Riigi Infosüsteemi Amet

RIIGI INFOSÜSTEEMI AMETI KOKKUVÕTE KÜBERTURVALISUSE TAGAMISEST 2012

Küberruum on taristust ja teenustest koosnev ökosüsteem ehk keskkond, kus ja mille kaudu toimuvad samasugused ühiskondlikud suhted ja protsessid kui tavamaailmaski. Küberruum on tänapäeval käsitletav ainult tavamaailma osana, sest on palju selliseid protsesse ja suhteid, mis saavad eksisteerida ainult infotehnoloogia abil ning leiavad aset küberruumis: digitaalne kommunikatsioon, infotöötlus, teabe säilitamine jne. Sellise ökosüsteemi arengutase, ulatus ja kasutamine, nagu ka ühiskonna sõltuvus sellest, on riigiti erinev. Eesti kuulub kaheldamatult kõrge kübersõltuvusega riikide hulka, mille jaoks on küberjulgeoleku tagamine riikliku julgeoleku ja ühiskonna turvalisuse küsimus. Küberkeskkonna kaitsmiseks on vaja aru saada riskidest, ohud ära tunda ning olla valmis keskkonda nende eest kaitsma ja võimalike tagajärgedega toime tulema. Häid teadmisi küberkeskkonna, tehnoloogia ja selle kasutamise riskidest on tarvis nii ettevõtete ja asutuste juhtidele kui ka koolilastele. IT ei ole juba ammu enam inseneride pärusmaa, vaid on muutunud igapäevaelu lahutamatuks osaks, seda koos kaasnevate riskide ja ohtudega, mida peavad lahendama kõik tehnoloogia kasutajad.

RIA küberturvalisuse tagajana

Eestis on alates 2007. aastast riiklikul tasemel tegeletud aktiivselt küberturvalisuse tagamisega, et kindlustada riiklike institutsioonide ja elutähtsate teenuste turvalisust ja kättesaadavust igas olukorras. 2008. aastal välja töötatud küberjulgeoleku strateegia nägi ette riikliku tegevusprogrammi kuni 2013. aastani. Riigi Infosüsteemi Amet loodi küberturvalisuse keskse kompetentsi- ja koordineerimiskeskusena 2011. aastal ning küberjulgeoleku valdkonna koordineerimise võttis Kaitseministeeriumilt üle Majandus- ja Kommunikatsiooniministeerium. 21. märtsil 2013 kiitis valitsus heaks ettepaneku, millega hakatakse koostama Eesti küberjulgeoleku strateegiat aastateks 2014–2017.

RIA põhiülesanded küberturvalisuse tagamisel on:

- järelevalve elutähtsa teenuse[1] osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise üle;
- riigi infosüsteemi ja Eesti kriitilise informatsiooni infrastruktuuri infoturbega seotud tegevuste korraldamine;
- Eesti arvutivõrkudes toimuvate turvaintsidentide käsitlemine;

2012. aasta jooksul mehitas RIA küberturvalisuse valdkonna spetsialistidega, kes tagavad esmase vajaliku kompetentsi ameti põhiülesannete täitmisel ning koostöövõrgustiku kriitilise infrastruktuuri intsidentide lahendamisel. Kokku töötab täna RIA vahetult küberturvalisuse tagamisega seotud ametikohtadel 22 inimest. RIA peamised prioriteedid on olnud turvalisuse tagamiseks vajaliku kompetentsi koondamine, koostöövõrgustike loomine ja arendamine, spetsiifiliste võimekuste (nt SCADA/ICS turvalisus) arendamine ning elutähtsate teenuste osutajate ning kriitilise

1 Elutähtsad teenused ja nende osutajad on määratletud hädaolukorra seaduse paragrahvis 34

infrastruktuuri haldajate toetamine küberturvalisuse tagamisel.

2012. aasta möödus suuremate vahejuhtumiteta

Kuigi aasta jooksul anti RIAle teada mitmetest intsidentidest (Järelevalve registreeris 41 olulist intsidenti), polnud neist ükski selline, mis oleks kaasa toonud hädaolukorra. Meedia tähelepanu pälvis peale talitluspidevuse häiretega seotud intsidentide (näiteks Elioni katkestused, kaardimaksete süsteemi tõrked või lennujuhtimissüsteemi häired) ka nn "#opEstonia" juhtum, mis ei mõjutanud kriitiliste infosüsteemide tööd ning lahendati tavapärasest intensiivsema töö käigus. Tõsiseks saab veel lugeda paari kuritegelikku rünnet, mille käigus üritati petukirjade abil saada juurdepääsu pangakontodele. RIA turvaintsidentide käsitlemise osakond tegeleb tavapäraselt kümnete juhtumitega päevas, kuid enamjaolt piirdub intsidentide lahendamiseks vajalik tegevus kasutajate nõustamise ning koordineeriva rolliga, kohapealset tehnilist abi peab RIA osutama harva.

Turvalisuse tagamine teadlikkuse tõstmise kaudu

Küberjulgeoleku valdkonnas korraldasime Euroopa Liidu struktuurifondide programmist „Infoühiskonna teadlikkuse tõstmine" aasta jooksul 5 seminari, 1 konverentsi, 1 infopäeva ja 17 koolitust, milles osales kokku 684 inimest. Lisaks toimus Tallinnas CERT-EE rahvusvaheline sümpoosium küberintsidentide lahendamise teemadel, millel osales 226 inimest, sh 114 väljastpoolt Eestit. Korraldati nii praktilisi turvakoolitusi IT-spetsialistidele, ISKE rakendamise ja auditi ning riskihalduse koolitusi asutuste infoturbejuhtidele kui ka sissejuhatavaid koolitusi tavakasutajatele.
RIA osales asutusena või ekspertide osalusega nii siseriiklikel kui ka rahvusvahelistel küberõppustel, mille käigus testiti korduvalt nii tsiviil- kui militaarküberkriiside lahendamist ning kaasati ka elutähtsate teenuste osutajaid.

Küberkuritegevus

Avalikku arvamust küberjulgeoleku kohta mõjutab väga palju küberkuritegevuse tase. Tinglikult loetakse küberkuritegudeks kõiki IT-vahenditega või ITga seotud kuritegusid. Üldistatult on arvutikuritegevuse tase jäänud samale tasemele varasemate aastatega. 2012. aastal alustas Politsei- ja Piirivalveameti Keskkriminaalpolitsei menetlusbüroos tööd V talitus, mille põhiülesandeks määrati kohtueelse menetluse teostamine infotehnoloogiaga seotud rasketes ja rasketes peitkuritegudes, samuti osalemine valdkonna tervikkoordineerimises.

Politsei- ja Piirivalveameti hinnangul mõjutasid politsei tööd küberkuritegevusega võitlemisel 2012. aastal enim:

- Trojanite sõjad (Venemaa ja USA ning ka Hiina viirusetootjate vahelised vastasseisud) raha parast jätkusid. Sõjad on muutunud kommertslikumaks.
- Küberkurjategijad otsisid jätkuvalt varastatud infole müügikanaleid.
- Jätkus teenusteks muutunud ja teenustena pakutavate kelmuste arendamine.
- Küberkurjategijate võrgust eraldamised sundisid neid arenema (Man-in-the-browser (MITB) – st püüdu varastada infot otse brauserist).

- Häktivismi tõus.
- Kiire infovahetus lihtsustas gruppide tabamist ja botnettide operaatorite (e pahavara kasutajad, kes juhivad ja koordineerivad ründeid) tabamist.
- Erinevad teismeliste küberkiusamised saavutasid Child Groomingu (veebi kaudu ahvatletakse laps endast alasti pilte tegema ning siis algab raha väljapressimine ähvardusega, et muidu pannakse pildid nt Facebooki) mõõtmed.
- Tabatud lapsporno levitajad peavad enda moraalselt väärastunud tegevusi tavanormiks.

Samad trendid jätkuvad PPA hinnangul ilmselt ka 2013. aastal.

Turvameetmed ja järelevalve

RIA töötas välja ja esitas aasta jooksul ettepanekuid küberturvalisust ja selle järelevalvet kindlustavate regulatsioonide täiendamiseks ja muutmiseks, sealhulgas avaliku teabe seaduse, hädaolukorra seaduse, elektroonilise side seaduse, riigisaladuse ja salastatud välisteabe seaduse muutmiseks ning valitsuse mitme määruse vastuvõtmiseks. Olulisemate muudatustena võib välja tuua 2013. aastast jõustunud määruse riigiasutuste infoturbemeetmete karmistamiseks, mille kohaselt peavad kõik riigiasutused määrama infoturbe eest vastutava juhtivtöötaja, ning pikalt ette valmistatud turvalisuse nõuded elektroonilistele süsteemidele, millest sõltub elutähtsate teenuste toimimine. Huvitav on see, et elutähtsate teenuste osutajatest eraettevõtted on väljendanud positiivset huvi selgete regulatsioonide ning riiklikult kehtestatud turvameetmete vastu, mis võimaldaksid suuremat selgust ja läbipaistvust ühiskonna ootuste mõistmisel ja sotsiaalse vastutuse kandmisel.

Järelevalvet turvameetmete rakendamise üle riigiasutustes alustas RIA enda olukorra hindamisest. Amet moodustati endise Riigi Infosüsteemide Arenduskeskuse baasil ning seega osutab RIA endiselt IT-teenuseid riigiasutustele ja korraldab riigi baastaristu tööd. Järelevalve käigus avastati RIAs mitmeid puudusi, mis võimaldas sarnaseid puudujääke hinnata ka teistes asutustes. Pärast seda kaardistati ja hinnati turvameetmete ja ISKE rakendamist riigiasutustes. Olukorda ei saa hinnata täiesti rahuldavaks: üheteistkümnest ministeeriumist neli möönab, et nende haldusalas on ISKE rakendamisel puudujääke ja meetmete rakendamine on alles algusjärgus.

Masinate interneti turvalisusest

Automaatjuhtimissüsteemide, robootika ja integreeritud nutilahenduste (*Smart Technologies*) lai levik on toonud kaasa riskid, mis sunnivad küberturvalisuse tagamisel järjest rohkem panustama valdkondadesse, kus küberrünne toob kaasa vahetu kineetilise tagajärje, mis võib halvemal juhul kaasa tuua elutähtsate teenuste katkemise. Nutimõõtjate (*Smart Meters*) kasutuselevõtmine Eesti Energias ning erinevad kaug- ja automaatjuhtimisüsteemide turvaprobleemid on näited, millega seoses oleme suunanud rohkem ressurssi elutähtsate teenuste ICS/SCADA süsteemide turvalisuse tagamisse. RIA korraldas 2012. aastal koostöös elutähtsate teenuste osutajatega mitu läbistustesti, mille käigus testiti elutähtsate teenuste infosüsteemide turvalisust. Saadud andmete alusel oli ettevõtetel võimalik parendada ja muuta oma turvapoliitikat.

Rahvusvaheline koostöö

Küberjulgeoleku edukas tagamine eeldab hästitoimivat igapäevast rahvusvahelist koostööd nii intsidentide lahendamisel kui ka turvameetmete väljatöötamisel. 2012. aasta jooksul tihendasime oma kontakte USA, Prantsusmaa, Saksamaa ja teiste riikide ameti- ja teadusasutustega. Eraldi võib välja tuua koostöö Saksamaa BSIga (*Bundesamt für Sicherheit in der Informationstechnik)*, kellelt pärineb Eesti riigiasutustes kasutatav ISKE turberaamistik ning USA Idaho National Laboratoryga ICS/SCADA süsteemide turbe vallas. RIA esindajad osalesid aktiivselt nii erialaorganisatsioonides kui ka rahvusvahelistes töögruppides ning panustasid ka välisriikide partnerite koolitamisse.

Siseriiklik koostöö

RIA teeb aktiivselt koostööd nii riigi- kui erasektoriga koostöögruppide ja komisjonide kaudu. Eraldi tasub märkida Kriitilise Informatsiooni Infrastruktuuri Kaitse komisjoni, CERT-EE koostöövõrgustikku ja igakuist perioodilist koordinatsioonikohtumist teiste riigiasutustega. Aktiivne on koostöö Andmekaitse Inspektsiooni, Tehnilise Järelevalve Ameti, Kaitsejõudude ja julgeolekuametkondadega, samuti Kaitseliidu Küberkaitseüksusega.

Kokkuvõte

2012. aasta oli Eesti küberruumis rahulik ja andis meile aega tegevusi planeerida ning teistelt õppida. 2013. aastal peavad RIA alustatud projektid andma meile juurde tehnilist seirevõimekust näha riske riigi infosüsteemis. Tugevnev järelevalve peab aitama tõsta Eesti üldist valmisolekut ohtudega toime tulla. Hea koostöö erasektoriga, eriti elutähtsate teenuste osutajate ning turvaettevõtetega, peab tõstma Eesti ettevõtete konkurentsivõimet ja jätkusuutlikkust.
Turvalist küberruumi!

Toomas Vaks,
RIA Peadirektori asetäitja küberturbe alal

Käesoleva kokkuvõtte koostamisel on kasutatud Riigi Infosüsteemi Ameti ja Politsei- ja Piirivalveameti andmeid.