CERT Eesti tegevuse aastakokkuvõte 2007

Tarmo Randel,

CERT Eesti infoturbe ekspert

CERT Eesti on rahvuslik turvaintsidentide lahendamise meeskond (ingl. k. Computer Emergency Response Team), mille peamine eesmärk on tagada Eesti riigi infosüsteemide ja kriitiliste infosüsteemide pidev toimimine. Selle tarvis teeb CERT Eesti koostööd asutuste ja ettevõtetega peamiselt spetsialisti tasemel.

Aasta 2007 oli tõsine proovikivi CERT Eestile – riigi vastu suunatud turvaintsidendi käsitlemist ei saa just paljud turvaintsidentidega tegelevad meeskonnad enda tehtud tööde nimekirja kanda. Aprillis ja mais toimunu tõi Eesti taas kord maailmakaardile ning nii mõneski mõttes võib öelda, et hoolimata sündmuste negatiivsest iseloomust oli nende efekt positiivne. Seda kasvõi ainuüksi selle poolest, et paljud riigid hakkasid analüüsima riikliku IT infrastruktuuri haavatavust reaalse näite varal, kus sihtmärgiks oli riik tervikuna.

2007. a kevadised sündmused on ainult osa CERT Eesti tavapärasest tegevusest: intsidentide käsitlemine, kus on peamiselt tegemist info "kalastamisega" (*phishing*), pahavara levitamisega Eesti serverite kaudu ja arvutite nakatamisega. 2007. aastal alustati turvalise arvutikasutamise raamprojektiga, mille osa on eestikeelse OpenBSD koolituse organiseerimine süsteemiadministraatoritele ja palju muud (OpenBSD on kõrgete turvastandarditega operatsioonisüsteem). Kõigest täpsemalt allpool, ent alustame siiski aasta suursündmusega.

Ründed Eesti riigi infotehnoloogiliste lahenduste vastu

26. aprillil 2007. aastal said alguse sündmused, mida tunneme koondnimetuse "pronksiöö" all, ning mis tol hetkel oli peamiselt füüsiline konflikt poerüüstajate ning politsei vahel. See ei jäänud aga pelgalt füüsilise vastasseisu tasemele: 27. aprillil laienes tekkinud konflikt küberruumi. Ründed eesmärgiga häirida erinevate Eesti infotehnoloogiliste süsteemide käideldavust kestsid kokku 22 päeva. Ründed pärinesid valdavalt Eestist väljaspool asuvatest arvutivõrkudest.

Küberründed algasid suhteliselt lihtsate meetoditega – venekeelsetes foorumites esitati üleskutsed käivitada MS Windows käsurealt käsk *ping* (lihtne käsk kontrollimaks, kas teine arvuti vastab) foorumis toodud parameetritega. Hiljem lisandusid BAT failid, mida oli mugav arvutisse kopeerida ja käivitada ning mis automatiseerisid *ping*-käsu kasutamise. Sihtmärkidena levitati reeglina riigi veebilehtede aadresse, nagu www.riik.ee, www.valitsus.ee, www.peaminister.ee ning hiljem ka mõnede valitsuserakondade veebisaitideaadresse.

Pingimisele lisandusid peagi vigased veebipäringud, mida esitati massiliselt peamiselt riigi ja meediaväljaannete veebilehtedele. Nende päringute kasutusele võtmine vihjas juba spetsiaalsete vahendite kasutamisele.

Kirsina tordil võeti kasutusele nakatunud arvutitest moodustatud virtuaalne arvutivõrk – *botnet*. Seda kasutati peamiselt pankade ründamiseks. Hansapanga vastu suunatud peamised ründed toimusid 10. ja 15. mail, 15. mail olid sihtmärgiks ka SEB Eesti Ühispank ning Krediidipank. Lisaks pankadele said *botnet* - rünnakute osaliseks ka suuremad meediaväljaanded japortaalid.

Eesti riigi ametlikud suhtluskanalid Internetis olid pideva ründe all 27. aprillist kuni mai lõpuni. 9. maile

suunatud ründelaine algas aga 8.mail kell 23:00, mis annab vihje ründajate võimaliku ajavööndi osas. Rünnatavateks sihtmärkideks olid www.riik.ee, www.president.ee, www.peaminister.ee ning ka tuvasta.pol.ee, kuhu olid riputatud fotod rüüstajatest ja vara lõhkujatest.

Kui ründeid riigiserveritele võis tõlgendada kui poliitilist protesti, siis süstemaatiline kommerts-struktuuride ründamine viitab riigi vastu suunatud organiseeritud tegevusele, nimetatagu seda siis küberrünneteks või küberterrorismiks. Rünnati pankasid, et halvata majandustegevust ja meediaväljaanded, et tõkestada info edastamist. Rünnakutega häiriti lisaks suurtele tegijatele ka väikefirmade igapäevaelu – koormati e-posti servereid, võrguseadmeid ja veebiserverid sedavõrd, et ettevõtete normaalne äritegevus oli häiritud.

CERT Eesti peamine ülesanne aprilli lõpust kuni juunikuuni oli tagada riigi infokanalite kättesaadavus Eestis ja välismaal. CERT organiseeris riigi kui terviku vastu suunatud rünnete tõkestamist nii riigis sees kui piiridest väljaspool. Nende eesmärkide saavutamiseks mobiliseeris CERT Eesti parimad IT spetsialistid. Väga palju aitas küberrünnakute tõrjumisel Soome CERT meeskond, kelle kaasabil tehti koostööd välismaiste teenusepakkujate ja teiste riikide CERT meeskondadega.

Pettused

Jättes kõrvale aprilli- ja maikuu rahutused küberruumis, oli CERT Eesti põhitegevus 2007. aastal seotud pahavara ja pettustega. Pahavara ja pettused eksisteerivad viimasel ajal lahutamatult koos, sest üldine suundumus pahavara loojatel on raha teenimisele, varasema kuulsuse saamise asemel. Tavakasutaja jaoks tähendab see tänapäeval, et tema arvutis pesitsev viirus on seal eeskätt eesmärgiga võtta tema rahakotist raha või kasutada tema arvutit lüüsina teiste raha varastamisel. Vargusest jäävad jäljed viivad mitte varga, vaid süütu arvutikasutajani.

Tegevuse käigus puututi kokku *Sinowali*-nimelise pahavaraga, mis on oma olemuselt paroolide varastaja. Lisaks tavapärasele paroolide varastamisele on ta võimeline varastama ka SSL sertifikaate ning vajadusel avama varjatud ligipääsu nakatunud arvutile. SSL sertifikaati on vaja siis, kui veebisait töötab üle HTTPS protokolli. HTTPS protokollis krüpteeritakse kogu suhtlus serveri ja kliendi veebilehitseja vahel nii, et kolmas osapool ei saa suhtlust pealt kuulata ega võltsida. Sinowali eripäraks on veel võime näidata veebibrauseris päritud veebilehe asemel pahavara genereeritud lehte, näiteks veebipanga esilehte. Samal ajal korjab pahavara sisestatud info endale enne, kui see panga serverisse jõuab.

Sinowaliga on seotud Neosploidi levik – legaalsed veebilehed on täiendatud koodiga, mis installeerib arvutisse pahavara kasutaja teadmata. Tavaliselt levivad sellelaadsed nakkused veebifoorumite kaudu, ent antud pahavara koodi leidsime ka tavalistelt firma veebilehtedelt. See viitab võimele ennast levitada, kasutades kasutajate arvutitest varastatud FTP või veebisaitide haldamiseks mõeldud keskkondade pääsufraase. Siit saame teha ühe järelduse – kui aasta-paar tagasi võis kasutajat kaitsta, blokeerides ligipääsu teatud veebilehtedele, siis tänapäeval võib kasutaja arvuti nakatada näiteks lemmikportaali külastades. Seega, blokeerimine ei ole enam nii efektiivne meede, kui ta veel mõned aastad tagasi oli. Näitena probleemist võib lisaks eelpooltoodule tuua populaarseid suhtluskeskkondi www.myspace.com ja www.facebook.com, mis nakatasid külastajaid veebilehe reklaamibännerite kaudu.

Suhteliselt palju avastati kompromiteerunud pääsufraase, mis oli enamasti seotud troojalase Nethell (tuntud ka nimega Banker) tegevusega. Nethell on troojalane, mis peamiselt tegeleb pääsufraaside varastamisega, lisaks võib ta veebist laadida täiendavaid programme ning suunata liiklus kasutaja soovitud veebisaidi asemel hoopis teise serverisse. Viimast teeb ta loomulikult selleks, et varastada

pääsufraase või muud kurjategijatele kasulikku infot (krediitkaardi detailid vms). CERT Eesti teavitas teadaolevatest paroolivarguse juhtudest asjassepuutuvaid teenusepakkujaid.

2007. aasta alguses tegeleti kiirelt muutuva nimelahenduse infrastruktuuriga (fastflux DNS), mis tekitati Warezov nimelise pahavara abil. Kiirelt muutuvat nimelahendust kasutatakse kuritegelikel eesmärkidel veebilehtede näitamiseks. Nimetatud tehnoloogia muudab veebisaidi sulgemise ja kurjategijate tabamise raskeks, kuna sekundite jooksul muutub veebilehte näitav arvuti – olles ühel hetkel füüsiliselt näiteks Rootsis ja teisel hetkel Koreas. Selline teenuse ülesehitus tagab kurjategijate tegevuse edukuse, sest serverite arv on suur ning vahetub pidevalt. CERT Eestit teavitati pahatahtliku infrastruktuuriga seotud Eestis paiknevatest serveritest, meie nõudmisel ligipääs leitud serveritele suleti.

2007. aasta lõpus oli palju kära Interneti teenusepakkuja Russian Business Network-i ehk RBN tegevuse ümber. RBNi tegevust kajastati peamiselt välismaises ajakirjanduses. Tegemist on n.ö. bullet-proof hostinguga ehk serverimajutaja ja IT teenuse pakkujaga, kes osutab teenust kuritegelikele rühmitustele. Kära RBNi tegevuse ümber ja rahvusvahelise surve tagajärjel suleti RBNi Interneti ühendus, ent nende tegevust see ei lõpetanud: nad olid eelnevalt enda serverid kolinud seni tuvastamata kohta. Ilmselt õppisid nad enda vigadest ning profileerisid enda tegevuse ümber, mis muutis nad hetkel tuvastamatuks.

Koostöö

Eelmine aasta oli murdeline Eestisisese kommunikatsioonivõrgustiku loomisel. Ühiste eesmärkide ja tööülesannetega inimeste koondamiseks ja info jagamiseks loodi keskkond Internetis. Eesti andmeturbega seotud inimeste omavahelise suhtluse arendamiseks ning mujal maailmas toimuva tutvustamiseks korraldati mitmeid mitteformaalseid kokkusaamisi koos välismaiste esinejatega Soomest ja Šveitsist. Aasta võttis kokku traditsiooniline CERT Eesti teabepäev, millest osavõtnute ring oli väga lai – huvilisi oli kohalikest omavalitustest, riigiasutustest ja ka eraettevõtetest.

Eesti sisese koostöö arendamise kõrval tegeles CERT Eesti 2007. aastal intensiivselt väliskontaktide arendamise ja hoidmisega. Aprillikuu sündmused osutasid selgelt, et edukaks võitlemiseks suuremastaabiliste rünnakutega on vajalikud formaalsed ja mitteformaalsed kontaktid CERT organisatsioonide, suurte Interneti teenusepakkujate ning andmeturbe ekspertidega üle kogu maailma.

Rahvusvahelise suhtluse lihtsustamiseks alustasime liikmestaatuse taotlemise protsessi mitmes rahvusvahelises CERT katusorganisatsioonis. Kuulumine rahvusvahelistesse organisatsioonidesse avab CERT Eestile ligipääsu mitmete ekspertide töögruppide tegevusele ning organisatsiooni liikmete kogemuspagasile ja töövahenditele.

Aasta 2007 osutas selgelt vajadusele tõsta arvutikasutajate turvateadlikkust, sellest tulenevalt võeti 2008. aasta üheks eesmärgiks laiendada nii tavaliste arvutikasutajate kui ka spetsialistide silmaringi. Näitena võib välja tuua kevadel planeeritava turvalise arvutikasutuse kampaania ja OpenBSD koolitusprojekti süsteemiadministraatoritele.