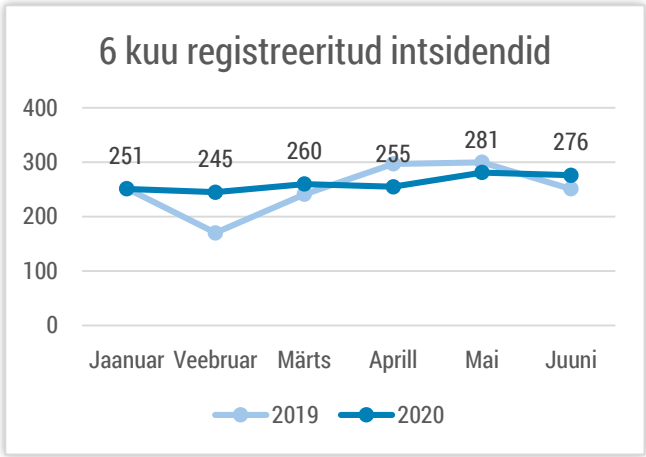
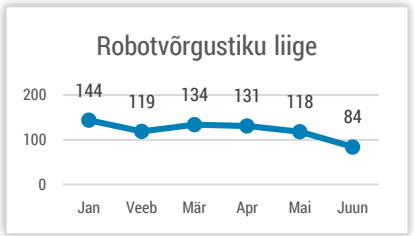
Olukord küberruumis – juuni 2020

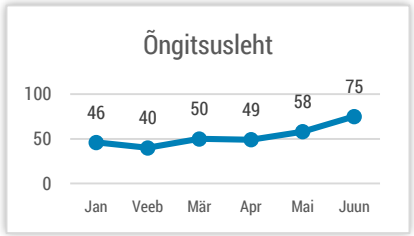
- Juunis registreerisime 276 intsidenti. Intsidentide hulk püsib tavapärasel tasemel.
- Arvepettuste veenvuse tõstmiseks läheb vaja kõikvõimalikke andmeid, Eestis on petturid hakanud kasutama riigihangete registrist leitud hangete detaile.
- Eestis levis mais ja juunis Eesti asutuste sümboolikat kasutav kontoandmete õngitsuskampaania.
- Alustasime Eesti vee-ettevõtetele suunatud küberturvalisuse pilootprogrammi.
- Lunavara on maailmas jätkuvalt kurjategijatele tulus.



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



Teated robotvõrgustikega nakatumistest on langustrendis. Alates juulist eemaldame kahe neutraliseeritud võrgustiku intsidendid statistikast.



Õngitsuslehtede hulk jätkuvalt kasvab, jõudes aasta kõrgeimale tasemele. Õngitsetakse nii kontoandmeid, kui ka petetakse välja raha.

Olukord Eesti küberruumis

Ida-Tallinna Keskhaigla andis märku arvepettusest, kus kaaperdati meilivestlus allhankijaga. Kurjategijad kasutasid ära avalikult kättesaadavat infot ühest ITKH rahvusvahelisest hankest, kaaperdasid meilivestluse ja vahetasid arvetel pangakonto numbrid. Mitme kuu jooksul peteti haiglalt niimoodi välja üle 10 000 euro. Sama käekirjaga proovisid kurjategijad tüssata veel üht rahvusvahelisi hankeid korraldavat Eesti asutust – detaile hangetest jagatakse meie riigihangete registri kõrval ka üle-Euroopalistes keskkondades (nt ted.europa.eu). Intsident näitab, et petturid teevad oma kodutöö hästi ära, eriti kui info on avalikult kättesaadav.

Mai lõpust alates, terve juunikuu jooksul oleme märganud õngitsuskirjade lainet, mis püüab selges eesti keeles meelitada jagama oma kontoandmeid võõrastele lehekülgedele. Õngitsuskirjade teemaks oli enamasti küll inglisekeelne „Re: Invoice", kuid kirja sisus kasutati juba Eesti asutuste ja ettevõtete sümboolikat.

Meile teadaolevalt on niimoodi kompromiteeritud kümmekond kontot erinevatest ettevõtetest ja asutustest. Kompromiteeritud kontolt saadetakse välja taas sadu või tuhandeid meile, kuid seadistatakse meilikontodele ka uued reeglid, mis võivad anda kurjategijatele ligipääsu kirjadele ka pärast paroolide lähtestamist. Niimoodi varastatud infot võidakse hiljem ära kasutada arvepettuste korraldamiseks. Juuni keskel tegime ka sellekohase teavituse avalikkusele.

Juunis saime teada, et Eesti ühe spordialaliidu meilikontot on niimoodi jälgitud ja hetkel, kui tekkis koroonapandeemia tõttu vajadus võistluste osalustasud tagasi saada, sekkuti meilivestlusesse, paluti pangakontot muuta ja maailma vastav spordiliit saatis ca 4000 euro ulatuses tagasimakseid kurjategijatele.

Kontoandmete õngitsemise kõrval oli taas Eestis näha korduvalt SEB panga nime ära kasutavaid õngitsuskampaaniaid eesmärgiga varastada kontodelt raha. Õngitsuskirjade teemaridades kasutati tavapäraseid meelitamisvõtteid, et panna inimesi uudishimu tundma, kas keegi on tõepoolest neile makseid tagasi saatnud või neile on laekunud ootamatu pangaülekanne.

Juunis laekus meile informatsiooni, et aasta varem, 2019. aasta maikuus oli lekkinud ühe Eesti kuulutuskeskkonna 27 000 kasutaja kontoandmed (meilikontod ja paroolide räsid). Kuna samade kontoandmetega enam keskkonda sisse ei saa, on lekke puhul eelkõige ohuks paroolide korduvkasutamine teistes keskkondades. Omanik kinnitas, et on lekkest teavitanud kasutajaid ja Andmekaitse Inspektsiooni.

Juunis teavitati meid kahel korral lunavaraintsidentidest, ohvriteks olid seekord üks kontoritarvete jaemüüja ning üks piimandusettevõte. Mõlemal korral tekitasid intsidendid ettevõtetele teatud määral lisatööd, kuid ei katkestanud äritegevust.

Tegevused küberturvalisuse parandamisel Eestis

Juunis alustasime vee-ettevõtetele suunatud pilootprogrammi, mille eesmärgiks on väikse ja keskmise suurusega elutähtsate teenuste osutajate küberturbe teadlikkuse ja taseme tõstmine. Programmi raames kaardistame koos ettevõtte töötajatega hetkeolukorra, aitame vajadusel juurutada põhilised küberturbe tagamiseks vajalikud protsessid ning leiame koos sobivad tööriistad IT-halduse lihtsustamiseks ning küberturbe tagamiseks.

Praktilise suunitlusega programm tugineb Center of Internet Security Controls (CIS20) meetmetele, mille rakendamise sobilikkust ja vajalikkust ettevõtted testivad. Kõik osalevad ettevõtted asuvad väljaspool Tallinna ja suve jooksul on nendega plaanis ka individuaalsed kohtumised.

Muutsime riigivõrgu turvalisemaks, võttes kasutusele marsruutimisinfo valideerimislahenduse RPKI (Resource Public Key Infrastructure). RPKI kasutamine vähendab riske, mis on seotud Internetis andmete juhtimiseks kasutatava marsruutimisprotokolli (Border Gateway Protocol BGP) disainist tulenevate ja laialt ekspluateeritavate haavatavustega. RPKI valideerimislahendus vähendab oluliselt näiteks BGP kaaperdamise riski, mille tulemuseks võivad olla teenusekatkestused, pettused või andmevargused. Soovitame RPKI kasutuselevõttu kaaluda kõikidel Eesti ettevõtetel, kes omavad internetivõrku. Pikemalt saab lugeda marsruutimisprotokolli BGP riskidest ja nende maandamise võimalustest RIA ohuhinnangust.

Juunis lõpetasime 15 kohaliku omavalitsuse järelevalvemenetlused. Mitmel juhul oli tegemist omavalitsustega, kus varasemalt välja toodud puudused said nüüd tähtajaks kõrvaldatud.

Muudame Eesti küberohupildi selgemaks. Alates juulikuust lõpetame robotvõrgustikega Avalanche ja Necurs nakatumiste kajastamise CERT-EE intsidentide statistikas. Avalanche'i võrgustik peatati rahvusvahelise politseioperatsiooni tulemusel 2016. aasta detsembris (kuid nakatumised jätkusid hiljemgi), Necurs võrgustiku sai Microsoft enda kontrolli alla käesoleva aasta märtsis. Aktiivselt need enam Eesti küberruumi ei ohusta. Esialgu aga võib muudatuse tulemusel näha olla üldist intsidentide hulga langust. Muudatuse tagamaadest ja päevakajalistest trendidest küberruumis saab lugeda meie värskest kvartaliülevaatest.

Rahvusvaheline keskkond

Lunavaraintsidendid maailmas jätkuvad ja selgelt on näha suuremate ettevõtete sihtimist. Lunavara Maze operaatorid väitsid, et on enda kätte saanud Lõuna-Korea tehnoloogiafirma LG mitmeid konfidentsiaalseid projekte hõlmavaid dokumente. Samal ajal tabas DoppelPaymer lunavararünnak Jaapani suurkorporatsiooni Mitsubishit.

Lunavara on kurjategijatele üsna tulus. California ülikool maksis hiljuti pahalastele 1,14 miljonit USA dollarit krüpteeritud andmete – sh. kriitilise väärtusega teadusuuringud – taastamiseks. Oma kvartaliülevaates rõhutame veelkord trendi, et lunavararünnakutega käib üha tihedamini kaasas andmete vargus ja andmete avalikustamise ähvardused.

Juunikuus oli taas näha geopoliitiliste pingete ulatumist küberruumi. India ning Hiina vahelise relvakonflikti järel kirjutati ulatuslikest Hiina päritolu DDoS rünnakutest India riigiteenuste ja finantssektori vastu. India valitsus vastas 59 Hiinaga seotud mobiilirakenduse keelustamisega, mille sekka jäid ka Indias laialdaselt kasutusel olevad TikTok, Weibo ja WeChat.

Sotsiaalmeediaplatvorm TikTok on kasutajaandmete kogumisega jäänud mitmel korral uurijate ja poliitikute hambusse (eelkõige seetõttu, et tegemist on Hiina päritolu firmaga). Apple'i uue operatsioonisüsteemi iOS14 turvameetmete tõttu tuli avalikuks TikToki lõikelaua kopeerimise võte, mida ettevõte selgitas spämmimisvastase meetmena. USA president Donald Trump andis märku, et kaalub äpi keelustamist ka ühendriikides vastukäiguna Hiina tegevustele, tekitades selle tõttu ka paanika platvormi kasutajate hulgas.

Lisaks Indiale, on Hiina jätkanud agressiivset taktikat Austraalia suunas. Austraalia küberamet ASCS avaldas põhjaliku raporti Hiina APT rühmitustega seonduvate rünnakute detailide kohta.

Juunikuus teavitati ka mitmest märkimisväärsest teenustõkestusrünnakust. Ühte Euroopa panka tabas ühel ajahetkel 809 miljonit paketti sekundis, mis on seni suurim sellelaadne DDoS-rünne. Amazon teavitas, et nende vastu suunati 2,3Tbps suuruse teenusetõkestusründe. Mõlemal puhul suudeti rünnakud ilma suuremate kahjudeta peatada.

Juunikuus tuli ilmsiks mitmeid andmelekkejuhtumeid, millest mõned olid seotud COVID-19 kontekstis kiiresti püstitatud andmebaasidega. Indoneesias paisati pimeveebi 230 000 koroonaviiruse patsiendi andmed. Ulatuslik andmeleke tabas Kanada e-õppeplatvormi OneClass, mille tulemusena saadi kätte mitme miljoni õpilase andmed, mis ulatusid üldistest isikuandmetest kuni õppetulemusteni välja.