RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE JUULI 2017

Olukord Eesti küberruumis

Eesti küberruumis registreeriti juulis 798 juhtumit, millest 242 olid küberturbeintsidendid.

Avaliku sektoriga oli seotud 85 juhtumit ja (senise käsitluse järgi) elutähtsa teenuse osutajaid puudutanud juhtumeid oli juulis kokku 46. Võrreldes möödunud aasta keskmisega on kaks korda kasvanud elutähtsa teenuse osutajaid puudutavate juhtumite arv; põhjuseks eeskätt aktiivsem teavitamine ja tõhusam monitooring.

18. juuli hilisõhtul saadeti hulgale adressaatidele kahes riigiasutuses Ursnif nn pangatroojalasega nakatunud manusega e-kiri. Ursnif varastab pangakontonumbreid, krediitkaardiandmeid ja *online* sisselogimisandmeid. Asutuste antiviiruseprogramm tuvastas pahavara ja kahju ei tekkinud. Küll on see aga meeldetuletus, et Eesti asutused on endiselt ründajatele atraktiivsed sihtmärgid ning siinsete asutuste vastu suunatud kampaaniad on üha keerukamad.

15. juulil langes lunavara ohvriks Tallinnas asuv perearstikeskus. Krüpteeritud 3985 faili lahtilukustamise eest nõuti 1,5 *bitcoini* (ca 3420€) lunaraha. Kuigi andmed olid varundatud, ei saadud neid tehnilise vea tõttu kasutada ja otsustati maksta lunaraha. Paraku annab lunaraha maksmine ründajale positiivse sõnumi ründamise tulususest ja on riskantne ka seetõttu, et andmete tagasisaamine ei ole garanteeritud. Juhtunu on järjekordne näide, et sarnaselt teistele arenenud riikidele on ka Eesti meditsiinisektor küberrünnetele haavatav.

Teavitamata hooldustöödest tingitud teenusekatkestused põhjustasid mitmel juhul asjatut tööd nii CERT-EEle kui teenusepakkujale. Plaanilistest hooldustöödest informeerimine säästab nii CERT-EEd vajadusest näilise intsidendi tekkepõhjust välja selgitada kui ka teenusepakkujat asjatust päringutele vastamisest.

Tegevused küberjulgeoleku parandamisel Eestis

Jätkub küberturvalisuse seaduse eelnõu koostamine, milles sätestatakse ühiskondlikult oluliste teenuste turvanõuded ja pädeva asutuse õigused koordineerida küberintsidentide ennetamist, tuvastamist ja lahendamist. Seadusega võetakse Eesti õigusesse üle Euroopa Liidu võrgu- ja infoturbe direktiiv. Eelnõu jõuab ministeeriumitevahelisele kooskõlastusringile sügisel.

Jätkusid ka kohtumised ettevõtjatega, et arutada koostööd elutähtsate teenuste küberturvalisuse parandamiseks. Samuti konsulteeris RIA ettevõtjaid juulis jõustunud uue hädaolukorra seaduse rakendamisel.

RIA on olnud üheks eestvedajaks ELi liikmesriikide küberturbeintsidentide käsitlemise üksuste võrgustiku (NIS direktiiviga loodud *CSIRT Network*) käimalükkamisel ning infovahetuse parandamisel. Tõhustunud koostööst annab tunnistust reageerimine Petya/Not Petya kampaaniale, kus CERT-EE koos viie riigi partneritega tagas operatiivse teabe edastamise lunavara mõjust ja levikuvektorist ning juhised intsidentide ennetamiseks ja lahendamiseks.

Rahvusvaheline keskkond

Ohtrat rahvusvahelist meediatähelepanu pälvisid jätkuvalt **Petya/NotPetya küberründe järelmid.** Ehkki võrreldes WannaCryga levikult piiratum (ohvritest 70% asusid Ukrainas), oli selle majan-

duslik mõju ohvritele märkimisväärne. FedExil ja Taani transpordiettevõttel Maersk kulus rohkem kui kuu oma infosüsteemide tavapärase töö taastamiseks ning osa FedExi andmekaost on ettevõtte teatel jääv; Maersk on kahju suuruseks hinnanud kuni 300 miljonit dollarit. Tervise- ja hügieenitoodete hiiu Reckitt Benckiseri hinnangul mõjutavad intsidendist põhjustatud tarnehäired märgatavalt ettevõtte aastatulemusi.

Mitme allika hinnangul sarnanes pahavara käekiri Ukrainas 2016. aasta detsembris elektrijaamade vastu korraldatud küberründega. Ukraina julgeolekuteenistuse väitel viitavad kogutud faktid Vene eriteenistuste osalusele; rahvusvahelise ekspertkogukonna valdav seisukoht on, et ründe tegelik eesmärk oli võimalikult suure kahju tekitamine ja lunarahanõue oli vaid kattevari.

Nii Petya/NotPetya kui WannaCry kasutasid ära sama Microsoft Windows tarkavarahaavatavust ning oodata on, et nende juhtumitega oht ei piirdu. Microsoft väljastab sügisel Windows 10 operatsioonisüsteemile turvauuenduse kaitsemehhanismiga seesuguste rünnete vastu. Turul kaugelt enim levinud Windows 7 süsteemidele, mis moodustasid ka lõviosa Petya/NotPetya ohvritest, see siiski kaitset ei paku.

USA teatas **üheaegsest suunatud küberründest USA elektrijaamade vastu**. Ründevahendina kasutati pahavara alla laadivaid e-kirju, mille abil saadi juurdepääs vähemalt tosina ettevõtte kontorivõrgule, nende seas ka Kansases paiknev Wolf Creeki tuumajaam. Vähemalt ühel juhul tuvastati tootmise eest vastutava töötaja kasutajaandmete vargus.

Oletatakse, et intsidendid võivad olla seotud hiljutise sissemurdmisega energiatööstuses kasutatavate seadmete kontrollsüsteeme tootva ettevõtte infosüsteemidesse. Mõlema ründe eest arvatakse vastutavat välisriigi heaks töötavad häkkerid ning peamine kahtlusalune on Venemaa, ent selget kinnitust kahtlusele pole.

Ehkki intsidendid ei mõjutanud vahetult energiatootmist ega energiavõrkude toimimist laiemalt, suurendab kontorivõrgule juurdepääsu saamine tootmissüsteemide haavatavust. Energiatootmist korraldavad süsteemid on küll eraldatud eraldi võrgusegmenti, aga ligipääs kontorivõrgus töödeldavale teabele tootmise korralduse ja riskide kohta (kirjavahetus, taristu dokumentatsioon jne) hõlbustab hilisema ründe ettevalmistamist. Konkreetsel juhul viitas pahavara disain häkkerite eesmärgile võrke kaardistada ja leida viis tootmissüsteemidele juurdepääsuks. Sama grupeeringut seostati ka kevadsuvel toimunud rünnetega energiatootjate vastu Ühendriikides, Iirimaal ja Türgis.

Kuu lõpul sai avalikuks **Rootsi ajaloo suurim avaliku sektori andmeleke**. 2015. aastal anti transpordiameti andmekogude haldamine hankega üle kahele Tšehhi ja Serbia ettevõttele ning transpordiameti andmebaas laaditi nende kahe ettevõtte pilveteenusesse. Alles 2016. aastal sai teatavaks, et andmete seas oli ka salastatud teavet ning transpordiamet oli lepingut sõlmides eiranud salastatud teabe kaitse nõudeid. Muu hulgas sisaldas andmebaas tunnistajakaitse programmi osaliste, õhuväe pilootide ja kaitseväe erioperatsioonide üksuse liikmete nimesid, fotosid ja elukohaandmeid; samuti sisaldus seal detailne teave valitsuse ja kaitseväe sõidukite ning riigi maanteede ja sildade kandevõime kohta. Lisaks pääses Serbia ettevõte ligi andmesideliiklusele Rootsi valitsusasutuste vahelises salastatud teabe võrgus, millega on liidestatud ka ELi STESTA turvaline andmesidevõrk.

Juhtum vallandas Rootsis valitsuskriisi, mis päädis sise- ja taristuministrite väljavahetamisega. Uurimine selgitab välja, kuivõrd said volitamata isikud juurde ELi salastatud teabe võrgule. Serbia ettevõttel ei olnud salastatud teabe töötlemise luba ning töötajad ei olnud läbinud julgeolekukontrolli, Serbia puhul teeb eraldi muret asjaolu, et tegemist on Venemaa sõjalise liitlasega.

Transpordiamet korraldab andmete töötlemise ümber, aga muudatusi ei tehta enne sügist ning seni on andmebaas jätkuvalt välisfirmade hallata.

Sagedaste pangandussektori küberrünnete kõrval on tõusuteel **krüptorahaga seotud pettused**. Juulis leidis paarinädalase ajavahemiku jooksul aset koguni neli mastaapset krüptoraha varguse juhtumit, mille summaarne kahju oli üle

48 miljoni USD. Kõigil juhtudel rünnati erinevaid krüptorahaga kauplemise platvorme, mitte krüptograafiliselt turvatud valuutat ennast.

WikiLeaks avaldas taas kord salastatud teavet **USA Luure Keskagentuuri** kübertööriistade ja meetodite kohta – seekordne kogum oli 17nes.