



RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE JAANUAR 2017

Olukord Eesti küberruumis

Sarnaselt detsembrile jätkus jaanuar Eesti küberruumis sündmusterohkelt. Kuu jooksul registreeris CERT-EE 921 juhtumit, millest intsidendiks kvalifitseerus kolmandik (273). Elutähtsate teenuste osutajaid puudutas 47 juhtumit; neist enamiku moodustasid teavitused pahavaraga nakatunud seadmete kohta sideettevõtjate võrkudes. Pahavara levitavad e-kirjad ja domeenid olid jaanuaris ülekaalukalt suurima osa registreeritud juhtumite põhjuseks.

Kõrge prioriteediga intsidente oli jaanuaris seitse. Elu või tervist ohustanud kriitilisi intsidente ei esinenud.

Tegevused küberjulgeoleku parandamisel Eestis

Tutvustasime osalenud asutustele eelmisel aastal läbiviidud [ISKE](#) (infosüsteemide turvameetmete süsteemi) rakendamise uuringu tulemusi. Valminud on ka uus versioon ISKE rakendusjuhendist, mis arvestab pilvandmetöötuse turvariskidega.

Euroopa Liidu (EL) eesistumise ettevalmistuste käigus korraldasime infoturbekoolitused riigikogu kantselei, riigikantselei, justiits-, sotsiaal- ning majandus- ja kommunikatsiooniministeeriumi töötajatele. Esmakordselt korraldasime sarja venekeelseid koolitusi elutähtsate teenuste osutajatele Ida-Virumaal, et tõsta personali teadlikkust küberriskidest ning parandada suutlikkust intsidente ennetada ning nende tagajärgedega toime tulla.

Alustasime turvaseiresüsteemi prototüübi väljatöötamist elutähtsate teenuste osutajate jaoks, et parandada võimekust küberrünnete ja pahavara avastamiseks viimaste arvutivõrkudes ning võimaldada ohuteadete edastamist. Paranenud ohuteadlikkus ja rünnete varane avastamine aitab vähendada küberrünnetest tulenevat kahju ning maandada teenuste toimepidevuse riske.

Rahvusvaheline keskkond

Endiselt on rahvusvahelise tähelepanu keskses valimisprotsessi küberriskid, kuna Euroopas sel aastal toimuvate üldvalimiste eel on hoogustunud peamiselt Venemaalt lähtuv mõjutustegevus ning ühes sellega küberründed riigiasutuste ja poliitiliste sihtmärkide suunas.

6. jaanuaril avaldasid Ameerika Ühendriikide (USA) [luureametkonnad](#) ühisraporti Vene Föderatsiooni (VF) luureteenistuste küberrünnete kohta USA presidendivalimiste eel. Raporti põhijärelduste kohaselt kujundas VF selge eelistuse Donald Trumpi kui oma eesmärkidele soodsama kandidaadi suhtes. Et tagada viimase edu valimistel, keskenduti vastaskandidaat Hillary Clintoni diskrediteerimisele ja avalikkuse usalduse kahjustamisele USA valimis- ja valitsemisprotsessi suhtes, kombineerides selleks küberrünnete, andmete lekitamist ning riiklikult rahastatud propagandat meedias ning sotsiaalvõrgustikes. Analüüs tõdeb ühtlasi, et VF luureteenistused said juurdepääsu mitme osariigi valimiskomisjonide infosüsteemidele, ent ei kinnita häältega manipuleerimist valimisseadmetes.

Prantsusmaa ja Saksamaa on teatanud [küberrünnete](#) drastiliselt suurenenud arvust riigi digitaalsete taristu vastu viimastel kuudel. Mõlemad on võtnud kasutusele abinõusid valimistega seotud intsidentide ärahoidmiseks, pöörates enam tähelepanu erakondade [teadlikkusele](#) küberriskidest ning otsides [viise](#) libaandiste leviku tõkestamiseks sotsiaalmeedias.

Kuu lõpul [teatas](#) Tšehhi välisministeerium küberspionaažioperatsiooni avastamisest ministeeriumi vastu ning tuhandete kirjade lekkimisest ministri ja kümnete kõrgemate ametnike e-posti kontodelt. Intsident puudutas ministeeriumi välist e-postiserverit, sealhulgas ametkondlikku teavet NATO ja liitlaste kohta; salastatud teabele ligipääsu ei saadud. Kasutatud meetodid ja operatsiooni kestus viitavad uurijate sõnutsi ründe välisriigi päritolule. Tšehhis seisavad sügisel ees üldvalimised. Keeruka [õngitsemiskampaania](#)

sihtmärgiks sattumisest teatas ka Poola välisministeerium; seal õnnestus intsident ära hoida.

Jaanuaris aset leidnud rea värvikate lunavara-juhtumite kõrval [haridus-](#) ja [turismisektoris](#) ning korrakaitseasutustes (nt [politseijaoskond](#) USA Texase osariigis kaotas lunavara tõttu kaheksa aasta ulatuses elektroonilisi tõendeid, mida ei õnnestunud varukoopiatelt taastada) on oluline, et lunavara rakendusala laieneb üha enam ka [nutiseadmetele](#) – nii mobiiltelefonidele kui ka [nn asjade interneti seadmetele](#). Ühtlasi on ilmne, et väljapressimine on end küberkurjategijate jaoks ärimudelina tõestanud ning krüptolunavara kõrval kasutatakse nii [teenustökestusründeid](#) kui ka andmevargust, nõudmaks ohvrilt raha ründe lõpetamiseks või andmete [avaldamisest](#) hoidumiseks.

Muud olulist

Jaanuari alguses suurendas Riigi Infosüsteemi Amet kauguuendatavate ID-kaartide hulka, eesmärgiga paigaldada ID-dokumentidele tugeval krüptograafial põhinev sisu. Juhised sertifikaatide uuendamiseks leiab RIA [kodulehelt](#) ning amet soovib uuenduse ära teha 2017. a esimese poolaasta jooksul. Uuendamist vajavate ID-kaartide koguarv ulatub praeguseks ühe miljoni ni.