Riigi Infosüsteemi Amet



RIA küberturvalisuse teenistuse

2014. aasta kokkuvõte

Sisukord

Vaja pole mitte ainult plaan B-d, vaid ka C-d 4
Olulised trendid Eesti küberturvalisuses 2014 6
2014. a intsidendid 7
- Ründed 8
- Pahavara 8
- Turvavead tarkvaratoodetes 9
- Mobiilivõrk, mobiilsed seadmed ja „asjade internet“ 11
- Õngitsuskampaaniad 11
- RIA-le raporteeritud intsidendid 12
  - Intsidentide hulk ja sagedus 13
  - Intsidentide tüüp (käideldavus, konfidentsiaalsus, terviklus) 14
  - Intsidentide mõju 15
  - Intsidentide kriitilisus 16
  - Intsidentide põhjus 17

Uuringud ja juhendid 18
- IT-riskide tunnetus riigiasutustes ja ETOdes 18
- Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring 19
- Krüptograafiliste algoritmide elutsükli uuring 19
- Andmekeskuste turvanõuete juhend 19

Küberohtude ennetamine 20
- Küberkirjutised 20
- Koolitused 20
- Õppused 20
- Infoturbejuhtide komisjon 21
- DNSSEC 21
- Riskianalüüsi metoodika 21
- Elanikkonna küberjulgeolekualane teadlikkus 22

Rahvusvaheline koostöö 2014 22
Olulisemad arengud küberjulgeoleku õiguslikus ja strateegilises raamistikus 23
- RIA uued pädevused ja kohustused 23
- Küberjulgeoleku strateegia 2014–2017 23
- Ulatuslikeks küberintsidentideks valmistumine 24
- ISKE 24

Kokkuvõte 25
Soovitusi lisalugemiseks 27

2014. aasta
Eesti küberturvalisuses

Eestis tervikuna:



1151 käsitletud juhtumit
(**1164** aastal 2013)

22 teenusetõkestusrünnet
(**13** aastal 2013)

295 näotustamisjuhtumit
(**240** aastal 2013)

127 koond- ja intsidendiraportit esitati RIA-le
(**73** aastal 2013)

Riigiasutustes:

486 intsidenti riigiasutustes
(**135** aastal 2013)

Levinuimad intsidentide põhjused:

- rünne
- elektrikatkestus
- andmesidekatkestus
- tarkvaraviga



20% raporteeritud intsidentidest olid kõrge kriitilisusega

Ohtlikud haavatavused:
Heartbleed ja Shellshock

23 küberturvalisuse koolitust,
osalejate koguarv oli **744**

Rahvusvahelised küberõppused:
Cyber Europe, Cyber Coalition ja Locked Shields

60% Eesti inimestest kasutab nutiseadmeid.
75% lastest ütleb: "Vanemad ei tunne huvi, millega nutiseadmes tegelen."

Vaja pole mitte ainult plaan B-d, vaid ka C-d

> *Tragöödia olemus on see, et maailm pole meeldiv väike pesa, mis on tehtud meie kaitsmiseks, vaid tohutu ja suuresti vaenulik keskkond, kus võime saavutada suuri asju ainult jumalaid trotsides ja see trots toob vältimatult kaasa karistuse.*
>
> Norbert Wiener,
> The Human Use of Human Beings: Cybernetics and Society (1950)

Kui kaasaegse küberneetika isaks kutsutud Norbert Wiener 1950. aastal oma tõdemuse maailmast kui ebaturvalisest paigast kirja pani, oli ta usutavasti rohkem mõjutatud äsja lõppenud Maailmasõjast kui nägemusest tuleviku digitaalse ühiskonna ohtudest. Täna, rohkem kui pool sajandit hiljem, kätkeb meid ümbritsev maailm, sh ka küberkeskkond, endas hulka ohtusid ja riske. Võimekus nendega toime tulla sõltub aga endiselt peamiselt meist endist – võimest ohtusid näha ja valmisolekust nendega toime tulla.

Eesti võimekust küberohtudega toime tulla võib pidada rahuldavaks. Rahvusvahelise Telekommunikatsiooni Liidu (ITU) poolt 2014. aastal avaldatud uuring asetab meid kübervõimekuselt maailmas auväärsele 5. kohale ning Euroopas asetatakse meid lausa teisele kohale. Eesti ühiskond usaldab oma e-riiki: äsja lõppenud e-valimised lõid järjekordse rekordi, kus oma hääle andis elektrooniliselt 176 491 valijat. Kõrge usaldus seab ka järjest kõrgemad ootused turvalisuse tagamisele ja võimekusele intsidentide ja kriisidega toime tulla.

2014. aasta tõi meile kaasa palju uusi väljakutseid. Tuntavalt halvenes julgeolekukeskkond – tegutseme Euroopas, kus peetakse sõda. Halvenenud julgeolekuolukord kajastus ka intsidendistatistikas – märgatavalt on suurenenud välisriikide eriteenistuste tegevusega seotud juhtumite arv. Aasta jooksul esines mitmeid Eesti e-teenuste piire katsetavaid teenusetõkestusründeid. Mitmete kriitiliste katkestuste tõttu sai ilmeka tõestuse fakt, et Eesti riigivõrgust ja riigiasutuste vahelistest andmesidest sõltub täna Eesti riigi toimimine, sealhulgas välispiiri valve ja sisejulgeoleku toimimine.

Rahvusvahelises mõõtmes mõjutab küberturvalisuse valdkonda endiselt ka 2013. aasta PRISMi skandaal, mistõttu on avalikkuse huvi julgeolekuvaldkonna tegevuste vastu suur.

Avaldati mitmed suure mõjuga vead krüptograafiliste algoritmide teostustes (nt OpenSSLi vead). Tõhusama arvutusvõimsuse tõttu odavnes ka nõrgemate krüptograafiliste algoritmide (DES ja RSA1024) murdmine. Selliste vigade kuritarvitamise tuvastamine võib aga olla keeruline või ka võimatu. Sealjuures said haavatavused meedias suurt tähelepanu nädalaid, enne kui tootjad neile paigad suutsid luua. Samal ajal levisid veebis lihtsad ründejuhised, mille abil haavatavusi ära kasutada ja süsteemidele kahju teha. Eriti murettekitav oli see näiteks nn *Heartbleed*'i juhtumi puhul, mil ründe hilisem tuvastamine ja tõestamine on väga komplitseeritud. Pole põhjust arvata, et olukord järgmistel aastatel muutuks, näiteks kohe 2015. aasta algul leidis tehnoloogiameedias palju kajas-

tamist Linuxi kriitiline haavatavus *Ghost*.

Nii ID-kaart kui ka muu oluline e-Eesti taristu põhineb krüptograafial. Krüptoalgoritmide turvalisuse „eluiga" on aga järjest vähenenud, mis tähendab, et tegutsemisaeg enne krüptoalogritmide murdumist on veelgi piiratum. Lähiaastatel tuleb Eestis seetõttu krüptograafia arendamisele varasemast hoopis rohkem tähelepanu pöörata, tagamaks e-riigi baastaristu turvalist toimimist.

Tehtud uuringud ja riskianalüüsid annavad küll tunnistust, et Eesti inimeste ja asutuste riskiteadlikkus on suhteliselt suur, kuid esineb ka probleeme. Näiteks on kriitilise taristu toimepidevuse tagamiseks kindlasti vajalik taristu ettevõtete arusaam mitte ainult sellest, kellest nemad sõltuvad, vaid ka sellest, kelle teenused sõltuvad neist. Lihtne on tõdeda, et ilma elektrivarustuseta teenus katkeb, kuid kas mõtleme ka selle peale, et võib-olla sõltub elektrivarustuse tagamine omakorda telekommunikatsiooniteenuste toimimisest?

2014. aastal koondas RIA oma küberturvalisuse tagamisega seotud funktsioonid küberturvalisuse teenistusse. Intsidentide käsitlemine, riskide hindamine ja regulatsioonide järelevalve ning uurimis- ja arendustegevus on nüüd selgemalt määratletud, mis võimaldab ka ressursse tõhusamalt kasutada. Oleme saanud panustada oma töökeskkonna turvalisuse tõstmisesse ning erialase kompetentsi kasvule. Rahvusvahelises koostöös on meil võimalus järjest rohkem panustada ka teiste riikide kübervõimekuse tõstmisele – saame tõsta nii Eesti rahvusvahelist tuntust, kui suurendada ka küberturvalisust üldiselt. Küberkeskkond on globaalne ning ohtudega hakkamasaamine sõltub kõigi riikide panusest.

Järgnevatel aastatel on RIA jaoks väga prioriteetsed need valdkonnad, kus toimuvatel intsidentidel on vahetu mõju inimeste elule ja tervisele või ühiskonnale tervikuna. Arengud meditsiinitehnoloogias, asjade internet ja uued väljakutsed Eesti riigi julgeoleku tagamisel on vaid mõned näited valdkondadest, mis vajavad lähiajal palju rohkem tähelepanu.

Ulatuslikku küberintsidenti ja selle täielikku mõju on raske ennustada või ära hoida. Põhiline, millega nii organisatsioonid, riik kui ka iga inimene saavad oma küberturvalisuse taset tõsta, on oskuste ja teadmiste suurendamine ohtude äratundmiseks ja toimivate varuplaanide olemasolu puhuks, kui midagi juhtub. Intsidendi mõjude leevendamiseks pole vaja ainult plaan B-d, vaid ka plaan C-d.

Toomas Vaks
RIA peadirektori asetäitja küberturvalisuse alal

Olulised trendid Eesti küberturvalisuses 2014

2014. aasta juhtumeid iseloomustavad märksõnad on:

- Suure mõjuga vead krüptograafiliste algoritmide teostustes (nt OpenSSLi vead). Tõhusama arvutusvõimsuse tõttu odavnes ka nõrgemate krüptograafiliste algoritmide (DES ja RSA1024) murdmine. Selliste vigade kuritarvitamise tuvastamine võib aga olla keeruline või ka võimatu.

- Palju avastatud vigu üldkasutatavates tarkvaratoodetes (näiteks Wordpress, Joomla, Drupal, Saurus).

- IT-ressursside hoolduskohustuse ignoreerimine. Kahte esimest probleemi võimendab tugevalt see, et mitmed organisatsioonid ei reageeri turvavigadele mõistliku aja jooksul. Selline reageerimislünk pole oht mitte ainult veebirakendustele, vaid kõikidele infosüsteemidele, sh internetti ühendatud automaatjuhtimissüsteemidele, mis reguleerivad näiteks vee, elektri ja kütte toimimist.

- Pidev ja nutikas pahavara levitamine nii e-kirjade kui veebilehtede kaudu, sealjuures tuvastavad traditsioonilised tõrjevahendid pahavara halvasti. E-postiga leviv pahavara on järjest nutikamalt koostatud. Ühe organisatsiooni töötajad võivad saada küll sama sisuga kirju, ent kirjaga kaasnev pahavara on igaühel pisut erinev. Esialgu ei pruugi ükski viirusetõrje tabada, et tegu on millegi kahtlasega. Lisaks on keerulisem pahavara sageli konstrueeritud nii, et suudab mõista, kui teda lihtsamate vahenditega analüüsida üritatakse ja näiteks virtuaalmasinas käivitatakse. Sellisel juhul käitub pahavara hoopis teisiti ja ohutumalt kui ohvri arvutis.

- Oskuslik pilveteenuste kontode (nt Gmail, Hotmail) andmepüük, mis on jätkunud seninägematu hooga ka 2015. aasta algul. E-kirjad saabuvad sageli justkui usaldusväärsest allikast ja on nii sisult kui keeleliselt teinud kvaliteedihüppe, mis tähendab, et meilisaaja peab pettuse märkamiseks rakendama senisest veelgi teravamat tähelepanu ja kriitilist meelt.

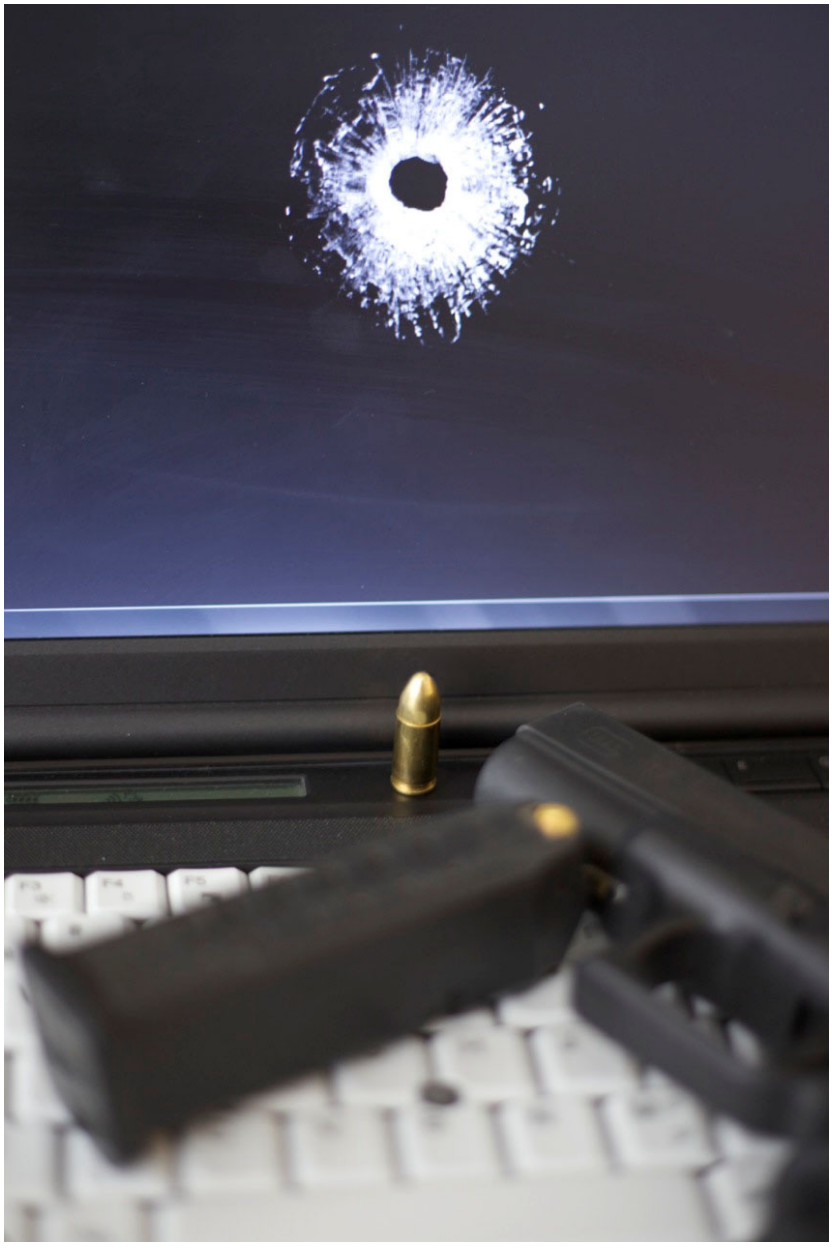
- Suuremahulised (nii kanali mahtude kui ründes kasutatavate nakatunud arvutite hulga osas) ja mitmelõimelised teenusetõkestusründed. St esmalt kasutab ründaja ühte meetodit, mille interneti teenusepakkuja blokeerib. Seejärel läheb ründaja üle uuele meetodile. See tähendab korduvat ja aktiivset lisatööd liikluse seadistamisel nii interneti teenusepakkujale kui ka kasutajale, olenevalt sellest, kus ründeid tõrjuvaid reegleid rakendatakse.

- Veebilehtedele sissemurdmist on raskem tuvastada. Sagenenud on trend, kus veebilehe nakataja hoiab pahavara üleval väga lühikest aega ja arvestab, milliselt IP-aadressilt lehte külastatakse. Näiteks kui kasutaja külastab veebilehte Eestist, serveeritakse talle ühte, kui Ameerikast, siis teistsugust pahavara.

2014. a intsidendid

Intsidentide mõju on võrreldes varasemaga üha tõsisem, ehkki 2014. aasta ei erine numbritelt väga palju 2013. aastast. CERTi käsitletud juhtumite kogusumma on ligikaudu sama (1151 käsitletud juhtumit 2014; 1164 juhtumit 2013). Ka eri tüüpi juhtumite (näiteks näotustamised, nakatamised, andmepüük) osakaalud on sarnased. Juhtumite iseloomu hinnates selgub, et rohkem on targalt ja täpselt sihitud ründeid, mille eesmärk näib olevat riigi teenuseid ja/või mainet kahjustada.

Suurim muutus RIA kogutavas intsidendistatistikas on toimunud riigiasutuste poolt raporteeritavate juhtumite arvus, mis on märkimisväärselt kasvanud. Kui 2013. aastal raporteerisid riigiasutused RIA-le 135 intsidenti, siis 2014. aastal juba 486 intsidenti, seega ligi neli korda rohkem (vt põhjalikumat ülevaadet raporteeritud intsidentidest peatükis “RIA-le raporteeritud intsidendid riigiasutustes”).



Ründed

Viimastel aastatel on järk-järgult kasvanud nii rünnete tehniline mitmekülgsus kui ka suured mahud. Samas suureneb ka Eesti ühiskonna igapäevane sõltuvus e-teenustest ja andmesidest, seega on ka tavapärasemate tehniliste rikete mõju enam tuntav.

Kui mõned aastad tagasi puutusid teenusetõkestusrünnetega Eestis kokku peamiselt riigiasutused või finantssektoris opereerivad ettevõtted, siis praeguseks hetkeks on olukord muutunud ning teenusetõkestusründed on muutunud igapäevaseks nähtuseks ka teistes tegevusvaldkondades. Märkimist väärivad e-Kooli teenuse vastu suunatud ründed, mis on aegamööda muutunud kooliõpilaste katsetustest suuremahuliseks ja kestvaks probleemiks.

Lühiajalistest rünnetest ja ründekatsetest ei pääsenud ka traditsioonilised nn ikoon-veebilehed: riigiportaal, EV Presidendi, Välisministeeriumi ja NATO küberkaitse keskuse veebileht. Institutsioonide tööle sellised intsidendid erilist mõju ei avalda, küll aga tekitavad mainekahju ja ärevust avalikkuses.

Märgatavalt on tõusnud interneti teenusepakkujate võimekus kaitsemeetmeid rakendada ja teenusetõkestusründeid tõrjuda. Seetõttu on mitmeid juhuseid, kus ründaja eesmärgini ei jõua.

2014. aastal teravnes, tulenevalt tõsiste intsidentide sagenemisest, vajadus riigivõrgu täiendava kaitse järele ning lähiajal on RIA rajamas ööpäevaringset mehitatud turvaseiret, mis tagab esmase reageerimise CERTi haldusalas toimunud intsidentidele ka töövälisel ajal.

Pahavara

Jaanuaris jõudsid CERTini esimesed teated lunavara levikust Eestis. Õnneks oli *Cryptolocker* (pahavara, mis nõuab krüpteeritud andmetele ligipääsu eest lunaraha), erinevalt Euroopa teistest riikidest, Eestis üsna tagasihoidliku levikuga. Ettevaatust tuleb siiski säilitada – aasta hiljem on CERTi teavitatud paarist juhtumit, kus *Cryptolocker*'i ohvriks pole langenud mitte üksikud kasutajad, vaid ka organisatsiooni võrgukettad, millel mitmete kasutajate failid. Otsest ohtu kujutab *Cryptolocker*'i tüüpi pahavara valdkondades, millede puhul võib infole ligipääsu tõkestamine või info hävitamine muutuda otseseks ohuks inimese elule ja tervisele, näiteks meditsiiniasutused ja meditsiinitehnika, häirekeskused, lennujuhtimiskeskus jms. Et pahavara levitajad ja heausklikud kasutajad on turvatiimidest sageli sammu võrra ees, pole nakatumist alati võimalik ära hoida ja valmis tuleb olla tagajärgedeks. Need on leebemad, kui organisatsioonis on korralikult paika pandud kasutajate õigused – iga kasutaja (ja tema nakatunud arvuti) ei peaks tingimata ligi saama kõikidele võrguketastele ja sealsetele failidele. Samuti tuleb *Cryptolocker*'i vaimus vaadata üle asutuse varundus-poliitika ja hoolitseda selle eest, et kui juba kord krüpteeriva pahavaraga pihta saadakse, siis oleks võimalik olukorda päästa ja andmeid taastada.

Käsitletud pahavarajuhtumitest väärivad märkimist nakatumised, mis leidsid aset Elroni veebilehe vahendusel. Olulist transporditeenust osutava ettevõtte veebilehele murti sisse ning kasutati seda korduvalt ära pahavara levitamisel. See tõestab ilmekalt vajadust teadvustada infoturbe teemasid

mitte ainult IT-osakonna tasemel, vaid organisatsioonides ja ühiskonnas laiemalt, tõsisemalt ja pidevamalt.

Arvestades, et Elron oli 2014. aastal otsituim eestikeelne sõna Google'is, oli sel juhtumil kahtlemata ulatuslik mõju.

Turvavead tarkvaratoodetes

Juba mitmeid aastaid teeb RIA-le muret olukord, kus ettevõte, MTÜ või ka eraisik valib teenuse osutamiseks tasuta kättesaadava tarkvara ning pärast teenuse tööle hakkamist loobutakse igasugusest hooldusest ja turvauuenduste paigaldamisest.

RIA statistika näitab, et Eesti interneti (.ee) nimeruumis on enimlevinud sisuhaldustarkvara Wordpress (26,2% .ee domeenis päringule vastanud kõikidest saitidest), sellele järgnevad Joomla (7,1%), Drupal (2,6%) ja viimaks kodumaine Saurus (1,2%). Mida enam kasutajaid, seda suurem ründajate huvi. Küllaltki sageli ilmuvate sisuhaldustarkvara kriitiliste vigade puhul peaks veebilehe haldaja kohe reageerima ja tarkvara uuendama. Reaalsuses on veebilehe püsti pannud IT-spetsialist aga palgatud või palutud vaid veebilehte üles seadma. See, mis hiljem saab, pole enam justkui haldaja ega veebilehe omaniku mure ning peamine meetod nakatunud veebilehe kahjutuks tegemiseks on CERTil suhelda majutusteenuse pakkujaga.

2015. aastal teeb RIA-le erilist muret Sauruse sisuhaldustarkvara toe lõppemine. Realistlik-pessimistlik prognoos ütleb, et paljud Sauruse saidid jäävad internetti ka pärast toe lõppu, mis tähendab turvavigade ilmnemise korral ründajatele magusaid võimalusi veebilehtede näotustamiseks ja pahavaraga nakatamiseks. Riigivõrgus ASO on 16 domeeni, mille sisuhaldustarkvarana kasutatakse Saurust, nende hulgas ka RIA enda koduleht.

2014. aastal ilmnenud tarkvaravigade juures on tähelepanuväärne nende kommunikatsioonipool. Kaks markantsemat juhtumit, nii vabavaralise tarkvara OpenSSL haavatavus *Heartbleed* kui ka Unixiga hallatavaid süsteeme ohustav *Shellshock* said avastajatelt endale kõlava nime ja kireva logo, mis lasi probleeme publitseerida jõuliselt ka massimeedias. Nende hästi bränditud vigade puhul jõudsid meediasse ulatuslikult ja detailselt nii vea iseloom kui ründamisjuhised. Seda päevi ja isegi nädalaid enne, kui neid komponente kasutavad tarkvaratootjad suutsid välja töötada vajalikud paigad.

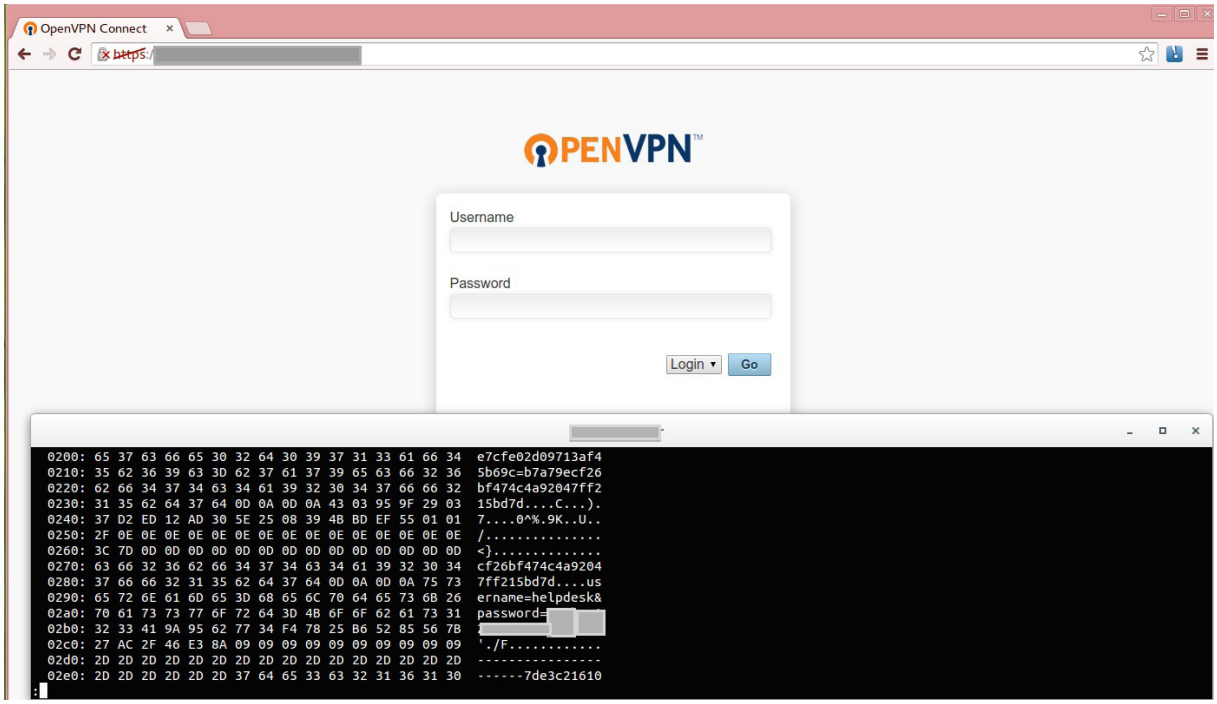
Heartbleed

7. aprillil teavitasid Soome ja Google'i turvaeksperdid OpenSSLi turvanõrkusest. Avastajad panid haavatavusele nimeks *Heartbleed*. *Heartbleed* on tõsine haavatavus vabavaralises tarkvaras OpenSSL, mida kasutatakse laialdaselt: näiteks veebiliikluse krüpteerimisel, e-posti lahendustes, turvalise kaugligipääsu tagamiseks ja vestlusprogrammides. Riigivõrgus ASO tuvastas RIA sadakond haavatavat serverit ja teavitas nende haldajaid paikamisvajadusest. Riigivõrgus said serverid paigatud mõne päevaga. Ühtekokku puudutas viga Eestis hinnanguliselt 5% serveritest.

Heartbleed'i muutis lisaks laiale levikule tõsiseks asjaolu, et vea ärakasutamisest ei jää jälge tee-

nust osutava serveri logidesse. Seega pole logide põhjal võimalik tagantjärele tuvastada, kas, millal ja kui palju on OpenSSLi kasutavates paikamata serverites andmete konfidentsiaalsust ja/või terviklust rikutud.

Kuigi riigivõrgus olevad seadmed said tänu intensiivsele teavituskampaaniale kiiresti paigatud, leidub ikka ja jälle mõni asutus, kes ühendab võrku uue seadme, kus see haavatavus on paikamata. Näiteks tuvastas RIA veel 9 kuud pärast haavatavuse ilmnemist riigivõrgust ASO ühe värskelt lisandunud VPNi teenuse, mille administraatori kasutajanimi ja parool oli *Heartbleed*'i haavatavuse abil hõlpsasti leitav.



XP toe lõpp

Tarkvaratootja Microsoft lõpetas 2014. aasta aprillis Windows XP operatsioonisüsteemi tehnilise toetamise. See tähendab, et selles Windowsi versioonis ilmnevaid turvanõrkusi enam ei parandata. Windows XPga arvuti võib küll töötada tõrgeteta, kuid on turvaohtude suhtes oluliselt haavatavam. Sellise aegunud tarkvara puhul on murettekitav tavakasutajate hulk, ent veelgi kriitilisem nõrkus on see, et vananenud tarkvara võib leiduda laialdaselt ka olulistes asutustes ja ettevõtetes, näiteks meditsiinivaldkonnas.

RIA alustas avalikkuse teavitamist aegunud tarkvarariskidest juba 2013. aasta kevadel, mil Windows XP kasutajaid oli Eestis hinnanguliselt viiendik. Kampaania käigus andsid mitmed suure külastatavusega veebilehed aegunud operatsioonisüsteemi kasutajale teada, et nende arvutis tuleks tarkvara uuendada. 2014. aasta novembris oli riigiportaali eesti.ee XP operatsioonisüsteemiga kasutajate osakaal langenud 10,4%-ni.

Mobiilivõrk, mobiilsed seadmed ja „asjade internet“

Mobiilivõrkude puhul on maailmas oluliseks trendiks muutunud mobiilsete tugijaamade kättesaadavus. Lisaks tavalistele tehnikahuvilistele tavakodanikele võivad need seega sattuda ka pahatahtlike kavatsustega tegutsejate kätte nagu juhtus Norras 2014. aasta lõpus[1]. Kuigi libatugijaamu puudutavaid juhtumeid ei ole RIA-le raporteeritud, peame sellisteks ohtudeks siiski valmis olema.

Asjade internetiga seonduvate juhtumite käsitlemises on levinuim probleem vaikeparoolide muutmata jätmine. Näiteks oktoobris said ka Eesti meedias palju tähelepanu internetti ühendatud turvakaamerad, mille kasutajanime ja parooli on omanik jätnud kaamerat karbist võttes samaks. Sellise seadme edastatav pilt on internetis kõigile nähtav. Teine probleem on see, et seadmete tarkvara reeglina ei uuendata või puudub tootjapoolne huvi tarkvarauuendusi luua ja levitada. Olukorras, kus järjest rohkem kodusid ühendab oma seadmeid energiasäästu ja nutikuse nimel võrku, tähendavad sellised haavatavused potentsiaalsele ründajatele lihtsaid võimalusi seadmete kuritarvitamiseks.

Õngitsuskampaaniad

2014. aastal tegid Eestis ringlevad õngitsuskirjad kvaliteedihüppe. Kampaaniad sihiti nii riigiasutuste töötajatele, raamatupidajatele, ülikoolitöötajatele, üliõpilastele kui välisteenistujatele. Sealjuures torkas näiteks riigiasutuste puhul silma trend, kus kirja ei saadeta kõikidele veebis leiduvatele kontaktidele, vaid on hoolikalt välja otsitud kontaktid, kellele selle konkreetse võltskirja sisu võiks korda minna – näiteks juhtkond või raamatupidajad.

Politsei sai, nagu 2013. aastalgi, teateid end Microsofti või Windowsi töötajana esitlevatest kelmidest, kes teatasid telefonitsi, et inimese arvutis on viirus. Viiruse kõrvaldamiseks paluti inimesel edastada enda internetipanga paroolid või siseneda internetipanka.

Suvel jõudsid ka Eestisse kogu maailmas levinud õngitsuskirjad, mis pärinesid justkui Apple'ilt ja hoiatasid sealse kasutajanime ja parooli aegumise eest. Kasutajatel paluti sisestada oma kasutajanimi ja parool veebilehel, mis oli äravahetamiseni sarnane Apple'i enda teenusega. Ohvrite kontod lukustati ja nõuti avamise eest lunaraha.

Vaid veidi hiljem jõudsid paljude kohalike omavalitsuste töötajateni heas eesti keeles e-kirjad organisatsioonilt, mis esines Euroopa kohalike valitsusametnike, Euroopa Parlamendi liikmete, Euroopa Komisjoni liikmete ja riikide valitsuste ministrite andmebaasina ELGO (*European Local Government Officers Database*). Kiri kutsus üles andmebaasis enda, kolleegide ja asutuse kontakte uuendama ja parandama sinna omavalitsuste teadmata sisestatud andmeid. Lisaks pakuti võimalust lisada andmebaasi Eesti omavalitsuste ametnikke. Selle tarvis oli kirjas toodud ka andmebaasi sisenemiseks vajalik kasutajanimi ja parool. Euroopa Liidu CERTi (EU-CERT) hinnangul ei ole ELGO seotud ühegi Euroopa institutsiooniga ning ilmselt on tegu eraettevõttega, kes üritab endast usutava Euroopa institutsiooni

[1] Vt Aftenposteni uudist Norra parlamendis avastatud mobiilside libatugijaamadest (inglise keeles) http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html

muljet jätta. Ei saa välistada, et kampaania on osa keerukamast kuritegelikust ründest – hiljem aitab andmestiku kasutamine konfidentsiaalsemate andmete saamiseks usaldusväärsemana näida. Samuti pole üllatav, kui ühel hetkel saabub andmebaasi kasutajatele kasutatud teenuse eest arve.

```
Näide kirja sisust:

Lugupeetud XXX (saaja nimi)

Käesolevaga saadame teile Euroopa kohalike valitsusametnike, Euroopa Parlamendi
liikmete, Euroopa Komisjoni liikmete ja riikide valitsuste ministrite andmebaasi
kasutajanime ja parooli. Sisselogimisandmetega pääsete juurde rohkem kui 220 000
kontaktile kõigis Euroopa kohalike omavalitsuste valdkondades.

Kui leiate oma asutuse piires vigu, võite enda, oma kolleegi või asutuse andmeid
julgelt parandada. Kui soovite mõne kolleegi andmebaasi lisada, saatke meile
kontaktivormi kaudu e-kiri. Seejärel saame saata neile kasutajanime ja parooli,
mis võimaldavad andmebaasile juurde pääseda.

Username XXX (meiliaadress)
Password

hXXps://www.elgo.

Lugupidamisega
Marcin Bialas
andmebaasi haldur

ELGO
119 Altenburg Gardens
London
SW11 1JQ
```

Aasta kulmineerus Gmaili kontode kaaperdamise kampaaniaga, mille raames ringlesid usaldusväärselt saatjalt pärinevad peaaegu veatus eesti keeles e-kirjad, mis kutsusid üles hätta sattunud kontaktile raha üle kandma. Automaatsed tõlkeprogrammid nii korrektset eesti keelt ei tooda, seega on mängus tõlkijate käsi. Täpsemad asjaolud on uurimisasutustes välja selgitamisel.

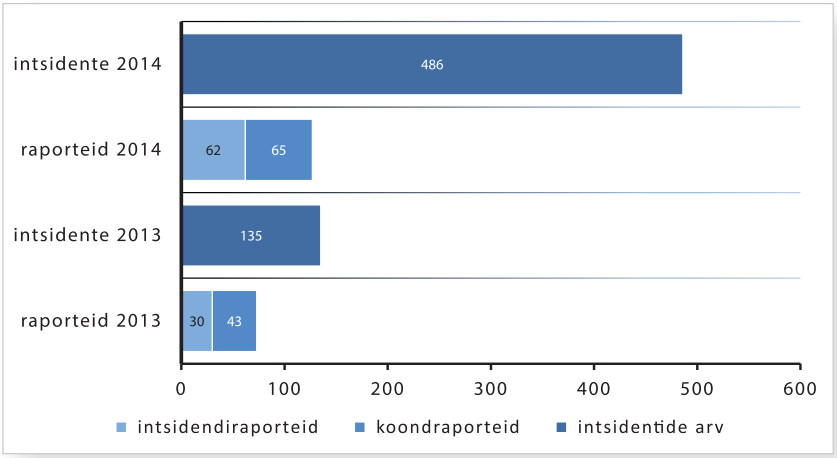
Kokkuvõttes tähendab õngitsuskampaaniate kvaliteedihüpe, et eesti keele õigekiri ja grammatika kui kirjade usutavuse oluline takistus on ületatud ja kampaaniate edu ja neist tulenev rahaline kahju on tõusuteel. Kasutajalt nõuab taoliste kirjade äratundmine senisest palju rohkem tähelepanelikkust.

RIA-le raporteeritud intsidendid

2014. aastal kasvas nii esitatud intsidendiraportite kui ka koondraportite hulk. Valdavalt antakse intsidentidest teada siiski korra kvartalis koondraporti vormis. Võrreldes 2013. aastaga raporteerisid riigiasutused RIA-le ligi neli korda rohkem intsidente. Ühelt poolt näitab see trend nii aktiivsuse kasvu küberruumis (intensiivsem infosüsteemide kasutus, rohkem planeerimata katkestusi, rohkem pahatahtlikku tegevust) kui ka turvajuhtimise süsteemi küpsuse kasvu. Asutused pööravad rohkem tähelepanu intsidentide teadvustamisele, analüüsimisele ja teavitamisele. Intsidentide asjatundlik raporteerimine näitab, et organisatsioonis on toimiv infoturbepoliitika – osatakse tuvastada intsidenti, selle mõju teenustele ja toimunust õppida ja järeldusi teha.

Raportite kvaliteet on üldiselt tõusuteel. Valdavalt kirjeldatakse raportites IT-poolelt intsidenti üsna täpselt (nt tegu oli ühe või teise seadme tarkvara konkreetse versiooni tõrkega), ent arenguruumi on ärilise mõju analüüsimisel ehk analüüsil, mida tähendas intsident asutuse tööle. Näiteks kui e-posti süsteem tunni vältel ei toimi, siis kui paljusid ja kui kriitilisi kasutajaid ja toiminguid see tõrge puudutas, millised on alternatiivid.

Intsidentide hulk ja sagedus

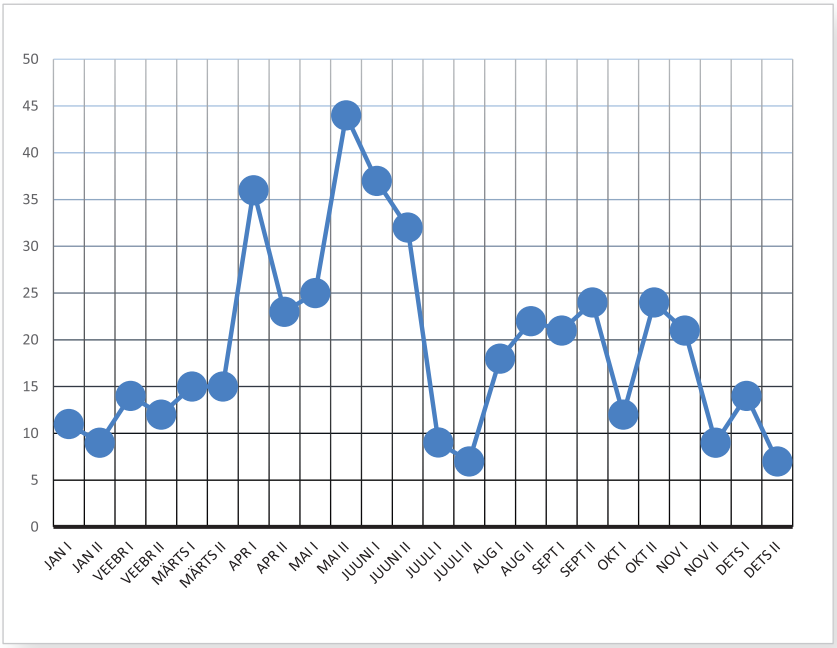


Joonis 1: intsidentide ja RIA-le esitatud raportite arv 2013. ja 2014. aastal.

Enim raporteeritud intsidente toimus hiliskevadel mai teises pooles ja juunis. Valdavalt oli tegu pahavarale viitava liiklusega ja portide skaneerimisega, mille otsest mõju asutuste tööle pole kirjeldatud ja mida raporteerijad hindavad madala kriitilisusega intsidentideks. RIA hinnangul on seega tegemist ründajate katsetustega, mitte asutuste tööle otsest mõju omanud juhtumitega. Juunisse langes ka nn OLAF-kampaania (OLAF — European Anti Fraud Office), mil mitme riigiasutuse raamatupidajaid said e-postiga näiliselt asjalikke, kuid tegelikult nakatavaid kirju (vt lähemalt https://www.ria.ee/kes-on-olaf/).

Ka III kvartalis toimus mitu intsidenti, mis mõjutas mitmeid asutusi. Nii raporteerisid septembri keskel mitmed riigiasutused kasutajate nakatumisest pahavaraga, mis saadi Elroni kodulehelt. Intsidendi mõju hinnati valdavalt keskmiseks. Samas on oluline märkida, et „Elron“ oli 2014. aastal otsituim Eesti sõna Google'is, seega on nakatumise mõju Eestis tervikuna laiem kui raporteeritud nakatumised riigiasutustes.

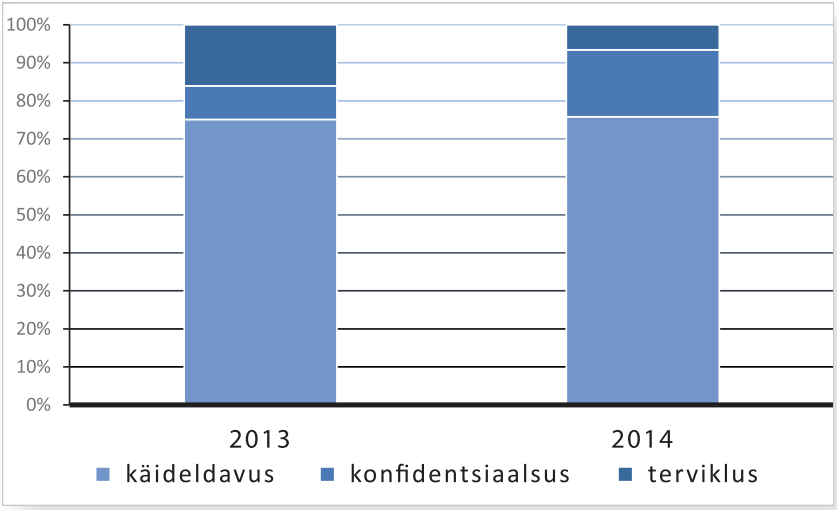
Augusti lõpus ja septembri alguses toimus 3 katkestust riigi andmesidevõrgu töös. Katkestused olid tingitud tehnilistest riketest ja mõjutasid paljusid riigiasutusi. Raportid, mis puudutasid nende katkestuste mõju, laekusid kokku 8 asutuselt. Mõjutatud asutusi oli rohkem, sest mõned raporteerijad on kesksed IT-asutused, mis pakuvad teenust mitmetele organisatsioonidele. Kuuel juhul hinnati intsidendi kriitilisust kõrgeks, kolmel keskmiseks. Näiteks kannatas seetõttu nii digiretsepti kui ka piiripunktide töö.



Joonis 2: raporteeritud intsidentide sagedus 2014. aastal

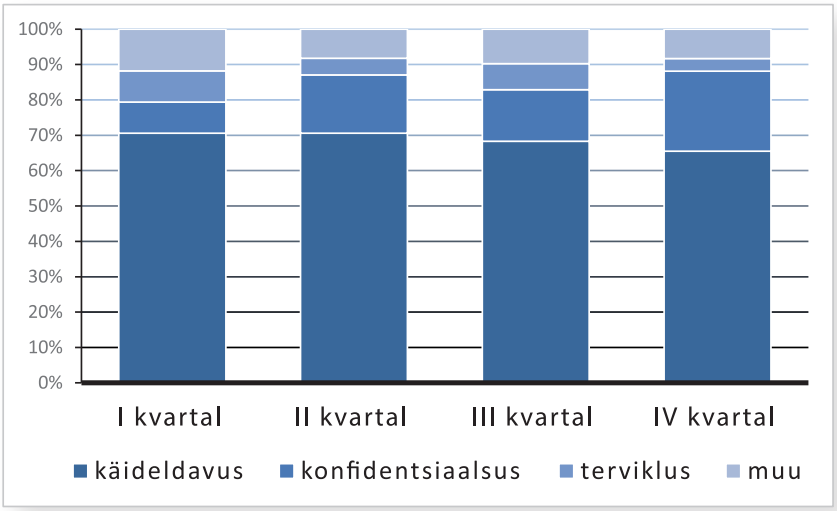
Intsidentide tüüp (käideldavus, konfidentsiaalsus, terviklus)

2014. aastal (nagu ka aasta varem) raporteerisid riigiasutused valdavalt käideldavusintsidente, ent silma hakkab konfidentsiaalsusintsidentide osakaalu märgatav kasv. Oluline on siinkohal märkida, et mitme intsidendi puhul märgitakse raportis tüübina mitu kategooriat, näiteks mõne pahavara iseloom võib anda ründajale võimaluse mõjutada nii andmete terviklust kui ka konfidentsiaalsust. Seega näitavad alltoodud tulbad pigem intsidenditüüpide mainimiste osakaalu, mitte intsidentide iseloomu osakaalu.



Joonis 3: Käideldavus-, konfidentsiaalsus- ja terviklusintsidentide osakaal 2013. ja 2014. aastal

Konfidentsiaalsust ohustavate intsidentide mainimist esines kõige sagedamini IV kvartalis, mil suurenes ka rünnete, peamiselt õngitsuskirjade ja nakatunud arvutite hulk (vt joonis 10).

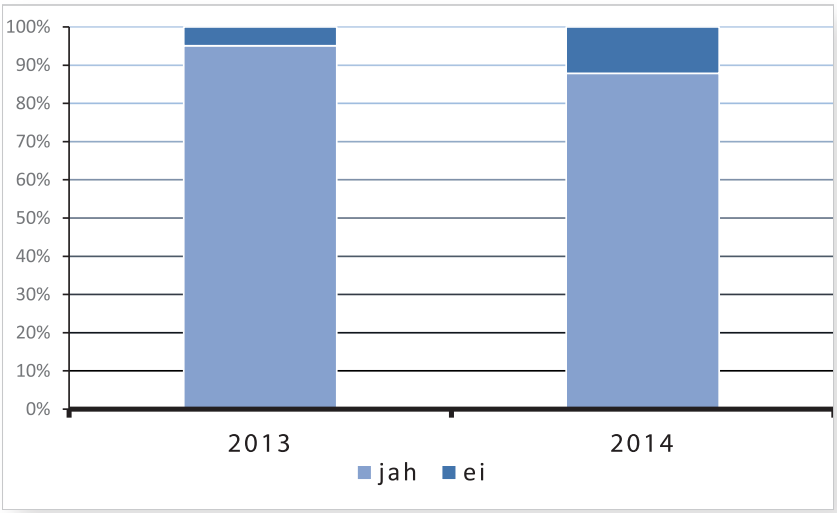


Joonis 4: Käideldavus-, konfidentsiaalsus- ja terviklusintsidentide osakaal kvartalite kaupa

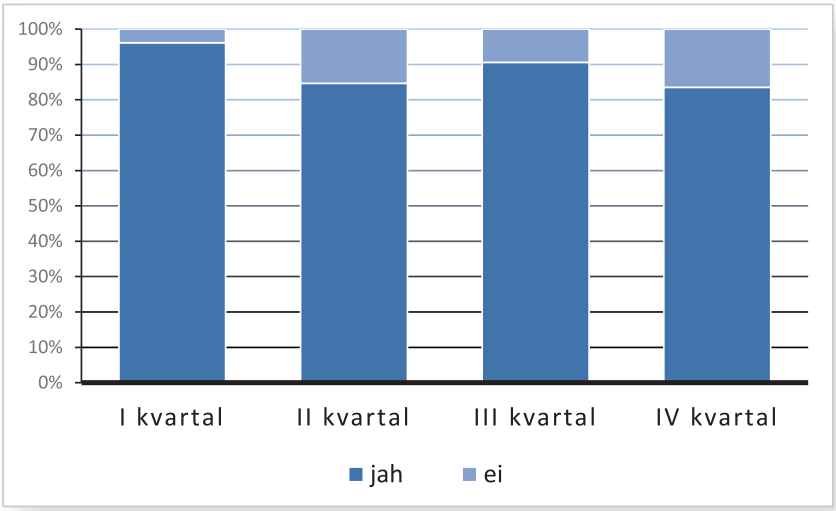
Intsidentide mõju

2014. aastal kasvas mõnevõrra selliste intsidentide osakaal, millel oli reaalne tagajärg ka asutuse ja kasutajate jaoks, näiteks pole võimalik kasutada dokumendihaldussüsteemi või tõsisematel juhtudel näiteks digiretsepti või Schengeni infosüsteemi. Endiselt on raporteeritud intsidentide hulgas palju selliseid, mille mõju pole kirjeldatud ja/või mille mõju nii infosüsteemile kui ka teenusele on teksti põhjal raske tuvastada – 2013. aastal oli selliseid tuvastamatu mõjuga ja raporteeritud intsidente 10% kõigist raporteeritutest, 2014. aastal aga suisa kolmandik. Pisut kasvas 2014. aastal ka selliste intsidentide osakaal, mida suudeti enne realiseerumist tõkestada või oli tegu lihtsalt tuvastatud ohuga, mitte intsidendiga.

Raporteerimise kvaliteedi parandamiseks on RIA-l plaanis jätkata teavitustööd raporteerimise olulisusest nii riigiasutuste kui elutähtsa teenuse osutajate seas. Plaanis on astuda samme ka raporteerimisprotsessi korrastamiseks: raporti vormi täiendamiseks ja masinloetavale kujule viimiseks.



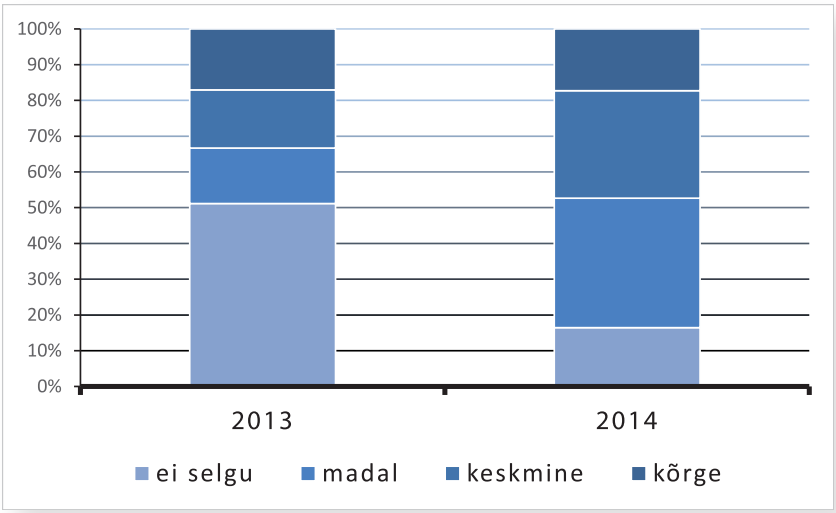
Joonis 5: intsidendi mõju 2013. ja 2014. aastal



Joonis 6: intsidentide mõju kvartalite kaupa 2014. aastal.

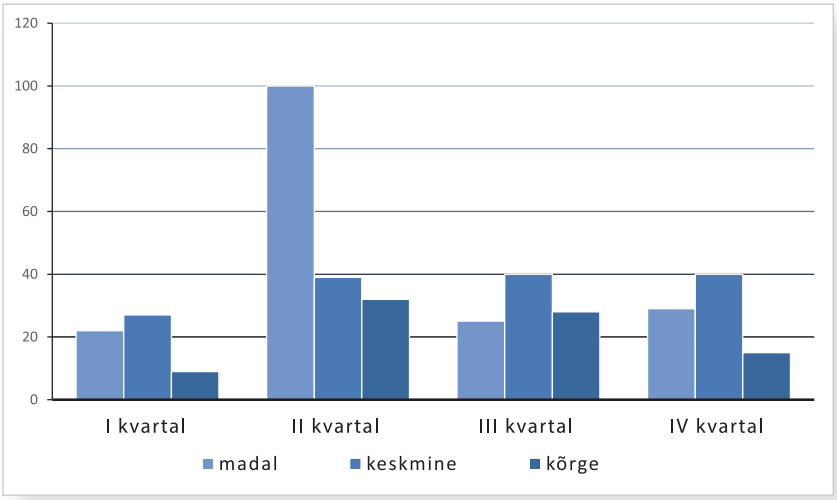
Intsidentide kriitilisus

2014. aastal andsid riigiasutused märksa parema ülevaate intsidendi kriitilisusest. Sealjuures on kriitiliste intsidentide osakaal kõigist raporteeritutest jäänud umbkaudu samaks, ligi 20% ehk viiendik. Samas mahus on suurenenud nii keskmiste kui madala kriitilisusega intsidentide osakaal.



Joonis 7: intsidentide kriitilisus 2013. ja 2014. aastal

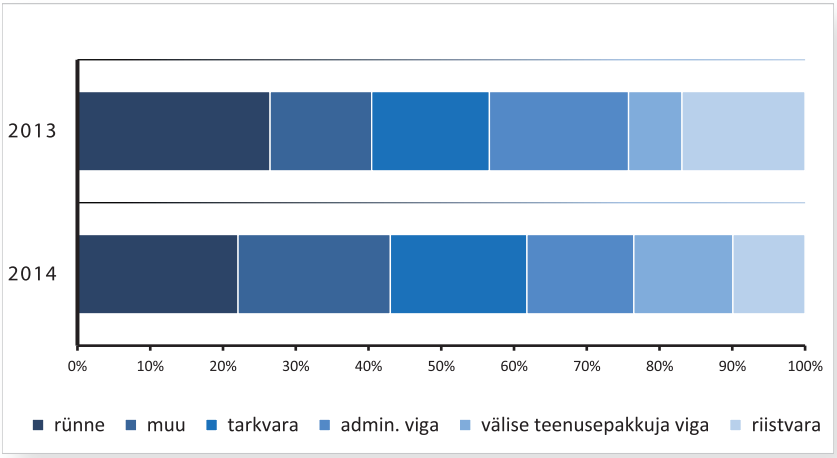
Enim kriitilisi intsidente raporteerisid riigiasutused II kvartalis. Peamiselt oli tegu andmesidekatkestustega, mis mõjutasid korraga mitmeid asutusi. Samasse kvartalisse langes aga ka *Heartbleed*'i haavatavuse avastamine. Reaalseid kuritarvitusi *Heartbleed*'iga seoses RIA-le kevadel ei raporteeritud, küll aga on selliseid teateid tulnud hiljem juhtudel, mil IT-spetsialistid on võrku ühendanud mõne uue seadme, millel see ohtlik ja laialdaselt teadaolev haavatavus on paikamata. Taolistel juhtudel on RIA reageerinud kiiresti ja otsustavalt ning probleem on leidnud lahenduse. Ka IV kvartalis oli kriitiliste intsidentide seas enim andmeside katkemisest põhjustatud intsidente, ent tööd andis raporteerijatele ka järjekordne laia levikuga haavatavus *Shellshock.*



Joonis 8: 2014. aasta intsidentide kriitilisus kvartalite kaupa

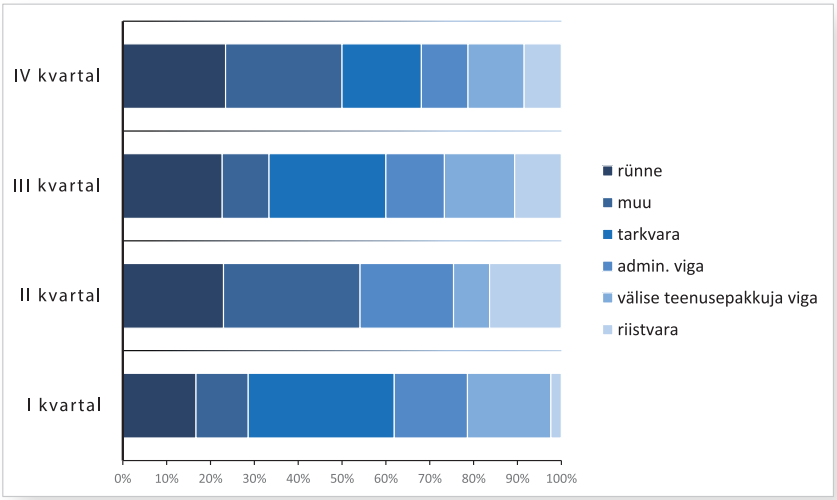
Intsidentide põhjus

Rünnete osakaal kõigist raporteeritud intsidentidest 2014. aastal küll mõnevõrra langes, samas on rünne 2014. aastal levinuim intsidendi põhjus, edestades napilt „muid" põhjusi (reeglina peitub sildi „muu" all elektrikatkestus). Levinud põhjus raporteeritud intsidentidel oli ka tarkvaraviga ja välise teenusepakkuja viga (siia kategooriasse märgitakse samuti reeglina elektrikatkestusi ja andmesidekatkestusi).



Joonis 9: levinumad intsidentide põhjuste osakaalud 2013. ja 2014. aastal

Arvuliselt enim raporteeriti ründeid aasta viimases kvartalis, kuigi rünnete osakaal võrreldes teist tüüpi intsidentidega on suurim teises kvartalis. Valdavalt oli aasta lõpus tegu viirusepuhangute ja hästi sihitud õngitsuskirjadega, aga ka teenusetõkestusrünnetega, millest mitmed ei kestnud eriti kaua, vaid paistsid RIA hinnangul pigem kaardistavat süsteemide vastupidavust. Selliste pealtnäha mõttetute ja lühiajaliste hajusate teenusetõkestusrünnete (DDoS) kasv on ühelt poolt murettekitav, samas on DDoSide sagenemine üleilmne trend, mis tuleneb järjest lihtsamast kättesaadavusest ja madalamast hinnast.



Joonis 10: 2014. aasta intsidentide levinumate põhjuste osakaal kvartalite kaupa

Uuringud ja juhendid

2014. aastal tellis RIA kolm suuremat uuringut: nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring, järjekordne krüptograafiliste algoritmide elutsükli uuring ja suurte oluliste andmekeskuste turvanõuete juhend. Lisaks tegi RIA omal käel väiksema uuringu, et selgitada riigiasutuste ja elutähtsa teenuse osutajate riskitunnetust.

IT-riskide tunnetus riigiasutustes ja ETOdes

Sügisel tegi RIA riigiasutuste ja elutähtsa teenuse osutajate IT-juhtide ja turvajuhtide seas küsitluse, et uurida IT-riskide tunnetust riigiasutustes ja ETOdes. Küsitlus oli anonüümne, sellele vastas 16 ETOt ning 25 riigiasutuse IT-juhti ja infoturbejuhti.

- Suurima ohuna näevad organisatsioonide IT-juhid ja turvajuhid rikkeid. Sellele järgnevad poliitiliselt motiveeritud ründed ja teabehanked.
- Vaid mõnel üksikul vastanud organisatsioonil pole paigas infoturbe nõudeid ja infoturbe eest vastutavat isikut.
- 88% vastanutest on kõrgeks või väga kõrgeks hinnanud organisatsiooni tegevuste sõltuvust IKT-süsteemidest. Sealjuures tõdes 78% vastanutest, et viimase kolme aasta jooksul on organisatsioonis riske analüüsitud/hinnatud.

RIA jaoks oli küsitluse tulemustest oluline järeldus see, et parandada tuleb raporteerimise kvaliteeti ja juhtkonna riskiteadlikkust – vajalik on turvajuhtide ja juhtkonna süsteemne koolitamine. Targaks riskide hindamiseks on oluline panustada küberriskide tuvastamisse ja analüüsi, eriti sõltumatute auditite ja testide kaudu.

Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuring

Sügisel tegi TNS Emor Riigi Infosüsteemi Ameti ja Vaata Maailma sihtasutuse tellimusel uuringu, mis käsitles nutiseadmete kasutajate turvateadlikkust ja turvalist käitumist.

Uuringust selgus, et 2014. aastal omab nutiseadmeid ja/või neid on võimalik kasutada 60% Eesti elanikkonnast alates kuuendast eluaastast. Samas selgus, et inimeste arusaamad nutiseadmetega seotud ohtudest on lünklikud ning sageli puuduvad vajalikud praktilised oskused. Näiteks seitse last kümnest saavad nutitelefoni kasutada igal ajal ja täpselt nii palju kui nad ise soovivad ning 75% nendest ütlevad, et vanemad kas ei tunne üldse huvi (19%) või tunnevad väga harva huvi (56%) selle vastu, mida nad oma nutiseadmetes teevad.

Uuring valmis EL-i struktuurifondide programmist „Infoühiskonna teadlikkuse tõstmine" Euroopa Regionaalarengu Fondi rahastusel. Selle tulemused on kättesaadavad Vaata Maailma kodulehelt: http://www.vaatamaailma.ee/wp-content/uploads/veeb-Nutiseadmete-kasutajate-turvateadlikkuse-ja-turvalise-k%C3%A4itumise-uuring_ARUANNE-2014.pdf

Krüptograafiliste algoritmide elutsükli uuring

2015. a kevadel valmib teine Eestis kasutatavate krüptograafiliste algoritmide uuring, mis muuhulgas rõhutab veelkord mitmeid juba 2014. aastal avaldatud soovitusi. Kokkuvõtlikult – lähimate aastate jooksul tuleb krüptograafilisi meetodeid uuendada mitmetes Eesti olulistes tarkvaratoodetes ja -teenustes. See võib kohati tähendada kasutajate jaoks ebamugavusi, sest keerukate süsteemide puhul pole alati võimalik kõiki muudatuste mõjusid ette ennustada.

Et kõikide algoritmide eluiga on piiratud, on veelgi piiratum aeg, mille vältel tegutseda, et teenuste krüptograafilised meetodid ajakohasena hoida. Ühel hetkel võib selguda, et sujuv üleminekuaeg pole olnud piisav, näiteks kui krüptograafia murdmiseks rakendatakse võimsaid kvantarvuteid. Sellisel juhul on vaja juba rakendada tegevusplaani juhuks, kui selgub, et mõni Eesti e-teenuste jaoks oluline algoritm on murdunud. RIA näeb selget vajadust, et sellised plaanid oleksid olemas ja läbi harjutatud.

Andmekeskuste turvanõuete juhend

Mais valmis RIA tellimusel koostöös AS Elion Ettevõttetega andmekeskuse turvanõuete juhend. See on juhis eelkõige kõrge käideldavusnõuetega riiklike ning elutähtsa teenuse osutajate andmekogusid majutavate serveriruumide ja andmekeskuste planeerimiseks, ehitamiseks ja hooldamiseks. Dokument on kättesaadav ISKE juhendite lehelt (https://www.ria.ee/iske-dokumendid/).

Küberohtude ennetamine

Küberkirjutised

2014. aastal lõi küberturvalisuse teenistus blogi, et anda kiireid ja praktilisi juhiseid Eesti internetikeskkonda ohustavate haavatavuste paikamiseks ja pahavarakampaaniate tõkestamiseks. Blogist leiab ka postitusi, mis avavad muid Eesti küberturvalisuse seisukohast olulisi teemasid. Blogi asub aadressil https://kyberkirjutised.ria.ee/.

Koolitused

2014. aastal korraldas RIA Euroopa Regionaalarengu Fondi rahastusel EL-i struktuurifondide programmist „Infoühiskonna teadlikkuse tõstmine" kokku 23 küberturvalisuse koolitust, seminari ja teabepäeva, mille osalejate koguarv oli 744. Nende seas oli nii turvalisuse tagamiseks vajalikke oskusi arendavaid praktikume (IDS, IPv6, OpenDNSSEC), mitte-IT-spetsialistile suunatud seminare kui ka laiemate teemaderingiga teabepäevi.

Õppused

Rahvusvahelistel õppustel tegeleb RIA nende planeerimise ja korraldamisega ning juhib lisaks neil osalemisele siseriiklikult rahvusvahelisi küberõppusi. Planeerimine algab enamasti aasta enne õppust ning seisneb osalejate värbamises, nende juhendamises ja mängitavate intsidentide kohaldamises Eesti oludele.

Cyber Europe. 2014. aasta jooksul toimus nii tehnilisel kui ka ametkondade-vahelisel operatiivsel tasandil ENISA juhitud rahvusvaheline õppus Cyber Europe 2014. Õppusel osales 20 liikmesriiki, Euroopa infoturbe ja küberkaitse organisatsioonid, samuti Island ja Norra. Kokku oli õppusega seotud üle 670 inimese rohkem kui 200 asutusest. Õppuse esimene etapp 2014. aasta aprillis oli tehniline ja pakkus osalejatele võimalust lahendada kokku 16 erinevat turvaintsidenti/ülesannet. Kahe päeva jooksul paluti neil uurida ja analüüsida sündmusi, mis võivad mõjutada nende asutuse andmete konfidentsiaalsust ja terviklikkust, tundliku informatsiooni lekkimist või kriitilist infrastruktuuri. Eestist osales Cyber Europe 2014 tehnilisel õppusel 9 meeskonda ja 34 inimest 6 erinevast asutusest. Õppuse teises, operatiivses etapis harjutasid samad ametkonnad koostööd, informatsiooni vahetust ja tegevuste koordineerimist nii riigisisesel ametkondadevahelisel kui ka EL-i tasandil. Õppuse kolmas, strateegiline etapp viidi läbi 2015. aasta veebruaris Brüsselis. RIA täitis õppusel planeerija, moderaatori, riikliku kontaktisiku, mängija ja hindaja ülesandeid.

Õppust Cyber Coalition korraldas NATO teist aastat järjest Tartus. Õppusel osalenud Eesti ametkonnad paistsid silma tehniliste intsidentide lahendamisega. Näiteks oli Eesti üks kahest riigist, kelle spetsialistid suutsid õppusel lahendada Androidi pahavara süvaanalüüsi puudutava ülesande. Õppus nõudis oma sisult ka ametkondade vahelist tööde koordineerimist ja infovahetust. Õppuselt saadud õppetunde rakendatakse edasiste tegevuste ja õppuste planeerimisel.

NATO küberkaitse koostöö keskuse tehnilist õppust **Locked Shields** võõrustatakse alaliselt Tallinnas. Tegemist on õppusega, kus mängukeskkonnas loodud süsteeme rünnatakse ja kaitstakse reaalajas. Õppus tõestas taaskord Eesti tehnilist kompetentsi: Eesti tunnistati Locked Shields'i kõige paremaks kriminalistika (*forensics*) tiimiks. Üldarvestuses saavutas Eesti võistkond õppusel III koha. Selle aasta meeskond koosnes nii riigiasutuste, telekommunikatsiooni kui ka elutähtsat teenust osutavate ettevõtete spetsialistidest.

Infoturbejuhtide komisjon

2014. aastal sai ametliku vormi ja töökorra seni mitteametlikult koos käinud riigi infoturbejuhtide komisjon. See on riigiasutuste turvajuhte ühendav organ, millel on juhatus, regulaarsed istungid ja otsused. 2014. aastal käsitles komisjon näiteks ISKE rakendamisega seotud teemasid, vahetas infot ja kogemusi turvameetmete rakendamisel ja ohtlike haavatavuste ilmnemisel.

DNSSEC

Jaanuaris avas Eesti Interneti Sihtasutus DNSSEC teenuse .EE domeenidele. DNSSEC (*Domain Name System Security Extensions* ehk domeeninimede süsteemi turvalaiendused) kaitseb internetikasutajaid ja domeeniomanikke, andes kindluse, et kasutajat pole tema teadmata soovitud kodulehe asemel ümber suunatud mõnele muule lehele. Esimene turvalaiendusega allkirjastatud domeen oli riigiportaal eesti.ee.

Domeenisüsteemi kaitsmine DNSSEC-iga on oluline samm turvalisema interneti poole Eestis. Selle teadvustamiseks organiseerisid RIA ja Eesti Interneti Sihtasutus ka domeeniomanikele suunatud teavituskampaania. RIA pakub tasu küsimata DNSSECi juurutamist oma partneritele: riigiasutustele ja kohalikele omavalitsustele, sellest DNS-teenusest saab lisainfot veebiaadressilt: www.ria.ee/vorguteenused.

Riskianalüüsi metoodika

2014. aastal alustas RIA elutähtsate teenuse osutajatele suunatud IT-riskianalüüsi metoodika täiendamist. Tulenevalt hädaolukorra seadusest on ETOd kohustatud riske, sh IKT-riske hindama. Olles läbi töötanud üle saja riskianalüüsi ja toimepidevuse plaani pidi RIA tõdema, et IKT-riskide kohta on analüüsides infot pigem napilt ja pealiskaudselt, seega tuleks riigi ootusi IKT-riskianalüüsile täpsemalt ja ühtsemalt kirjeldada. Põhjalik ja ajakohane IKT-riskianalüüs on kasulik ennekõike nii ETO-le endale, aga ka riigile, et hinnata täpsemalt IKT-taristu ja teenuste ristsõltuvusi.

Juhendi koostamise lõpetab RIA 2015. aastal, kaasates Siseministeeriumi ja elutähtsa teenuse osutajaid ja korraldajaid. Juhendit on kavas kasutada siseministri 08.06.2010 määruse nr 16 „Toimepidevuse riskianalüüsi koostamise juhend" (https://www.riigiteataja.ee/akt/13326405) täiendamiseks.

Elanikkonna küberjulgeolekualane teadlikkus

Eurobaromeetri 2014. aasta küberturvalisuse küsitlusest selgub, et Eestis usaldatakse riiki oma isikuandmete hoidjana rohkem kui Euroopas keskmiselt. Samuti on eestlased muretumad küberrünnete tagajärgede osas ja enda sõnutsi hoolikad võltskirjade tuvastajad.

40 protsenti Eesti vastajatest tunneb muret, et riigiasutused ei hoia nende isikuandmeid turvaliselt. Euroopa Liidu keskmine protsent on 67. Andmete hoidmist võrgulehtedel üldiselt umbusaldab Eesti vastajatest 53 protsenti, Euroopa Liidus keskmiselt umbusaldab seda andmete säilitamise viisi 73 protsenti vastanutest.

Eesti vastajad muretsevad kõige vähem Euroopa Liidus selle pärast, kui nad ei peaks küberrünnaku korral pääsema ligi internetile ning avalikele ja pangateenustele. Eesti vastajatest muretseb selle pärast 39, Euroopas keskmiselt 50 protsenti vastajatest.

Eesti vastajad on küberohtude tõttu Euroopa keskmisega võrreldes enam paigaldanud enda arvutisse viirusetõrjetarkvara, pigem ei ava e-kirju, mille sisu on tundmatu, kasutavad ainult enda arvutit ja muudavad regulaarselt oma salasõnu. Eestlased on ka Euroopa Liidu keskmisest selgelt vähem mures andmepüügikatsete pärast.

Uuringu Eesti faktileht: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_ee_ee.pdf
Kogu uuring: http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#423

Rahvusvaheline koostöö 2014

2014 oli väliskontaktide poolest aktiivne aasta. RIAt külastas arvukalt välidelegatsioone, kes tulid saama kogemusi küberturbe (-organisatsioonide) ülesehitamisel ja arendamisel. Lisaks Euroopa ja Põhja-Ameerika partneritele võtsime vastu delegatsioone Lähis-Idast, Aafrikast, Jaapanist, Lõuna-Koreast, Singapurist ja Uus-Meremaalt.

Toimus mitmeid kahepoolseid ekspertkohtumisi oluliste partnerasutustega Euroopas (Ühendkuningriik, Saksamaa, Prantsusmaa, Holland) ja USAs, et vahetada kogemusi kriitilise informatsiooni taristu kaitse, riskihalduse, küberturbe õppuste ja koolituste teemal. Sügisel korraldasime Tartus ametkondadevahelise küberturbe seminari Ühendkuningriigi kolleegidega, kus osalesid CERT-i ja politseiasutuste esindajad. Koostöös George Washingtoni ülikooliga USAs toimus oktoobris Washingtonis Eesti küberseminar, kus tutvustasime arvukale kuulajaskonnale USA riigiasutustest, erasektorist ja ülikoolidest Eesti küberturbe arenguid, lahendusi ja Eesti küberjulgeoleku strateegiat 2014–2017.

Uue prioriteedina otsustasime arendada RIA nähtavust Ameerika mandril ning sõlmisime 2014. a oktoobris koostöökokkuleppe Ameerika Riikide Organisatsiooniga (OAS) regiooni küberturbe võimekuste arendamise toetamiseks. RIA on 2014. a suvest olnud kaasatud 5 OASi koolitusprojekti –

Kolumbias, Dominical, Trinidadis ja Tobagol, Washingtonis ja Jamaical. Koolituste fookus on olnud erinev, ametkondadevahelise koordinatsiooni ja küberjulgeoleku organisatsioonilise ülesehituse küsimustest tehniliste baaskoolitusteni.

Olulisemad arengud küberjulgeoleku õiguslikus ja strateegilises raamistikus

RIA uued pädevused ja kohustused

1. juulil 2014. a jõustus korrakaitseseaduse muutmise ja rakendamise seadus. Selle alusel on RIA 2014. aasta suvest korrakaitseorgan. Vastavalt muudatustele läks elektroonilise side seaduses sätestatud Tehnilise Järelevalve Ameti järelevalvepädevus sidevõrkude ja -teenuste turvalisuse ja tervikluse tagamise üle RIA-le. Sama eelnõuga sätestati RIA järelevalvepädevus ka hädaolukorra seaduses ja avaliku teabe seaduses.

RIA on asutus, keda sideettevõtjad peavad teavitama kõigist olulistest sidevõrgu ja -teenuse turvalisuse ning terviklikkuse tagamist ohustavatest juhtumitest. Elutähtsate teenuste osutajate määratud kontaktisikud peavad RIAt viivitamata teavitama olulise mõjuga turvaintsidendist. RIA on väärtegude kohtuväline menetleja elektroonilise turvalisuse nõuete rikkumise üle hädaolukorra seaduse alusel ja sidevõrkude ja -teenuste turvalisusele ning terviklikkusele kehtestatud nõuete rikkumise üle elektroonilise side seaduse alusel.

Avaliku teabe seaduse alusel sai RIA 2014. aastal andmekogu registreerimise kontrollimise ja kooskõlastamise pädevuse – varem oli see seaduses sätestatud Majandus- ja Kommunikatsiooniministeeriumi ülesandena, kuigi suurem osa kooskõlastusprotsessist viidi varemgi läbi tihedas koostöös RIAga.

Küberjulgeoleku strateegia 2014–2017

11. septembril kiitis valitsus heaks „Küberjulgeoleku strateegia 2014–2017" ja selle rakendusplaani. Strateegia jätkab mitmete eelmises küberjulgeoleku strateegias seatud eesmärkide elluviimist, kuid on lisandunud ka uusi ohte ja vajadusi. Riigi toimimise sõltuvus infotehnoloogiast on kasvanud, samuti on süvenenud ristsõltuvused – mitmete elutähtsate teenuste osutamine ei sõltu ainult Eesti IT-süsteemide heast tervisest, vaid ka piiritagusest IKT-taristust ja e-teenustest. Küberjulgeoleku strateegia nelja aasta põhiline eesmärk on suurendada küberturvalisuse alast võimekust ja inimeste teadlikkust küberohtudest, tagamaks jätkuvat usaldust küberruumi vastu.

Strateegia elluviimist rahastatakse RIA eelarvest ja Euroopa struktuurifondide vahenditest. Väljakutse on samas see, et struktuurifondidest viiakse ennekõike ellu infoühiskonna arengukava tegevusi, mis küberjulgeoleku strateegia eesmärkidega otseselt ei arvesta.

https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

Ulatuslikeks küberintsidentideks valmistumine

2014. aastal töötas RIA koostöös partnerasutustega välja ühtsed põhimõtteid hädaolukorraks valmisoleku ja koostöö tagamiseks ulatuslike küberintsidentide korral. RIA juhitud ametkondadevahelise töörühma töö tulemusel on valminud Vabariigi Valitsuse korralduse eelnõu „Ulatusliku küberintsidendi hädaolukorra lahendamise plaan“, mis saadetakse Vabariigi Valitsusele kinnitamisele 2015. aasta sügisel pärast selle testimist 2015. aastal planeeritud siseriiklikel kui ka rahvusvahelistel õppustel.

Väärtuslikud õppetunnid RIA-sisese valmisolekuseisundite ja -protseduuride kehtestamiseks saadi nii 2014. aasta kevadise kõrgendatud valmisoleku rakendamisel kui ka USA presidendi Barack Obama visiidi ajal. Saadud kogemuste ja kirjeldatud vajaduste pinnalt valmistati ette „RIA valmisoleku seisundite kord“, mis kinnitatakse peadirektori käskkirjaga 2015. aasta I kvartalis.

ISKE

Infosüsteemide kolmeastmeline etalonturbe süsteem ISKE on infoturbe standard, mis on loodud rakendamiseks eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infovaradele.

2014. aasta suvel kinnitas majandus- ja taristuminister ISKE rakendusjuhendi versiooni 7.0. Selles täiendati ohte, turvameetmeid ja tüüpmooduleid, uuendati ID-kaardi meetmeid ning lisati ISKE rakendamise 11 sammu vastutajate (RAC) tabel.



Juurutamisel on ISKE kataloogide veebipõhine rakendus, mis muudab ISKE kataloogid kasutajasõbralikumaks – enam ei pea ISKE rakendaja töötama PDF-failidega, vaid saab mugavalt ohtude, meetmete ja moodulite veebikeskkonnas navigeerida. 2016. aastal valmib plaanitavalt uus ja ajakohane ISKE rakendustööriist, mis kasutab sisendina 2014. aastal tehtud eelanalüüsi (ISKE rakendustööriista täiendusettepanekute analüüs).

RIA pöörab ISKE raamistikus eraldi erilist tähelepanu krüptograafiateemadele ja pilvetehnoloogiatele. 2014. aastal selgitati välja ISKE kataloogide muutmise vajadus, lähtuvalt Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuringust (www.ria.ee/public/PKI/kruptograafiliste_algoritmide_elutsukli_uuring_II.pdf). Need muudatused avaldatakse järgmises ISKE rakendusjuhendi versioonis 2015. aastal.

Novembris 2014 käivitati projekt **„Pilvetehnoloogiate infoturbe analüüs“**, mille tulemusena selgub 2015. aastal, kas ja kuidas on võimalik riigi infosüsteeme pilvtöödelda. Valmib juhendmaterjal riigiasutustele, teenusepakkujatele ja audiitoritele. Samuti selguvad analüüsist soovitused ISKE kataloogide pilvetehnoloogiate teemaliseks täiendamiseks.

Oluline õigusalane muudatus ISKE juurutamiseks riigis on 2015. a veebruaris kooskõlastusringile saadetud valitsuse määrus. See seab avalike teenuste arendamiseks antavatele EL-i struktuurifondide toetustele üheks tingimuseks ka selle, et toetatav projekt tõstab riigi infosüsteemi turvalisust lähtuvalt ISKEst või muust asjakohasest ja samaväärsest standardist.
https://eelnoud.valitsus.ee/main/mount/docList/dbc25685-0631-4e7f-9ac5-cfab37154bea

Kokkuvõte

2014. aasta ei erinenud 2013. aastast eriti intsidentide arvukuse poolest, ent selgelt oli märgata juhtumite mõju tõsinemist. Teenusetõkestusründed on minetanud oma uudsuse ja esinevad paljudes valdkondades, mis sõltuvad andmesidest ja tehnoloogiast.

Ka riigiasutused mainisid intsidentide põhjusena enim rünnet, mõistes selle all nii teenusetõkestusründeid kui ka näiteks pahavara levitamise kampaaniaid. Riigi e-teenuste tõrgete sage põhjus on ka elektri- ja andmesidekatkestused. Iga e-teenuse pakkuja, ka riigiasutuse, jaoks on need väga tõenäolised ja keeruliselt maandatavad riskid. See tähendab, et üha enam tuleb teenuse elujõu tagamiseks mõelda pigem õnnetuste ja pahatahtlike intsidentide tagajärgedega toimetulemisele, sest intsidendi põhjust ära hoida ja ette ennustada on väga keeruline. Vaja on head plaani puhuks, kui midagi juhtub ning sellele omakorda varuplaani.

Positiivne oli see, et 2014. aastal kasvas nii riigiasutuste esitatud intsidendiraportite kui ka koondraportite hulk. Ühelt poolt näitab see trend nii aktiivsuse kasvu küberruumis (intensiivsem infosüsteemide kasutus, rohkem planeerimata katkestusi, rohkem pahatahtlikku tegevust) kui ka turvajuhtimise süsteemi küpsuse kasvu, st asutused pööravad rohkem tähelepanu intsidentide

teadvustamisele, analüüsimisele ja teavitamisele. Võrreldes 2013. aastaga raporteerisid riigiasutused RIA-le ligi neli korda rohkem intsidente.

Eestis ringlevad õngitsuskirjad tegid möödunud aastal kvaliteedihüppe. Massiliselt levivad kirjad saabuvad nüüd reeglina usaldusväärsena näivast allikast, on heas eesti keeles ja mõistliku sisuga ning sisaldavad pealtnäha asjalikku manust või usutavat linki, mis viib arvuti nakatumiseni. Kasutajalt nõuab võltskirjade laviinis orienteerumine senisest enam tähelepanelikkust ja umbusku, vastasel juhul võib ilma jääda nii oma kirjakasti sisust kui halvemal juhul korralikust rahasummast.

Käsitletud pahavarajuhtumitest väärib märkimist paljude asutuste, eraettevõtete ja tavainimeste nakatumine Elroni veebilehe vahendusel. Olulist transporditeenust osutava ettevõtte veebilehele murti sisse ning kasutati seda pahavara levitamisel mitu korda järjest. Ilmekas on sealjuures asjaolu, et Elron oli 2014. aastal otsituim eestikeelne sõna Google'is.

Nii maailma kui Eesti turvakogukonda jahmatasid eelmisel aastal mitmed suure mõjuga vead krüptograafiliste algoritmide teostustes (nt OpenSSLi vead). Tõhusama arvutusvõimsuse tõttu odavnes ka nõrgemate krüptograafiliste algoritmide (DES ja RSA1024) murdmine. Riigivõrgus suudeti RIA agressiivse seire- ja teavitustöö tulemusena haavatavused küll paari päevaga paigata, ent hiljem on olnud juhuseid, kus võrku ühendatakse uuesti mõni paikamata seade. Taoliste üldlevinud ja enne paikamist laialdaselt meedias publitseeritud vigade levikuks tuleb valmis olla ka tulevikus.

Ennetustegevustest jätkas RIA küberturbe koolituste ja seminaride korraldamist, rahvusvahelistel õppustel osalemist, aktiivset rahvusvahelist koostööd riikidega üle kogu maailma, aga ka jooksvat teavitustööd ja kampaaniaid Eesti avalikkuses, näiteks aegunud tarkvara kasutamise riskide ja nutiseadmete turvalise kasutamise kohta. Oluline avalikkusele suunatud teavituskanal on aprillis loodud küberkirjutiste blogi (https://kyberkirjutised.ria.ee), kust saab haavatavuste ja intsidentide ilmnemisel infot ja juhiseid nii spetsialist kui ka näiteks võimalik õngitsuskampaania ohver.

Eesti inimeste teadlikkus küberohtudest on Euroopa keskmisega võrreldes üllatavalt hea ja võimalikesse probleemidesse suhtutakse rahulikult. Eesti vastajad muretsevad kõige vähem Euroopa Liidus selle pärast, kui nad ei peaks küberrünnaku korral pääsema ligi internetile ning avalikele ja pangateenustele. Samas ei istu Eesti inimene käed rüpes – Euroopa keskmisega võrreldes on Eestis enam paigaldatud arvutisse viirusetõrjetarkvara; pigem ei avata e-kirju, mille sisu on tundmatu; kasutatakse ainult enda arvutit ja muudetakse regulaarselt oma salasõnu. Samas selgus pisut spetsiifilisemast RIA ja Vaata Maailma sihtasutuse tellitud nutiseadmete turvalise kasutamise uuringust, et nutiseadmete turvaliseks kasutamiseks võiks teadlikkus olla parem, eriti kui jutt on vanema huvist lapse tegemiste vastu nutiseadmes.

2015. aastal on lisaks igapäevasele haavatavustele ja ohtudele reageerimisele RIA jaoks olulised märksõnad riigi andmeside seire ja toimepidevuse tugevdamine, koostöö meditsiinivaldkonnaga ning e-residentidega seonduvad lahendused ja riskid. Jätkuvalt nõuavad tähelepanu omaniku poolt hooletusse jäetud ja seetõttu kergesti nakatuvad Eesti veebilehed, e-postiga pahavara levitamise kampaaniad ja aegunud tarkvara kasutamisest tulenevad ohud.

Soovitusi lisalugemiseks

RIA küberkirjutiste blogi
https://kyberkirjutised.ria.ee/

Euroopa võrguturbeagentuuri 2014. aasta ohtude ülevaade (avaldatud jaanuaris 2015, inglise keeles)
https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

Rahvusvahelise telekommunikatsiooni liidu üleilmne küberturvalisuse indeks (inglise keeles).
Eesti on selle riikide küberturvalisuse võimekust kaardistava indeksi alusel maailmas koos Brasiilia, India, Jaapani, Lõuna-Korea, Saksamaa ja Ühendkuningriigiga viiendal kohal.
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Saksamaa kokkuvõte 2014. aasta IT-turvalisusest (inglise keeles)
https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

Soome küberturvalisuse keskuse aasta ülevaade (soome keeles).
Ülevaade toob sarnaselt Eesti hinnangutele esile õngitsejate professionaliseerumise: ka soome keele tase on õngitsuskirjades märgatavalt tõusnud.
https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/kyberturvallisuuskeskuksenvuosikatsaus2014.html