüptograafilised algoritmid tasapisi ebaturvaliseks, on krüptograafia seisukohalt tavapärane areng.

Kuna 90% Eesti internetikasutajatest kasutab kas Microsofti, Google Chrome'i või Mozilla Firefoxi veebilehitsejat, analüüsiti 2015. aastal nende tarkvaratootjate baasnõudeid (*baseline requirements*) ja alustati Eesti ID-kaartide turvalisuse suurendamist koos eelkirjeldatud sertifikaatide uuendamisega. Tarkvaratootjad on oma selleteemalistes seisukohtades olnud suhteliselt ebaselged, seega otsustati turvalisust tõsta, et ennetada kasutajate probleeme tulevikus.

Riigi infosüsteemide turve ja rahastamine

Vahendame infoturbe korraldusega seotud parimat praktikat.

Eestis on riigiasutustel ja kohalikel omavalitsustel kohustus kasutada infoturbe tagamisel etalonturbe süsteemi (ISKE). ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavate infosüsteemide ning nendega seotud infovarade turvalisuse tagamiseks. Riigi infosüsteemi turvalisuse korraldamiseks ja arendamiseks toimuvad regulaarselt valdkondlikke eksperte koondava turvajuhtide komisjoni koosolekud. Selle kaudu koordineerime turvajuhtide tegevust ja vahendame infoturbe korraldusega seotud parimat praktikat.

ISKE riigiasutustes ja kohalikes omavalitsustes rakendamise hõlbustamiseks valmis 2015. aastal ISKE portaali esmaversioon. Seni oli ISKE kättesaadav üksnes RIA kodulehel, koosnedes mitmest dokumendifailist ja enam kui 4000 leheküljest. Nüüd on ISKE kättesaadav ühest mugavast ja kasutajasõbralikust portaalist. Lisaks korraldatakse 2016. aastal neli infoturbe halduse koolitust ISKE rakendajatele ja seitse infoturbe teadlikkuse tõstmise koolitust rii-

giasutuste tavakasutajatele.

Eesti küberjulgeoleku strateegia on sisult väga ambitsioonikas ning sellest tulenevad ülesanded on eeldanud suuri kulutusi tervelt riigilt, sealhulgas RIA-lt. Seetõttu on paljudes tegevustes kasutatud Euroopa Liidu struktuuritoetust, mis moodustas 2015. aastal ligikaudu 40% RIA küberturvalisuse teenistuse küberturvalisuse arendamise eelarvest.

Kuigi Euroopa Liidu struktuuritoetus on olnud tänuväärne tugi Eesti küberjulgeoleku arendamisel, on selge, et pikemas perspektiivis ei ole säärane olukord, mis kehtib tegelikult ka kogu riigi IT arendamise juures, riigi jaoks jätkusuutlik. Eesti julgeolekut küberruumis peaks ennekõike tagama riigi enda vahenditega, seega tuleb senisest enam rahastada IT-arendust ja küberjulgeoleku valdkondi. Tegu on loomuliku sammuga: Euroopa Liidu struktuuritoetuse abil oleme pannud aluse korralikule IT-infrastruktuurile kogu riigis ning nüüd tuleb võtta ise põhivastutus IT-investeeringute ja küberjulgeoleku eest.

Järelevalve

Küberjulgeoleku tagamiseks Eestis on oluline riskipõhisest, koostööle suunatud ja konservatiivsest lähenemisest lähtuv järelevalve.

Tervishoiuteenuse osutajate infoturbekorraldus vajab tähelepanu.

Lisaks infoturbetaseme hindamisele kontrollisime 2015. aastal seitsmes ministeeriumis infoturbemeetmete rakendamist ja tegevuskavade täitmist. Lisaks vaatasime asutuste dokumentatsiooni ja andsime nõu, kuidas puudujääke kõrvaldada ja milliseid täiendusi teha.

Analüüsisime ka infoturbemeetmete rakendamist ja seda, kuidas asutused täidavad auditite tegemise kohustust. 11 ministeeriumi ning 24 ametit ja asutust hõlmanud analüüs näitas, et infoturbemeetmete rakendamise tase on avaliku sektori asutustes rahuldav – vaid mõnes asutuses on auditikohustuse täitmisel puudusi. Infoturbemeetmete rakendamise olukorra analüüsi tulemusi tutvustasime avaliku sektori asutustes, infoturbejuhtidele ja Eesti Infosüsteemide Audiitorite Ühingu liikmetele.

Sideteenuse osutamise üle järelevalvet tehes on meil kohustus koostada asetleidnud intsidentidest aastakokkuvõte, mille peame edastama Euroopa Liidu võrgu- ja infoturbeametile (ENISA). Olgugi et Eestis sideteenust osutavad firmad hindavad oma riske regulaarselt ja on endi hinnangul võimelised tõrgetele ja rünnakutele adekvaatselt reageerima, on selge, et sõltuvus sideteenusest avaldab mõju ka teistele (sh elutähtsatele) teenustele. Hoiame sideteenustega seotud riskidel püsivalt silma peal, kuivõrd need on Eesti küberturvalisuse tagamisel kriitilise tähtsusega.

Jätkuvalt vajab tähelepanu ka tervishoiuteenuse osutajate infoturbekorraldus. Eesti tervishoiuvaldkond sõltub olulisel määral IT-süsteemide toimimisest. 2015. aastal kaardistasime koostöös Andmekaitse Inspektsiooniga põhjalikult infoturbe olukorda Eesti perearstikeskustes ja jätkame seda tege-

vussuunda ka 2016. aastal.

Rahvusvaheline koostöö

Eesti küberjulgeoleku korraldus ja kogemused on jätkuvalt suure rahvusvahelise tähelepanu all. Huvi Eesti küberturvalisuse poliitika ja tegevuste vastu on kasvanud ka geopoliitilise ebastabiilsuse tõttu Venemaa suhetes Euroopa ja NATOga. Hübriidsõda Ukrainas ning Moskva agressiivne retoorika naabrite ja NATO suunal on andnud võimalusi kaalukalt kaasa rääkida arvukatel rahvusvahelistel foorumitel nii Eestis kui välismaal. RIA analüüsi ja hinnanguid küberjulgeoleku rahvusvahelistele trendidele jälgitakse huvi ja tunnustusega.

Sõlmisime küber-julgeoleku koostöö-lepingu Jaapaniga.

2015. aastal jätkus tihe koostöö oluliste partnerriikidega Euroopas ja Põhja-Ameerikas. Kolme Balti riigi vahel sõlmiti novembris küberjulgeoleku koostööleping, mis võimaldab suurendada piiriülest koostööd küberintsidentide ärahoidmisel ja tõrjumisel. Märkimist väärib ka asjaolu, et Balti ministrid allkirjastasid dokumendi digitaalselt ning see on teadaolevalt esimene kolme riigi vahel digiallkirjastatud leping.

RIA koostööraamistikke täiendas detsembris sõlmitud küberjulgeoleku koostööleping Jaapaniga. Leping allkirjastati kolmandat aastat toimunud Eesti-Jaapani küberjulgeoleku dialoogil Tokyos.

Küberturvalisust käsitleti novembris Tallinnas toimunud D5 (Digital Five) võrgustiku kohtumisel. D5 on 2014. aastal Londonis loodud formaat, mis liidab viis maailma digitaalselt arenenuimat riiki: Eesti, Iisraeli, Lõuna-Korea, Suurbritannia ja Uus-Meremaa. Võrgustiku eesmärk on vahetada kogemusi ja teha koostööd e-riigi lahenduste arendamisel.

RIA eksperdid jagasid oskusteavet mitmes küberjulgeoleku võimekusi edendavas koolitusprojektis Ida-Euroopas ja Lõuna-Ameerikas. RIAt külastas ka mitu välisdelegatsiooni Aafrika ja Aasia arenguriikidest, kellele jagati soovitusi nii CERTide ülesehitamise, avaliku ja erasektori koostöömudelite rakendamise kui küberjulgeoleku strateegia elluviimise ja regulatsioonide koostamise kohta.