RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE MÄRTS 2017

Olukord Eesti küberruumis

Märtsis käsitles CERT-EE 1221 juhtumit, millest infosüsteemide tööd mõjutanud küberturbeintsidente oli 317 ehk ligikaudu viiendik. Kõrge prioriteediga intsidente oli 15 ning elutähtsa teenuse osutajaid puudutanud juhtumeid 58. Erasektoris registreeriti 819 ning avalikus sektoris 118 juhtumit.

Võrreldes möödunud aasta sama perioodiga on nii küberturbejuhtumite kui -intsidentide arv kasvanud ligi kolmandiku.

Kuu keskel leidis aset andmepüügikampaania, kus näiliselt Maksu- ja Tolliameti nimel saadetud kirjadega püüti inimestelt petta välja krediitkaardiandmeid, viidates „enammakstud tulumaksu tagastamisele". CERT-EE operatiivse tegutsemise tulemusel suleti õngitsemisleht paari tunni jooksul ning kahju õnnestus vältida. Mainimist väärt on ka ulatuslikum kasutajaandmete leke (üle 550 kasutajakonto) Eesti suurimas kutse- ja täiendõppeasutuses Tartu Kutsehariduskeskuses arvutitesse paigutatud nn klahvinuhi kaudu.

Märtsis registreeritud intsidentidest üle 70% põhjustas taas pahavara. Näotustamisjuhtumite osakaal oli 10% ja teabeõngitsemise juhtumite osakaal 3% piirimail. Muud põhjused jäid üksikjuhtumite tasemele.

Tegevused küberjulgeoleku parandamisel Eestis

9. märtsil toimus RIAs regulaarne turvajuhtide komisjoni kohtumine, kus vahetasime teavet aktuaalsetest teemadest ja tutvustasime RIA koostatud turvajuhendeid e-kirjavahetuse ja avalike pilveteenuste kohta. Kohtumisest võttis osa üle 40 infoturbe- ja turvajuhi eri riigiasutustest.

Jätkasime koostööd ja kohtumisi teenuseosutajatega elutähtsate teenuste turvaseiresüsteemi väljatöötamiseks. Ettevõtmise eesmärk on parandada ettevõtjate ohuteadlikkust, tõsta võimekust avastada pahavara ja küberründeid oma arvutivõrkudes ning seeläbi maandada riske elutähtsate teenuste toimepidevusele. Samuti keskendume sel aastal infoturbe etalonraamistiku ISKE arendamisele.

Jätkasime ka ettevalmistusi Eesti eesistumisega seotud taristu küberturvalisuse tagamiseks ning koolitusi eesistumisega seotud riigiametnikele.

Rahvusvaheline keskkond

Rahvusvahelistest sündmustest kajastati laialdaselt nn **Vault 7 teabeleket** USA Luure Keskagentuuri (CIA) küberoperatsioonide meetodite ja tööriistade kohta. 7.-31. märtsini avaldas WikiLeaks kolmes jaos üle 8700 dokumendi, mis muu hulgas käsitlesid erinevate tootjate (Samsung, Apple, Cisco) nuti- ja võrguseadmete, krüpteeritud sidet võimaldavate nutirakenduste, enimlevinud veebilehitsejate ning operatsioonisüsteemide (Windows, MacOS) haavatavusi ning nende ärakasutamist. CIA tööriistu või rünnevahendeid endid WikiLeaks ei avaldanud, lubades (seni lubadust küll täitmata) need üle anda tehnoloogiaettevõtetele, et viimased saaksid haavatavad tooted ära turvapaigata.

Avaldatud CIA dokumendid pärinevad aastatest 2013-2016 ning sisaldavad nii juba teadaolevaid kui ka varem teadmata nn nullpäeva haavatavusi. Dokumente hinnatakse autentseteks ning seega lükkab leke ümber USA varem kinnitatud ja valdavalt kahtluse alla seatud väite, et USA ei kogu teavet turvanõrkuste kohta, et neid rünneotstarbel kasutada. Segadust tekitas ka Valge Maja poolt tootjatele antud hoiatus, et haavatavuste kui salastatud teabe kasutamisele võib järgneda õiguslik vastutus. CIA teabelekked tõstatasid taas debati, kuivõrd peaksid luureasutused jagama tootjatega teavet avastatud turvanõrkustest, et vältida nõrkuste kurjategijate kätte langemist ning kahju ettevõtjatele ja eraisikutele.

Hollandi üldvalimiste eelõhtul sattusid küberründe alla populaarsed valimisinfot sisaldavad

veebilehed (*a la* Valimiskompass), mida rahastab riik ja kasutab pea pool valijaskonnast. Ründeid analüüsinud Hollandi küberturbeettevõtte Fox IT hinnangul pärinesid need Türgi häkkerirühmitustelt; teenus õnnestus taastada valimispäeva lõuna paiku. Lunavara tabas ka Hollandi parlamenti, kelle koduleheküIg jäi lühiajaliselt kättesaamatuks.

Samuti jäid USA Senati Pennsylvania osariigi demokraatidest esindajad lunavaraintsidendi tagajärjel enam kui nädalaks ilma ligipääsust oma infosüsteemidele ja dokumendikeskkonnale. Juhtunu mõju raskendas intsidendi toimumine keset eelarveläbirääkimisi. USAs on presidendivalimistest saati toimunud mitu sarnast lunavaraintsidenti väidetavalt just liberaalset maailmavaadet esindavate mittetulundusühenduste seas; nõuete suurus on olnud kuni 150,000 USD.

Saudi Araabiast on märtsikuust teada lunavaravariant, mis failide lahtilukustamiseks nõudis ohvri kodulehel poliitilise sõnumi avaldamist.

Märtsikuust on teada juhtum, kus valik erinevate tootjate (Samsung, LG, ZTE jt) nutitelefone jõudis tarnijani eelpaigaldatud nuhk- ja lunavaraga. Seadmete logianalüüs viitas, et pahavararakendused ei olnud osa tootja tüüprakenduste paketist, vaid olid paigaldatud tarneahelas, samuti ei olnud lõppkasutajal võimalik neid telefonist eemaldada.

Kuu algul teatas Luksemburgi riiklik IT-keskus – mis ühtlasi on riigiasutustele internetiteenuse pakkuja – ööpäeva väldanud teenustõkestusründest (DDoS) sajakonna Luksemburgi riigiasutuse veebiserveri vastu. Ründamiseks kasutati robotvõrku; ründe päritolu ega motivatsiooni kohta teavet ei ole. Tegemist oli esimese nii mahuka DDoS-ründega Luksemburgi ajaloos. Veebilehtede juurdepääs oli häiritud, riigiasutuste toimimine jätkus normaalselt.