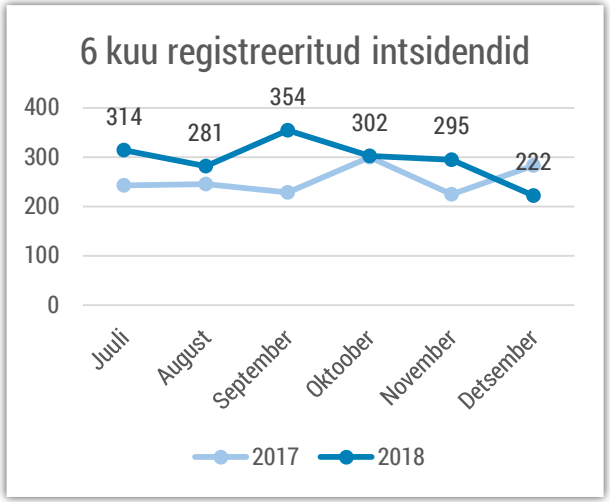
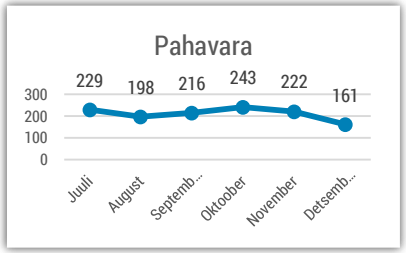
Olukord küberruumis – detsember 2018

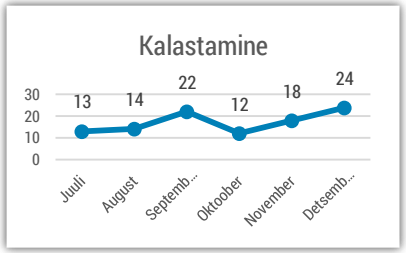
- Detsembris registreerisime 222 intsidenti, mis on vähem kui aastas keskmiselt.
- Nägime lühiajalisi teenusekatkestusi oluliste teenuste juures.
- Saime jätkuvalt teateid finantspettuste katsetest, kuid vähem teateid intsidentidest, kus ettevõtted oleks reaalselt ohvriks langenud.
- Eesti toetas USA ja Suurbritannia hinnangut, et Hiina valitsusega seotud häkkerid on püüdnud varastada maailma suurtelt ettevõtetelt intellektuaalomandit.
- Pea 400 miljoni Starwood hotelli külastaja andmed olid ründajatele kättesaadavad



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



Registreeritud intsidentidest on jätkuvalt kõige suurem osa pahavaral. Jätkuvalt saame kõige rohkem teateid robotvõrguga nakatunud arvutitest.



CERT-EE-le edastatud teated edukatest kalastamise (phishing) intsidentidest on tõusulainel.

Olukord Eesti küberruumis

Detsembris teavitati meid mitmel korral Häirekeskuses kasutuses oleva kõnejaotustarkvara lühiajalistest katkestustest. Kuigi enamasti suunati kõned varutelefonidele ning kõik kõned said teenindatud, siis ühel korral oli kümnekonna minuti jooksul Häirekeskusesse helistamine takistatud. Siseministeeriumi infotehnoloogiaja arenduskeskus on tegelenud probleemide lahendamisega, mis tulevkus sellised juhtumid välistab. Teadaolevalt üksi inimene vahejuhtumi tõttu abita või teenindamata ei jäänud.

Detsembris laekus varasemate kuudega võrreldes **vähem teateid ettevõttete langemisest finantspettuste ohvriteks meilikontode kaaperdamise kaudu**. Samas saatsime koostöös Politsei- ja Piirivalveametiga välja sellesisulise hoiatuse kõigile Eestis registreeritud ettevõtete kontaktidele, millele saime üsna palju konstruktiivset tagasisidet. Jätkuvalt on näha katseid, kuidas õngitsuskirjadega püütakse järgmisi ohvreid leida.

Lihtsamate finantspettuste (kus saadetakse justkui ettevõtte või asutuse juhi nime alt kiri raamatupidajale napisõnalise küsimusega, kas saaks saata välismaal asuvale kontole kohe raha) katsetuste kohta tuli detsembris jätkuvalt teateid. **Niinimetatud tegevjuhi petuskeemi kirjade hulk kasvas vahetult enne pikki jõulupühasid** (ehk enne pikemat pangaülekannete peatumist). Meile teadaolevalt sai aga vähemalt üks ettevõte pea 30 000 eurot niimoodi kahju.

Tegevused küberturvalisuse tagamisel Eestis

3. detsembrist alates väljastab Politsei- ja Piirivalveamet (PPA) uuendatud kujunduse, turvaelementide ja kiibiga ID-kaarte. See tähendab, et paljude e-teenuste ja süsteemide omanikel on vaja oma süsteeme uuendada nii, et need uue kaardiga ka toimiksid. Kriitilisemad ja enimkasutatavad teenused juba töötavad uue ID-kaardiga (vanematega probleeme pole), kuid mitmed ettevõtted peaksid näiteks oma kliendikaardirakenduste jaoks oma süsteemid üle vaatama. Teenusepakkujad saavad selleks RIA-lt tellida ka testkaardi.

Detsembri teises pooles saatsime koos PPA-ga välja teavituse Eesti ettevõtjatele, kus hoiatasime neid viimasel ajal levivate arvepettuste eest. Nendest petuskeemidest oleme rääkinud ka varasemates infokirjades, meie kvartaliülevaates ja meedias. Teavitus jõudis veerand miljoni adressaadini.

12. detsembril korraldasime koos PPA ja elektroonilise identiteedi sertifikaatide väljastaja SK ID Solutions esindajatega lauaõppuse, kus mängisime koos läbi eID teenuse toimepidavuse lahenduskäike. Taolised õppused on tavapärased, kus püüame läbi mängida võimalikke probleeme usaldusteenustega.

Detsembri lõpust on nendele kohalikele omavalitsustele, kes kasutavad Riigivõrku, ligipääs RIA tellitud küberhügieeni digitestile. Umbes pool kohalikest omavalitsustest on Riigivõrguga ühinenud ja Digitest on kindlasti oluline võimalus neile organisatsioonidele oma töötajate küberhügieeni arendamiseks.

Kohalike omavalitsuste ja riigiasutuste turvalisuse eest vastutajad osalesid detsembri alguses meie poolt korraldatud **konverentsil admin@gov**, kus arutati muu hulgas võrguliikluse seiramise ja e-kirjade turvalisuse küsimusi.

Pöörame jätkuvalt eraldi tähelepanu tervishoiusektorile. **Detsembri alguses korraldasime aasta viimase koolituse tervishoiutöötajatele, seekord Pärnu haiglas.** Septembrist kuni aasta lõpuni on toimunud kaheksa suuremat küberturvalisuse koolitust – lisaks väiksemaid koolitusi perearstide juures. Koolitustega jätkame ka järgmisel aastal.

Rahvusvaheline olukord

Ameerika ühendriigid esitasid detsembri keskpaigas ametliku süüdistuse kahele Hiina rahvavabariigi julgeolekuministeeriumi töötajale era- ja avalikest asutustest informatsiooni varastamises. Need ametnikud kuulusid rünnakugruppi, mida tuntakse rahvusvaheliselt nimetuse APT10 all. APT10 on alates 2014. aastast sihtinud ettevõtetele pakutavaid pilveteenuseid, mille kaudu pääsesid nad ligi ettevõtete intellektuaalomandile. Valitsusametnikele süüdistuse esitamisega omistas USA APT10 tegevuse ametlikult Hiina valitsusele.

USA kõrval omistasid APT10 tegevuse Hiinale ja mõistsid riigipoolse küberspionaaži hukka ühendriikide liitlased üle terve maailma, toetudes muu hulgas G20 riikide juhtide poolt 2015. aastal kokku lepitule, et riigid ei tohiks oma konkurentsivõime edendamise nimel küberspionaažiga tegelema ega seda toetama. **Teiste hulgas teatas ka Eesti välisministeerium meie toetusest liitlaste hinnangule APT10 suhtes,** öeldes et rahvusvaheliste normide ja kokkulepete järgimine on globaalse küberturvalisuse huvides ülioluline.

Novembri viimasel päeval teatas ülemaailmne hotellikett Marriott, et alates 2014. aastast on 500 miljoni Starwood hotelli klientide andmed lekkinud nende broneerimissüsteemi turvanõrkuse kaudu. Hiljem alandasid nad mõjutatud inimeste hulga 383 miljonini. Mitu meediaväljaannet, toetudes USA allikatele, viitavad Hiinaga seotud rünnakugruppidele.

Euroopa komisjon korraldab niinimetatud puugipreemiajahi (*bug-bounty program)* 15st tasuta või avatud lähtekoodiga programmidest haavatavuste leidmiseks. Nende hulgas on euroliidu institutsioonides laialdaselt kasutatavad programmid nagu Filezilla, VLC ja Keepass.

Inimõiguste eest võitlev organisatsioon Amnesty International näitas, **kuidas ajakirjanikke ja inimõiguslasi häkkida püüdes on kurjategijad saanud mööda kahefaktorilisest autentimisest nii Gmailis kui Yahoo e-postkastis.** (Sellest hoolimata on mitmefaktoriline autentimine kindlasti turvalisem kui selle puudumine.)

Sotsiaalvõrgustikud Facebook ja Twitter teatasid, et võtsid enne valimisi Bangladeshis maha kümneid opositsioonierakondi mustavaid võltskontosid. Facebooki lehekülgedel oli meelega jäljendatud uudisteportaale, Twitteri kontod võisid olla seotud mõne teise riigiga.

Detsembri viimasel päeval otsustas Kongo demokraatliku vabariigi valitsus kogu riigis peatada internetiühendused, tekstisõnumite süsteemi ja ka Prantsusmaa raadio RFI signaali, et välistada presidendivalimiste mitteametlike tulemuste levitamist ja nende tõttu vägivalla õhutamist.