RIIGI INFOSÜSTEEMI AMET

RIA KÜBERTURVALISUSE TEENISTUSE KOKKUVÕTE MAI 2018

Olukord Eesti küberruumis

Eelnevatel kuudel kasvas intsidentide arv Eesti küberruumis pidevalt, kuid **maikuus** täheldasime kasvu peatumist – mais registreeriti 276 intsidenti võrreldes näiteks aprilli 303ga. Mais esines kõige enam kompromiteerumis-, pahavara ning administreerimisvigadest tingitud juhtumeid. Lisaks tavapärasele Avalanche'le tuvastati ka Necursi robotvõrgustikuga nakatunud seadmeid. Necurs on 2012. aastal loodud robotvõrgustik, mida on aastatega veelgi arendatud ning laiendatud. Käesoleva aasta alguses oli võrgustik suuteline päeva jooksul välja saatama 47 miljonit pahavara sisaldavat rämpsposti.

Eesti riigivõrgus pahatahtlikule tegevusele viitava liikluse seire tulemusena avastasime **videokonverentsi seadmeid, mille telneti põhised haldusliidesed olid avalikust internetivõrgust kättesaadavad**. See lihtsustab potentsiaalseid ründeid seadmete vastu, mille tulemusena on võimalik saada ligipääs seadmele ning seeläbi näha kaamera ulatuses olevat pilti ja kuulda hääli. Lisalugemist siit.

Maikuu lõpuga **tunnistati kehtetuks 12 500 turvanõuetele mittevastava ID-kaardi sertifikaadid**. Garantiikorras vahetati mai jooksul välja 3300 ID-kaarti, mille probleem seisnes turvanõuetele mittevastavate ID-kaartide võtmetes, mis ei olnud genereeritud kiibi sees, vaid olid sinna kopeeritud.

Mais sai **Ühisteenuste veebilehelt parkimine.ee turvavea tõttu iga huviline näha kaaskodanike trahve** ja auto omaniku andmeid. Firma on kinnitanud, et tänaseks on probleem lahendatud.

Tegevused küberjulgeoleku parandamisel Eestis

7.–8. mail korraldasime esmakordselt sõjalise õppuse Siil 2018 osana ka **üleriigilise küberõppuse „KüberSIIL 2018"**. Õppuse peamiseks eesmärgiks oli harjutada tsiviil-militaarkoostööd küberturvalisuse tagamisel. Nagu tõdeti hiljutisel Riigikaitsekomisjoni visiidil RIAsse, peaks üleriigiline küberõppus toimuma igal aastal koos Kaitseväe suurõppusega. Selleaastasel õppusel harjutati olukorda, kus mitut elutähtsa teenuse osutajat, ettevõtet ja ametiasutust olid tabanud ulatuslikud küberrünnakud.

9. mail korraldasime Tallinnas **rahvusvahelise ID-kaardi õppetundide konverentsi *„The Lessons We Learned"***, et arutleda eelmise aasta sügisel ilmnenud kiibi turvanõrkusest puudutatud riikide ja asutuste kogemuste ning vastutuse üle. Konverentsi peaesinejaks oli ID-kaardi turvariski avastanud Tšehhi Masaryki ülikooli teadlane, samuti tutvustasime Tallinna Tehnikaülikooli analüüsi ID-kaardi kaasuse õppetunnide kohta. Nii mõnegi riigi kolleegid imestusid Eesti väga avameelsest kommunikatsioonist ID-kaardi kriisi tekke ja lahenduste osas.

Mai algul võttis Riigikogu vastu **küberturvalisuse seaduse (KüTS)**, mille eesmärk on kaasajastada olemasolevaid nõudeid riigiasutustele ja ettevõtjatele küberohtudeks valmistumiseks, infosüsteemide ja andmebaaside haldamiseks kui ka küberintsidentidest teavitamiseks. **Seadus jõustus 23. mail** ning põhineb 2016. aastal Euroopa Liidus vastu võetud võrgu- ja infoturbe (NIS) direktiivil, mis tuli kõigil liikmesriikidel oma seadusandlusse üle võtta selle aasta maikuuks.

Rahvusvaheline keskkond

25. mail jõustus **ELi uus andmekaitsemäärus** ehk *General Data Protection Regulation* (**GDPR**). Määrus on endaga kaasa toonud palju furoori nii Euroopas kui kogu maailmas ning tekitanud ebakõlasid määruse jõustumise osas. Näiteks on Microsoft lubanud kehtestada GDPRiga kaasa tulnud privaatsussätted kõigile kasutajatele üle maailma, kuid samas tõi määrus juba ühe päevaga Google'le ja Facebookile miljardite dollarite väärtuses kohtuprotsesse. Samuti on mitmed välismaised uudisteportaalid blokeerinud ligipääsu eurooplastele, et end GDPRiga kaasnevate trahvide eest kaitsta.

Maikuu viimane nädal tõi Tallinna üle 600 küberjulgeolekuga tegeleva otsustaja, arvamusliidri ja eksperdi üle maailma nii avalikust kui ka erasektorist. Ühe nädala jooksul toimusid seljakuti esmakordselt Eestis **Müncheni Julgeolekukonverentsi kübertippkohtumine** ning juba kümnendat korda NATO Küberkaitse Koostöökeskuse poolt korraldatud **CyConi konverents**. Selliste maailma tipptasemel ürituste toimumine Tallinnas aitab meil üha paremini Eestit küberjulgeoleku maastikul tutvustada ning kaardistada.

Taani on andnud teada oma soovist **liituda NATO Küberkaitse Koostöökeskusega Tallinnas**. Taani liitumisel jääb Keskuse liikmete seast välja vaid üks Skandinaavia riik – Island.

Märtsikuus lahvatanud Cambridge Analytica skandaalist tulenevalt käis **Facebooki CEO Mark Zuckerberg mais Euroopa Parlamendi ees aru andmas**. Üldiselt peetakse kuulamist suureks pettumuseks formaadi tõttu, mis ei andnud Parlamendi liikmetele piisavalt aega küsimuste esitamiseks, küll aga andis Zuckerbergile piisava võimaluse vastamisest möödahiilimiseks. Tänaseks päevaks on Cambridge Analytica välja kuulutanud pankroti, kuid töötab edasi uue nime all – Emerdata.

Anonymous häktivistide võrgustik **näotustas mais Venemaa Rahvusvahelise Koostöö Föderaalasutuse** (*Rossotrudnichestvo*) **kodulehe** protestimaks valitsuse tsensuuride vastu, eelkõige vihjates Telegrami keelustamisele. Vene võimud keelustasid eelmisel kuul Telegrami äpi, sest ettevõte keeldus andmast FSB-le kasutajate krüpteerimisvõtmeid.

Mai keskel sattus **DDoS rünnaku ohvriks Taani riiklik raudteeoperaator DSB**, mille tulemusena olid ühe päeva jooksul häiritud piletiostu süsteemid ja sideinfrastuktuur. Ettevõtte ainuke viis klientidega suhtlemiseks oli läbi sotsiaalmeedia.

Mai lõpus teavitas US-CERT, et **sajad tuhanded internetiruuterid** nii Ameerikas kui üle maailma on **küberrünnete poolt kompromiteeritud**, millest tulenevalt on kaotanud konfidentsiaalset teavet nii eraisikud kui ka väiksemad organisatsioonid. See on endaga kaasa toonud rahalisi väljaminekuid ning organisatsioonidele ka mainekahju.

USA Kaitseministeerium **keelas mais ära Huawei ja ZTE telefonide müügi Ameerika sõjaväebaasides**, mida põhjendatatakse potentsiaalse Hiina luure turvariskiga. Sõjaväelastel säilib õigus antud telefonide isiklikuks kasutuseks. USA valitsus on Hiina tehnoloogiaettevõtete vastu teinud samme juba detsembrist alates, kui näiteks Senat hoiatas Ameerika rahvast Huawei ja ZTE seadmete kasutamise eest.