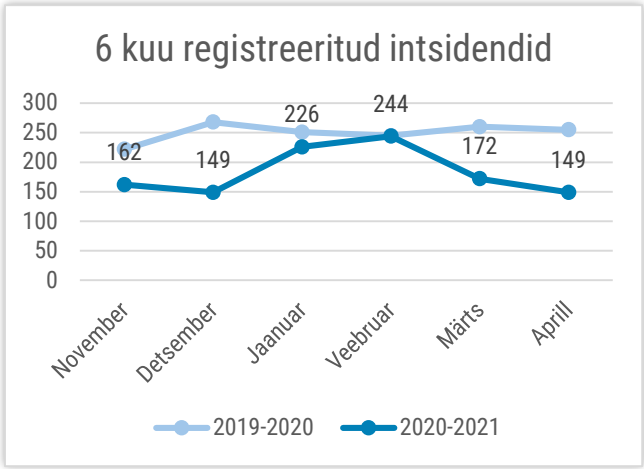
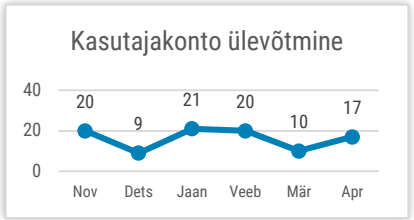
Olukord küberruumis – aprill 2021

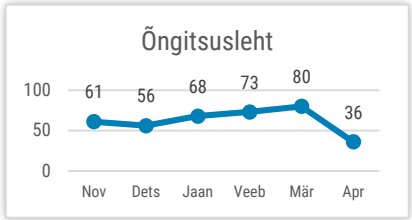
- Aprillis registreerisime 149 mõjuga intsidenti, mis on keskmisest madalam näitaja.
- Aprillis nägime mitut suure mõjuga teenusekatkestust, häiritud oli muu hulgas riikliku autentimisteenuse TARA ja Eesti.ee portaali töö.
- IT-teenusepakkuja rünnaku kaudu levis lunavara nelja Eesti ettevõtteni.
- Osalesime koos kolleegidega era- ja avalikust sektorist maailma suurimal küberkaitseõppusel Locked Shields.
- USA rakendas sanktsioone Venemaa vastu SolarWindsi kompromiteerimise intsidendi järel.



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



Meilikontode ja sotsiaalmeedia-kontode ülevõtmine on jätkuvalt päevakajaline.



Aprillis langes õngitsuslehtede intsidentide hulk märgatavalt.

Olukord Eesti küberruumis

Aprillis iseloomustasid olukorda Eesti küberruumis mitmed häirivad katkestused riiklike teenuste töös. 22. aprilli pealelõunal ei saanud paari tunni vältel kasutada eesti.ee portaali ja kolmveerand tunni jooksul riigi autentimisteenust (TARA), mille tagajärjel ei olnud võimalik ühtegi TARA kasutavasse teenusesse sisse logida. Katkestuse põhjustas riistvara rike. Teenuste ümber lülitamisel tekkis mõningaid viivitusi, ent sama päeva õhtuks õnnestus kõik teenused taastada.

28. aprilli õhtul ei saanud kahe ja poole tunni jooksul kasutada riiklikku allkirjastamisteenust, põhjuseks tarkvara viga. Samuti oli aprillis tõrkeid haigekassa e-teenuste kättesaadavusega. Neist pikaajalisem oli 13. aprillil digiretsepti kasutamise töös, kestes pea 7 tundi.

Jätkuvalt kimbutavad Eesti ettevõtteid lunavararünnakud. Aprillis saime teada juhtumist, kus lunavara tabas IT-teenust pakkuvat ettevõtet ning laienes selle kaudu veel nelja firmasse. Krüpteerimiseks kasutati LockBiti nimelist pahavara ning kuna ettevõttel oli rünnaku ajal kaugtöölaua protokolli (RDP) kaudu ligipääs nelja kliendi süsteemidesse, nakatusid needki. Kõik viis taastasid andmed varukoopiatest ning esialgsel hinnangul andmeleket ei toimunud. Intsident näitab, et lisaks oma süsteemidele tuleb kriitiliselt hinnata ka oma IT-teenusepakkuja küberturvalisust.

Lisaks tabas eelmisel kuul lunavararünnak ühte väiksemat Lõuna-Eesti IT-ettevõtet ning ühte külmaseadmetega tegelevat ettevõtet, mõlemal juhul kaotati olulisi andmeid.

Eestit puudutas aprillis ka ühe varasema Facebooki kasutajaandmete hiigellekke andmete avalikustamine. Andmed tehti tasuta kättesaadavaks ühes häkkerite foorumis ning selles leidusid ka 87 533 Facebooki Eesti kasutaja andmed (peamiselt telefoninumbrid). Leke ise toimus 2020. aastal, kui kurjategijatel õnnestus kätte saada 533 miljoni Facebooki kasutaja isiklikud andmed kokku 106-st riigist.

Oleme viimastel kuudel mitmeid kordi kirjutanud teenusetõkestusrünnetest ning aprillis nägime taas üht rünnet veebimajutusega tegeleva ettevõtte vastu. Pisut üle pooleteist tunni väldanud rünne tabas ettevõtte nimeservereid, mistõttu oli häiritud teenuste kasutamine. Võrreldes aasta alguses nähtud ummistusrünnetega kestis seekordne lühemat aega ja oli väiksema mõjuga.

Tegevused küberturvalisuse parandamisel Eestis

Panime kokku Eesti meeskonna, mis osales NATO küberkaitsekoostöö keskuse CCDCOE korraldatud rahvusvahelisel õppusel Locked Shields. Locked Shields on suurim taoline küberkaitseõppus, millest võttis tänavu osa rohkem kui 2000 eksperti enam kui 30 riigist. Eesti meeskond koosnes oma ala parimatest tegijatest nii erasektorist kui avalikust sektorist, kellest valdav osa oli tehnilise intsidendihalduse ja kriminalistika taustaga küberkaitse eksperdid.

Locked Shieldsi tehnilise õppuse kõrval toimunud strateegiamängus osalesid RIA esindajate kõrval ka kolleegid Kaitseministeeriumist, Eesti Pangast, Majandus- ja Kommunikatsiooniministeeriumist, KV Küberväejuhatusest, Välisministeeriumist ja Riigikantseleist. Täname kõiki, kes said õppusel Eesti meeskonda panustada!

Alustasime Eesti uue infoturbestandardi (E-ITS) tutvustamise ja juurutamise tegevustega. Märtsis avalikkuse ette jõudnud E-ITS peaks pika üleminekuperioodiga aastaks 2024 välja vahetama senise avaliku sektori infoturbestandardi ISKE. Selleks korraldasime aprillis esimesed koolitused infoturbejuhtidele ja standardi rakendajatele. Esimese poolaasta jooksul toimub veel neli taolist koolitust, teise poolaasta koolituste kohta anname jooksvalt teada E-ITSi portaalis eits.ria.ee.

Lisaks koolitustele alustasime aprillis ka standardi pilootprogrammiga kümnes asutuses – kohalikest omavalitsustest haiglate ja ministeeriumiteni. Töötame paralleelselt ka õigusruumi korrastamisega E-ITSi kasutusele võtmiseks. .

Aprillis avaldasime küberturvalisuse aastakokkuvõtte, mis rääkis möödunud aasta rekordarvust õngitsustest, ummistusrünnakutest, Emotet pahavarast ja ministeeriumeid tabanud küberrünnakutest. Intsidentide kõrval saab lugeda COVID-19 mõjust Eesti küberruumile, RIA suuremast rollist valimistel ning tutvuda uue Eesti infoturbestandardiga ja olulisemate arengutega rahvusvahelises küberkoostöös. Aastakokkuvõte on leitav ka inglise keeles.

Rahvusvaheline keskkond

Möödunud kuu jooksul pöörati kürberturbe maastikul jätkuvalt olulisel määral tähelepanu SolarWindsi ja Microsoft Exchange'i intsidentide järelmitega tegelemisele. SolarWindsi küberrünnaku eest rakendas USA Venemaa vastu sanktsioone ning saatis riigist välja 10 vene diplomaati, mille kohta tegi toetava avalduse ka EL ja Eesti. Microsoft Exchange'i intsidendi puhul nägime, et neid, kes serverid kiiremas korras paikamata jätsid, tabasid eri tüüpi rünnakud, alustades lunavarast kuni robotvõrkude poolt krüptoraha kaevamiseni välja.

Paroolihaldur Passwordstate langes rünnaku ohvriks, kui kurjategijad suutsid ettevõtte süsteemid kompromiteerida ning tarneahelarünnakus klientidele saata pahavaraga tarkvarauuenduse. Pahavara hakkas seejärel saatma paroolihaldurisse salvestatud paroole kurjategijatele. Ettevõte väitel on paroolihalduril enam kui 29 000 korporatiivkasutajat.

Aprillis tabasid tähelepanuväärsed lunavararünnakud Itaalia panka Banca di Credito, Brasiilia Rio di Grande do Sul osariigi kohtusüsteemi, Ühendkuningriigi raudtee-ettevõtet Merseyrail, Prantsusmaa farmatseutikaettevõtet Pierre Fabre ning USA haiglate IT-teenuse pakkujat Unitingcare. Võttes arvesse lunavara järjest kasvavat halvava mõju majandusele ning ühiskonna toimepidevusele, koondusid ligi 60 ülemaailmset küberturbe valdkonna tegijat kokku lunavara vastu võitlemiseks loodud rakkerühma, mis proovib kriminaalsete rühmituste finantstehingutele jälile saades nende tööd tõkestada.

Üle 533 miljoni Facebooki kasutaja, sealhulgas ligi 90 000 Eesti kasutaja, isiklikud andmed lekkisid ja on avalikult kättesaadavad. Tegemist oli kasutajate endi poolt avalikuks jäetud andmete laiaulatusliku automaatse kogumise tagajärjel ehitatud andmebaasiga. Facebooki seisukoht on, et nende süsteemi ei olnud kuritarvitatud. Iirimaa andmekaitse amet algatas aprilli keskel intsidendi suhtes järelevalvemenetluse.

Erinevate intsidentide taustal toimuvad aga olulised muutused interneti valitsemise ning konkurentsi valdkonnas üle maailma, millest kirjutas kokkuvõtlikult New York Times. Arengud puudutavad peamiselt tehnoloogiahiidude tegevust eelkõige EL-is, USA-s, Hiinas ja Austraalias, kus poliitikakujundajad on luubi alla võtnud laia ringi teemasid nagu tehisintellekt, terroristliku sisu platvormidelt eemaldamine ja aus konkurents.

Möödunud kuul täheldati, et riikliku taustaga küberrühmitused (APT-d) kasutavad ära rünnakutes Pulse Secure VPNi nullpäeva turvaauku, mille kaudu langesid ohvriks asutused nii USA-s kui Euroopas. Turvanõrkused pärinesid juba mitme aasta tagant.