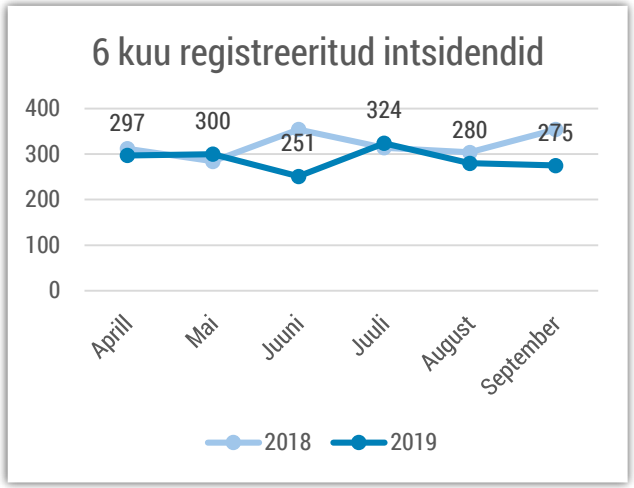
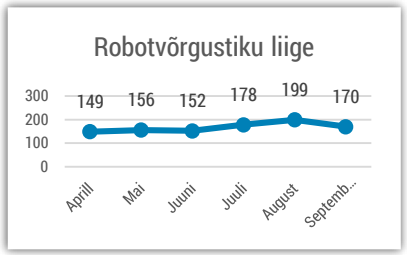
Olukord küberruumis – september 2019

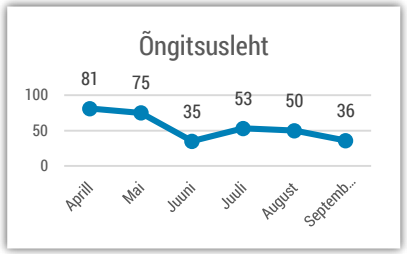
- Septembris registreerisime 275 intsidenti, mis on veidi kõrgem aasta keskmisest, kuid vähem võrreldes sama ajaga mullu.
- Eesti internetipankade õngitsuslehti oli septembris näha vähem kui suveperioodil. Samas jätkusid meilikontode andmete õngitsused.
- Ekspertrühm hindas Smart-ID-le vastavuse tasemele „kõrge“ ning see võeti kasutusele riigi keskses autentimisteenuses TARA.
- 27 riiki lubasid koostööd teha, et võtta kübernorme eiravad riigid ühiselt vastutusele.



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



Jätkuvalt saame kõige rohkem teateid robotvõrgustikega nakatunud arvutitest Eesti küberruumis.



Õngitsuslehtedega seotud intsidentide hulk septembris vähenes, eelkõige nägime vähem internetipankade lehekülgi imiteerivaid õngitsuslehti.

Olukord Eesti küberruumis

Ööl vastu 25. septembrit oli tarkvararikke tõttu 20 minutit häiritud Häirekeskusega suhtlemine. Probleemide ilmnemisel teavitas Häirekeskus kohe SMITi, kes Häirekeskuse tarkvara haldab ja asus probleemi kõrvaldama. Rikke ajal ei kuulnud päästekorraldajaid nendeni jõudnud kõnedes helistajat ja helistajad ei kuulnud päästekorraldajat. Tegemist oli öise ajaga, kus kõnekoormus on madalam ja sellel perioodil helistas Häirekeskusesse 26 inimest. Kõigile neile helistas Häirekeskus tagasi ja teadaolevalt inimesed abita ei jäänud.

Võrreldes suvekuudega nägime septembris vähem pankadega seotud õngitsuskirju, kuid õngitsuskirjad ja -lehed on Eesti küberruumis jätkuvalt oluliseks probleemiks. Septembris tabas Tartu ülikooli (@ut.ee) meiliaadresse õngitsuskirjade laine, kus ohvritele saadeti lakooniline eestikeelne teade sellest, et nende meilboksi maht hakkab täis saama. Õngitsuslehele sisestas oma kontoandmed üle kolmekümne kasutaja (@ut.ee kasutajate hulgas on näiteks tudengeid, õppejõude, teadureid jne), kellest paljude kontodelt hakati edasi saatma rämpspostikirju.

Taoliste meilikontode kompromiteerimise mõju võib ilmneda olulise viivitusega, kus kurjategijad töötavad läbi kättesaadud kirjade sisud ning leiavad sealt informatsiooni võimalike uute sihtmärkide kohta.

Septembris anti meile märku järjekordsest kompromiteeritud meilikonto kaudu tehtud pettusekatsest, kus kurjategijate poolt kontrollitavale pangakontole suunati 112 000 euro suurune ülekanne. Transpordisektoris tegutsev ettevõte sai meile teadaolevalt koostöös pangaga ülekande peatada ja raha tagasi.

Ida-Tallinna keskhaiglas toimus septembri alguses sisevõrgus teenusekatkestus, mis takistas tavapäraseid tööprotsesse nii palju, et haigla pidi lühiajaliselt paberrežiimile üle minema. Samuti mindi erakorralise meditsiini osakonnas üle hädaolukorra režiimile. Intsidendi põhjustas inimviga uue võrguseadme paigaldamisel ning vähem kui kaks tundi hiljem suudeti tavapärane töö taastada.

Ööl vastu 16. septembrit, vahemikus 02.27 – 09.44 ei olnud tehnilise rikke tõttu võimalik kasutada riikliku autentimisteenust TARA, mille tõttu ei saanud kasutajad sisse logida mistahes autentimisvahendiga riiklikesse e-teenustesse, seal hulgas eesti.ee-sse. Teenuse katkestuse põhjustas sertifikaatide uuendamine süsteemis. Katkestuse tõttu oli takistatud TARA klientide ehk ligikaudu 60 avaliku e-teenuse kasutamine.

Tegevused küberturvalisuse parandamisel Eestis

Septembri alguses leppisime SK ID Solutionsiga kokku, et võimaldame riiklikes e-teenustes kasutada autentimisvahendina ka Smart-ID-d. See lisandub kesksesse autentimiseteenusesse TARA, mida kasutab rohkem kui 60 avaliku sektori asutust või avaliku ülesande täitjat. Teenus võimaldab autentimist ID-kaardiga, Mobiil-ID-ga, pangalinkidega ja EL liikmesriikide eID vahenditega ning nüüd ka Smart-IDga.

Enne Smart-ID kasutusele võtmist hindas ekspertrühm, et Smart-ID vastab elektroonilise isikutuvastuse tasemele „kõrge". See tähendab, et Smart-ID hinnang on samaväärne ID-kaardi ja mobiil-ID tasemega. 2018. aastal tunnustati Smart-ID kui QSCD tasemel teenust, mis on kõige kõrgem võimalik tase Euroopa Liidus.

Septembri keskel korraldasime konverentsi eID Forum 2019, kus eksperdid enam kui kolmekümnest riigist arutasid isiku tuvastamise ja füüsiliste dokumentide tuleviku, digitaalse piiri ja piirikontrolli võimaluste ning e-demokraatia väljakutsete üle.

Jätkame järelevalvemenetlusi kohalike omavalitsuste suhtes, millest oleme rääkinud ka varasemates kuuülevaadetes ja meedias. Aasta algusest oleme algatanud menetlusi juba rohkem kui poolte omavalitsuste suhtes ning mitmed neist ka lõpetanud ilma ettekirjutusteta, kui menetluse käigus on puudujäägid heas koostöös kõrvaldatud.

Rahvusvaheline keskkond

ÜRO peaassamblee nädalal kirjutasid 27 riiki (Eesti nende hulgas) alla kübernormidele viitavale avaldusele, kus andsid märku, et kavatsevad vajadusel koostööd teha selleks, et võtta küberruumis reegleid mittejärgivaid riike vastutusele. 27 riigi seas olid ka kõik niinimetatud Five-Eyes riigid – USA, Ühendkuningriigid, Kanada, Austraalia ja Uus-Meremaa.

Septembris jõudis lõpule massiivne rahvusvaheline politseioperatsioon, mille käigus arreteeriti nelja kuu jooksul kümnes riigis kokku 281 inimest, keda kahtlustatakse finantspettuste läbiviimises meilikontode kaaperdamise teel (inglise keeles *Business Email Compromise* ehk BEC-skeem). 167 inimest vahistati Nigeerias, 74 inimest Ameerika ühendriikides, 18 inimest Türgis, 15 Ghanas. Lisaks neile toimusid vahistamised veel Prantsusmaal, Itaalias, Jaapanis, Keenias, Malaisias ja Ühendkuningriikides. Operatsiooni käigus suudeti tagasi saada ülekandeid umbes 105 miljoni euro ulatuses.

BEC-skeemid on ka Eestis üks kõige suurema mõjuga intsidendiliike, mullu said Eestis ettevõtted vähemalt 600 000 eurot niimoodi kahju, käesoleval aastal on meile teada antud kaotustest umbes 250 000 euro ulatuses.

Pea kõigi Ecuadori elanike (ca 17 miljonit) isikuandmed lekkisid avalikkusele tohutus andmebaasis, kuhu oli kokku pandud mitmest erinevast allikast saadud andmed. Andmebaasis olid peale nimede ja isikukoodide veel kodused aadressid, paljudel puhkudel ka töökohad ja palgaandmed, pereliikmete informatsioon ja autode registreerimisandmed. Pärast esimest leket avastati andmebaas veel ühest serverist.

Andmelekked kimbutavad mujalgi. **Kagu-Aasia suurima lennukipargiga lennufirma Lion Airi tütarfirmad Malindo Air ja Thai Lion Air klientide andmebaasidest lekkisid 35 miljoni kliendi** nimed, sünnipäevad, telefoninumbrid ja aadressid. Klientide pangakaartidega seotud andmeid mõjutatud serverites ei olnud. Esialgu peetakse süüdlasteks ettevõtete endisi töötajaid.

Poolas vormistati 12. septembril ära otsus, millega loodi küberväejuhatus, mis peaks operatsioonidega alustama 2022. aastal ning mis peaks jõudma 2024. aastaks täieliku valmisolekuni.