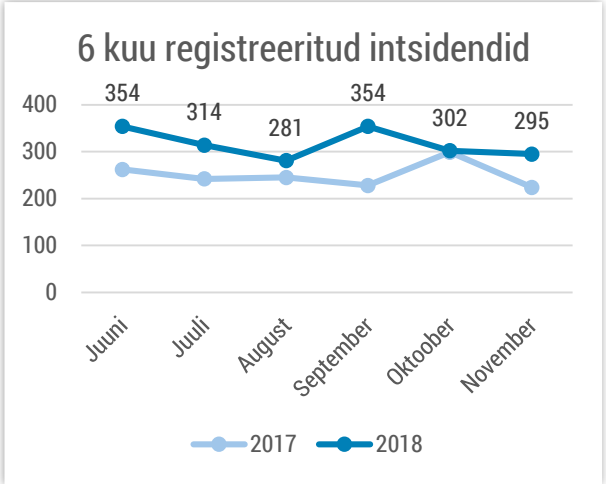
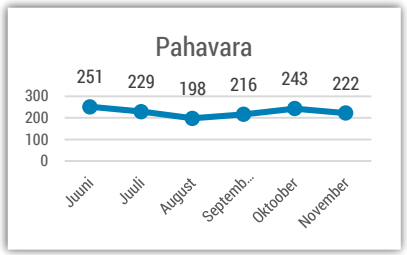
Olukord küberruumis – november 2018

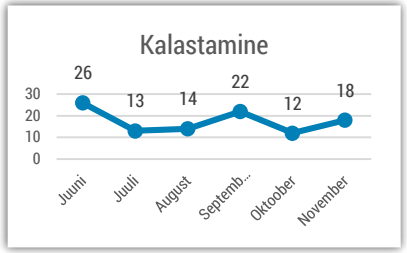
- Novembris registreerisime 295 intsidenti, mida oli küll vähem kui oktoobris, kuid rohkem kui mullu samal ajal.
- Jätkuvad tuntud ettevõtteid imiteerivad õngitsuskampaaniad, millega püütakse kätte saada kasutajaandmeid või jagatakse pahavara.
- Jätkuvad finantspettused, kus ettevõtteid palutakse tegema tavapärast ülekannet uuele pangakontole.
- Valitsus kiitis heaks küberturvalisuse strateegia.
- Märkimisväärsete kübervõimetega riigid jätkavad omavahelist mõõduvõtmist – USA soovitab liitlastel vältida Hiina tooteid, Iraan süüdistab Iisraeli sabotaažis, Venemaa püüab lääne ühtsust lõhkuda.



Intsidendid, millel oli mõju infosüsteemide konfidentsiaalsusele, terviklikkusele või käideldavusele.



Registreeritud intsidentidest on jätkuvalt kõige suurem osa pahavaral. Jätkuvalt saame kõige rohkem teateid botnet-*idega nakatunud arvutitest Eesti küberruumis.*



CERT-EE-le edastatud teated edukatest kalastamise (phishing) intsidentidest on viimase kuuga tõusnud.

Olukord Eesti küberruumis

Novembris jätkus finantspettuste laine ettevõtete vastu, millest rääkisime nii septembri-, kui ka oktoobrikuu ülevaates. Kurjategijad saavad ligipääsu mõne ettevõtte meilikontole ja jälgivad sealset vestlust, kuni ettevõte hakkab oma koostööpartnerile raha üle kandma, seejärel sekkuvad vestlustesse ja paluvad muuta pangakonto andmeid. Niimoodi on said novembris kümneid kuni sadu tuhandeid eurosid kahju nii Eesti ettevõtted, aga ka Eesti ettevõtete partnerid välisriikides.

Meile teadaolevalt on Eesti ettevõtted saanud niimoodi sel sügisel kahju vähemalt 500 000 eurot.

Kirjeldasime sellist finantspettust ka oma kvartaliülevaates ning hoiatame veelkord, et kui koostööpartner palub arve maksmiseks ootamatult meili teel muuta pangakonto andmeid, tuleks see igaks juhuks muude kanalite pidi üle kontrollida. Pettust kasutavad pangakontod on seni asunud välisriikides ja samuti on omavaheline suhtlus toimunud inglise keeles.

Novembris täheldasime kahte Facebookiga seotud laiaulatuslikumat kampaaniat. Näiliselt Facebooki turvameeskonnalt saadeti teateid konto blokeerimisest, kui ei kinnitata oma kontot. Tegelikkuses oli tegemist õngitsusega, mille eesmärgiks oli varastada kasutajaandmeid ning osta reklaami kolmandatele ettevõtetele. Teises kampaanias saadeti justkui Facebooki meeskonnalt õnnitluskirju, mille puhul õnnitleti 1 mln dollari võitmise eest ning paluti raha ülekandmiseks kontaktandmeid jm infot.

Samuti teavitati meid **USA-sse reisimiseks vajaliku ESTA** (Electronic System for Travel Authorization) veebilehe võltsingust. Nimelt on küberkurjategijad loonud ESTA veebilehega sarnaseid veebilehti, millega püütakse eksitada kasutajaid sisestama oma andmeid ja tasuma „avalduse“ tegemise eest märkimisväärselt suuremas ulatuses summa kui tegelikkuses tasuda tuleb. Lisaks isikuandmetele saavad kurjategijad teada ka krediitkaardiandmed.

Tegevused küberturvalisuse parandamisel Eestis

Valitsus kiitis novembris heaks küberturvalisuse strateegia aastateks 2019-2022. Tegemist on pikalt ette valmistatud raamdokumendiga, mis näitab ette, kuhu Eesti küberturvalisuse valdkonnas soovib lähiaastatel jõuda. Strateegial on neli suuremat eesmärki, mille nimel RIA ja partnerid töötavad:

- Eesti on jätkusuutlik digitaalne ühiskond, millel on tugev tehnoloogiline vastupanuvõime ja valmisolek kriisidega toimetulekuks.
- Eestis on tugev, innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus ning teadus- ja arendustegevus, mis katab riigi jaoks olulised võtmekompetentsid.
- Eesti on arvestatav ja tugev partner rahvusvahelisel areenil.
- Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide järelkasv.

Pöörame eraldi tähelepanu valimiste küberturvalisusele. Suvel valmis Eesti ja Tšehhi eestvedamisel Euroopa-ülene käsiraamat valimistehnoloogiate küberturvalisusest, seetõttu püüame eraldi vaadata igat üksikut infotehnoloogiat kasutavat osa Riigikogu ja Euroopa Parlamendi valimistest – mitte ainult e-hääletust. Kuna oleme näinud, kuidas teistes riikides on kampaaniate meilikontode häkkimisest tekkinud palju segadust, pöörame tähelepanu ka kandidaatide ja kampaaniate korraldajate küberturvalisusele. Novembris korraldasime kandidaatidele ja erakondade töötajatele kaks küberturvalisuse koolitust nii Tallinnas kui Tartus. Samuti pakkusime erakondadele võimalust kontrollida üle, kas nende e-mailiserverite ja koduleheküljegede turvalisuse osas tuleks olukorda parandada. Kõik kuus parlamendierakonda kasutasid seda võimalust.

Kirjutasime esimest korda ülevaate ka ohtude kohta, mida me usume, et näeme lähiajal veel. Esimene kvartaliülevaade rääkis ettevõtete kirjavahetusse vahelesegamise trendist, Office 365 atraktiivsusest kurjategijatele, lunavararünnakutest ja erinevate seadmete teadaolevate turvanõrkuste ärakasutamisest.

Eesti ja Iisrael leppisid kokku, et hakkavad koostööd tegema elektroonilise identiteedi valdkonnas, mis tulevikus peaks tähendama seda, et mõlema riigi infosüsteemid võiksid tunnistada teises riigis antud digiallkirju. Selle tulemusel võib Iisrael tulevikus liituda ka X-tee platvormiga, mis annaks meie riikidele veel paremaid võimalusi info vahetamiseks.

Rahvusvaheline keskkond

USA vahevalimiste vahetult eelneval perioodil USA sisejulgeolekuministeerium (DHS) ei täheldanud, et keegi oleks püüdnud takistada hääletamist, muuta hääli või häirida häältelugemist. Sellest hoolimata märgati valimiste-eelsel perioodil korduvalt tegevusi sotsiaalmeedias, mille eesmärgiks oli välisriikidest mõjutada USA valijaid.

Euroopa komisjoni tellitud uuring valijate murede kohta Euroopa parlamendi valimiste eel näitas, et **enam kui 60% eurooplastest on mures, et küberrünnakud võivad valimisi saboteerida**. Kõige vähem muretsevad selliste küberrünnakute pärast eestlased (42%).

USA ja Hiina vahelised suhted teravnesid novembris, kui USA ametnikud on asunud survestama oma liitlasriike, et need ei lubaks Hiina ettevõttel Huawei osaleda riikides telekomitaristu ehitamisel, sealhulgas 5g võrkude arendamisel, kuna kahtlustab, et Hiina luureasutustel on Huawei seadmete kaudu otseliin seal vahetatavale infole. Peale USA on veel Austraalia ja Uus-Meremaa piiranud Huaweil võrkude hangetel osalemise. Neil on palju kahtlusi, mida nad on otsustanud avalikkusega mitte jagada, kuid näiteks Huawei oli Etioopia pealinnas asuva Aafrika Ühenduse konverentsikeskuse IT-partner ajal, kui sealt avastati suur Hiinaga seotud luureoperatsioon.

Novembris teatas **USA küberväejuhatus**, et hakkab püsivate, tihtipeale riikidega seotud rünnakugruppide (niinimetatud *Advanced Persistent Threat* ehk APT) **pahavaranäidiseid vabalt kättesaadavasse andmebaasi Virustotal üles laadima.**

Novembri keskel kirjutasid enam kui 50 riiki, 130 ettevõtjate gruppi ja 90 mittetulundusühingut **Prantsusmaa eestvedamisel Pariisis alla küberturvalisuse paktile**, mis on järjekordne katse multilateraalselt kehtestada norme küberturvalisuses. Paktiga ei liitunud mitu olulise kübervõimega riiki nagu USA, Hiina, Venemaa, Iraan ja Iisrael.

Venemaa lõi novembris koos Hispaaniaga küberturvalisust arutava koostöövormi. Selle taustaks tuleb ära mainida, et Venemaalt pärinevaid sotsiaalmeedia mõjutusi (sealhulgas valeuudiste levitamine) kahtlustatakse osaliselt Kataloonia iseseisvuspüüdlustega kaasnenud ebastabiilsuse taga.

Iraan teatas novembris, et kahtlustab Iisraeli, et nemad püüdsid uuendatud Stuxneti pahavara versiooniga rünnata Iraani telekommunikatsioonitaristut. USA ja Iisraeli poolt loodud Stuxnet lõhkus Iraani tuumarajatiste tsentrifuuge kümmekond aastat tagasi.