RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE VEEBRUAR 2016

Olukord Eesti küberruumis

Veebruaris 2016 käsitles CERT-EE 781 juhtumit, millest 128 kohta teavitas riigisektor ning 653 kohta erasektor. Nagu eelnevatelgi kuudel, olid ka veebruaris CERT-EE käsitletud juhtumitest kõige kõrgema prioriteediga erinevat tüüpi lunavaradega nakatumised. Veebruaris käsitleti nii TeslaCrypt lunavara juhtumeid, mis hakkas lisaks varasema Wordpressi kõrval levima ka Joomla sisuhaldustarkvaraga seotud ning uuendamata jäetud kodulehtede kaudu. Seetõttu olid need lunavara juhtumid ka veebruaris Eestis laiemalt levinud kui Locky-nimelise lunavara juhtumid, mis on tõusuteel mujal maailmas. Paljud teavitajad andsid CERT-EE-le veebruaris teada sellest, kuidas lunavara arvutitesse jõudis ja kuidas arvuteid pärast töökorda saadi, mida omakorda jagasime edasi ka neile kasutajatele, kes sellega ise hätta jäid. Veebruaris sai seega taaskord tõestust, kui oluline on Eesti üldise parema küberturvalisuse saavutamiseks see, et CERT-EE-le antaks teada isegi juba lahenduse leidnud juhtumitest.

Lisaks lunavarajuhtumitele käsitleti veebruari alguses ja keskel mitmeid Dridex-tüüpi pangatroojalasega nakatumisi. Dridexi voog on nüüdseks raugenud, seoses selle juhtimiseks kasutatud botneti likvideerimisega erinevate organisatsioonide koostöö tulemusel veebruari lõpus. Lisaks näitas veebruaris tõusutrendi ka Ramnit-tüüpi pangatroojalane, mida 2015. aasta lõpus taas levitama hakati.

Olulisemad rahvusvahelised teemad

Kõige olulisemalt küberjulgeolekut mõjutav rahvusvaheline teema oli veebruaris kindlasti FBI ja Apple'i vaidlus selle üle, kas suurfirma peaks looma n-ö „tagaukse" võimaldamaks julgeolekuasutusel minna mööda Iphone 5 turvasätetest ja saamaks ligipääsu telefonis olevatele andmetele. Eesti on juba enne seda vaidlust olnud seisukohal, et „tagauste" loomine võib küll lühiajaliselt olla kasulik terrorismivastases võitluses, kuid pikemas plaanis vähendaks see usaldust krüptograafia vastu ja sellele usaldusele rohkemal või vähemal määral tuginevate e-teenuste vastu, mis omab Eesti jaoks üliolulist väärtust.

Küberjulgeolekuga tegelevad asutused üle maailma jätkasid veebruaris analüüsi sellest, kuidas tekitati pühade-aegsed elektrikatkestused Lääne-Ukrainas, millest olulisim oli juhtimissüsteemidele keskenduva ICS-CERTi teemakohane ülevaade.

Eestis, kus viimase aasta jooksul on samuti aset leidnud mitmed suurt kahju tekitanud lunavara-ründed, tasub kindlasti tähelepanu pöörata Los Angelese ühe haiglaga juhtunule, mis langes veebruari algul lunavara ohvriks. Infosüsteemide vabastamiseks maksis haigla ca $17 000 ja juhtumi käigus seiskus teatud määral ka haigla ravitegevus – ning infovahetuseks oldi sunnitud kasutusele võtma faksid. Võime eeldada, et Eesti suured meditsiinikeskused on veelgi suuremas sõltuvuses IT toimimisest kui see haigla USAs ning Eestis võiks säärane juhtum omada veelgi laiemat mõju, kuna Eestis ilmselt infovahetuse tagamiseks vajalikku kogust faksiaparaate olla ei pruugi.

Tehnoloogiakogukondades leidis veebruaris käsitlemist ka see, kui palju edastab Windows 10 kasutajate kohta infot erinevatesse serveritesse üle maailma – ja seda isegi juhul, kui kasutaja on kõik privaatsust riivavad sätted üritanud miinimumini viia.

Tegevused küberjulgeoleku parandamisel Eestis

RIA juhtimisel viidi veebruaris infoturbe teadlikkuse tõstmiseks koolitus Tartu Ülikooli Kliinikumis. Märtsis jätkuvad sarnased koolitused nii Tartu Ülikooli Kliinikumis kui ka Põhja-Eesti Regionaalhaiglas.

RIA võõrustas Eestis Euroopa Liidu hindamismissiooni eksperte, kes tutvusid laiemalt Eesti kriisireguleerimise ja

hädaolukorraks valmisoleku korraldusega.

9. veebruaril toimus Briti saatkonna korraldatud koostööseminar elutähtsate teenuste ja nende juhtimissüsteemide kaitse teemal, mille raames said Eesti spetsialistid tutvuda UK vastava korraldusega ning sõlmida kontakte UK ettevõtetega, kes sel teemal lahendusi võiksid pakkuda.

23. veebruaril toimus küberturvalisuse infopäev, kus RIA tutvustas Eesti ettevõtetele oma eelseisvaid hankeid, mis tulenevad kübejulgeoleku strateegia elluviimisest. Samuti koguti tagasisidet ettevõtetelt ja audiitoritelt.

Muud olulist

Eesti võtab alates 1. märtsist toodetavatel ID-kaartidel, elamisloa- ja digi-ID-kaartidel kasutusele senisest tugevama krüptograafia. Märtsis algab ka kõigi seni väljastatud kaartide krüptograafia asendamine tugevamaga, uuendamine viiakse lõpule käesoleva aasta jooksul. Koos tugevama krüptograafia kasutuselevõtuga tehakse uuendamise käigus korda ka need 2014. ja 2015. aastal väljastatud kaardid, mille isikusertifikaadid ei vasta suurte tarkvaratootjate oluliselt karmistunud tõlgendusele standarditest. Sertifikaatide uuendamiseks, mis algab märtsis, tuleb arvutisse paigaldada ID-kaardi tarkvara uus versioon, käivitada ID-kaardi haldusvahend ning järgida juhiseid sertifikaatide uuendamiseks.