RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE APRILL 2017

Olukord Eesti küberruumis

Aprill oli Eesti küberruumis keskmisest veidi rahulikum. Registreerisime 781 juhtumit, millest intsidendiks kvalifitseerus pea viiendik (188), neist 13 kõrge prioriteediga. Elutähtsa teenuse osutajaid puudutanud juhtumeid oli 58.

Kõrge prioriteediga intsidentide peamiseks põhjuseks olid seadmerikked ja hooldustööde käigus ilmnenud probleemid, mis mõnel juhul mõjutasid ka teiste oluliste teenuste toimimist – näiteks tõi sideettevõtja tugijaama probleem ühel juhul kaasa häired ka siseministeeriumi infosüsteemide toimimises. Aprilli sündmustest on oluline märkida ligi 10 tundi väldanud häireid SEPA maksete edastamises Põhja- ja Baltimaades, mis puudutas üht kommertspanka, ning ööl vastu 26. aprilli aset leidnud katkestust Telia kõnesideteenuses. Viimane mõjutas ligi 80 000 lauatelefoni klienti, põhjuseks oli riistvararike.

Tegevused küberjulgeoleku parandamisel Eestis

26. aprillil korraldasime 2007. aasta küberrünnete 10. aastapäevale pühendatud konverentsi „Küberturvalisuse olevik ja tulevik", kus rääkisime küberrünnete evolutsioonist viimasel kümnendil, praegusest valmidusest küberkriisidega toime tulla ning küberpoliitika kujundamisest.

CERT-EE juhtis Eesti meeskonna osalust 24.-28. aprillil toimunud NATO Küberkaitse Koostöökeskuse *Locked Shields* õppusel. Lisaks RIA küberturvalisuse teenistuse töötajatele osalesid õppusel Elektrilevi, Kaitseministeeriumi, Kaitseväe, Linx Telecomi, SEB panga, Starmani, Telia ja Zone Media eksperdid. Õppuse põhirõhk oli tehnilistel oskustel, kuid osalevad meeskonnad lahendasid ka meedia-, õigus- ja strateegilise tasandi ülesandeid.

Toimusid kahepoolsed kohtumised RIA rahvusvaheliste partnerasutustega ning Balti küberkoostöö koordinatsioonikohtumine Vilniuses. Samuti jätkasime küberturbekoolitustega riigiasutustele ning Eesti Euroopa Liidu esindusele.

Rahvusvaheline keskkond

WikiLeaks avaldas nädalaste vahedega veel viis kogumit dokumente CIA küberoperatsioonide tööriistade kohta. Nende seas on CIA *Marble Framework*iks nimetatud lähtekood pahavara koodi hägustamiseks, mis võimaldab takistada rünnete omistamist. Avaldati ka Marble'i pöördkonstrueerimisvõti, mis teeb võimalikuks varasemate – või ka käimasolevate – operatsioonide ja pahavara seostamise CIAga. Lisaks sisaldas seekordne kogum teavet erinevate seadmete ja tarkvaraplatvormide turvanõrkuste ning koostöös Ühendkuningriigi vastuluureteenistusega loodud lahenduste kohta.

Aprilli keskpaiga seisuga, mil oli avaldatud viis osa nn Vault 7 lekkest, seostatakse CIA tööriistu rohkem kui neljakümne sissemurdmiskatsega 16 riigis, sh Euroopas. Sihtmärkide seas on valitsusasutused ning pangandus-, IKT- ning lennufirmad.

Aprillis aktiveerus taas ka Shadow Brokersi nimeline häkkerirühmitus, kes lekitas internetti rea USA riikliku julgeolekuagentuuri NSA häkkimistööriistu, mis kasutasid ära erinevate Windowsi operatsioonisüsteemide haavatavusi. Microsoft oli märtsis väljastatud neile turvapaigad, ent juba esimese paari nädalaga levis DoublePulsar tagauksetarkvara vähemalt kahesajale tuhandele seadmele, kus tarkvarauuendusi paigaldatud ei olnud. ShadowBrokersi leke hõlmas NSA dokumente, mis viitavad, et NSA võis jälgida Lähis-Ida pankadevahelist SWIFT arvelduslliklust. SWIFT soovitab klientidel pöörata makseteenuse pakkuja valikul tähelepanu viimase suutlikkusele turvalist kommunikatsiooni tagada.

Aprillis ilmunud uudised pankade vastu korraldatud küberrünnetest eri riikides viitavad, et finantssektori vastased ründed muutuvad ühtaegu nii mitmekesisemaks kui ka keerukamaks. Küberturbefirma Kaspersky Lab

avaldas kuu algul raporti Lazarus Groupiks nimetet APT grupeeringu tegevusest, keda peetakse vastutavaks möödunud aastal Bangladeshi keskpanga vastu toime pandud suuremahulise kelmuse eest ning pahavararünnete eest Poola pankade vastu sel hilistalvel. Laialdaselt Põhja-Koreaga seostatud grupeeringu tegevusfookus on viimasel paaril aastal üha enam liikunud pankade, hasartmänguplatvormide, finantstarkvara tootjate ning krüptorahaäri osaliste ründamisele. Ründevektorid varieeruvad: manipuleeritakse SWIFT liideseid ja tehingute kontrollimehhanisme või kasutatakse spetsiaalselt sihtmärgile kohandatud pahavara. Aprillis avalikustati ka üht Brasiilia suurimat panka tabanud küberrünne, kus pangalt kaaperdatud internetidomeeni kaudu suunati kliendid võltslehele, kus kasutaja seade nakatati pahavaraga, mis muutis arvuti turvasätted ning varastas pangateenuse kasutajatunnused. Andmevargus puudutas sadu tuhandeid panga kliente ning on ekspertide hinnangul esimene sedavõrd mastaapne omataoliste seas. Aprilli lõpus leidis aset ka juhtum, kus paarikümne globaalse finantsteenusepakkuja (sh Visa ja Mastercard) võrguliiklus suunati lühiajaliselt läbi Rostelekomi sidevõrgu. Juhtumi asjaolud loovad kahtluse, et tegemist võis olla liikluse tahtliku kaaperdamisega, mis võimaldas Vene Föderatsiooni administratsiooni kontrollitud ettevõtjal liiklust pealt kuulata ja sellesse sekkuda.

Tuntud Vene küberturbelahenduste tootja Kaspersky Lab kirjeldab juhtumit, kus Venemaa panga sularahaautomaatidest varastati nn failita pahavara abil sadade tuhandete dollarite väärtuses raha. Rünne pandi toime, manipuleerides sularahaautomaatides kasutatavat tarkvara ja algkäivitades seejärel seadme, mis kustutas sissemurdmise jäljed süsteemist. Sarnase „failita“ pahavara kaudu on Kaspersky andmetel varem kompromiteeritud vähemalt 140 panka, riigiasutust ja sideettevõtjat.