RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE VEEBRUAR 2017

Olukord Eesti küberruumis

Veebruaris registreeriti CERT-EE küberintsidentide süsteemis 1005 juhtumit, millest intsidente (st juhtumeid, millel oli reaalne mõju infosüsteemide käideldavusele, terviklusele või konfidentsiaalsusele) oli ligikaudu kolmandik (360). See tegi veebruarist taas ühe sündmusterohkeima kuu viimase aasta jooksul. Keskmisest enam oli ka kõrge prioriteediga intsidente (15). Elu või tervist ohustanud kriitilisi intsidente ei esinenud.

Elutähtsate teenuste osutajaid puudutanud intsidente oli veebruaris 68, sh katkestused suuremate sideteenuse osutajate võrkudes ning panga kaardimaksete ja sularahaautomaatide ristkasutuse toimimises. Vabariigi aastapäeva varahommikul ei toiminud Tallinna Lennujaamas seadmerikke tõttu reisijate teenindamise infosüsteemid, mis tingis üheksa väljalennu hilinemise; probleeme oli ka reisijate teenindamisega jätkulendudel.

22. veebruaril põhjustas võrguseadme rike katkestuse RIA väliste ja sisemiste teenuste töös. Kättesaamatud olid mh riigiportaal eesti.ee ja ID-tarkvara allalaadimisleht; tõrkeid esines kolme tunni vältel.

Veebruaris registreeritud intsidentide põhjuste seas domineeris taas ülekaalukalt pahavara. Kõrge prioriteediga intsidentide põhjuseks olid valdavalt seadmerikked.

Tegevused küberjulgeoleku parandamisel Eestis

Kuu alguses toimus RIAs nädalane erikursus Euroopa Liidu eesistumise turvalisuse tagamisega tegelevatele julgeoleku-, korrakaitse- ja küberturbeametnikele. Koolitajateks olid USA Salateenistuse eksperdid, kes jagasid Eesti ametnikega valdkonna tippkompetentsi. Koolitus on jätkuks RIA kauasele heale koostööle USA partnerasutustega; Eesti ja USA vahel on alates 2013. aastast koostöölepe küberturvalisuse arendamiseks.

Jätkasime koolitustega eesistumisega seotud ametnikele, seekord Keskkonnaministeeriumis.

16.-17. veebruaril korraldasime CERT-EE igaaastase teabepäeva CERT@Voore IT- ja turbejuhtidele nii avalikust kui erasektorist.

Rahvusvaheline keskkond

Uudised Venemaa eriteenistustega seostatud küberrünnetest (APT29) NATO ja ELi riikide vastu on muutunud rutiiniks ja ründeid pannakse toime üsna varjamatult. Norra julgeolekuteenistus PST teatas sihitud andmepüügikatsetest riigivõimu institutsioonide (välisministeerium, kaitsevägi, julgeolekuteenistus, parlamendifraktsioon jt) vastu. Ükski sihtmärgiks sattunud asutustest ei ole kinnitanud, et sissemurdmiskatsed oleksid õnnestunud. Teisalt viitab Norra juhtum ka positiivsetele suundumustele: tõhustunud on liitlastevaheline infovahetus ja hoiatus ning tekkimas tava ründekatsed, sh nende päritolu, avalikustada (vt ka Poola juhtumit RIA jaanuari kokkuvõttes).

Veebruaris sai teatavaks pikaajaline kampaania peamiselt pangandussektori sihtmärkide vastu 31 riigis. Veebilehtede turvanõrkusi ära kasutades sisestati neisse senitundmatut pahavaravarianti, mis nakatas spetsiifilistele parameetritele (etteantud IP-aadressid) vastavate külastajate seadmed. Poola kommertspangad said nakkuse Poola finantsjärelevalveasutuse veebilehelt. Ründajaid seostatakse sama grupperinguga, keda usutakse olevat 2014. aasta Sony Pictures intellektuaalomandi varguse ja 2016. aasta üleilmse pankadevastaste rünnete laine taga. Rahalise kahju kohta seni andmeid pole.

Palju kajastust leidsid esemevõrgu seadmetega seotud küberturbeohud ja -intsidendid. Saksamaa sideturu regulaator BNetzA keelustas laste kõnet salvestavate internetiühendusega mänguasjade müügi, hinnates need laste privaatsust ohustavaks. Nädalajagu hiljem sai teatavaks andmeleke CloudPets mänguasjatootja serverist, mille tagajärjel sai avalikuks üle 800 000 e-postiaadressi ja salasõna ning üle kahe miljoni lapse

ja vanema häälsalvestuse. USA küberturbeettevõte TrendMicro ulatuslikust uuringust selgus rida tüüphaavatavusi USA linnade valitsussektori ja elutähtsate teenuste esemevõrgu seadmetes. Teisalt teatasid kolm tuntud IKT-ettevõtet (AT&T, IBM ja Nokia) koostööplatvormi asutamisest, et esemevõrgu turvalisust parandada – seda eeskätt kasutajate ja ettevõtjate harimise ning uurimistöö kaudu.

Muud olulist

Ilmus NATO Küberkaitse Koostöökeskuse toel valminud küberoperatsioonidele kohalduva rahvusvahelise õiguse käsiraamat ehk *Tallinn Manual* 2.0. Käsiraamat analüüsib riiklike küberoperatsioonide kogu spektrit – küberspionaažist relvastatud ründega võrreldavate küberrünneteni – kehtivate rahvusvahelise õiguse normide kontekstis ning selgitab riikide õigusi ja kohustusi küberoperatsioonide läbiviimisel. Muu hulgas keskendub käsiraamat sellistele teemadele nagu suveräänsus, hoolsuskohustus, jurisdiktsioon ja riigivastutus ning rahvusvahelise õiguse erivaldkondadele nagu inimõigused ja telekommunikatsiooniõigus. Täiendatud on ka rahvusvahelist sõjaõigust puudutavat osa, mille esmatrükk ilmus 2013. aastal.