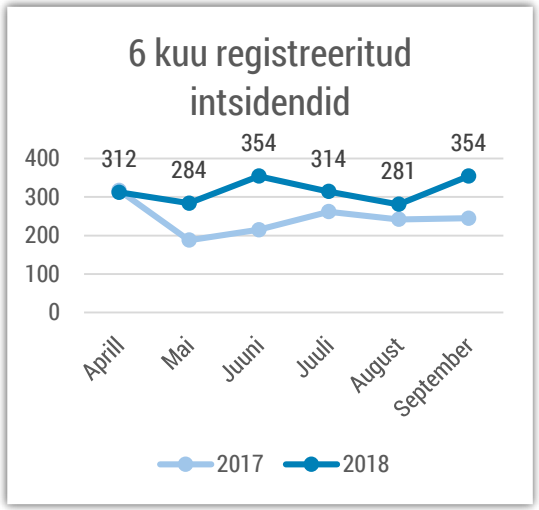
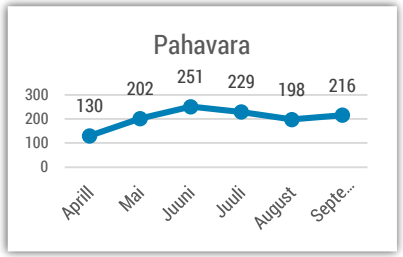
Olukord küberruumis – september 2018

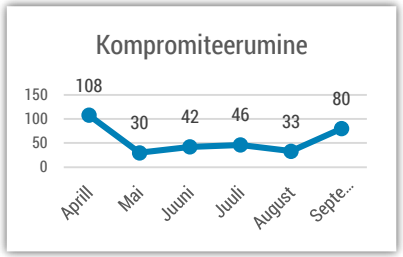
- Septembris registreerisime 354 intsidenti, mida oli rohkem kui augustis ja rohkem kui mullu samal ajal.
- Kurjategijad püüavad üha enam ära kasutada varasemaid infovarguseid uute kuritegude eesmärgil.
- Facebooki ja British Airwaysi turvaintsidendid näitasid, et eestlaste küberturvalisus sõltub jätkuvalt teistest.
- Tegime küberhügieeni digitesti kättesaadavaks perearstidele, jätkame tervishoiutöötajate koolitusi.
- USA justiitsministeerium püüab üha jõulisemalt rahvusvahelisi küberkurjategijaid vastutusele võtta.



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



Registreeritud intsidentidest on jätkuvalt kõige suurem osa pahavaral. Jätkuvalt saame kõige rohkem teateid botnet-*idega nakatunud arvutitest Eesti küberruumis.*



Enamus registreeritud kompromiteerumise intsidentidest on teated teiste riikide teenusepakkujatele, et CERT-EE avastas nende IP-aadressidelt jagatavat pahavara.

Olukord Eesti küberruumis

Juulis alguse saanud **Loki-Boti pahavara laine jõudis ka Eestisse**. Pahavara sisaldavad kirjad imiteerisid saatjatena tuntud ettevõtteid, Eestis olid nendeks AS Cybernetica, Läti ettevõte JSC RIKON, Leedu ettevõte UAB KOMEX. Kirjas palutakse kontrollida manuses olevaid pangaandmeid ja väidetakse, et tehtud ülekanne on ebaõnnestunud. Tegelikkuses sisaldab manus Loki-Boti pahavara edasiarendatud versiooni, mis nakatumisel püüab varastada paroole ja krüptorahakotte. RIAle on teada üksikud nakatamise juhtumid.

Septembris sai jätku õngitsuskirjade kampaania, mis algas juba suvel. Nimelt saadeti ühe Eesti ettevõtte kolme töötaja kontodelt juuli lõpus välja ligikaudu 600 õngitsuskirja. Hoolimata turvameetmete rakendamisest suvel **teavitas ettevõte taaskord 10. septembril RIAt, et nende nime kaaperdades saadetakse uuesti kirju firma partneritele, et neilt raha välja petta**. Kurjategijad olid nimelt salvestanud suvel kompromiteeritud meilikonto sisu ja asunud sealolevaid kirjavahetusi hiljem uues rünnakus ära kasutama. Hetkel ei ole RIAle teada, kas kurjategijatel õnnestus partneritelt raha välja petta.

Eelmises kuuülevaates kirjeldatud ***sextortion*-tüüpi väljapressimiste** (mis kasutavad ära varem lekkinud paroole ja meiliaadresse) lainet kinnitas septembris laekunud suur hulk teateid eraisikutelt.

Lennufirma British Airways teavitas 6. septembril **krediitkaardiandmete vargusest**, ohvrite seas oli ka eestlasi. Andmed saadi tänu veebilehe kompromiteerumisele. Kuigi Eestis kasutatakse kohalikes veebipoodides valdavalt pangalinke, ei tohi unustada, et paljud ostlevad ka välismaistes veebipoodides (nt Amazon, eBay jne) või kasutavad maksekeskkondi (nt PayPal), kus kasutatakse krediitkaarti ja seetõttu ei ole eestlased täielikult selliste lekete eest kaitstud.

28. septembril avalikustas **Facebook, et on tuvastanud turvavea**, mis mõjutas otseselt 50 miljonit ning ohustatud oli veel 40 miljonit kasutajat. Hetkel on selgusetu, kui paljude Eesti elanike kontod on turvaveast mõjutatud ning kas andmeid on kuritarvitatud. Facebook on lubanud jooksvalt teavitada turvaintsidendi uurimisest ning on RIAga kirjavahetuses.

Tegevused küberturvalisuse parandamisel Eestis

Suvel vastu võetud küberturvalisuse seadus (KüTS) kohustab mitmeid avaliku sektori asutusi ja ühiskonnale oluliste teenuste pakkujaid tegema riskianalüüse ja rakendama turvameetmeid oma infosüsteemide kaitseks. Suvel valmis vastavaid nõudeid täpsustav majandus- ja kommunikatsiooniministeeriumi määrus, septembris uuendasime vastavalt RIA poolt koostatud juhendit riskianalüüside teostamiseks. Alustasime ka koolitustega, mis tutvustavad uuendatud riskianalüüside koostamise metoodikat.

Pöörame jätkuvalt eraldi tähelepanu tervishoiusektori küberturvalisusele. 12. septembril andsime Haiglate liidu aastakonverentsil ülevaate küberturbest. 17. ja 19. septembril toimusid järjekordsed küberturvalisuse koolitused meditsiinitöötajatele, seekord vene keeles Ida-Viru Keskhaiglas, millest võttis osa 50 meditsiinitöötajat Ida-Virumaalt. Samuti jõudis RIA tellitud küberhügieeni digitest septembris perearstideni, mille tulemusel saavad perearstikeskuste juhid näha, millistele küberturvalisuse aspektidele peaks nende asutustes rohkem tähelepanu pöörama.

Septembri keskel korraldasime koos partneritega **rahvusvahelise elektroonilise ID foorumi**, millel osales üle 300 inimese era- ja avalikust sektorist ning kus arutleti muu hulgas eID tuleviku, tehnoloogilise arengu, hääletamise ja avaliku sektori teenuste üle.

Politsei- ja piirivalveamet (PPA) esitles koostöös RIAga uut ID-kaarti, millel on peale mitme visuaalse ja füüsilise turvaelemendi ka uus kiip, mille väljatöötamisel on arvestatud eelmise kiibi puhul avastatud nõrkustega. Suurema mahuga kiibile on võimalik lisada uusi rakendusi (ühistranspordi pileti või mõne sarnase tõendi) ning taoliste teenuste kasutamiseks on lisatud kiibile kontaktivaba liides. Isikut autentida ja digiallkirja anda saab jätkuvalt vaid kontaktse liidese kaudu. Uut kaarti hakkab PPA väljastama hiljemalt 1. jaanuarist 2019.

Rahvusvaheline keskkond

Facebooki 50 miljonit kontot mõjutanud turvaviga võib viia Euroopa liidu GDPR-i määruse esimese suurema praktilise kaasuseni. **USA** poliitikud on turvavea valguses rääkinud vajadusest reguleerida ettevõtet senisest enam.

USA kaitseministeerium pani kokku uue küberstrateegia, mille lühike kokkuvõte tehti ka avalikuks. Strateegia pöörab senisest rohkem tähelepanu heidutusele, annab vabamad käed kasutamaks kübermeetmeid ennetavalt vaenulike riikide vastu, samuti rohkem tuge liitlastele.

USAs mõistis kohus **14-aastase vanglakaristuse Läti residendile**, kelle teenus lubas pahavara arendajatel katsetada tooteid viirustõrjeprogrammidel. Samuti mõisteti **5,5-aastane vanglakaristus** endisele riikliku julgeolekuagentuuri NSA töötajale, kes viis aastatel 2010-2015 riigisaladusi sisaldavaid faile koduarvutisse, kust Kaspersky viirustõrjeprogrammi kaudu need lekkisid Vene luurele.

USA justiitsministeerium esitas süüdistuse ühele Põhja-Korea sõjaväeluure eksperdile, kes oli seotud lunavarakampaaniaga Wannacry ja 2014. aasta Sony filmitööstuse häkkimisega. Samuti esitas New Yorgi prokurör süüdistuse Vene kodanikule 80 miljoni kliendi andmete varastamise eest 2014. aastal pangast JP Morgan Chase. Süüdistatav arreteeriti Gruusias ja anti septembris USA-le välja.

Sõidujagamisteenuse pakkuja Uber maksab 148 miljonit dollarit trahvi, kuna ei teavitanud aasta jooksul 600 000 autojuhti nende andmete vargusest.

Austraalias võitlevad ettevõtted ja kodanikuühendused seaduseelnõu vastu, mis annaks politseile õiguse nõuda Austraalias kasutatavate teenuste pakkujatelt ligipääsu muu hulgas krüpteeritud sõnumitele.

India ülemkohus otsustas, et 1,2 miljardi kasutajaga biomeetriline identiteediprogramm Aadhaar (mis annab igale kodanikule unikaalse 12-kohalise isikukoodi) ei riku indialaste õigust privaatsusele, kuid eraettevõtted ja asutused ei tohi nõuda seda isikukoodi teenuste pakkumiseks. Samas avaldus järjekordne Aadhaari turvaviga, mis lubas genereerida lugematul hulgal Aadhaari koode, et petta riigilt välja näiteks toiduabi.

Hispaanias Barcelonas ja **USAs** San Diegos langesid sadamad küberrünnakute ohvriks. Mõlemad asutused olid turvameetmetele mõelnud ja laevaliiklus ei peatunud.

Septembris avas uksed **Tais** asuv küberturvalisuse keskus, mis hakkab Jaapani toel koolitama töötajaid kogu Kagu-Aasia riikide ühenduse (ASEAN) piirkonnast. Samuti avas **Venemaal** FSB uue küberintsidentide koordinatsioonikeskuse, mille ülesanne on ennetada, avastada ja vastata küberrünnakutele, mis on suunatud kriitilise infrastruktuuri vastu.