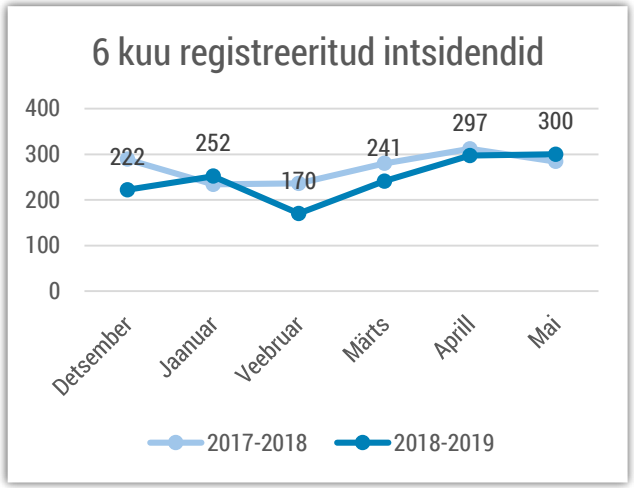
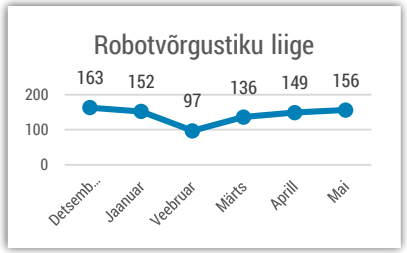
Olukord küberruumis – mai 2019

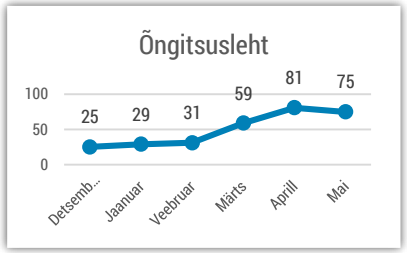
- Maikuus registreerisime 300 intsidenti, mis on võrreldav olukorraga aasta tagasi.
- Jätkusid rünnakud Eestis laialdaselt kasutatava autentimisvahendi Smart-ID kaaperdamiseks.
- Valitsus kinnitas Eesti seisukohad rahvusvahelise õiguse kohaldumise kohta küberruumis.
- Eesti uut infoturbestandardit hakkavad koostama KPMG Baltics, Cybernetica ja TalTech.
- USA otsus lisada Huawei musta nimekirja hakkab mõjutama ettevõtet ka väljaspool 5g tehnoloogiat.



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



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



Õngitsuslehtede intsidentide kasv sel kevadel on osaliselt seotud Smart-ID õngitsuskatsetega.

Olukord Eesti küberruumis

Maikuus nägime taas autentimisvahendi Smart-ID-ga seotud intsidente, kus õngitsussõnumite ja –kirjade kaudu püüti luua vale isiku käsutuses olevale seadmele uut Smart-ID kontot. Sarnastest intsidentidest kirjutasime ka aprillikuu ülevaates ja Eesti ajakirjanduses on juba räägitud maikuus toimunud intsidentidest.

Smart-ID teenusepakkuja SK ID Solutionsi teatel suutsid kurjategijad aprillis ja mais niimoodi luua 28 kontot, mille kaudu on jõutud vähem kui kümnel korral ka pankades neid kasutada ülekannete tegemiseks. Selliste intsidentide jaoks on loodud lainetena pankade sisselogimislehti imiteerivaid õngitsuslehti, mis selgitab õngitsuslehtede intsidentide kasvu kevadperioodil.

SK ID Solutionsi osas algatasime järelevalvemenetluse juba aprillis. Maikuus tegime SK ID Solutions'ile ettepanekud Smart-ID loomise protsessi tugevdamiseks ning ettevõte teeb nii RIAga kui Politsei- ja Piirivalveametiga pidevat koostööd järgmiste intsidentide ennetamiseks ja kurjategijate tabamiseks.

Eelmisest aastast alates nähtud **finantspettuste laine e-mailikontode kompromiteerimise teel näitas viimastel kuudel hääbumise märke**. Pettusekatsetest saame jätkuvalt teada, kuid maikuus teavitati meid vaid ühel korral intsidendist, kus ettevõte kandis 25 000 euro suuruse makse petturitele.

Euroopa parlamendi valimiste ajal e-hääletamisega seotud märkimisväärseid intsidente me ei registreerinud. Hääletusperioodil valimistega otseselt mitteseotud intsidentidest oli märkimisväärseks umbes pooletunnine **teenustõkestusrünnaku katse RIA hallatava lehekülje www.id.ee vastu** 19. mai hilisõhtul. Rünnaku takistas DDOS-vastane kaitseteenus, mis enne kevadisi Riigikogu valimisi selliste intsidentide tarbeks soetatud ning teenusekatkestust ei registreeritud.

9. ja 10. mai vahel oli enam kui 24 tunni jooksul häiritud Mobiil-ID teenuse kasutamine. Alustasime seetõttu ka järelevalvemenetlust, et välja selgitada, kuidas vältida taolisi katkestusi tulevikus.

Tegevused küberturvalisuse parandamisel Eestis

Koos Kaitseväe korraldatud igakevadise suurõppusega, milleks tänavu oli Kevadtorm, **harjutasime koos Kaitseväe küberväejuhatuse, Kaitseliidu küberkaitseüksuse ja Eesti energiavarustajatega läbi hädaolukorra lahendamise küberõppusel Kübertorm**. Õppuse eesmärkideks oli harjutada info vahetamist kõigi osapoolte vahel ning lahendada stsenaariumi järgi olukord, kus ligipääs ühele alajaamale oli raskendatud.

16. mail kinnitas Vabariigi Valitsus Eesti seisukohad rahvusvahelise õiguse kohaldumise kohta küberruumis, mis suurendavad õigusselgust selles valdkonnas ja muuhulgas kinnitavad, et riigid vastutavad oma tegevuse eest küberruumis ning peavad tegema pingutusi, et nende territooriumi ei kasutata teiste riikide ründamiseks. Seisukohad töötati välja Justiitsministeeriumi, Kaitseministeeriumi, Riigi Infosüsteemi Ameti, Välisministeeriumi ja MKM-i koostöös ning konsulteeriti ka NATO CCDCOE ekspertidega. Vabariigi President tõi need seisukohad rahvusvahelise avalikkuse ette oma 29. mail peetud rahvusvahelise küberkonverentsi Cycon 2019 avakõnes.

Mai lõpus korraldasime taas iga-aastase rahvusvahelise CERT-EE sümpoosiumi, kus kübereksperdid said jagada praktilisi kogemusi kolleegidega, kes igapäevaselt seiravad, analüüsivad ja lahendavad küberintsidente nii riiklikes, kui ka erasektori küberturvalisuse meeskondades. Sümpoosiumil käsitleti muu hulgas e-posti turvalisust, andmelekkeid, digitaalsete tõendite kogumist ja uusi tööriistu parema seirevõime jaoks.

Jätkasime küberhügieeni koolitustega kohalike omavalitsuste töötajatele. Mais käisime külas Lõuna-Eesti linnades ja valdades (Võru vald ja linn, Valga, Setomaa, Antsla ja Rõuge) ning seejärel jõudsime ka Tallinna linnaosavalitsustesse.

Oleme aasta algusest valmistanud ette riigihanget uue riikliku infoturbestandardi koostamiseks, mis hakkab asendama seni Eestis riigiasutustele kohustuslikku ISKE etalonturbe süsteemi. Mais jõudis riigihanke protsess lõpuni ning uut infoturbestandardit hakkavad kokku panema KPMG Baltics, Cybernetica ja TalTech. Uus standard ning sellega kaasnevad materjalid peaksid valmis saama järgmise aasta lõpuks.

Rahvusvaheline keskkond

Venemaa president Vladimir Putin kiitis heaks seaduseelnõu, mis teeks vajalikud ettevalmistused ja lubaks vajadusel eraldada Venemaa ülejäänud maailma internetist. Eelnõu autorite hinnangul on see vajalik, et kaitsta Venemaad teiste riikide rünnakute eest. Kriitikud aga näevad selles järgmist sammu sõnavabaduse vähendamiseks. Seadus jõustub novembris.

Ameerika Ühendriigid, kes soovitavad oma liitlastel tungivalt vältida Hiina elektroonikafirma Huawei seadmeid järgmise põlvkonna mobiilsidetaristu ehitamiseks, **otsustasid lisada Huawei ka kaubanduse musta nimekirja**, mis takistab USA ettevõtjatel nendega koostöö tegemise ka valdkondades, mis pole 5g tehnoloogiaga seotud. Nii võib Huawei kaotada ligipääsu näiteks Google'i mobiiliplatvormi Android uuendustele ja Qualcomm tehnoloogial põhinevatele mikrokiipidele.

Mai lõpus kirjutasid 47 maailma ettevõtet, privaatsuse eest võitlevat organisatsiooni ja õppejõudu – nende hulgas Microsoft, Google ja Facebookile kuuluv Whatsapp – **Ühendkuningriikide luureagentuurile GCHQ** avaliku kirja, kus nad kutsuvad agentuuri üles loobuma mõttest lisada krüpteeritud vestlusäppidesse vajadusel pealtkuulamise võimalus. Sellesisulise ettepaneku tegid GCHQ tehnikadirektorid mullu novembris.

Whatsapp teatas kriitilisest turvanõrkusest oma suhtlusäpis, kus ründajal oli võimalik sissehelistamise ajal saata ohvri telefonile nuhkvara, ilma et ohver oleks isegi kõnele vastanud. Whatsappi hinnangul on tegu riikidega koostööd tegeva eraturvafirma loodud pahavaraga, millega seostatakse enim Iisraeli päritolu NSO Gruppi. Üheks sihtmärgiks peetakse inimõiguste eest võitlevat organisatsiooni Amnesty International, kes kaebas NSO Grupi ka kohtusse.

Iisraeli kaitsevägi kasutas esmakordselt küberrünnakutele vastuseks pommirünnakut. Iisraeli kaitsejõud sihtisid Gaza piirkonnas hoonet, kust nende hinnangul pärinesid küberrünnakud Iisraelile.

Veidi enam kui poole miljoni elanikuga **Baltimore'i linn USA idarannikul** langes mai algul taaskord lunavararünnaku ohvriks. Ohtralt aegunud tarkvara kasutanud omavalitsuse taastumine on olnud pikk ja vaevaline ning nädalate kaupa ei olnud võimalik linnas maksta näiteks veearveid ja teha kinnisvaratehinguid.

Singapuri parlament võttis vastu seaduse, mille järgi peavad sotsiaalmeediaplatvormid ametnike nõudmisel selgelt märgistama või eemaldama valeks hinnatud uudised. Karistused ulatuvad 10-aastase vanglakaristuse ja 700 000 euroni.