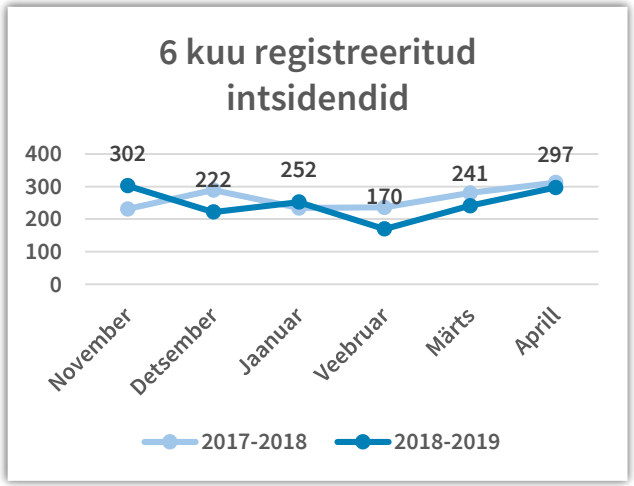
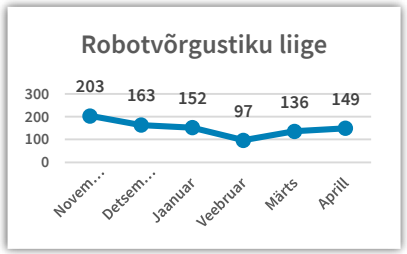
Olukord küberruumis – aprill 2019

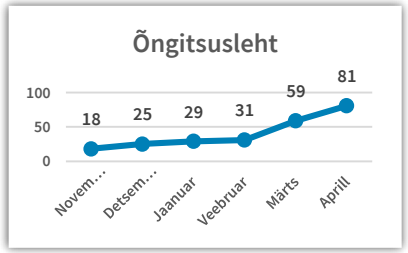
- Aprillis registreerisime pea 300 intsidenti ning intsidentide hulk on võrreldes aasta alguse madalseisuga hakanud tasapisi kasvama.
- Aprillis märkasime lunavararünnakute kasvu, samuti tegelesime tavapärasest enam õngitsuslehtedega.
- Eestis laialt kasutatav Smart-ID autentimisvahend võeti kurjategijate poolt sihikule.
- RIA juhtis maailma ühel suurimal küberkaitseõppusel Locked Shields Eesti meeskonda.
- Maailma suured veebiteenuste pakkujad võitlevad andmeleketega.



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



Kõige rohkem saame teateid robotvõrgustikuga nakatunud arvutitest Eesti küberruumis, mille kohta teated on hakanud taas sagenema.



Üha enam tuvastatakse õngitsemislehti, mille eesmärgiks on saada kasutaja sisselogimis- või krediitkaardi-andmeid.

Olukord Eesti küberruumis – Smart-ID ärakasutamine

Aprillis saime teada intsidentidest, kus õngitsus-sõnumeid ja õngitsuslehti ära kasutades üritati luua ohvrite nimel uut Smart-ID kontot, mis meile teadaolevalt mitmel korral ka õnnestus. Kasutajatele saadeti mobiiltelefoni tuntud panga nimelt sõnum, mis suunas näiliselt panga sisselogimisleheküljele. Seal suunati ohver õngitsuslehele Mobiil-ID-ga sisse logima. Kui ohver sisestas oma kasutajatunnuse ja isikukoodi ja PIN 1, alustasid kurjategijad samal ajal taustal hoopis uue Smart-ID konto loomist. Ohvri tähelepanu hajutades suunati teda tegema järgmisi vajalikke samme, et Smart-ID konto loomine taustal lõpetada. Niimoodi said kurjategijad luua uue Smart-ID konto ja logida ohvri andmetega sisse teenustesse, mis Smart-ID sisselogimist pakuvad, sealhulgas pankadesse. Meile teadaolevalt on üksikuid ohvreid, kes on kannatanud ka rahalist kahju.

Sisuliselt kasutavad kurjategijad ära olukorda, kus kasutaja ei pööra tähelepanu kontrollkoodidele ja teenusepakkujate nimedele ning sisestab oma PIN-koodid harjumusest.

Smart-ID teenusepakkuja SK ID Solutions tegeleb taoliste petuskeemide vältimise nimel ja töötab välja lisameetmeid kasutajate teavituseks. Oleme algatanud intsidendi tõttu järelevalvemenetluse.

Soovitame kõigil Mobiil-ID ja Smart-ID kasutajatel enne PIN-koodide sisestamist alati vaadata teenusepakkuja kontrollkoodi ning teenuse nimetust. Eestis kasutab Smart-ID-d 420 000 inimest, sellega on võimalik end autentida nii eraettevõtjate (finantsteenused, koduteenused), aga ka riiklike teenuste juures.

Olukord Eesti küberruumis

Täheldasime lunavaraga nakatunud infosüsteemide tõusu Eesti ettevõtete seas. Nakatunute seas oli ka üks elutähtsa teenuse osutaja, kellel olid andmed korrektselt varundatud, seega piirnes mõju teenusele suurenenud ajakuluga ning teenus ise ei katkenud. Intsident kinnitab taaskord, et enamalt jaolt kasutatakse lunavaraga nakatumisel ära kaughalduslahendusi (Remote Desktop Protocol ehk RDP), mis on jäetud kas täielikult avatuks või on kasutatud kergelt äraarvatavat parooli. Siinkohal palume taas kõigil üle kontrollida oma olemasolevad avatud teenused, millest oleme rääkinud ka varem ning rakendada tugevat paroolipoliitikat.

Jätkusid ettevõtete meilikontode kompromiteerimised, mille mõju piirnes valdavalt andmete konfidentsiaalsuse rikkumisega. Sellistel juhtumitel tuleb arvestada, et küberkurjategijad on saanud ligi meilikontodel olevale infole. Alates eelmise aasta sügisest oleme näinud, kuidas taoliste meilikontode kompromiteerimise tagajärjel võidakse mõne osapoole käest raha välja petta.

Tegevused küberturvalisuse parandamisel Eestis

Aprilli keskel juhtisime Eesti meeskonda maailma suurimal küberkaitseõppusel Locked Shields, mida korraldab NATO küberkaitsekeskus aastast 2010. Umbes 45-pealine meeskond pidi kahe päeva jooksul tõrjuma rünnakuid fiktiivse riigi Berylia vee-, energia- ja sidesüsteemide vastu. Eesti meeskond koosnes eelkõige erasektori spetsialistidest, taolised õppused aitavad Eesti küberturvalisuse kogukonnal üksteist paremini tundma õppida, et päris kriisiolukorras paremini koostööd teha.

Aprillikuus alustasime järelevalvemenetlusi järgmise kaheksa kohaliku omavalitsuse suhtes, seekord võtsime fookusesse Lääne-Virumaa. Haldusjärelevalve menetluste eesmärk on kontrollida seda, kuidas omavalitsused täidavad infosüsteemide turvameetmete süsteemi määrust, kuidas rakendavad kohustuslikku infoturbe standardit ISKE ning kuidas nad käsitlevad ja lahendavad turvaintsidente. Alates aasta algusest oleme algatanud menetlused kokku 26 omavalitsuse suhtes.

Osalesime koos Politsei- ja Piirivalveameti, Riigiprokuratuuri ja Andmekaitse Inspektsiooniga Saaremaa ettevõtjate küberturvalisuse päeval, kus sadakond huvilist said ülevaate küberturvalisuse hetkeseisust Eestis.

Tegime aprilli alguses koostöös Andmekaitse Inspektsiooniga teavituse ettevõtetele e-posti serverite turvalisuse tähtsusest. E-postist saavad alguse mitmed küberintsidendid ning e-posti serverite turvalisust saab lihtsasti parandada. Loe lähemalt siit.

Rahvusvaheline keskkond

Prantsusmaa valitsus otsustas luua valitsusametnikele eraldi sõnumite vahetamise keskkonna, äpi nimega Tchap, et valitsuse töötajad ei suhtleks omavahel enam kasutades erinevaid sõnumikeskkondi nagu Telegram, Whatsapp või Signal. Sõnumiäpp arendati avatud lähtekoodi põhjal ning selle arendust koordineeris Prantsusmaa küberturvalisuse agentuur ANSSI.

Hollandi luure- ja julgeolekuagentuur AIVD soovitas riigil mitte soetada uut tehnoloogiat riikidest nagu Hiina ja Venemaa, kus viiakse aktiivselt läbi küberoperatsioone Hollandi huvide vastu. Huawei küsimuses oodatakse maikuus ka Ühendkuningriikide valitsuse seisukohta; aprillis anti mõista, et lubatakse Hiina ettevõttel osaleda teatud piirangutega Ühendkuningriikide 5G võrkude ehitamisel. Ameerika ühendriigid jätkuvalt soovitavad Huaweid vältida, rõhutades nende seotust Hiina luureasutustega ning hoiatades, et vastasel korral võib USA piirata infovahetust liitlastega.

Sadade miljonite kaupa sotsiaalmeediavõrgustiku Facebook kasutajate andmeid leiti avalikult ligipääsetavast andmebaasist, kuhu võis ligi pääseda igaüks. Tegemist oli digitaalse meedia ettevõtte Cultura Colectiva poolt kogutud andmetega. Aprillikuus teatas Facebook, et oli kogemata kogunud 1,5 miljoni uue kasutaja meilikontodelt sõprade meiliaadresse ilma luba küsimata.

Microsoft teatas, et osa tema teenuse Outlook.com kasutajate kontodest olid kompromiteeritud. Algselt anti märku, et sissetungijad võisid näha vaid meilivestluste pealkirju ja meta-andmeid, siis hiljem teatas Microsoft, et osade kontode puhul oli häkkeritel võimalik ligi pääseda kõigile kirjadele.

Küberturvalisuse ettevõte Cisco Talos on tuvastanud DNS-i kaaperdamisi, mida kasutatakse ära näiteks kasutajakontode varastamiseks või võrguliikluse pealtkuulamiseks. Tegemist on erinevate meetoditega, kuid ühiseks jooneks on interneti põhialustala – DNSi ehk nimeserverite taristu – kaaperdamine.

Sarnaselt Eestile on ka maailmas lähiajal nähtud lunavararünnakute kasvu. Pihta on saanud mitmed ettevõtted, linnad ja maakonnad. Samamoodi jätkuvad maailmas finantspettused meilivestluste kaaperdamiste teel.