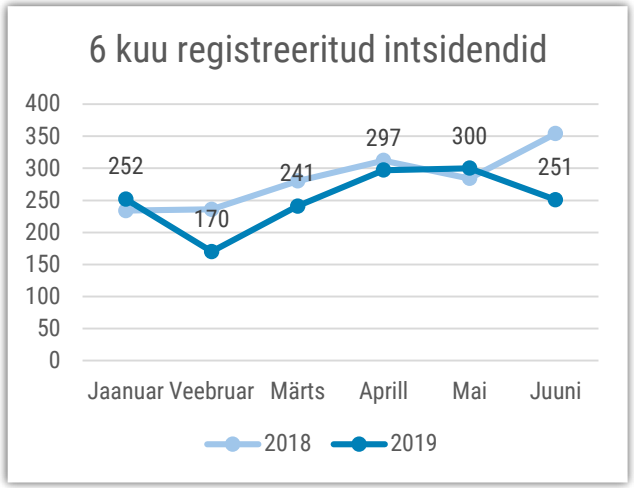
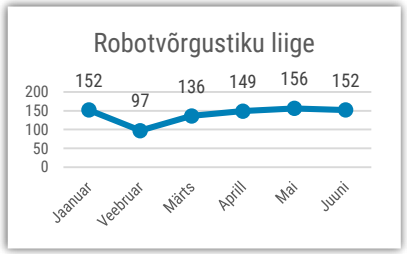
Olukord küberruumis – juuni 2019

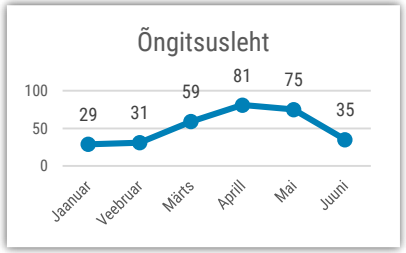
- Juunis registreerisime 251 intsidenti, mis on selgelt vähem võrreldes eelmise aasta sama perioodiga.
- Jätkusid rünnakud Eestis laialdaselt kasutatava autentimisvahendi Smart-ID kaaperdamiseks, teenusepakkuja muutis kontode loomise protsessi.
- Viie aasta jooksul jäi teatud hulk kehtetuks tunnistatud ID-kaarte jätkuvalt kehtima, mille kohta algatasime ka järelevalvemenetluse.
- Eesti liitus Euroopa energiavaldkonna küberintsidentide infovahetusplatvormiga EE-ISAC.



Intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.



Kõige rohkem saame teateid robotvõrgustikuga nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtedega seotud intsidentide hulk juunis vähenes, kuid nende hulk on kõrgem mullu registreeritud sarnaste intsidentide hulgast.

Olukord Eesti küberruumis

Juunikuus jätkusid (küll väiksemas mahus) õngitsuskampaaniad Smart-ID kontode loomise eesmärgil, millest oleme kirjutanud nii aprilli, kui ka maikuu ülevaadetes. Kokku kurjategijad loonud aprilli algusest saati 42 valekontot, millest kümne puhul jõuti ka kontode ärakasutamiseni.

RIA algatatud järelevalvemenetluse käigus otsustas Smart-ID teenusepakkuja SK ID Solutions 1. juulist muuta mobiil-ID kaudu tehtavate Smart-ID kontode loomise protsessi. Seetõttu otsustasime järelevalvemenetluse ka lõpetada. Samas jätkub kriminaalmenetlus kurjategijate välja selgitamiseks.

10. juunil alustasime järelevalvemenetlust politsei- ja piirivalveameti (PPA) suhtes seoses sellega, et viie aasta jooksul oli teatud hulka PPA poolt kehtetuks tunnistatud ID-kaarte siiski võimalik edasi kasutada. Menetluse käigus tuvastasime, et probleem peitus isikutuvastus- ja menetlusinfosüsteemis UUSIS, mille töötamise eest vastutab PPA. Viimase viie aasta jooksul on e-teenustes kasutatud 353 kehtetuks tunnistatud kaarti, neist 285 puhul oli tegemist surnud inimese dokumendiga. Näiteks kasutasid surnud inimeste omaksed nende ID-kaarte selleks, et tasuda matusekulusid ning lõpetanud lahkunu nimel olevaid teenuselepinguid.

Juuni keskel katkes pea viieks tunniks Eesti Rahvusringhäälingu veebisisu edastamine. Tegemist oli varutoiteallika seadme rikkega, mis omakorda vallandas gaasikustutussüsteemi viies rivist välja err.ee sisu teenindavad serverid. Tele- ja raadioprogrammide edastamine jätkus tavapäraselt, kuid häiritud olid ka ERRi sisemised võrguteenused.

Juuni oli esimene kuu alates eelmise aasta augustist, kus **meile ei antud märku ühestki kaaperdatud meilivestlusest alguse saanud edukast finantspettusest.** Oleme alates mullu septembrist hoiatanud Eesti ettevõtjaid ja laiemat avalikkust taolistest petuskeemidest ning soovitame edaspidigi olla ettevaatlikud nii enda meilidega, kui ka teistega suheldes. Taolised, inglisekeelse nimega *Business Email Compromise* rünnakud jätkuvad igal pool maailmas ning kompromiteeritud kontodest anti ka meile märku. Arvestades, et Eesti ettevõtted suhtlevad meilitsi oma koostööpartneritega üle maailma, tuleb jätkuvalt olla valvas, kui partner palub ootamatult saata makseid mõnele tavapärasest erinevale pangakontole.

Tegevused küberturvalisuse parandamisel Eestis

RIA liitus Euroopa energeetika valdkonna küberinfovahetusplatvormiga EE-ISAC. Tegu on võrgustikuga, mis koondab endas energeetika valdkonna tööstusettevõtteid, uurimisasutusi ja valitsusasutusi selle platvormi liikmesus on oluline parandamaks teadlikkust Eestis energeetikat ohustada võivatest küberriskidest.

Nõustasime erinevaid riigiasutusi pilveteenuste (näiteks Office365) kasutuselevõtmisel, mille käigus soovitasime lähtuda olemasolevast RIA juhendist avalike pilveteenust turvaliseks kasutamiseks. Pilveteenuste kasutamise puhul peavad ühe olulise nõudena kõik asutused pidama meeles seda, et asutusesiseseks kasutamiseks (AK) mõeldud andmed peavad olema krüpteeritud nii üle võrgu edastamise ajal kui ka pilveteenuses salvestatud olekus, sest selle abil saab hoida ära AK andmete väljumist asutuse kontrolli alt.

Alustasime järelevalvemenetlusi 20 kohaliku omavalitsuse suhtes, mille eesmärgiks on kontrollida seda, kas nende infosüsteemides on turvameetmed nõuetekohaselt rakendatud. Nende menetluste käigus saame ka senisest selgema ülevaate sellest, milline on infoturbeteadlikkus Eesti omavalitsustes ja tõstame seejuures ka nende üleüldist suutlikkust infoturbe tagamise minimaalseid nõudeid täita.

Tallinnas toimus iga-aastane Balti riikide ja USA küberturvalisuse ja kriitilise infrastruktuuri valdkonna konsultatsioon, kus käsitleti valdkonna päevakajalisi probleeme ja arutati võimalusi Balti riikide ja USA koostöö suurendamiseks selles valdkonnas.