Riigi Infosüsteemi Amet

RIA Küberturvalisuse teenistuse 2013. aasta kokkuvõte

2013. aasta
Eesti küberturvalisuses

135 intsidenti raporteerisid riigiasutused

25% **neist põhjustasid ründed**

2–5 aasta jooksul

tuleb Eestis välja vahetada mitmed krüptolahendused

Eestis: 13 ummistusrünnet

240 näotustamisjuhtumit

Küberturbeõppusel

Locked Shields sai Eesti 2. koha

RIA korraldas

18 turbeteemalist koolitust, **497** koolitatut

43 koondraportit esitasid riigiasutused

lähtuvalt uuest infoturbe juhtimise süsteemi määrusest

Sisukord

Eessõna: 2013. aastast küberturvalisuses

2013. aastat jäädakse küberturvalisusega tegelevates ringkondades mäletama kui Snowdeni-aastat. 20. mail 2013 Hongkongi põgenenud NSA lepinguline töötaja näitas järgnevate kuude jooksul kogu maailmale, kuidas toimib tänapäevane luureteenistus ning kui vähe on inimestel õigupoolest lootust privaatsusele küberruumis. Peaaegu sada aastat varem, 1929 saatis USA tollane riigisekretär Henry L. Stimson riigi tollase luureasutuse laiali ajalukku läinud sõnadega: "Härrasmehed ei loe võõraid kirju." Kuigi salastatud sõnumite lahtimõtestamisega tuli uuesti peale hakata juba õige pea, ei kujutanud tänapäeva luure mastaapseid võimalusi ilmselt tollal keegi ette.

Küberruumi kolinud inimsuhtluse jälgimine võimaldab suurriikidel end paremini julgeolekuohtude eest kaitsta, kuid paraku on selle eest makstav hind väga kõrge. Privaatsust pole küberruumis võimalik eeldada. Peale uudishimulike eriteenistuste, erafirmade ja küberpättide on nuhkimist ja jälgimist võimaldavad vahendid üha kättesaadavamad igaühele. Tavalise e-posti kasutamine on piltlikult nagu postkaartide saatmine. Võõraste postkaartide lugemine on küll ebamoraalne… kuid lihtne ja mugav. Hoolimata privaatsuse kaitsjate jõupingutustest ei kipu internet ka midagi unustama: kunagi tehtud rumaluste kohta jääb infoajastu koopaseintele väga kauaks jälg maha. Seega peab terve mõistuse, enesekontrolli ja ettevaatuse säilitama ka küberruumis.

Teine oluline teema oli Eesti jaoks kindlasti küberjulgeoleku strateegia uuendamine. Alates 2008. aastast on selginenud meie arusaamad riigi küberturvalisuse tagamise vajadusest, et kindlustada riigi ja ühiskonna toimimine aina enam arvutitest sõltuvas maailmas. Küberründe tagajärgi saab piltlikult võrrelda ühiskonna, riigi või indiviidi närvisüsteemi kahjustamisega: see võib tekitada pettekujutlusi ja kahjustada meeli (küberründed info- või psühholoogise sõjapidamise vahenditena), see võib meid halvata (sidevahendite ja elektrooniliste automaatjuhtimissüsteemide töö takistamine) ja kahjuks lõpuks ka tappa (terrorirünnakud elutähtsate teenuste vastu). Hirmuäratav on kübersõja efektiivsus – suhteliselt odava, ülikiire ja täpse rünnakuga saab kahjustada just oluliste teenuste toimimist. Lisaboonus on võimalus ründajat paremini varjata ja kaitsta, kui see vahetu füüsilise ründe korral kunagi võimalik oleks. Suurenenud tehnoloogiasõltuvus ja muutunud julgeolekusituatsioon tingivad vajaduse ohud ümber hinnata ning leida uued riskide maandamise võimalused.

Rahvusvaheliselt on küberteema järjest olulisemaks muutunud ning teadlikkus küberriskidest on kindlasti parem kui veel paar aastat tagasi. Kahjuks napib aga endiselt võimalusi ning oskusi tuvastatud riske maandada. Seetõttu mõjub väga meeldivalt näiteks Hollandi uue küberjulgeolekustrateegia üks eesmärke: muutumine riskiteadlikkust ühiskonnast (riskide maandamiseks vajalike) oskustega ühiskonnaks. On ju oluline silmas pidada, et turvalisus sõltub valdavalt just kasutaja oskustest. Oskamatu kasutaja suudab endale ka tavaliste söögiriistadega palju kahju teha, lauanoa valest otsast kinnivõtmisel võivad lausa fataalsed tagajärjed olla. Eestlased on õppinud internetipanga, e-riigi ning tehnoloogiaga juba päris hästi toime tulema. Sestap tundub mõne eksperdi val-

justi väljendatud mure Eesti e-lahenduste turvariskide pärast vahel tublide Euroopa misjonäride murena hommikumaal pulkadega söömisel tekkiva vigastusohu pärast. Eesti inimesed on "pulkadega söömist" juba üle kümne aasta harjutada saanud ja oskavad sellega enamasti end vigastamata toime tulla.

Hea on tõdeda, et suuri ja tõsiseid küberintsidente ei juhtunud ka sellel aastal ning Eesti elanikud võivad ennast meie e-Eestis päris turvaliselt tunda.

Küberturvalist 2014. aasta jätku!

Toomas Vaks

RIA peadirektori asetäitja küberturvalisuse valdkonnas

Raporti kokkuvõte

See raport on kokkuvõte 2013. aasta olulisematest sündmustest ja teemadest Eesti ja maailma küberjulgeolekus.

2013. aasta oli Eestis tõsiste intsidentide poolest võrdlemisi rahulik. Klassikalisi üksikintsidente oli varasemaga võrreldes vähem, samas nägime laia kõlapinda saanud juhtumeid, kus küberintsidendid moodustasid vaid ühe osa infosõjaoperatsiooni hoolikalt planeeritud tervikust. Sellistest kombineeritud operatsioonidest värvikaim oli kindlasti #opindependence'i juhtum. **Ummistusründeid** registreeris RIA Eestis 2013. aastal ühtekokku **13 juhtumit, näotustamisi** oli märksa rohkem: **240 juhtumit.**

Küberohtude ennetamisel pööras RIA ka eelmisel aastal palju tähelepanu koolitustele, rahvusvahelistele küberõppustele, riigiasutuste ja elutähtsate teenuste süsteemide läbistustestidele. Oluline verstapost oli järjekordse krüptograafiliste algoritmide elutsükli uuringu valmimine. See tuletas mustvalgel meelde, et Eestis tuleb lähema 2–5 aasta jooksul vahetada välja mitmed krüptolahendused, mis on kasutusel ka näiteks digi-IDs, m-IDs ja enne 2011. a välja antud ID-kaartides.

Oluline murrang toimus 2013. aastal RIA-le esitatud riigiasutuste raportite arvus, regulaarsuses ja kvaliteedis. 1. jaanuaril jõustus valitsuse määrus, mis kohustab riigiasutusi teavitama RIAt olulistest intsidentidest ja tegema neist kvartalikokkuvõtteid. Kokku teavitasid riigiasutused RIAt möödunud aastal 135 intsidendist. Kõige enam raporteeriti käideldavusintsidente. Vähem anti teada tervikluse ja konfidentsiaalsusega seotud juhtumitest. Kuigi suhtlus riigiasutuse infoturbejuhtidega oli pidev ning info olulisematest intsidentidest jõudis RIAni ka enne määruse jõustumist, on määrusepõhine raporteerimine süsteemi märgatavalt korrastanud, samuti annab see võimaluse pöörata senisest suuremat rõhku intsidentide mõjule.

Mitmed teated õngitsuskampaaniatest, nakatunud veebilehtedest ja teenuste ründamisest pärinesid 2013. aastal (kõrg)koolidest: toimus vähemalt seitse kampaaniat haridusasutuste vastu, tülitati ka lasteaedu. Tähelepanuväärne oli ka juhtum, kus häkiti haridusasutuse telefonisüsteemi ja tehti sadu kaugekõnesid.

Uudne oli nn kõngitsemislaine – õngitsemine telefonikõnede abil. End Microsofti esindajana tutvustanu ärgitas pahaaimamatuid arvutikasutajaid internetist alla laadima programmi ja/või avaldama paroole, mis annaksid petturile ligipääsu ohvri arvutile ja sealtkaudu pangakontole.

Õiguslikus raamistikus oli oluline 2013. aastal algatatud korrakaitseseaduse muutmise ja rakendamise seadus. Vastavalt nendele muudatustele läheb Tehnilise Järelevalve Ameti järelevalvepädevus sidevõrkude ja -teenuste turvalisuse üle RIA-le. Sama eelnõuga sätestatakse RIA järelevalvepädevus ka hädaolukorra seaduses ja avaliku teabe seaduses. Muudatus jõustub 1. juulil 2014.

Raport on suunatud küberturvalisust tagavatele ning valdkonnast huvituvatele strateegidele ja spetsialistidele. Autorid ei eelda lugejalt süvateadmisi ITst ja ootavad heal meelel küsimusi ja kommentaare meiliaadressil riskihaldus@ria.ee või RIA küberkirjutiste kommentaariumis https://kyberkirjutised.ria.ee/2013kokkuvote/.

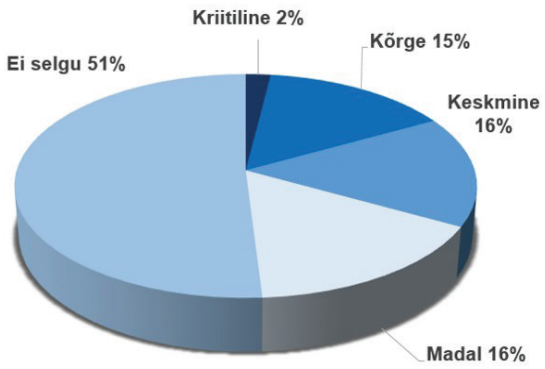
Intsidendid Eesti riigiasutustes

2013. aasta 1. jaanuaril jõustus valitsuse määrus, mis kohustab riigiasutusi teavitama RIAt olulistest intsidentidest ja tegema neist kvartalikokkuvõtteid. Kokku teavitati RIAt möödunud aastal 135 intsidendist. Kõige enam raporteeriti käideldavusintsidente. Vähem andsid riigiasutused teada tervikluse ja konfidentsiaalsusega seotud juhtumitest (nt tahtlikud ründed). Põhjus võib peituda selles, et taoliste intsidentide avastamine on raskem ja võtab enam aega. Täpsemalt jagunesid intsidendid selliselt:

- Käideldavus 65%
- Käideldavus ja terviklus 11%
- Terviklus 9%
- Terviklus ja konfidentsiaalsus 7%
- Konfidentsiaalsus 3%
- Terviklus, käideldavus ja konfidentsiaalsus 3%
- Määramata 2%

Kord kvartalis RIA-le esitatavas turvaintsidendi koondraportis peaksid asutused hindama ka toimunud intsidentide kriitilisust. 2013. aastal oli see info olemas ligikaudu pooltel juhtudel, 66 intsidendi puhul kriitilisust ei hinnatud.

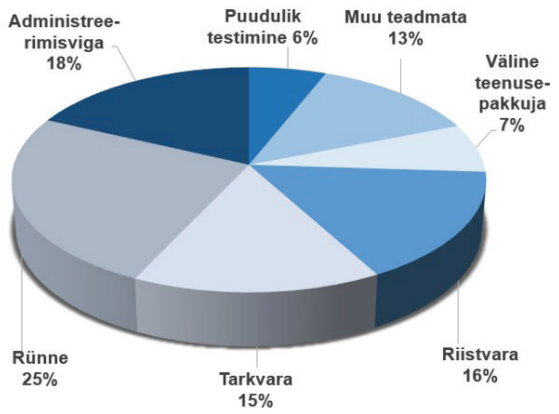
Intsidentide kriitilisus



Samas olid 135 juhtumist 116 realiseerunud intsidendid, mis tähendab, et need avaldasid süsteemide/teenuste toimimisele otseselt mõju. Ülejäänud juhtumite puhul oli tegemist kas avastatud nõrkustega või ei olnud raportist saadud info järelduste tegemiseks piisav.

Intsidentide põhjustena toodi enim välja ründeid ja administreerimisvigu, samuti tarkvara ja riistvara vigu.

Intsidentide põhjused



Rünnetest saab raportites toodu põhjal eristada kaudseid ja otseselt tuvastatavaid ründeid. Kaudsete rünnetena teavitati viiruse või pahavaraga nakatumistest, mis põhjustasid palju ebameeldivusi (näiteks massiline rämpskirjade edastamine). Esines ka viiruse/pahavaraga nakatumise intsidente, mille puhul mõju ei olnud või seda ei avastatud (või ei selgunud see raportist). Otseselt tuvastavate intsidentidena jäid silma:

- sihilikult tekitatud teenusetõkestusründed,
- üksikud sissemurdmised infosüsteemidesse,
- üksikud serveri kasutajakontode ülevõtmised,
- üksikud õngitsemiskirjad.

Kuigi suhtlus riigiasutuse infoturbejuhtidega oli pidev ning info olulisematest intsidentidest jõudis RIAni ka enne määruse jõustumist, on määruse alusel raporteerimine süsteemi märgatavalt korrastanud, samuti annab see võimaluse pöörata senisest suuremat rõhku intsidentide mõjule.

Kokkuvõtlikult – raporteerimine on hästi tööle hakanud. See teeb RIA küberturvalisuse teenistusele heameelt ja võimaldab lisaks riigivõrgu seireandmetele analüüsida riigiasutuste turvalisust regulaarselt ka riigiasutuste endi hinnangute põhjal. Erilist tunnustust väärivad Justiitsministeeriumi, Sotsiaalministeeriumi ja Välisministeeriumi raportid. Samas on mitmes raportis intsidentide põhjuste ja tagajärgede analüüs napp, kuigi infovarade kaardistamine ja neile turvaklassidele määramine võiks olla hea lähtepunkt intsidendi olulisuse hindamisel.

Ebapiisavale põhjuste-tagajärgede analüüsile plaanib RIA riskihalduse osakond edaspidi erilist tähelepanu pöörata.

2013. a olulisemad intsidendid ja tähelepanu pälvinud teemad Eestis

- Jaanuaris toimus **Elionis ulatuslik rike**, mille põhjustas probleem keskse andmesalvestusseadme tarkvaras. Katkesid nutiTV, e-posti, veebimajutuse ja hot.ee teenused. Juhtum tekitas IT-ringkondades elava arutelu varundusmeetoditest ja nende dubleerimisest.

- Jaanuaris selgus, et 2012. aasta lõpus häkiti Lennuakadeemia telefonisüsteemi ja tehti sadu kaugekõnesid. Juhtunut märkas Elion.

- Jaanuaris alustas Andmekaitse Inspektsioon järelevalvemenetlust Tallinna ühistranspordi piletisüsteemi suhtes, neid aitasid ka Riigi Infosüsteemi Ameti infoturbespetsialistid. Maikuus lõppenud järelevalve käigus leiti, et kogu andmestiku üldine 7-aastane säilitustähtaeg ei olnud põhjendatud ja isikustatud andmestiku hoidmise turvameetmed (andmete räsimine) ei olnud piisavad.

- Veebruari alguses tabas Elioni ja Elisa webmaili ning Eesti Maaülikooli analoogse meiliteenuse kasutajaid **õngitsemisrünnak**. Kasutajad suunati võltsitud veebilehele oma e-posti aadressi ja parooli sisestama, et „turvaprobleemiga" tegeleda. Sarnane õngitsusrünnak tabas mai alguses ka Tartu Ülikooli meilikasutajaid ning haridusasutuste võrgu EENeti kasutajaid.

- Mais levisid Eestis Skype'i kasutajate hulgas võltssõnumid, mis sisaldasid linke saaja Skype'i kasutajanimega ja klikkimisele ahvatlevat ingliskeelset teksti (nt *„this is a very nice photo of you* http://miski.koht/string? id<kasutajanimi>". CERT-EE levitas selliste rünnakute tõkestamiseks infot domeeninimede ja IP-aadresside vahemike kohta, mida jälgida ja blokeerida.

- Aprillis 2013 tõstatas RIA teema, mis võinuks aasta hiljem seada ohtu kolmandiku Eesti arvutikasutajatest. Populaarse operatsioonisüsteemi (OS) **Windows XP** kasutajaid kutsuti üles tarkvara uuendama või mõne muu tootja operatsioonisüsteemiga asendama. 2014. a aprillis lõpetas Microsoft XP toetamise, mis jättis selle kasutajad ilma turvauuendustest. Teavitamine on olnud tulemuslik. Kui aprillis 2013 kasutas hinnanguliselt **1/3 Eesti arvutikasutajatest** internetis XPd, siis aasta hiljem oli XP kasutajate arv vähenenud umbes 1/5-ni. Riigiportaalis eesti.ee käis 2014. a märtsis-aprillis XPga arvutitega 15% külastajatest. Riigivõrgust ühendus 2014. a aprillis XPga internetti hinnanguliselt 10% arvutitest.

- Aimates, et ka 2013. aasta kohalike omavalitsuste valimiste e-hääletus ei möödu poliitiliste rünneteta, kutsus RIA aprillis kokku e-hääletamise teemal spetsialistide kärajad, kus osalesid mitmed e-hääletamise turvalisusest huvituvad eksperdid ning e-hääletamise lahenduste ja protseduuride eest vastutavad Vabariigi Valimiskomisjoni liikmed. Kogunemine andis viimase tõuke e-hääletuse serverikoodi avalikustamiseks ja sellele **järgnenud turvatestimiseks,** mille viisid läbi vabatahtlikud spetsialistid. Testijad raporteerisid valimiskomisjonile mitmeid pisivigu, mis eemaldati enne valimisi. Spetsialistide üldine tõdemus oli, et tervikuna on süsteem endiselt usaldusväärne ja turvaline. Seda tõdemust ei kõigutanud ka 2014. aastal vahetult Euroopa Parlamendi valimis-

tele eelnenud järjekordne poliitiline rünnak e-hääletamisele.

- 2013. aasta kevadel jõudsid RIAni teated mitmete **koolide infosüsteemide ründamisest** internetis saadaolevate ründevahenditega. Süsteemide logid ja sotsiaalmeedia postitused viisid õiguskaitseorganid alaealisteni. Augustis oli mitu kooli hädas kooli veebiserverisse istutatud pornolehtede, pahavara levitavate ja ravimimüügile keskendunud veebilehtedega. Koolivõrkude ummistusrünnete tõttu käisid veebipolitseinikud ja CERT-EE koolides kõnelemas küberhuligaansuse tõsistest tagajärgedest. Samateemalisi Anto Veldre praktilisi soovitusi koolide võrguhalduritele saab lugeda **Õpetajate lehest.**

- Nagu ka mujal maailmas kandus mõni kurivara Eestisse aktuaalsete uudiste tuules: pärast aprillis **Bostoni maratonil** toimunud terrorirünnakuid levisid **e-kirjad**, mis ahvatlesid saajat värskete Bostoni plahvatuste fotodega, ent viisid hoopis nakatavale veebilehele.

- Juulis said paljud eestimaalased **ingliskeelse petukõne, kus end Microsofti esindajana** tutvustanu ärgitas internetist alla laadima programmi ja/või avaldama paroole, mis annaksid petturile ligipääsu ohvri arvutile ja sealtkaudu pangakontole.

- Augusti lõpus pälvis suurt avalikkuse tähelepanu **ID-tarkvaras esinenud teoreetiline haavatavus (st märke selle pahatahtlikust ärakasutamisest polnud)**. Haavatavusele oli väljastatud ka paik, seega oli kära teema ümber rohkem kui olukord tegelikult oleks väärinud – tegemist polnud ju esimese ega viimase turvaparandusega ID-tarkvaras. Nagu iga tarkvara puhul, tehakse ka ID-tarkvaras töökindluse ja turvalisuse tagamiseks regulaarseid uuendusi. Avaliku paanika õhutamine oleks mõistetav vaid olukorras, kus toimub ulatuslik haavatavuse ärakasutamine, teisisõnu rünne ID-tarkvara mõnd paikamata nõrkust kasutades. Samas diskussioonis kerkis üles asjaolu, et ID-tarkvarasse pole seni sisse kirjutatud nn **sunduuendamise** mehhanismi, sestap on tarkvara paiga rakendumisel oluline roll ka kasutajal, kes peab pakutud tarkvarauuenduse oma arvutis vastu võtma. Sunduuendamine ehk olukord, kus tarkvara uueneb automaatselt ja kasutaja ei pea selleks midagi tegema, lisandub ID-tarkvarasse 2014. aastal.

- Augustis pälvis avalikkuse tähelepanu ilm.ee ja oktoobris veebiarendajate seas populaarse veebilehe php.net külastajaid nakatanud pahavara. Ilm.ee intsidendi põhjus oli reklaaminäitamistarkvaras OpenX sisaldunud tagauks, mida kasutades lisasid kurjategijad lehele pahavara.

- Oktoobris toimusid kohalike omavalitsuste valimised. E-hääletusel osales 21,2% kõikidest osalenud hääletajatest. Ka sel korral möödus e-hääletamine tõrgeteta, kuigi juba traditsiooniks saanud e-hääletamise vastase poliitilise propaganda saatel.

- **Novembris toimus tarkvarahiiu Adobe'i teenustes andmeleke**, mille tõttu avaldati internetis ka kümnete tuhandete .ee lõpuga meiliaadressi kasutajate Adobe'i teenustes kasutatud parooliräsi ja parooli arvamist hõlbustav paroolivihje.

- Novembri alguses, samaaegselt NATO õppusega Steadfast Jazz, sattusid ründe alla mitmed veebilehed nii Eestis kui Euroopas. Ummistusrünnetest anti sotsiaalmeedias teada sildiga **#opinde-**

pendence ja Anonymous Ukraine, juhtum pälvis ka palju meediatähelepanu. Olulist kahju Eesti riigiasutuste ja ettevõtete infosüsteemidele ei sündinud. Pikemat raportit **#Opindependence'ist saab lugeda siit.**

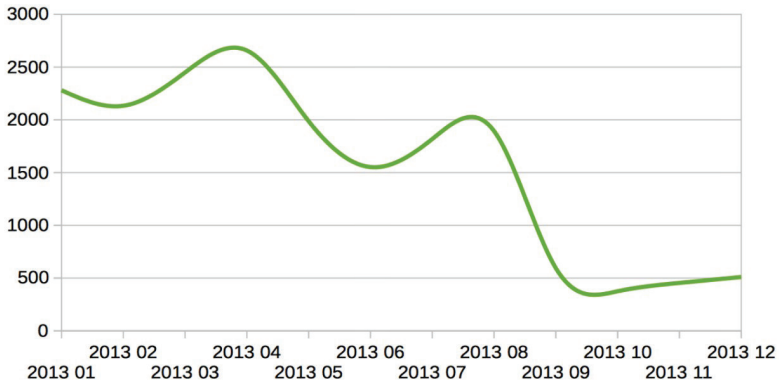
- Novembris käivitasid RIA ja mitmed eraettevõtted ühiselt projekti **NutiKaitse 2017,** mille eesmärk on tõsta nutiseadmete kasutajate, arendajate ja müüjate turvateadlikkust ning kasutamisoskusi, luues seejuures võimalusi, et turvaline tarkvara oleks lihtsalt ja kasutajasõbralikult kättesaadav.

- Sügisel murti Eestis sisse mitmesse serverisse, et ülevõetud masinas bitimünte kaevandada. Vähemalt ühel juhul saadi sisse PHP5 turvaaugu kaudu. Tegu on uue ja küberkurjategijate jaoks üsna lihtsa viisiga serveriparke kuritarvitades tulu teenida.

- Teiste intsidentide seast nähtavuse poolest esile tõusvaid **ummistusründeid** registreeriti Eestis 2013. aastal ühtekokku **13 juhtumit, näotustamisi** oli märksa rohkem: **240 juhtumit**.

- Märke APTst ehk sihitud ründeohust on tuvastanud ilmselt suurem osa lääneriikide riigiasutustest, olgu selleks võrkude skaneerimine või tõetruult koostatud petukirjad, mis toovad endaga kaasa arvuti kõvaketta sisu mujale edastava pahavara. Analoogiliselt oma välismaa kolleegidega pööravad ka Eesti õiguskaitse- ja julgeolekuasutused sellistele juhtumitele suurt tähelepanu.

Pahavarasündmused Eestis 2013. aastal:



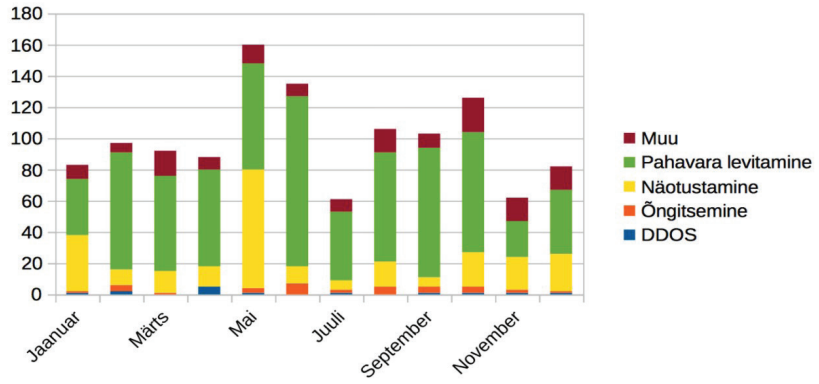
See graafik on CERT-EE koondatud statistika pahavarasündmustest (arvutid/veebielehed, mis osalesid rämpspostikampaanias, ummistusründes, levitasid pahavara jms). Statistika põhineb mitme rahvusvahelise reputatsiooniteenuse andmetel Eesti IP-aadressiruumi kohta.

Graafik näitab trendi, mitu pahavarasündmust toimus igas kuus keskmiselt ühes päevas. Sellises automaatstatistikas kajastuvad pigem nakatunud või muus mõttes halba kirja sattunud (personaal)arvutid / IP-aadressid. Samas tuleb meeles pidada, et arvestatud sündmused ei ole suure

tõenäosusega unikaalsed, seda tulenevalt näiteks dünaamilistest (muutuvatest) IP-aadressidest ning partneritelt pärit andmestiku võimalikust kordumisest. Andmestiku kattumine tuleneb nii ühe sündmuse erinevast nimetamisest kui ka teavituste eri saabumisaegadest. Seega ei saa automaatstatistikale viidates väita, nagu oleks 2013. a detsembris Eestis leidunud üle 15 000 nakatunud arvuti või veebilehe, mis halvemal juhul levitasid pahavara, osalesid rämpspostikampaanias või ummistusründes vms.

Suur langus sel viisil loendatud sündmuste arvus 2013. a varasügisel tuleneb muudatusest reportatsiooniteenuste arvepidamises: loobuti Confickeriga nakatunud arvutite loendamisest. Conficker on pahavara, mis avastati juba viis aastat tagasi, ent selle negatiivset mõju pole seni maailmas tuvastatud.

CERT-EE-le raporteeritud ja CERT-EEs registreeritud pahavarasündmused:



Nii pahavara, näotustamiste, õngitsemiste kui ummistusrünnete hulk ja osakaal olid aasta jooksul võrdlemisi stabiilsed. Eristuvad vaid mai näotustamiste suure hulga ning juuni pahavara levitamiste ebatavaliselt suure arvu poolest. Maikuu statistikas kajastuvad näotustamised toimusid tegelikult pikema perioodi jooksul ning jõudsid statistikasse ühekordse leiu põhjal tehtud skaneeringu tulemusena. Näotustamiste poolest rikkaim kuu 2013. aastal võiks domeenipõhise arvu poolest olla hoopis juuni, mil ühe veebimajutaja serverisse sisse murti ning lausa 600 veebilehe sisu millegi muuga asendati. Juunikuise pahavara levitamise intsidentide hulk tuleneb tõenäoliselt tüüpilisest küberkurjategijate enne-suvepuhkust-rahakogumise lainest.

RIA tegevus küberohtude ennetamisel

Koolitused. RIA korraldas mullu EL struktuurifondide programmist „Infoühiskonna teadlikkuse tõstmine" 18 turbeteemalist koolitust, kus osales 497 inimest riigiasutustest, elutähtsat teenust osutavatest ettevõtetest ja kohalikest omavalitsustest. Korraldati nii tehnilisi (näiteks Apache'i ja veebiserverite koolitus, ipv6 praktikum, IDS koolituspraktikum), praktilisi (ISKE praktiline rakendamine) kui ka üldisi infopäeva-tüüpi üritusi.

Läbistustestid (e pen-testid). 2012. aastast on RIA korraldanud ja tellinud ligi 50 läbistus- ja haavatavustesti. Sageli on nõustatud partnereid läbistustesti tellimisel ja lähteülesande kirjeldamisel. Läbistustestid on võrkude ja süsteemide turvalisuse tagamiseks tõhusamaid meetodeid, aidates haavatavusteni jõuda enne pahatahtlikke ründajaid. RIA skaneerib ka regulaarselt Eesti avalikke võrke ja käib nii riigiasutustes kui kohalikes omavalitsustes võrkude turvalisust testimas ning neid nõustamas. 2013. aastal hindas RIA järelevalve infoturbe taset 20 linna- ja vallavalitsuses, samuti kontrolliti koos Andmekaitse Inspektsiooniga kolme riigiasutust. Hindamise käigus kontrolliti asutuste protseduuride ja arvutivõrkude vastavust ISKE nõuetele. RIA tegi ka hanke kohalike omavalitsuste teenusportaali (KOVTP) turvataseme hindamiseks.

Õppused. Aprillis toimunud **NATO küberkaitsekoostöö keskuse rahvusvahelisel küberharjutusel „Locked Shields 2013"** harjutasid riigi ja ettevõtete esindajad küberrünnete tõrjumist reaalajas õppuseks ehitatud süsteemides. Harjutusel tunnistati parimaks NATO meeskond, Eesti jäi teiseks. Eesti meeskond koosnes elutähtsa teenuse osutajate ja RIA esindajatest. Koos saadi väärtuslikke õppetunde nii kolmandate osapoolte usaldamisest, võrguliikluse ja logide analüüsi olulisusest kui meeskonnatööst.

RIA panustas ka **NATO harjutuse Cyber Coalition** organiseerimisse ja osales riikide tehnikute oskusi ja infovahetust testinud õppusel ka mängijana. 2013. aastal juhiti seda 30 riigi ja 300 osalejaga üritust Tartust.

2013. aasta lõpul valmis **RIA tellitud ja Cybernetica ASi koostatud uuring krüptograafiliste algoritmide kasutusvaldkondadest ja elutsüklist**. Uuring annab teaduskirjandusele ja rahvusvahelistele raportitele tuginedes mitmeid soovitusi ja juhiseid, kuidas võimalikke krüptograafiast lähtuvaid nõrkusi ennetada nii riigiasutustes kui ka erasektoris. Uuring rõhutas, et Eestis tuleb 2–5 aasta jooksul välja vahetada mitmed krüptolahendused, mis on kasutusel näiteks mõnes pangas, m-IDs, digi-IDs, aga ka enne 2011. aastat välja antud ID-kaartides.

Olulisemad muudatused küberjulgeoleku õiguslikus raamistikus

Märtsis 2013 jäi RIA konverentsil **„Küberturvalisus – vajadus ja võimalus"** elutähtsa teenuse korraldajate ettekannest kõlama seisukoht, et suuremahuliste küberintsidentide korral tegutsemiseks ja ühiskonna huvide arvestamiseks on vaja täpsemaid riiklikke regulatsioone, mis reguleeriksid ka elutähtsat teenust korraldavaid ettevõtteid. Juba samal kuul jõustus valitsuse määrus, mis täpsustas tingimused näiteks elektrivarustuse, telefonivõrgu ja makseteenuste toimimiseks.

Küberturvalisust mõjutavatest õigusaktidest ja nende muudatustest on olulisemad järgmised:

- 2013. aastal avaldas RIA beetaversioonina uue **ISKE rakendusjuhendi ja kataloogide versiooni 7.0.** Sellesse lisandusid näiteks Windows 7 ja Mac OsXga töötavad klientsüsteemid, Open LDAP,

logimine ja veebirakendused. 2013. aastal valmis ka ISKE-rakendustööriista analüüs, mille põhjal tehakse 2014. aastal mitmeid muudatusi. 2013. aastal lisandusid ISKEsse ID-kaardi ja X-tee meetmed. Suurem ISKE auditeerimiste laine jõuab riigiasutustesse jälle 2014. ja 2015. aastal.
Riigiasutuste turvajuhtide ettepanekul viis RIA omavahel kooskõlla ISKE ja ITILi käideldavuse arvutamise põhiprintsiibid.

- 1. juulil 2014. a jõustub 2013. a **algatatud korrakaitseseaduse muutmise ja rakendamise seadus.** Vastavalt nendele muudatustele läheb Tehnilise Järelevalve Ameti järelevalvepädevus sidevõrkude ja -teenuste turvalisuse üle RIA-le. Sama eelnõuga sätestatakse RIA järelevalvepädevus ka hädaolukorra seaduses ja avaliku teabe seaduses.

- 2013. aastal koostati RIA eestvedamisel koos teiste kaasatud asutustega hädaolukorra „Ulatuslik küberintsident" riskianalüüs, kus analüüsitakse hädaolukorra tekkimise tõenäosust ja tagajärgi ning tuuakse välja abinõud hädaolukorra ennetamiseks ja tagajärgede leevendamiseks. Riskianalüüs on edasise planeerimisprotsessi ning hädaolukorra lahendamise plaani koostamise eeldus. Riikliku avaliku kokkuvõtte hädaolukorra riskianalüüsidest leiab **siit.**

- 1. jaanuaril **jõustunud määrus "Infoturbe juhtimise süsteem"** kohustab valitsusasutusi tegelema süstemaatiliselt infoturbega, sealhulgas määrama turvalisuse eest vastutavad isikud ehk infoturbejuhid. Määruse kohaselt juurutab infoturbejuht asutuses turvaintsidentide haldamise korra, teavitab ISKE nõuetest lähtuvalt RIA infoturbeintsidentide käsitlemise osakonda (CERT-EE) olulistest turvaintsidentidest ning esitab CERT-EE-le kolme kuu jooksul intsidentide koondraporti. 2013. aastal esitasid valitsusasutused RIA-le kokku 43 koondraportit.

- Märtsis kinnitas valitsus **turvalisuse nõuded elektroonilistele süsteemidele,** millest sõltub elutähtsate teenuste toimimine. Uued nõuded täpsustasid näiteks elektrivarustuse, telefonivõrgu ja makseteenuste toimimise tingimusi.

- 2013. aasta möödus mitmetele küberturvalisuse eest vastutavatele spetsialistidele riigiasutustes küberjulgeoleku strateegia uuendamise tähe all. Aruande kirjutamise hetkel on strateegia ametkondade kooskõlastusringi lõppjärgus ning jõuab avalikkuse ette hiljemalt sügisel 2014.

Globaalsed trendid

Järgnevalt on välja toodud paari suurema turvatarkvara tootja ja küberturvalisusega tegeleva rahvusvahelise organisatsiooni järeldused 2013. aasta kohta.

- **APT ehk sihitud ründeoht on endiselt oluline oht**. Selle peamised sihtmärgid on poliitikud, ettevõttete juhtkonnad ja kaitsevaldkond, märgib F-Secure. Mandianti hinnangul on samuti enim ohustatud kaitsevaldkond, aga ka lennundus, tarkvaratootmine, kõrgtehnoloogiline tootmine ja energiavaldkond. Lennundusele ja kaitsevaldkonnale on Mandianti mõõtmiste tulemusena suunatud enim (17%) kõigist sihitud rünnetest. Ligipääsu hankimiseks kasutavad ründajad järjest elegantsemaid ja tõhusamaid tööriistu, millega **rünnatavat võrku kaardistada**. APT-ründajad on visad. Isegi

kui sihtmärk kahtlase tegevuse oma süsteemidest avastab, **proovivad ründajad peagi uuesti**. ENISA märgib, et APT organiseerijad **pole enam üksikud riigid**, vaid sellega tegeleb üha enam riike. Symantec täheldab, et sihitud ründekampaaniate hulk kasvas drastiliselt: 91%. Tavapärasele taktikale lisaks on ründajajad viimastel aastatel lisanud sihtimise arsenali **kaevuründed** (ingl. k *watering hole attacks*). Kaevuründed on pahavara lisamine veebilehele, mida külastab kindel sihtgrupp (nt raamatupidajad, ülikooli õppejõud, tarkvaraarendajad). Ründaja plaan on nakatada vähemalt üks sihtgrupi liige ja jõuda tema kaudu ka teisteni.

- Kui 2011. aasta oli Symanteci hinnangul suure häktivismilaine tõttu Andmelekke Aasta, siis 2013. aastat võiks nimetada **Megalekke aastaks**. Lekkejuhtumite kasv võrreldes eelmise aastaga oli 62%. Kaheksa juhtumit olid sellised, millest igaühe tagajärjel lekkisid enam kui 10 miljoni kasutaja andmed. Kokku lekkis möödunud aastal üle 552 miljoni identiteedi, mis andsid küberkurjategijatele ligipääsu kasutajate krediitkaardiandmetele, paroolidele, telefoninumbritele, koduaadressidele jms isiklikule infole.

- Nutiseadmeturul on **populaarseim sihtmärk endiselt Androidi operatsioonisüsteem**. Pea kõik näited F-Secure'i kohatud nutipahavarast olid mõeldud Androidile. Enim raporteeritakse Androidi pahavara Saudi Araabias ja Indias. (Probleem peitub endiselt kolmandate osapoolte rakenduste levitamise lehtedes („poed"). Symanteci mõõtmise tulemusena on 38% mobiilikasutajatest nutiseadme pahavaraga kokku puutunud. TrendMicro hinnangul on maalimas üle 1,4 miljoni potentsiaalselt pahatahtliku Androidi-rakenduse.

- **Bitcoini tehnoloogia**, levik ja Bitcoini kaevandamiseks eraldatud ressursid. 2013. aasta alguses maksis 1 bitcoin 7 USA dollarit, sügisel juba 130 dollarit. F-Secure'i teeb murelikuks asjaolu, et virtuaalraha on võimalik kuritegelikel eesmärkidel kaevandada ka nakatatud võõraste arvutitega, st botnettidega. Maailma suuruselt teine botnet teenib F-Secure'i arvates päevas umbes 50 000 dollarit.

- Bitimüntide tuules sõidab ka ohtlik väljapressimistarkvara **Cryptolocker** – pahavara, mis krüptib kasutaja andmed ning nõuab lahti saamiseks lunaraha bitimüntides. Pole teada muud ravi peale Cryptolockerile ligipääsmatute varukoopiate. Esimesed teated Cryptolockeri juhtumitest Eestis jõudsid RIAni 2014. a jaanuaris. Symanteci hinnangul kasvasid väljapressimisründed 2013. aastal 500%.

- **Edward Snowdeni** paljastustele ulatuslikest USA valitsuse jälgimisprogrammidest turvatarkvara tootjad oma aastakokkuvõtetes eriti mahtu ei pühenda. F-Secure toob välja, et paljastused tõid kaasa surve mitmele veebiettevõttele, mil määral ja millistel tingimustel valitsusasutustega koostööd tehakse. Koostöö kohta küsitakse ka viirustõrjetootjatelt: kas ja millal jätavad nad valitsusasutuste toodetud pahavara tähelepanuta. F-Secure'i (avalik) positsioon on kindel: valitsusasutustega ei ole pahavara tuvastamata jätmiseks koostööd tehtud ega plaanita seda teha ka tulevikus.

- Ummistusründed on endiselt populaarsed. Suure ummistusrünnete-vastaseid turvalahendusi pakkuva ettevõtte Prolexicu hinnangul kasvasid ummistusründed 2013. aastal 47%. Keskmise ründe andmemaht kasvas samal ajal 9%. Ummistusrünnete kestus langes aga 2013. a 35 tunnilt 17-le.

Soovitused ja sissevaade 2014. aastasse

Aastast aastasse on RIA igapäevamure suur näotustamiste hulk Eesti küberruumis. Lõviosa nendest juhtudest tuleneb kodulehe uuendamata tarkvarast. Soovitame tungivalt igal kodulehe omanikul, eriti neil, kes kasutavad Wordpressi ja Joomla sisuhaldustarkvara, veenduda selles, et koduleht töötab uusimal tarkvaral. Näotustamised pole ainult piinlikud, vaid toovad tõsisematel juhtudel kaasa ka veebilehele istutatud pahavara ja külastajate arvutite nakatumise.

Soovitame kõigil IT-juhtidel ja turvajuhtidel nii riigis kui erasektoris tutvuda aasta alguses RIA kodulehele jõudnud krüptouuringuga ja vaadata selle valguses üle oma asutuses või ettevõttes kasutatavad krüptoalgoritmid.

RIA on 2014. aastal jätkanud nii õppuste, koolituste kui turvatestimistega. Tulenevalt Euroopa eelarveperioodi lõppemisest on koolitusi kavas mõnevõrra vähem kui eelmisel aastal: umbes 10 koolitust 350 inimesele. 2014. aastal toimub lisaks traditsioonilistele rahvusvahelistele õppustele Locked Shields ja NATO Cyber Coalition ka Euroopa Liidu võrgu- ja infoturbeameti (ENISA) Cyber Coalition.

Aasta alguses käivitas Eesti Interneti Sihtasutus (EIS) koos akrediteeritud registripidajatega Eesti rahvusliku internetidomeeni .ee jaoks **DNSSEC-teenuse.** RIA ja EISi koostöös alustati EL sf programmist „Infoühiskonna teadlikkuse tõstmine" domeeniomanike teavitamist. Lihtsaim võimalus oma domeeni DNSSEC-turvalaiendusega kaitsta, on kasutada selleks oma registripidaja või nimeserveri teenuse pakkuja abi. Ülevaate, missugused registripidajad DNSSECi teenust oma klientidele pakuvad, leiab internet.ee avalehelt .ee akrediteeritud registripidajate võrdlustabelist.

Pärast Windows XP toeperioodi lõppemist hoiab RIA endiselt tähelepanu uuendamata arvutitest tulenevatel riskidel. Aprillis 2014 oli riigivõrgus internetis käivatest arvutitest kümnendik selliseid, mis kasutasid XP operatsioonisüsteemi, riigiportaali eesti.ee külastajatest kasutasid seda aegunud süsteemi 15%. Aasta teises pooles viib RIA läbi veel ühe tarkvara uuendamisvajadust ja tasuta alternatiive selgitava kampaania.

Kevadel 2014 valmis RIA tellimusel **andmekeskuse turvanõuete juhend**. See on mõeldud eelkõige kõrgete käideldavusnõuetega riiklike ning elutähtsa teenuse osutajate andmekogusid majutavate serveriruumide ja andmekeskuste planeerimise, ehitamise ja hooldamise juhisena.

Eestis nagu mujal maailmaski jätkub nutiseadmete levik ja sellega kaasnev elu-olu reaalajas dokumenteerimine ja andmemahtude kasv. Võrgus liigub üha rohkem andmeid, mis tähendab, et üha enam on teemasid, mille terviklus, käideldavus ja konfidentsiaalsus on tarbijatele rohkem või vähem oluline. Aasta lõpus valmib NutiKaitse initsiatiivis RIA tellitud põhjalik uuring kasutajate turvakäitumise kohta nutiseadmete kasutamisel.

Elektroonilise identiteedi turvalisuse eest hoolitsemiseks loodame 2014. aastal astuda olulise ja kauaoodatud sammu ning alustada ID-baastarkvara avaliku veahaldusega. RIAst saab ka m-ID tehno-

loogiliste lahenduste verifitseerija. Jätkub üleminek uuele digiallkirja formaadile .bdoc, mis toob kaasa nii teiste Euroopa (tuleviku) digiallkirjadega ühildumise kui tugevama krüptograafiaga kaitstud digiallkirjad.

Mõisteid

Seletused on pärit RIA kodulehelt ning **andmekaitse ja infoturbe seletussõnastikust**.

ISKE ehk infosüsteemide kolmeastmeline etalonturbe süsteem on turvastandard, mida rakendatakse eelkõige valitsusasutuste ja kohalike omavalitsuste süsteemide ja nendega seotud infovarade kaitseks.

Hajus ummistusrünne (DDoS = *distributed denial of service*) on ummistusrünne, milles kasutatakse sihtsüsteemi või -võrgu liikluse mahu tunduvaks suurendamiseks suurt arvu ründavaid süsteeme, eriti zombivõrke.

Kaevurünne on sihtkoha (või sihtrühma) nakatamine kahjurvaraga sellise veebisaidi kaudu, mida ohver eelluure andmetel (või tõenäoliselt) tihti külastab – nagu loom joogikohta või inimene kaevu; üksikasju vt näiteks http://blogs.cisco.com/security/watering-hole-attacks-an-attractive-alternative-to-spear-phishing ja http://about-threats.trendmicro.com/dumpImages/132201375838.jpeg.

APT e sihtründeoht võimaliku peamiselt mingi välisriigi poliitilistest, majanduslikest või sõjalistest huvidest lähtuva, ettemääratud eesmärgi saavutamisele suunatud sihikindla kohanduva ulatuslike ressursside ja erioskustega kestusründe oht. Vt ka: http://www.arvutikaitse.ee/apt-jouliselt-eba-maarane-kuber-oht/.

Globaalsete trendide kokkuvõtte aluseks olnud allikad

Symantec. (2. April 2014). *Endpoint, Cloud, Mobile; Virtual Security Solutions | Symantec*. Kasutamise kuupäev: 31. mai 2014, allikas b-istr_main_report_v19_21291018.en-us.pdf: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

F-Secure. (kuupäev puudub). Kasutamise kuupäev: 31. mai 2014, allikas F-Secure H1 Threat Report: http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H1_2013.pdf

Mandiant. (kuupäev puudub). Kasutamise kuupäev: 31. mai 2014, allikas M-Trends® 2013: Attack the Security Gap™: https://www.mandiant.com/resources/mandiant-reports/

ENISA. (December 2013. a.). Kasutamise kuupäev: 31. mai 2014, allikas ENISA Threat Landscape 2013 – Overview of current and emerging cyber-threats: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

TrendMicro. (2014). Kasutamise kuupäev: 31. mai 2014, allikas Trend Labs SM 2013 Annual Security Roundup: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cashing-in-on-digital-information.pdf