RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE DETSEMBER 2017

Olukord Eesti küberruumis

Aasta viimane kuu oli küberturbesündmuste poolest tavapäraselt aktiivne – CERT-EE registreeris Eesti küberruumis 924 sündmust, millest küberintsidente oli veidi alla kolmandiku ehk 283. Kõrge prioriteediga juhtumeid oli detsembris seitse ja ühiskonna jaoks oluliste teenuste osutajaid puudutas 56 juhtumit.

Detsembris registreeritud intsidentidest kõige laialdasema kõlapinnaga oli kahtlemata lahtimurtud paroolide andmebaasi avaldamine tumeveebis. Lisaks eestlaste kasutajakontodele LinkedIni, Twitteri, DropBoxi, Google'i jpt keskkondades sisaldas andmebaas ka pea 200 000 .ee-meiliaadressi koos avateksti parooliga; neist 2830 olid Eesti avaliku sektori ja ca 2587 elutähtsa teenuse osutajate meiliaadressid. Puudutatud teenuseosutajatega võttis RIA ka enne info avalikustamist ühendust, et identiteedivarguse riski minimeerida.

Teist kuud järjest on Eestis languses **lunavara** levik, kuid liikvel oli uus, peamiselt reklaamkirjade ja võltsuuenduste kaudu leviv lunavara, mille jaoks veel dekrüpteerimisvõimalust ei ole. Endiselt levib ka trend kasutada kehva turvalisusega veebilehti ära veebikülastajate arvutiressursi abil **krüptoraha kaevandamiseks** – detsembris tuvastas CERT-EE monitooring selliseid intsidente 12.

Tegevused küberjulgeoleku parandamisel Eestis

5.-6. detsembril toimus Sagadis MKMi eestvedamisel korraldatud **küberjulgeoleku strateegia seminar**, mis tõi kokku Eesti küberjulgeoleku tagamisse panustavate osaliste esindajad riigi- ja teadusasutustest ning erasektorist. Mõttetalgute eesmärk oli sõnastada ühine arusaam Eesti küberturvalisuse ees seisvatest peamistest väljakutsetest ning prioriteedid järgmisel strateegiaperioodil. RIA aitas kaasa seminari sisustamise ja arutelude läbiviimisega.

7.-8. detsembril korraldas CERT-EE traditsioonilise **Admin@gov** seminari avaliku sektori infoturbejuhtidele, eesmärgiga jagada teavet aktuaalsetest teemadest ja toetada kogukonna-sisest infovahetust.

Lõppes **küberturvalisuse seaduse** (KüTS) eelnõu ametlik kooskõlastusring. Olulisemad muudatused eelnõus seisnevad erisuses neile Kaitseministeeriumi valitsemisala infosüsteemidele, millele rakenduvad NATO vm rahvusvahelised kokkulepped, täpsustustes RIA rakendatavate erimeetmete osas ning perearstide väljajätmises seaduse rakendusalast.

Eesti ELi eesistumise lõpuks saavutati liikmesriikide heakskiit ELi **küberstrateegia tegevuskavale**, mis tagab mehhanismi Nõukogu novembrikuiste järelduste elluviimiseks. Töövõiduks tuleb kahtlemata lugeda, et selles sisalduv – elutähtsate teenuste küberturvalisus (NIS direktiivi rakendamise näol), küberõppused, püsiva ja tugeva mandaadiga ENISA, teadlikkuse tõstmine, võimearendus jt – vastab selgelt eesmärkidele, mille eest Eesti ELis aastaid on seisnud.

Rahvusvaheline keskkond

Kuu alguses maailma tähelepanu köitnud **välispoliitilised sündmused** ei jäänud taas reaktsioonita ka küberruumis. Vastusena USA otsusele tunnustada Jeruusalemma Iisraeli pealinnana avaldas häkkeriliikumine Anonymous nimekirja USA ja Iisraeli valitsusasutustest, kutsudes mõttekaaslasi nende vastu küberrünneid korraldama. #OpIsrael kampaania raames oli Anonymous detsembri keskpaigaks teatanud edukast ründest kümmekonna Iisraeli organisatsiooni (sh kolme riigiasutuse) veebi vastu, samuti avalikustati hulga riigiametnike e-posti kasutajatunnused ja salasõnad. Väidetavalt osutusid edukaks ka USA asutuste vastased ründed, mille ohvreid Anonymous ei avalikustanud. Kuni USA saatkonna kolimine ei ole lahendatud, võib oodata rünnete aeg-ajutist hoogustumist, eriti seoses iga-aastase Iisraeli-vastase küberkampaania päevaga aprillis.

Anonymous võttis vastutuse ka Brasiilias detsembri algul aset leidnud andmelekke eest, milles – väidetavalt reaktsioonina venivale korruptsiooniuurimisele – avalikustati avaliku sektori sidevõrkude detailne topoloogia, sh ruuterite ja tulemüüride konfiguratsioon ning juurdepääs politsei ja elutähtsate teenuste osutajate serveritele. Juhtum näitab, et ehkki Anonymoust teatakse küber-aktivistiliikumisena, on nad endiselt suutelised poliitiliselt tundlike teemade ümber vägagi professionaalselt organiseeruma.

Saksamaa luureteenistus (BfV) hoiatab järjest aktiivsema **Hiina päritolu küberspionaaži** eest eeskätt professionaalidele mõeldud sotsiaalvõrgustike kaudu. Kontakti otsitakse nt teaduskoostöö, ärisuhte või talendiotsingu ettekäändel ning vahetuks sihtmärgiks on peamiselt üksikisikud, kuid ründajate siht on usaldatud kontakti staatuse saavutamine, et kompromiteerida pahavara abil huvipakkuvate organisatsioonide sisevõrke ning seeläbi dokumente varastada ja liiklust pealt kuulata. Samal põhjusel otsitakse kliendisuhteid asutuste IT-personaliga.

USA küberturbeettevõtte CrowdStrike detsembri lõpul avaldatud raport hoiatab samasuguse suundumuse eest. Varasemad Hiina päritolu juhuslikku laadi ründed, mis keskendusid hõlpsasti kättesaadava teabe vargusele, on asendunud oluliselt täpsemini sihitud kampaaniatega; ka on 2017. aasta teises pooles märgatavalt kasvanud rünnete hulk. Kui varem kulus Hiina põhitähelepanu Kagu- ja Ida-Aasia riikidele, siis järjest enam on sihtmärkide seas lääneriikide adressaadid. Eraldi sihtmärgiks on mõttekojad ja valitsusasutuste lähedased MTÜd.

19. detsembril tegi USA valitsus ametliku avalduse, milles teatas, et peab Korea RDV-d vastutavaks WannaCry lunavararünnete eest 2017. aasta mais. **WannaCry omistamise** alusena viitas Valge Maja USA ametkondade ja erasektori (sh Microsoft ja küberturbeettevõtted) koostöös kogutud tõenditele, mis kinnitavad ründe tööriistade ja -võtete ning kasutatud infrastruktuuri kattuvusele Põhja-Korea varasemate küberoperatsioonidega. USA seisukohaga WannaCry omistamisest ühinesid ka Ühendkuningriik, Austraalia, Kanada, Uus-Meremaa ja Jaapan.

USA rõhutas, et tegemist oli valimatu küberrünnakuga, mis kahjustas nii ettevõtjaid, riigiasutusi kui ka eraisikuid ning seadis lisaks varale ohtu ka inimeste elu ja tervise. Valge Maja märkis, et rünnete omistamine ei ole Põhja-Korea vastutusele võtmisel viimane samm ning USA teeb koostööd teiste riikide ja ettevõtjatega küberriskide maandamiseks ja rünnete kulukuse suurendamiseks – selleks on suured tehnoloogiaettevõtted nagu Microsoft ja Facebook teinud kahjutuks Põhja-Korea küberrünnete tööriistu, tõkestanud nende operatsioone süsteemide turvapaikamisega ja sulgenud kasutajakontosid, mida rünnete toimepanemiseks kasutati.

Nende oluliste uudiste kõrval said vähem tähelepanu mitmesugused **finantssektori** küberründeid, mille sihtmärgiks kommerts- ja keskpankade kõrval on üha sagedamini krüptorahateenused ning mille toimepanemiseks kasutatakse järjest aktiivsemalt ka mobiilirakendusi. Nii näiteks leiti Google Play poest Poola pankade kasutajaandmeid õngitsevaid rakendusi, mis kuvasid kasutajale ehtsaga sarnaseid sisselogimisvorme ning olid suutelised pealt kuulama ka kaheastmeliseks autentimiseks saadetud SMS-sõnumeid. Ühes Bitcoini jt **krüptovaluutade** kursitõusuga on kasvanud huvi krüptorahaärist kuritegelikku tulu saada. Peamiselt andmepüügi kaudu varastatud kontoandmete abil rünnatakse nii krüptorahaettevõtteid, krüptovaluuta börse kui krüptoraha kaevandamise teenuseid. On selgeid märke, et oma tegevusampluaad on krüptorahale laiendanud ka Põhja-Korea, kes viimase paari aasta jooksul on väga aktiivselt rünnanud just pangandussektorit.

Ehkki enamik **lunavaratööriistu** sihib endiselt MS Windows süsteeme, on märgatavalt tõusnud **mobiilseadmete** ründamiseks mõeldud lunavararakenduste levik. 2017. aasta jooksul on tumeveebis tuvastatud üle 5000 Androidi lunavararünde komplekti, nende keskmine hind jääb paarisaja dollari kanti. Ka mobiiltelefoni puhul on lunavaranakkuse vältimiseks abi süsteemi- ja tarkvarauuenduste paigaldamisest, ent suur osa kasutajaid ei tee seda kogu telefoni kasutusea jooksul kordagi.