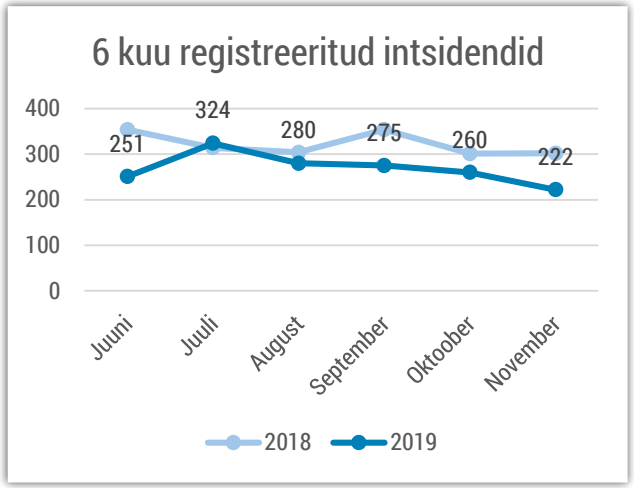
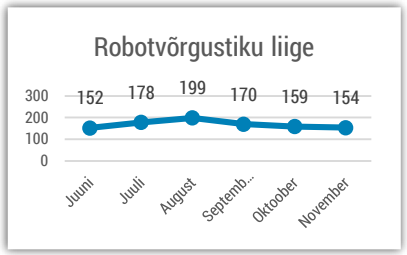
Olukord küberruumis – november 2019

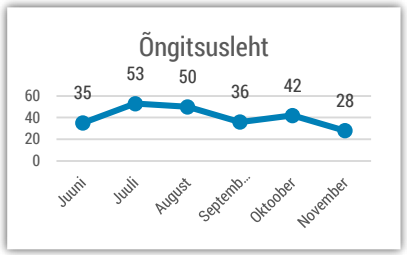
- Novembris registreerisime 222 intsidenti, mis on oluliselt madalam hulk võrreldes aasta keskmisega.
- Riigivõrgu hooldustööd häirisid mitme tunni jooksul ligipääsu digiretseptidele ja Eesti.ee-le.
- Pangakontodelt raha varastavad õngitsuskampaaniad ei taha kuidagi lõppeda.
- Teavituskampaania „Ole IT-vaatlik!“ kutsus rahvast kohalikesse raamatukogudesse nõu küsima.
- Meilide kompromiteerimiskatsed, lunavara ja teenusetõkestusrünnakud kimbutavad mitmeid riike.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtede intsidentide hulk on hakanud langema.

Olukord Eesti küberruumis

19. novembril ajavahemikul 17-22 vahel olid riigivõrgu erakorraliste hooldustööde häiritud mitme olulise mõjuga e-teenused – RIA sisesed teenused (sealhulgas eesti.ee riigiportaal), haigekassa teenused (sealhulgas digiretseptide väljastamine), Eesti Loto veebileht ja mitme Harku valla riigiasutuse internetiühendus.

Erakorralised hooldustööd võeti ette, kuna avastasime, et rotid on Harjumaal asuvat maa-alust riigivõrgu kaablit tõsiselt kahjustanud. Hooldustööde käigus kolis suur osa e-teenuseid automaatselt ümber teisele kanalile ning häiritud olid just need teenused, mis seda hetkel veel automaatselt ei tee, ning vajasid käsitsi ümber tõstmist teisele kanalile. Kuigi füüsiliselt on kõik riigivõrgu ühendused dubleeritud, on järgmise aasta jooksul plaanis paigaldada kõikidesse riigi sõlmpunktidesse ja andmekeskustesse seadmed, mis kolivad teenused automaatselt ümber. Päev hiljem toimunud plaanipärane katkestus enam taolisi katkestusi kaasa ei toonud.

Nägime novembrikuus taas pangakontoandmete ja PIN koodide õngitsuskampaaniat, millest oleme erinevates variantides kirjutanud kuukokkuvõtetes viimase poole aasta jooksul. Suvel kasutajatelt pangaülekannete jaoks PIN2 koodi küsinud õngitsuslehed said novembrikuus lisafunktsionaalsuse, mille kaudu kuvatakse Mobiil-ID-d või Smart-ID-d autentimiseks ja allkirjastamiseks kasutavale ohvrile ekraanil ka õige kontrollkood. Samas on PIN-koodide sisestamise hetkel siiski ka kasutajal telefoni ekraanil näha, et ta hakkab hoopis allkirjastama makset.

Novembri alguses korraldati mitme Eesti veebilehe vastu lühiajalisi teenustõkestusrünnakuid, nende hulgas oli nii eraettevõtteid, aga ka ministeeriumite ja ametite veebe. Näiteks ühe finantsteenuseid pakkuva ettevõtte vastu suunatud rünnaku järel saadeti neile ka väljapressimiskiri, kus nõuti järgmise rünnaku vältimiseks lunaraha.

Tegevused küberturvalisuse parandamisel Eestis

Koostöös Eesti Raamatukoguhoidjate Ühinguga korraldasime 20. novembril infopäeva, kus ligi sada raamatukogu üle Eesti pakkusid eelkõige vanemaealistele internetikasutajatele abi küberturvalisuse küsimustes. Rääkisime sellest, kuidas mõelda välja tugevaid paroole, uuendada arvuti või nutiseadme tarkvara, teha failidest varukoopiaid, tunda ära õngitsuskirju ja paljust muust. RIA "Ole IT-vaatlik" kampaania raames toimunud nõuandepäeva eesmärk oli õpetada eakamaid arvutikasutajaid pöörduma oma IT-muredega raamatukogusse. Tallinnas toetasid abivajajaid Tallinna Polütehnikumi õpilased, aitäh nii õpilastele kui ka koolile selle abi eest!

Novembri lõpus võõrustasime Põltsamaa Ühisgümnaasiumi küberkaitse õppesuuna õpilasi ja õpetajaid. Selgitasime noortele, millega RIA tegeleb, mida kujutab endast elektrooniline identiteet ja millised on selle võimalused, kuidas kasutada riigiportaali eesti.ee ning kuidas kaitsta end levinumate küberohtude eest. Põltsamaa Ühisgümnaasiumile oleme olnud koostööpartner alates 2015. aastast, kui seal avati küberkaitse õppesuund.

Korraldasime infopäeva RIA koostööpartneritele. 12. novembril toimunud seminaril rääkisime elektroonilise identiteedi, andmevahetuse, riigiportaali, riigivõrgu ja valimiste infosüsteemi teemadel. Samuti korraldasime 21. novembril infopäeva kriitilise informatsiooni infrastruktuuri kaitsega tegelevatele ettevõtetele ja asutustele, kus pöörasime eraldi tähelepanu tööstussüsteemide kaitsele.

Jätkasime kohalike omavalitsuste koolitamist ja järelevalve tegemist. Lõppeva aasta jooksul oleme kontrollinud kohalike omavalitsuste infosüsteeme ja aidanud neid turvalisemaks muuta. Novembris lõpetasime menetluse nelja omavalitsuse suhtes ning tegime ettekirjutuse kahele. Küberhügieeni koolitusi korraldasime Haabersti ja Nõmme linnaosavalitsustes.

Rahvusvaheline keskkond

Tehnoloogiaettevõte Google teatas, et on vaid viimase kolme kuu jooksul saatnud oma kasutajatele ligikaudu 12 000 turvahoiatust, et riikidega seostatud küberrühmitused on üritanud pääseda ligi nende kontole või arvutile. Kõige rohkem on kasutajaid teavitatud Ameerika Ühendriikidest, Lõuna Koreast, Pakistanist ja Vietnamist.

Novembris jõustus Venemaal regulatsioon, mis kohustab kõiki Venemaa internetiteenuse pakkujaid saatma veebiliiklust läbi kindlate sõlmpunktide, mis on Venemaa valitsuse kontrolli all. Seaduse eesmärgina on räägitud vajadusest tagada ligipääs kohalikule internetile ka juhul, kui välisriigid peaksid riigi globaalsest internetist eraldama. Kriitikud näevad plaanis aga tsensuuri ja jälgimise ohtu.

Saksamaa on teatanud enda eesmärkidest arendada valmimisjärgus pilveteenus Gaia-X Euroopa tasandil alternatiiviks Amazoni, Google ja Microsofti pilveteenustele. Algatusega on juba liitunud Prantsusmaa, kes väitis ühisavalduses Saksamaaga, et Euroopal on vaja suveräänset platvormi, millel saaks EL-i kodanikke puudutavaid andmeid säilitada, edastada ning arendada. Pilveteenuse eeldatav alustamise aeg on 2020. aasta teine pool. Projekti peamised investorid on äritarkvara pakkuv ettevõte SAP, Deutsche Bank, telekommunikatsioonioperaator Deutsche Telekom ja tehnoloogiaettevõtted Siemens ning Bosch.

Ameerika Ühendriikides, Hispaanias, Prantsusmaal ja Mehhikos teatati suuremahulistest lunavararünnakutest.

Ühendkuningriikide leiboristide erakonda tabas valimiskampaania käigus novembris kaks suuremahulist teenustõkestusrünnakut. Rünnakute eest võttis vastutuse tuntud häkkerite rühmitus, kes on varemgi ideoloogilistel põhjustel DDOS rünnakuid korraldanud.

USA sõjaväe küberspetsialistide meeskond saabus Montenegrosse, et aidata riigi valitsusel valmistuda järgmise aasta valimisteks. Meeskond aitab tugevdada riigi avaliku sektori vastupanuvõimet küberoperatsioonidele eelkõige Venemaa võimalike rünnete vastu.

Indias teatati Kudankulami tuumaelektrijaam süsteemide kompromiteerimisest, kus püüti ligi pääseda jaama tehnilistele andmetele. Intsidenti uurinud spetsialistide hinnangul on rünnaku taga Põhja-Koreaga seostatud häkkerite grupeering Lazarus Group.