RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE APRILL 2018

Olukord Eesti küberruumis

Aprillis registreerisime küberruumis 1264 juhtumit, mis on ligi kolmandiku võrra rohkem eelmise aasta aprillikuust (781). Ka intsidentide arv (303) ületas eelmise aasta aprillikuud (188) märkimisväärselt. Kasvas kompromiteerumiste-, kalastamiste ja pahavaraga seotud intsidentide arv. Pahavarast tuvastasime enim troojalasi (vawtrak) ja märkasime varasemast rohkem nuhkvara Pony. Pärast Oracle'i tarkvara kriitilise turvapaiga avalikustamist nägime **tõusu võrguskaneeringutes** eesmärgiga leida nimetatud turvanõrkust pahatahtlikul eesmärgil. Teavitasime seotud osapooli võrguskaneeringutest.

Aprilli algul ei saanud ligi kahe tunni jooksul **mobiil-IDga siseneda internetipankadesse ja teistesse e-teenustesse ega digitaalselt allkirjastada**. Mõju ID-kaardi kasutamisele oli minimaalne.

19. aprillil **plahvatas Maa-ameti serveriruumis katkematut elektrivarustust tagav seade UPS**, mis asus Keskkonnaministeeriumi Infotehnoloogiakeskuse (KEMIT) serveribaasis. Plahvatuse järel katkes Keskkonnaministeeriumi valitsemisala kõigi infosüsteemide töö. 21. aprilli pärastlõunaks oli kõigi katkenud teenuste töö taastatud.

Aprilli lõpus avaldas turvateadlikkusele tähelepanu pöörata sooviv isik ligi 215 000 Eesti **internetikasutaja konto ja paroolidega andmebaasi**, mis on kogum eri ettevõtetest ja e-teenustest aastail 2004–2017 lekkinud andmetest. Avaldasime uudise detsembris ning teavitasime kõiki riigiasutuste ja elutähtsatsate teenuste osutajaid, kelle paroolid suurest andmebaasist tuvastati.

Tegevused küberjulgeoleku parandamisel Eestis

Tellisime **ID-kaardi kriisi õppetundide kaardistamiseks** TTÜ uurimisgrupilt analüüsi, mis täiendas seniseid järeldusi ja arutelusid PPAga. Analüüsi tulemid vaatlevad ID-kaardi ökosüsteemi, kriisijuhtimist, osapoolte rolle ja mandaati ning pakuvad välja ettepanekuid tulevikuks. Kokkuvõttes võime öelda, et kriis ületati edukalt: säilis e-teenuste kasutamine, ei vähenenud usaldus ID-kaardi ja laiemalt digitaalse identiteedi vastu ning sertifikaatide peatamine ei toonud kaasa langust ID-kaardi digitaalses kasutuses. ID-kaardi turvanõrkus ja selle edukas lahendamine võimaldab analüüsida, kuidas tulevikus Eesti digitaalse baastaristu peamiste võimaldajate haavatavuste ja nendega seotud riskide jaoks paremini valmis olla. Ka riigikaitse nõukogu kohtumisel leidis president Kaljulaid, et Eesti vajab ühtset ID-kaardi poliitikat ja konkreetsemat tööjaotust kriisiolukorras.

Korraldasime aprilli esimeses pooles **proovirünnaku Eesti ID-kaardile**, et testida Tšehhi ülikooli poolt avastatud teoreetilist turvanõrkust. Kolleegi krüpteeritud dokument õnnestuski turvanõrkust ära kasutades lahti murda. Sellega tõestasime, et ID-kaarti ei ähvardanudki ainult teoreetiline oht ja kõik kriisi kõrvaldamiseks astutud sammud olid õigustatud.

25. aprillil avaldasime **aastaraamatu, mis kajastab 2017. aasta olukorda nii Eesti kui ka rahvusvahelises küberruumis**. Lisaks ülevaatele küberruumis toimunud sündmustest, aitab aastaraamatu lugemine lahti mõtestada ka seda, kuidas igaüks saab panustada sellesse, et Eesti oleks küberruumis paremini kaitstud.

Rahvusvaheline keskkond

Juba üheksandat korda toimus **maailma suurim rahvusvaheline küberkaitseõppus Locked Shields**, mida korraldab NATO Küberkaitse Koostöökeskus Tallinnas. Ekspertidega 30 riigist harjutati keeruliste infotehnoloogia võrgustike ja kriitiliste infrastruktuuride kaitset üle 2500 laiaulatusliku küberründe eest. Eesti poolt osales õppusel ligi 50 eksperti, meie võistlesime punase meeskonna koosseisus. Õppuse võitis NATO meeskond ning Eesti saavutas 4. koha.

Austraalia ja Portugal on andnud teada, et plaanivad liituda NATO Küberkaitse Koostöökeskusega Tallinnas. Austraaliast saab Jaapani järel teine globaalne NATO partner, kes keskusega liitub.

Hiljuti USA Pew Research Center'i poolt väljastatud raport väidab, et ligi **kaks kolmandikku Twitteri säutse postitatakse bot'ide ehk automatiseeritud võltskontode poolt**. Ka mitmed Eesti tuntud aktiivsed meediakasutajad on täheldanud hulka uusi boti tunnustega jälgijaid oma Twitteri kontodel. Ilma sügavama analüüsita võib seda pidada meediasuhtlust segavaks või pikemajalise kurja plaaniga botilaviiniks. Samas ei pruugi info või jälgijate puudumine koheselt robotkontodele vihjata. Sarnased paistavad välja ka uued väheaktiivsed twitterikasutajad, kes jälgivad peamiselt sotsiaalmeediakanali poolt soovitatud kasutajaid (kelleks tihti on tuntud inimesed).

McAfee analüütikud avastasid **rahvusvahelise andmevarguse kampaania *Operation GhostSecret***. Kokku on avastutud ründeid rahvusvaheliselt 17 organisatsioonis telekommunikatsiooni-, tervishoiu-, finants- ja teistes kriitilise infrastruktuuriga seotud tööstusharudes. Kampaaniat on seostatud Lazarus Group'iga, kuna on leitud sarnasusi 2014. aastal toimunud Sony Pictures andmelekkekampaaniaga.

Facebooki andmelekke skandaalist tulenevalt käis CEO **Mark Zuckerberg Ameerika Ühendriikide Kongressi kahepäevasel kuulamisel aru andmas**. Lisaks Zuckerbergi vabandustele ning peamiselt Facebooki loomislugu ja nn maailma parandavat visiooni käsitlenud esimesel päeval, sai CEO tunda tugevat „grillimist" paljude kongressiliikmete poolt teisel päeval. Küsimuse all olid peamiselt Facebooki kasutajate andmete privaatsus ja Cambridge Analytica skandaal, Venemaa sekkumine 2016. aasta presidendivalimistesse ning üleüldine Facebooki mõjuvõim maailmas.

Europoli koordineeritud rahvusvahelise küberoperatsiooni käigus suudeti internetist maha võtta mitmed **ISISe progandaga seotud meediakanalid** nagu Amaq ja Nashir. Varasemalt aprillis teatas UK, et korraldas küberrünnaku ISISe vastu, millest tulenevalt oli samuti ISISe tegevus oluliselt häiritud.