RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE JAANUAR 2018

Olukord Eesti küberruumis

Aasta esimese kuu jooksul ületas CERT-EE registreeritud juhtumite arv tuhande piiri (1045). Küberintsidentide osakaal oli sellest samas vaid viiendik (220), mis on viimase aasta madalaim näitaja. Üle poole intsidentidest põhjustas taas erinevat tüüpi pahavara. Endise aktiivsusega levib veebilehtede nakatamine, et külastajate arvutite abil krüptoraha kaevandada – jaanuaris registreeriti seitse sellist intsidenti, sh Äripäeva veebilehel kuvatud reklaambänneris. Keskmisest rohkem registreeriti jaanuaris ka näotustamisjuhtumeid ja teenusekatkestusi.

22. jaanuaril 2018 peatus Circle K **tanklaketi** automaatjaamade töö rahvusvahelise sidekatkestuse rikke tõttu.

24. jaanuaril 2018 ajavahemikul 09.50–18.45 ei olnud umbes pooltel Elisa võrgus olnud inimestel võimalik helistada **hädaabinumbritele** 112 ja 110. Ebaõnnestunud hädaabikõnedele kõlas vastus "number ei ole kasutusel". Intsidendi põhjustas inimlik eksitus. Järeldusena juhtumist andsime elutähtsate teenuste osutajatele soovitused lisaprotsesside rakendamiseks oluliste teenuste arenduse või hoolduse puhul, kui tegevusest sõltub mõne muu olulise teenuse osutamine.

Tegevused küberjulgeoleku parandamisel Eestis

RIA ja Eesti infoturbeettevõtteid koondav Eesti Infoturbe Assotsiatsioon allkirjastasid **koostööleppe ettevõtete ning teadus- ja riigiasutuste vahelise koostöö** raamistamiseks ja edasiseks arendamiseks. Detsembris asutatud infoturbe assotsiatsiooni liikmeteks on Eesti suuremad kübervaldkonna ettevõtted Cybernetica ja Guardtime; liitumisest on teada andnud ka Tartu Ülikool ja Tallinna Tehnikaülikool.

Eesti initsiatiivil ja juhtimisel käivitus NIS direktiivi (ELi võrgu- ja infoturbedirektiiv) koostöögrupi raames **valimistehnoloogia küberturvalisuse** töövoog, milles praegu osaleb 13 riiki. Eesmärk on anda riikidele paindlik juhiste kogum, mis aitaks paremini toime tulla valimiste küberriskidega – tehnoloogilistest kuni mainerünneteni. Lisaks valimiste küberturvalisuse töösuunale veab Eesti NIS direktiivi töövoogu piiriüleste sõltuvuste riskide haldamise teemal.

31. märtsini saab uuendada neid ID-kaardi sertifikaate, mis turvariski tõttu novembris peatati. 1. aprillist uuendamata sertifikaadid tühistatakse ja kaardiomanikel, kes soovivad ID-kaarti edaspidi elektrooniliselt kasutada, tuleb taotleda uus dokument. Jaanuari lõpu seisuga oli oma kaardi uuendanud üle 400 000 inimese.

Rahvusvaheline keskkond

Erakordselt palju meediatähelepanu said aasta alguses ilmsiks tulnud **Spectre ja Meltdown** turvanõrkused. Tegu on kahe eraldiseisva turvaveaga protsessorite arhitektuuris, mis mõlemad avalduvad üsna sarnaselt – tarkvara võimaldab „pealt kuulata" üheaegselt töös olevaid protsesse ning selle kaudu varastada seadme mälus leiduvat tundlikku infot (paroole, sisselogimisvõtmeid, ketta vahemälus leiduvaid faile jmt). Viga muudab haavatavaks praktiliselt kõik laua-, sülearvutid ning nutitelefonid, operatsioonisüsteemist sõltumata. Jaanuari jooksul andsid seadmete ja operatsioonisüsteemide tootjad ridamisi välja turvaparandusi, ent nendega kaasnes uus häda – arvutid muutusid talumatult aeglaseks või lakkasid sootuks töötamast, kuni selleni, et Microsoft andis kuu lõpus välja erakorralise uuenduse osade juba väljastatud turvapaikade blokeerimiseks, sest need panid süsteemid ettearvamatult käituma. Kuu lõpuks oli 75% kõigist seadmetest endiselt kaitseta, st uuendamata, ja eksperdid hindavad, et haavatavus jääb levinuks – ja rünnatavaks – veel aastateks. RIA soovitused turvanõrkuste parandamiseks ühes viidetega turvapaikadele leiab RIA kodulehelt.

Twitter alustas nende kasutajate teavitamist, kes USA presidendivalimiste eel Vene propaganda lõksu langesid. Peterburi **trollifarmina** tuntud Internet Research Agency libakontode järgijate arv küündis pea 680 000ni; libakontosid endid on praeguseks teada ligi 3800 ehk märksa enam kui Twitterile sügisese USA Kongressi kuulamise ajaks teada oli. Kokku tootsid libakontod valimiskampaania eel pea 170 000 postitust, mida lisaks edasisäutsujatele levitati poolesaja tuhande automaatpostitava konto abil. Twitteri kinnitusel on avastatud libakontod nüüdseks suletud, mis tähendab aga, et kasutajad ei saa enam kontrollida, mille õnge nad täpselt läksid. Üks „demokraatia häkkimise" järelmistest USAs on seegi, et rühm demokraatidest ja vabariiklastest senaatoreid esitas Kongressi menetlusse seadus-eelnõu valimiste turvalisuse parandamiseks. Selle ettepanekud hõlmavad mh praeguste elektrooniliste hääletusmasinate käibelt kõrvaldamist ja valimisjärgseid auditeid.

Hollandi vastuluurel (AIVD) oli vähemalt aastajagu juurdepääs Cozy Bearina tuntud ja Vene Föderaalse Julgeolekuteenistusega seostatud **APT29 rühmituse** infosüsteemidele, sh valvekaameratele, väidab Hollandi meedias avaldatud uurimusluqu. AIVD jälgis Vene häkkerirühmituse kasutatavaid ruume, isikkoosseisu ja käitumist ning tuvastas rühmituse sissemurdmiskatsed USA välisministeeriumi ja Valge Maja infosüsteemidesse. Raporti kohaselt informeeris AIVD rünnetest USA riiklikku julgeolekuteenistust, kellega tehti lähedast koostööd ründeoperatsiooni tõkestamiseks.

Paar päeva pärast häkkerirühmituse tegevust kajastava raporti avaldamist sattusid Hollandi maksuamet ja kommertspangad koordineeritud teenustõkestusrünnete alla, mis lühiajaliselt peatasid juurdepääsu maksuameti veebilehele ja digitaalsetele teenustele.

Jaanuari lõpul toimunud Davosi majandusfoorumil avaldas Taani laevandushiiu Maersk juhatuse esimees, et ettevõte paigaldas **NotPetya lunavararündest** taastumiseks kümne päeva jooksul uuesti sisuliselt kogu ettevõtte infosüsteemi – 4000 serveri ja 45 000 arvuti kogu tarkvara. Maersk on maailma suurim merelaevandusettevõte, kes veab viiendiku kogu maailma merekonteineritest.

Norra suurima, kagupiirkonna **terviseameti andmebaasidest** lekkisid 2,9 miljoni elaniku ehk üle poole rahvastiku terviseandmed. Norra tervishoiusektori CERT avastas kahtlase liikluse jaanuari alguses ja teavitas sellest terviseametit, kes kinnitas intsidenti. Juhtumi uurimiseks on antud lisaressursse ja selle kohta on algatatud kriminaalasi kriminaalseaduse sätte alusel, mis käsitleb luuretegevust salastatud teabe vastu. Ründe päritolu kohta seni kinnitust ei ole, ent ametkonnad on avaldanud, et tegu oli koordineeritud ja oskusliku operatsiooniga. Terviseameti murettekitavast infoturbeolukorrast kirjutas Norra meedia mullu suvel. Praeguse intsidendi kohta levib teateid, et ründajad otsisid süstemaatiliselt teavet Norra kaitseväelastele osutatud meditsiiniteenuste kohta seoses NATO Trident Juncture õppusega 2018. aasta oktoobris.

Google'i 2011. aastast pakutava **kaheastmelise autentimise** (2FA) on seadistanud alla 10% Google'i teenuste kasutajatest. Google on 2FA kasutusmugavust oluliselt suurendanud, ent on hoidunud seda kohustuslikuks muutmast, peljates mõju kasutajate käitumisele. Õngitsustest ja pettustest, mille vastu kaheastmeline autentimine aitab, on juttu RIA blogis, kust leiab ka juhised 2FA seadistamiseks eri teenustes.