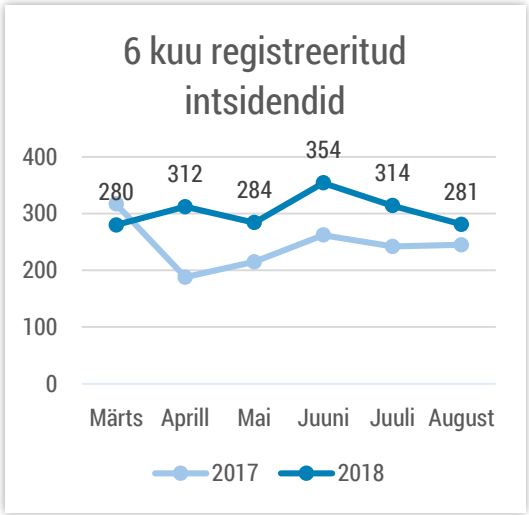
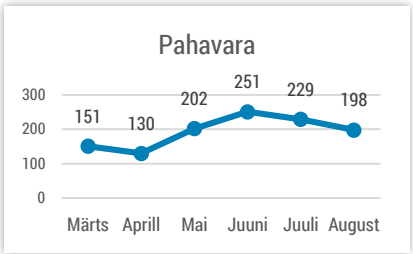
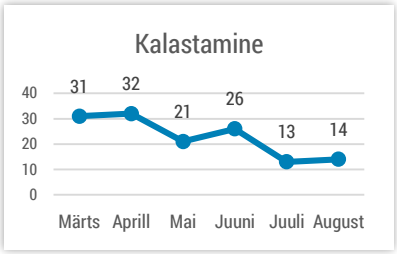
Olukord küberruumis – august 2018

- Augustis registreerisime 281 intsidenti, mida oli küll vähem kui juulis, kuid rohkem kui mullu samal ajal.
- Suvel üle maailma levinud väljapressimiskirjade laine, kus kasutatakse ära varasemaid infolekkeid, hoogustus augustikuus Eestis.
- Lunavaraintsidendid häirisid ettevõtteid ja koole, üks sanitaartehnikapood pidi neljaks päevaks poed sulgema.
- RIA teeb koostööd perearstidega, et testida nende infosüsteeme ja koolitada tervisekeskuste töötajaid.
- Ameerika ühendriikides pööratakse üha enam tähelepanu novembrikuiste valimiste küberturvalisusele.





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



CERT-EE-le edastatud teated edukatest kalastamise (phishing) *intsidentidest on viimaste kuude jooksul langustrendis.*

Olukord Eesti küberruumis

Oleme märganud Eestis tõusutrendi uut tüüpi väljapressimiste osas, mida **rahvusvaheliselt nimetatakse laias laastus *sextortion*-juhtumiteks**. Küberkurjategija leiab varem lekkinud paroolide ja e-posti aadresside andmebaasist ohvri ning saadab neile kirja, milles väidetakse, et tema arvutisse on paigaldatud nuhkvara ning veebikaameraga salvestatud video, kui kasutaja on külastanud pornograafilise sisuga veebilehti. Kui kasutaja ei maksa kurjategijale ettenähtud summat (summad varieeruvad sadadest tuhandete dollariteni), siis edastatakse video kõigile kasutaja kontaktidele. Veenvuse tõendamiseks näidatakse ohvrile samas lekkinud andmebaasis sisalduvat kunagist parooli. Oleme näinud ka kirju, kus veenvuse tõendamiseks näidatakse parooli asemel hoopiski adressaadi telefoninumbrit ja hirmutatakse, et telefoni paigaldatud nuhkvara on lindistanud „isikliku video“. RIA palub sellise sisuga kirjade õnge mitte langeda ja saata kirjanäidised cert@cert.ee aadressile.

30. augustil **algasid teenustõkestusründed Ekspress Grupi veebilehtede vastu**, rünnakud jätkusid veel septembris. Rünnakute tõttu oli raskendatud ligipääs veebiväljaannetele eelkõige välisriikidest, samuti kannatasid ettevõtte sisemised tööprotsessid.

Juhtumitest võib järeldada, et koordineeritud rünnakuid töö halvamiseks on tarvis endiselt pidada tõenäoliseks erinevates ohustsenaariumites. Toimunu näitab, et nende abil on võimalik ka oluliselt mõjutada info edastamist Eestis.

Augusti keskpaigas saadeti finantsasutustele **massiliselt pahavara linki sisaldavaid e-kirju**. RIA-le teadaolevalt ükski nende arvutitest ei nakatunud. Pahavarakirjades kasutati domeeninimesid, mis paistaksid nii, et nad viitaksid Euroopa maksete SEPA süsteemile.

Lisaks kahele väike-ettevõttele ja ühele koolile **langes augustis lunavararünnaku ohvriks** üks sanitaartehnika hulgi- ja jaemüügiga tegelev ettevõte. RIA-le teadaolevalt lunavaranõuet ei tasutud. Nakatumise tagajärjel oli ettevõte sunnitud sulgema neljaks päevaks kaheksa kauplust üle Eesti ja veebimüügikeskkonna.

Tegevused küberjulgeoleku parandamisel Eestis

Valminud on määrus **riskianalüüside koostamise nõuete ja turvameetmete kirjelduste kohta** ja nüüd on küberturvalisuse seaduses (KüTS) määratud teenuseosutajatel 2018. aasta lõpuni aega oma riskianalüüside vastavusse viimiseks. Mais kehtima hakanud KüTS kohustab elutähtsa teenuse osutajaid, aga ka muid ühiskondlikult olulist teenust pakkuivaid ettevõtteid tegema riskianalüüse ja rakendama turvameetmeid oma infosüsteemide kaitsmiseks.

Augustis lõppesid sellel aastal läbiviidud **turvatestimised elutähtsate teenuste suhtes** ja info on vastavatele asutustele ka üle antud selleks, et infosüsteemide turvalisust või riskide hindamist parandada. RIA korraldab riigi jaoks elutähtsate ja oluliste teenuste osutajatele turvatestimisi 2012. aastast. Kokku testiti sel aastal kuute asutust, 2019. aastal on planeeritud testida seitsme ettevõtte või asutuse infosüsteemi.

Külastasime augustis **kohalikke omavalitsusi Ida-Virumaal,** et rääkida nendega küberhügieenist (sealhulgas avaliku sektori töötajatele mõeldud küberhügieeni digitestist), infoturbest laiemalt ja KOV-idele kohustuslikust riiklikust infoturbe juhtimise süsteemist ISKE. Ringkäigu tulemusel selgus, et küberturvalisuse tase on omavalitsustes väga kõikuva tasemega, samas paistis silma suur huvi digitesti vastu ja soov küberturbest juurde õppida.

Augustis leppisime Eesti Perearstide Seltsiga kokku, et meie eestvedamisel auditeeritakse perearstide kasutatavaid IT-rakendusi ja infosüsteeme, et parandada tervishoiusektori küberturvalisust. Samuti toetame perearste küberturvalisuse koolitustega ja pakume neile võimalust teha digitesti, mis seni oli kättesaadav ainult avalikule sektorile.

Rahvusvaheline keskkond

Libauudiste ja küberrünnakute ohvriks langenud **Leedu** meediaväljaanded leppisid valitsusega kokku, et hakkavad küberrünnakute kohta valitsusele infot jagama. Neil võimaldatakse vastutasuks **osaleda riigi küberjulgeoleku nõukogu istungitel**.

Soome valitsusasutuste koduleheküljed langesid augustis viimase aja kõige jõulisemate küberrünnakute alla.

Ameerika ühendriikides pööratakse novembrikuiste vahevalimiste eel üha enam tähelepanu valimiste küberturvalisusele. Iga-aastasel maailma suurimal häkkerite koosviibimisel Def Con pakuti võimalust sisse murda hääletusmasinatesse, mis osutus erakordselt lihtsaks. Üks häkatonile oma hääletusmasinat mitte pakkunud tootja kritiseeris konverentsi, et selline üritus oli justkui üleskutseks kurjategijatele. Osariikide tasandil katsetatakse veel näiteks mobiiliga hääletamise varianti.

USA sisejulgeolekuministeerium korraldas valimiste eel lauaõppuse, kus harjutati föderaaltasandi ja kohalike valimiskomisjonide suhtlust ning reageerimist küberintsidentidele. Õppusel osalesid ametnikud 20st osariigist.

Tehnoloogiafirmad (sh Google, Cloudfare, Synack, Cylance, McAfee ja Microsoft) on selle tähelepanu tuules hakanud pakkuma USA kandidaatidele, kampaaniameeskondadele ja valimiskomisjonidele **tasuta küberturvalisuse teenuseid**.

Uudisteagentuur Reuters kirjutas, et USA valitsus nõuab Facebookilt kohtu kaudu, et nad looksid võimaluse oma sõnumiäppi Messengeri audiokõnesid pealt kuulata. Kuna Messengeri häälkõned on krüpteeritud, peaks Facebook valitsuse nõudmise rahuldamiseks programmi ümber kirjutama ja krüpteeringu eemaldama.

See on kooskõlas **USA, Suurbritannia, Austraalia, Uus-Meremaa ja Kanada** (nn Five-Eyes riikide) augustis tehtud ühisavaldusega, kus nad andsid märku oma üldisest rahulolematusest krüpteeritud suhtluskanalitega. Avalduses pakuti, et ettevõtted võiks ise leida lahenduse, kuidas julgeoleku-asutused võiksid sõnumitele ligi saada, ähvardades aga vastasel juhul kasutada neile antud tehnilisi või juriidilisi vahendeid ligipääsu saavutamiseks.

Samas jõudis augustis kõigi Skype'i kasutajateni võimalus teha krüpteeritud telefonikõnesid.