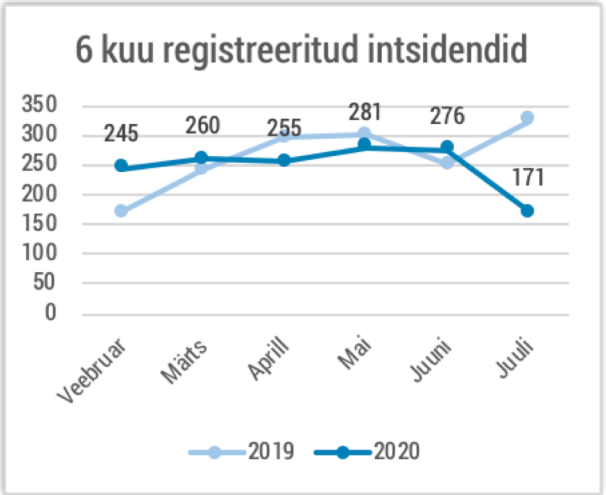
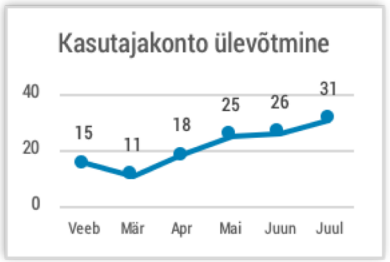
Olukord küberruumis – juuli 2020

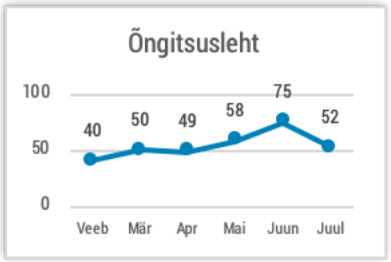
- Registreerisime 171 intsidenti. Tavapärasest väiksem intsidentide arv tuleneb asjaolust, et juulist ei kajastu statistikas enam robotvõrgustikega Avalanche ja Necurs nakatumised.
- Mitmed Eesti veebilehed ei kontrollinud ID-kaardiga autentimisel selle sertifikaatide kehtivust.
- Viisime läbi kampaania, mille eesmärk oli meelde tuletada, et PIN-koode tuleb hoida hoolikalt enda teada.
- Rahvusvahelist keskkonda iseloomustavad suure mõjuga lunavararünnakud ja andmelekked.



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



Varasemast rohkem saame teateid kasutajakontode ülevõtmistest.



Juulis langes õngitsuslehtede arv kolmandiku võrra. Enamus neist püüavad välja petta kontoandmeid.

Olukord Eesti küberruumis

Mitmed Eesti veebilehed ei kontrollinud ID-kaardiga autentimisel selle sertifikaatide kehtivust: CERT-EE tuvastas ligi paarikümmend turvanõrkustega veebilehte, mis ei kontrollinud ID-kaardiga autentimisel, kas selle sertifikaat on kehtiv või mitte. Kahel juhul puudus ka kontroll, kas sertifikaat on SK ID Solutionsi poolt allkirjastatud – see tähendab, et kasutaja võinuks nendesse teenustesse logimisel ise sertifikaadi allkirjastada ning logida keskkonda ükskõik kelle nime ja isikukoodiga.

Arvepettus tõi Viljandi ettevõtte partnerile üle 41 tuhande euro kahju. Saime teate justkui õpiku järgi läbi viidud arvepettusest: petturid kompromiteerisid Viljandi ettevõtte töötaja e-posti konto ja jälgisid tema ning koostööpartneri vahelist kirjavahetust. Hetkel, kui jutt läks arve tasumisele, võtsid sarnast meiliaadressi kasutanud petturid jutujärje üle ja teatasid koostööpartnerile, et Viljandi ettevõtte kodupank sattus uurimise alla, mistõttu palusid arve tasuda uuele kontole. Koostööpartner kandiski, paha aimamata, üle 41 tuhande euro petturite kontrolli all olnud arveldusarvele.

Juulis teavitati meid kolmest lunavararünnakust. Ühel juhul kasutati rünnaku läbiviimiseks RDP (Remote Desktop Protocol) protokolli nõrkust ja krüpteeriti ühe gümnaasiumi serveris olnud failid, mis taastati varukoopiast. Teisel puhul krüpteeris lunavara ühe ettevõtte kaks arvutit, selgi korral õnnestus andmed varundusest taastada. Kolmanda lunavararünnaku ohvriks eraisik, kelle arvutis olnud failid krüpteeriti.

Katkestus Riigivõrgu töös. 21. juuli õhtul katkes avalikule sektorile andmesideteenust pakkuva Riigivõrgu ühendus kõigil Tapa linnas asuvatel asutustel. Ühenduseta jäid ka osad kliendid Rakveres, Narvas ja Tartus. Ligi kaks tundi kestnud katkestuse põhjustas Riigi Infokommunikatsiooni Sihtasutuse (RIKS) poolt läbi viidud elektritööd, millest Riigivõrku eelnevalt ei teavitatud.

Tegevused küberturvalisuse parandamisel Eestis

Viisime läbi kampaania, mille eesmärk oli meelde tuletada, et ID-kaardi, mobiil-ID ja Smart-ID PIN-koode tuleb hoida hoolikalt enda teada. Oleme korduvalt näinud, kuidas hooletu ümberkäimine oma PIN-koodidega viib selleni, et inimesed annavad võõrale ligipääsu oma andmetele või pangakontole. Parim kaitse on ohtudest teadlik ja ettevaatlik kasutaja. Seepärast rõhutasimegi kampaaniaga, et PIN-koode ei tohi unustada, jagada teistega ega sisestada, kuhu juhtub. PIN1 oled sina, PIN2 on su allkiri. Kampaania videoklippe vaata siit.

Avaldasime ohuhinnangu varasemast ohtlikumaks muutunud lunavararünnakute kohta. Viimaste kuudel on lunavararünnakute seas sagenenud selliste rünnete osakaal, kus lisaks andmete krüpteerimisele need ka varastatakse ja ähvardatakse avalikustada. Olukorras, kus GDPRi ehk isikuandmete kaitse üldmääruse rikkumise eest võib määrata kuni 20 miljonit eurot trahvi, on tõenäoline, et ohvri survestamiseks kasutavad ründajad ka edaspidi ähvardust andmed lekitada. Seega ei piisa lunavararünnakute vastu võitlemisel andmete varundamisest. Loe RIA ohuhinnangut ja soovitusi, kuidas end lunavararünnakute eest kaitsta.

Juulis lõpetasime järelvalvemenetluse kuue kohaliku omavalitsuse suhtes. Neis on nüüd turvanõuded piisavas ulatuses täidetud.

Muudame Eesti küberohupildi selgemaks. Alates juulikuust lõpetasime 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. Nende kahe võrgustikuga nakatumised moodustasid ligikaudu 95% kõigist meie märgitud robotvõrgustikuga nakatumistest ja umbes 60% kõigist mõjuga intsidentidest. Aktiivselt need enam Eesti küberruumi ei ohusta. Esialgu aga võib muudatuse tulemusel näha intsidentide hulga langust.

Rahvusvaheline keskkond

Juulis pakkus kõneainet Twitterit puudutanud intsident. Selle käigus kaaperdati mõjukate poliitikute, ettevõtjate, muusikute, aga ka näiteks Apple'i ning Uberi ametlikud kontod, mida kasutati krüptoraha-pettuste läbiviimiseks. Kuigi rünnaku motiiv näib olevat rahalise kasu teenimine, kasutasid küberkurjategijad võimalust lugeda osade rünnaku ohvriks langenud inimeste privaatsõnumeid. Twitteri esindajad selgitasid, et ründaja sai manipuleerimisründe tagajärjel ligipääsu Twitteri sisemistele süsteemidele.

Nutikellade tootjat Garmin tabas laialdane lunavararünnak, mille tagajärjel lakkasid töötamast mitmed olulised teenused. Hispaania riiklikku raudteefirmat tabas REVili lunavararünnak, mille käigus sai küberrühmitus enda kätte suure hulga konfidentsiaalseid dokumente. Lunavararünnaku ohvriks sattus ka USA ettevõte Blackbaud, mis haldab ülikoolide ja rahvusvaheliste organisatsioonide administratiiv- ning finantssüsteeme. Prantsusmaa suurim telekomi-ettevõte Orange sattus lunavara-rünnaku ohvriks, mille käigus saadi ligipääs ettevõtte teabele ning suhtlusele partneritega.

Briti ja Kanada küberagentuurid väidavad, et Venemaaga seostatav häkkerirühmitus APT29 on WellMess ja WellMail pahavara kasutades **rünnanud koroonavaktsiini arendavaid laboreid.**

Põhja-Koreaga seotud küberrühmitused, sealhulgas APT Lazarus/Hidden Cobra, viivad läbi Magecarti pangakaardipettuseid USA ja Euroopa kodanike vastu, laiendades enda haaret väljapoole Korea poolsaart.

Ummistusrünnete hulk kasvas hüppeliselt. 2020.a esimeses kvartalis oli eelnevast 542% rohkem hajusaid ummistusründeid, mis võib osaliselt tuleneda pahaloomulise tegevuse kasvust COVID-19 pandeemia ajal.

Juulis lekkisid taas miljonite inimeste andmed. Pangandusrakenduse pakkuja Dave teatas ligi 7,5 miljoni kasutaja andmete lekkimisest. Lekkisid ka ligi 142 miljoni MGM hotelli külastaja isikuandmed.

Esmakordselt ajaloos kehtestas Euroopa Liit sanktsioonid küberrünnakute eest. Neid rakendati mitme Hiina ja Vene kodaniku ning ettevõtte vastu.