RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE VEEBRUAR JA MÄRTS 2018

Olukord Eesti küberruumis

Veebruaris registreerisime taaskord üle tuhande juhtumi (1034), mis jäi paari juhtumi võrra alla jaanuarile (1045). Samuti jäi samale tasemele küberintsidentide osakaal – moodustades ligikaudu viiendiku (233) juhtumitest – see on sarnane ka eelmise aasta trendiga. Üle poole intsidentidest põhjustas taas erinevat tüüpi pahavara. Endise aktiivsusega levib veebilehtede nakatamine eesmärgiga **kaevandada külastajate arvutite abil krüptoraha**, sh tuvastasime kaevandamisele omast liiklust ühe omavalitsuse ja haigla võrgus. Lisaks levis Facebookis R-Kioskit jäljendav petuskeem, kus lubati kinkekaarte küsitlusele vastanutele, kuid tegelikkuses suunati kasutajad krüptoraha kaevandavatele veebilehtedele.

Märtsis registreerisime juhtumeid 1350, mis on eelmise aastaga võrreldes jällegi rohkem (1221), kuid samas on ka see kuu intsidentide arv (271) jäänud käesoleval aastal madalale tasemele võrreldes varasema aastaga. Kahe eelmise kuuga on vähenenud näotustamisjuhtumeid, kuid kasvanud on kompromiteerumis-, finantspettus- ja teenusekatkestusjuhtumid. Sealjuures lekkisid taaskord **kasutajaandmeid**, mis puudutas ka Eestit. Samuti täheldasime, et viimasel kahel kuul suurenes valesti seadistatud veebirakenduse vahemäluteenuse (*memcache*) **ärakasutamine teenusetõkestusrünnete peegeldamiseks ja võimendamiseks**.

Tegevused küberjulgeoleku parandamisel Eestis

6. veebruaril tähistati **turvalise interneti päeva** teemal „Loo, suhtle ja jaga hoolivalt – parem internet algab Sinust“, kus tõstatati interneti suhtluskultuuri valukohti ja otsiti võimalikke lahendusi. Ürituse raames andsime välja turvalise inernetikäitumise põhireeglid.

Veebruaris saavutati **tehniline valmisolek vahetada X-tee kaudu andmeid Eesti ja Soome vahel**. X-tee ühildamine teeb asjaajamise kahe riigi vahel võimalikult mugavaks ning esialgsete asutuste seas on mõlema riigi haigekassad, maksu- ja tolliametid, liiklusregister ning rahvastikuregister.

Samuti avaldasime eelmise aasta lõpus tellitud **krüptouuringu**, mis annab ülevaate krüptograafia hetkeseisust keskendudes krüptoalgoritmidele, ID-kaardi intsidendile, plokiahelatele ja rakenduskrüptograafia ülevaatele. Soovitame seda lugeda infoturbega tegelevatel ekspertidel ja krüptograafia huvilistel.

Veebruaris **andsime välja ka uue ID-kaardi rakenduse DigiDoc 4**, mida on mugavam kasutada – varasema kolme rakenduse asemel piisab ühest. Sellegi poolest tuleb rõhutada, et tegu on alles beetaversiooniga ning hetkel on seda võimalik kasutada ainult Windows operatsioonisüsteemis. Ootame kasutajatelt ettepanekuid ja tagasisidet kuni 1. juunini.

1. märtsil kiitis **Vabariigi Valitsus heaks küberturvalisuse seaduse eelnõu** ning esitas selle Riigikogu menetlusse. Eelnõu **eesmärk** on tugevdada ühiskonna jaoks oluliste teenuste ning riigi ja kohaliku omavalitsuse üksuste võrgu- ja infosüsteemide kaitset. Eelnõu **kehtestab** oluliste teenuste osutajate kohustused võrgu- ja infosüsteemide turvalisuse tagamisel ning olulistest küberintsidentidest ja -ohtudest teavitamise korra. Samuti täpsustab see Riigi Infosüsteemi Ameti ülesandeid küberturvalisuse tagamise koordineerimisel ja piiriülese koostöö korraldamisel. Eelnõu Riigikogu menetlusse võtmise stenogramm on kättesaadav siit ja eelnõu etappi saab jälgida siit.

Märtsiga lõppes võimalus uuendada turvariskiga ID-kaardi sertifikaate. Kokku uuendati 494 000 kaarti, mis on 95% elektrooniliselt kasutatud kaartidest. Alates 1. aprillist on uuendamata sertifikaadid tunnistatud kehtetuks ning ID-kaardi elektrooniliseks kasutamiseks tuleb taotleda uus dokument ja tasuda riigilõiv.

Vastavalt aasta alguses levinud küberintsidentide trendidele koostasime **juhise pettuskeemi vältimiseks** ning **lühijuhendi teenustõkestusrünnete ennetamiseks ja lahendamiseks**. Juhendiga soovitame tutvuda asutuse infoturbe tagamisega seotud tehnilisel personalil.

Rahvusvaheline keskkond

Suurbritannia, **USA**, **Eesti** ja **Austraalia** valitsused andsid välja avalduse, milles **süüdistavad Venemaa valitsust ja sõjaväge** 2017. aasta juunis laialdaselt levinud pahavarakampaania **NotPetya korraldamises**. Rünnak oli suunatud Ukraina valitsuse ning finants- ja energiasektori vastu, mille mõju avaldus ka paljudes teistes riikides. Eelmise aasta lõpus omistasid USA, Suurbritannia, Austraalia, Kanada, Uus-Meremaa ja Jaapan 2017. aasta mais toimunud lunavarakampaania WannaCry Põhja-Koreale.

Taliolümpiamängude avatseremooniaga 9. veebruaril alustati ka **küberrünnakutega mängude korraldajate vastu**: ametlik veebileht võeti maha, pileteid ei saanud printida ning üritust kajastavatele ajakirjanikele mõeldud WiFi võrguühendus oli katkestatud jne. Arvatakse, et rünnakud võisid olla reaktsiooniks Rahvusvahelise olümpiakomitee otsusele peatada Venemaa liikmelisus dopinguskandaali pärast, mistõttu Venemaa sportlased ei saanud oma riigi lipu all osaleda. Ka varasemalt on täheldatud küberrünnakuid suurspordisündmuste vastu, kuid siis olid ründajateks organiseeritud küberkurjategijad või häktivistid eesmärgiga teenida raha või levitada oma poliitilist sõnumit.

Märtsis andsid USA sisejulgeolekuministeerium (DHS) ja FBI välja **ühisavalduse**, kus kirjeldavad **Vene Föderatsiooni korraldatud küberrünnakuid USA institutsioonide ja kriitiliste infrastruktuuri sektorite (energia, tuuma, vee, lennu, tööstus jne) vastu.** Avalduse eesmärk on tõsta teadlikkust Venemaale omastatavast tegevusmustrist, mis aitaks teistelgi kontrollida ja tuvastada pahatahtlikku tegevust. Ründes kasutatakse nii kompromiteeritud emaililt saadetud kalastuskirju, kasutajainfo kogumist, avalikest allikatest eelteabe kogumise ärakasutamist ründe korraldamisel jpm. Venemaa eitab süüdistusi.

Inglise ettevõte **Cambridge Analytica**, mis tegeleb andmeanalüüsi ja poliitiliste konsultatsioonide pakkumisega, väärkasutas Facebooki programmiliidest ning **kogus loata kasutajate andmeid**, kokku ligikaudu 50 miljoni isiku kohta, neist oli Eesti kasutajaid 5510. Kogutud infot kasutati suunatud reklaami edastamisel, mis sisaldas tellijale sobivat (poliitilist) sõnumit. Ettevõtte teenuseid rakendati ka näiteks USA presidendi Donald Trumpi kampaanias. Skandaali valguses kutsuti Facebooki looja Mark Zuckerberg juhtunust aru andma nii Suurbritannia ja USA kui ka Euroopa Parlament.

Lisaks tuvastati märtsis Demokraatide Rahvuskomitee (DNC) infosüsteeme häkkinud **Guccifer 2.0 isik GRU ohvitserina**, kui viimane unustas sotsiaalmeedia kontot külastades sisse lülitada VPNi.