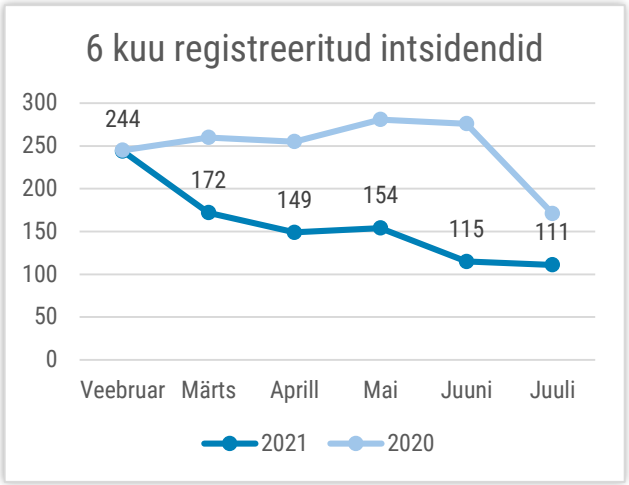
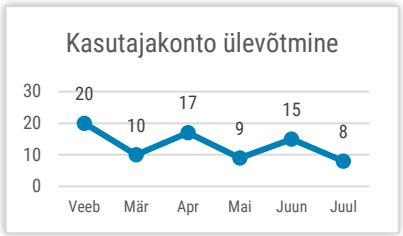
Olukord küberruumis – juuli 2021

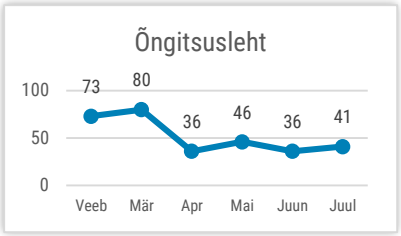
- Juulis registreerisime 111 mõjuga intsidenti. Intsidentide langustrend jätkub.
- Riigiportaalis olid tarkvaravea tõttu kättesaadavad ettevõtetega seotud isikute andmed.
- Peatasime massilise dokumendifotode andmevarguse, ründaja tuvastati ja peeti kinni.
- Cybernetica eksperdid analüüsisid e-hääletusel biomeetrilise isikutuvastamise võimalusi.
- Kurjategijad suutsid tarneahelarünnakus lunavaraga nakatada tuhandeid arvuteid üle maailma.



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



Meili ja sotsiaalmeedia-kontode ülevõtmine on jätkuvalt päevakajaline.



Õngitsuslehed moodustavad üha suurema osa kõigist mõjuga Intsidentidest.

Olukord Eesti küberruumis

Juulis nägime kaht suurema mõjuga isikuandmetega seotud intsidenti. Kuu alguses teavitas tähelepanelik Eesti.ee portaali kasutaja tarkvaraveast ettevõtjatele mõeldud iseteeninduskeskkonnas, mis näitas enam kui 300 tuhande juriidiliste isikutega seotud inimeste ees- ja perekonnanime, isikukoodi, töökohta ning osa puhul veel seoseid eelnevate ametikohtadega. Andmebaasile oli võimalik ligi pääseda ainult nendel inimestel, kelle andmed olid andmebaasis.

Avastasime ja peatasime ka ühe massilise andmevarguse, kus ründaja laadis isikut tõendavate dokumentide andmekogust alla 286 438 inimese fotod. Kahtlustatav ei saanud ligipääsu tervele andmekogule, vaid kuritarvitas turvanõrkust ühes RIA hallatavas teenuses, mis võimaldas tal matkida autentset päringut ja niimoodi kätte saada inimeste dokumendifotod. RIA sulges teenuse pärast väärkasutamise avastamist ja parandas turvavea. Kõigile neile, kelle dokumendifoto ebaseaduslikult alla laaditi, saatis PPA vastava teavituse riigiportaali eesti.ee kaudu suunatud e-posti aadressile. Ükski ohver ei pea tegema uut fotot ega taotlema uut dokumenti. Teavitasime juhtunust politseid, kes asus vargust uurima ning suutis kahtlustatava tuvastada ja kinni pidada. Juhtunu asjaolude väljaselgitamiseks alustati kriminaalmenetlust.

Juulis teavitati meid ka paarist lunavaraintsidendist. 12. juulil nakatus ühe kohtutäituri server lunavaraga. Süsteem taastati värskest tagavarakoopiast. Taoliste rünnakute puhul tuleb märkida, et ründajad võivad proovida enne krüpteerimist süsteemidest andmeid ka varastada ja lunaraha maksmata jätmise korral nende avalikustamisega ähvardada.

Juuli keskel teavitas meid lunavararünnakust üks suurem Eesti tööstusettevõte, rünnak häiris ettevõtte tööd märkimisväärselt.

Juuli teises pooles teavitas üks haigla meid intsidendist, kus võrguliikluse anomaaliate tõttu olid selgelt häiritud haiglasisesed teenused. Tuli välja, et intsidendi põhjustas sama haigla üks töötaja, kes pakkus abi WiFi-ühenduse parandamiseks ja lisas võrku uue seadme, kuid kaablite ringiühendamisega tekitas suurema probleemi, kui see, mida algselt lahendama asus.

Tegevused küberturvalisuse parandamisel Eestis

15. juulist alustas küberturvalisuse teenistuse juhi ametis tööd Gert Auväärt, kes seni töötas Eesti alalise esinduse juures ÜROs.

Juuli alguses avalikustati Cybernetica küberekspertide koostatud analüüs biomeetria rakendamise kohta e-hääletamisel. Analüüs tõdeb, et näotuvastuse lisamine e-hääletuse autentimisse on küll tehtav, kuid privaatsusriive ja tehnoloogilise keerukuse tõusuga kaasnevad riskid ei pruugi kaaluda üles sellest saadavat kasu. Meie seisukoht on, et näotuvastuse kasutamine vajab pikaajalist testimist ning sellele eelnevat ühiskondlikku debatti privaatsusest, ligipääsetavusest ja muidugi üldisest küberturvalisusest. Analüüsiga on võimalik tutvuda siin.

Biomeetrilise isikutuvastusega liigutakse maailmas edasi. Juulis andsime uue tegevusloa sertifitseerimisteenusega tegeleva ettevõtte SK ID Solutions'i biomeetriat kasutavale autentimisele nende Smart-ID isiku samasuse tuvastuslahenduses. Juba praegu on tegelikult võimalik varasematel Smart-ID klientidel kontot uuendada biomeetrilise isikutuvastuse abil (kasutades nt kiibiga passi ja NFC toega telefoni). Uue lahendusega võib SK ID Solutions pakkuda Smart-ID teenust biomeetriliste isikusamasuse tuvastuse abil ka klientidele teistes riikides

Järjekordses kvartaliülevaates kirjeldasime 2. kvartalis nähtud küberintsidente ja nende trende. Olulisteks teemadeks on jätkuvalt lunavara ja IT-teenusepakkujate kaudu klientide ründamine, samuti selgitasime Euroopa plaane ühise küberüksusega (Joint Cyber Unit). Kvartaliülevaadet on võimalik lugeda siit.

Rahvusvaheline keskkond

Rahvusvahelises küberruumis andis juulile tooni ulatuslik lunavararünnak USA tarkvaraettevõtte Kaseya pihta. Nimelt õnnestus Venemaal tegutseval rühmitusel REvil nakatada lunavaraga *ca* 1500 ettevõtet 17 erinevast riigist, mis kasutasid Kaseya pilvepõhist lahendust IT-süsteemide kaughalduseks (VSA ehk Virtual System Administrator). Üheks rünnaku ohvriks oli Rootsi COOP kaupluskett, mis pidi viieks päevaks sulgema 800 kauplust, sest arveldussüsteem ei töötanud. Rühmitus nõudis Kaseyalt universaalse dekrüpteerimisvõtme eest 70 miljonit dollarit lunaraha. Oma sõnul Kaseya lunaraha ei maksnud ja sai dekrüpteerimisvõtme hoopis usaldusväärselt kolmandalt osapoolelt.

Nii Kaseya pihta tehtud rünnak kui ka teised hiljutised küberintsidendid (nt JBS, Colonial Pipeline) suunasid ka poliitilise tasandi pilgud küberkurjategijate poole. USA president Joe Biden hoiatas korduvalt Venemaa presidenti Vladimir Putinit, et Venemaal on tagumine aeg võtta midagi ette nende territooriumilt vabalt tegutsevate küberrühmitustega. Juulis kaduski internetist rühmitus REvil (Kaseya ründaja), Darkside (Colonial Pipeline-i ründaja) oli kadunud juba varem. Pole endiselt teada, kas rühmituse kadumiste taga oli USA, Venemaa või otsustasid nad ise oma tegevusega tagasi tõmmata. Samas aga aktiveerus juuli lõpus uus lunavararühmitus nimega BlackMatter, millel on mitme väljaande teatel sidemed REvili ja Darkside-ga.

Juulis mõistis USA koos liitlastega (sh Eesti) ametlikult hukka Hiina Rahvavabariigi tegevuse küberruumis. Sealjuures süüdistati Hiinat ka tänavu kevadel Microsoft Exchange emaili serverite pihta tehtud rünnakus, millega said pihta ettevõtted ja riigiasutused üle maailma. Hukka mõistmisega ei kaasnenud Hiinale sanktsioone. Hiina ise eitas igasugust süüd.

Valgevene protestiliikumise häkkerid („*Cyber Partisans*"), kes võitlevad Valgevene praeguse režiimi vastu, pääsesid ligi Valgevene riiklikele andmebaasidele. Väidetavalt sai rühmitus kätte info näiteks valgevenelaste (sh KGB töötajate ja informaatorite) nimede, passinumbrite, töökohtade, autode kohta.

Uut infot tõi ka Solarwinds'i uurimine. Nimelt teatas USA justiitsministeerium, et Solarwinds'i ründajad pääsesid ligi Taani keskpanga süsteemidele ja 27 USA föderaalprokuröri või nende kaastöötajate meilikontodele.

Suurt rahvusvahelist tähelepanu pälvis seegi, et mitmed riigid kasutasid lisraeli ettevõtte NSO loodud Pegasuse tarkvara ajakirjanike, poliitikute ja aktivistide järele luuramiseks. Pegasuse tarkavaraga nakatudes saab käivitada sihtmärgi telefonikaamera ja mikrofoni, samuti pääseb ligi sõnumitele, fotodele ja saab salvestada kõnesid.