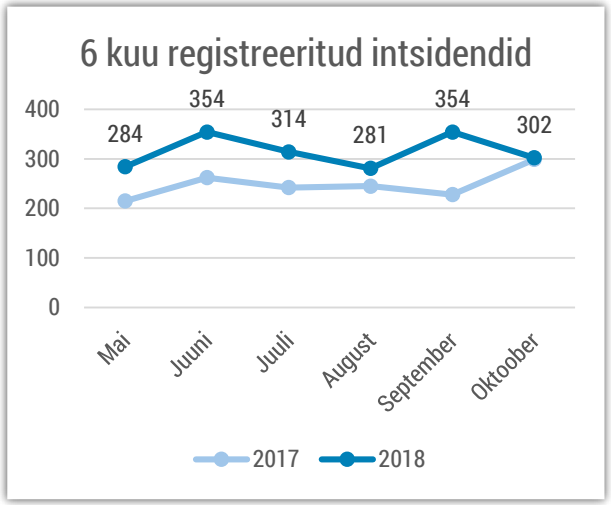
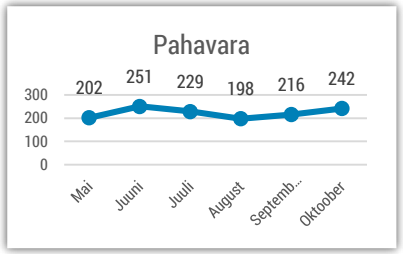
Olukord küberruumis – oktoober 2018

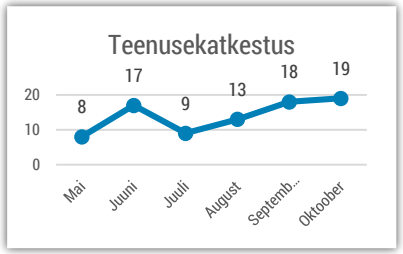
- Registreerisime 302 intsidenti, mis aasta keskmisest on veidi kõrgem ja umbes sama palju kui mullu.
- Nägime, kuidas kurjategijad püüavad ära kasutada kompromiteeritud kirjavahetusi selleks, et Eesti ettevõtetelt rohkem raha välja petta.
- Euroopa liit ja USA tähistasid oktoobris küberturvalisuse kuud. Eestis korraldasime sel puhul talgud, kus kõik huvilised said minna tegema küberhügieeni koolitusi.
- USA tehnoloogiahiiud nõuavad, et Bloomberg lükkaks ümber väited Hiina luuramiskiibi kohta nende toodetes.



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.*



Oktoobris registreerisime tavapärasest veidi enam lühiajalisi teenusekatkestusi.

Olukord Eesti küberruumis

Septembris ja oktoobris teavitati meid jätkuvalt ettevõtteid sihtivatest lihtsamatest ja keerulisematest petuskeemidest. Mõned juhtumitest on Eesti asutustele juba tuttavad ja lihtsamad tegevjuhi petuskeemi katsed, kus ettevõtte juhi nime võltsides saadetakse raamatupidajale või finantsjuhile lakooniline küsimus, kas oleks võimalik teha ühele väliskontole ülekanne.

Selle kõrval aga oleme näinud nüüd juhtumeid, kus **ettevõtte kompromiteeritud meilikontode ja -vestluste sisu on ära kasutatud edasistes pettustes,** millest kirjutasime ka eelmises kuuülevaates. Need petuskeemid on keerukamad ja nõuavad kurjategijatelt rohkem tööd ja aega. Mitu ettevõtet on teavitanud meid sellest, et nendele allhanget tegeva partneri e-mailikonto oli kompromiteeritud, seejärel jätkatud välispartneri nime võltsides suhtlust ja palutud teha ülekanne kolmanda osapoole valduses olevale kontole. Eesti ettevõtted on saanud selliste skeemide tõttu ka majanduslikku kahju.

Oktoobri algul avalikustati, et infosüsteemis EKIS on asutusesiseseks kasutamiseks mõeldud teave (sealhulgas lastega seotud delikaatne info, näiteks psühhiaatrilised hinnangud laste vaimsele tervisele jm) avalikult kättesaadav. Tegu on Eesti koolide haldamise infosüsteemiga, mida kasutavad ligi 500 kooli ja lasteaeda. Tehniline kontroll tuvastas 42 asutust, mis ei olnud korrektselt käsitlenud juurdepääsupiiranguga teavet. EKIS süsteemi haldav haridus- ja teadusministeerium hindas, et dokumentide avalikuks tulek oli põhjustatud dokumentide ebakorrektsest sisestamisest.

Augustis ja septembris tähelepanu tõmmanud **sextortion-tüüpi väljapressimiskirjad** (millest oleme eelmises kahes kuukokkuvõttes kirjutanud) jõudsid ka oktoobris mitme lainega Eesti inimesteni, kes meid sellest teavitasid.

Tegevused küberturvalisuse parandamisel Eestis

Oktoobris tähistas Eesti koos ülejäänud Euroopa riikide ja Ameerika ühendriikidega **küberturvalisuse kuud**. Eestis korraldasime sel puhul esimest korda 15. oktoobril küberturvalisuse talgud, kus kutsusime üles oma koostööpartnereid minema koolidesse, perearstikeskustesse ja muudesse kogukonnaga seotud kohtadesse tegema lühikesi koolitusi küberhügieenist ja ohtudest küberruumis.

Lisaks 16 RIA töötajale andis oma panuse talgutel pea sama palju vabatahtlikke koolitajaid, eelkõige Eestis tegutsevate küberturbeettevõtete esindajaid, aga ka näiteks juriste ja diplomaate. Küberturvalisuse kuu aga ei piirdunud vaid üheainsa päevaga, vaid koolitusi küsiti juurde ka järgmiste nädalate jooksul. **See tähendab, et mitusada Eesti õpetajat, õpilast, lapsevanemat, perearsti, -õde, Riigikogu töötajat, ajakirjanikku ja muud huvilist said küberturvalisuse kuu käigus osa mõnest talgu korras peetud koolitusest.**

Kampaania korras koolitusürituste korraldamise kõrval **jätkasime ka regulaarseid koolitusi Eestis elutähtsat teenust osutavate- ja korraldavate asutuste, olulise teenuse osutajate ning riigiasutuste võtmeisikutele ja spetsialistidele.**

Näiteks toimusid infoturbe teadlikkuse tõstmise koolitused erinevate asutuste ja ettevõtete juhtkonnale ning töötajatele; infoturbe halduse baaskoolitus ISKE rakendajatele; infoturbe teadlikkuse tõstmise koolitus tervishoiutöötajatele; riskijuhtimise koolitused asutuste riskijuhtidele jne. Oktoobri lõpus kutsusime koolitusele Eesti vee-ettevõtjad ja korraldasime neile ka lauaõppuse.

Meie tellimusel valmis analüüs perearstide infosüsteemide küberturvalisuse hetkeolukorra kohta. Perearstid peavad hakkama 2022. aastast jälgima küberturvalisuse seaduses sätestatud nõudeid, mistõttu aitame neil riskihinnangud ja turvameetmed enne seda tähtaega korda saada. Analüüsi eesmärk oli seetõttu koondada küberturvalisuse seaduses kirjeldatud nõuded perearstidele, kaardistada eesmärke ja soove ning anda nõu perearstide turbe-teemade efektiivseks rakendamiseks.

Rahvusvaheline keskkond

Läti parlamendi valimispäeval, 6. oktoobril, **näotustati Läti üks populaarsemaid sotsiaalvõrgustikke Draugiem.** Portaali avanedes võis veebilehel näha Vene lippu Kremli-meelse tekstiga ning slaidiprogrammi, mille taustaks mängis Vene Föderatsiooni hümn. Läti CERT on teatanud, et rünnak ei kujutanud endast ohtu riiklikule julgeolekule ning häkkerid ei suutnud varastada kasutajate andmeid.

USA meediaväljaanne Bloomberg kirjutas oktoobri alguses, et Hiina sõjaväeluure on lisanud laialt levinud elektroonikaseadmetes kasutatavatele Super Micro toodetud emaplaatidele väikeseid mikrokiipe, et luureandmeid koguda. Muu väitis väljaanne, et selliseid plaate kasutavad ja turvaintsidendist on teadlikud ettevõtted nagu Apple ja Amazon. Bloombergi artikkel tekitas palju segadust, sest Super Micro kõrval lükkas väljaande väited ümber nii Apple kui Amazoni pilveteenuse ettevõte AWS. Riiklikest agentuuridest ütlesid nii Suurbritannia riikliku küberturvalisuse keskuse NCSC ja USA riikliku julgeolekuagentuuri NSA esindajad, et neil ei ole põhjust Apple'i ja Amazoni sõnades kahelda. Mõlema suurettevõtte juhid kutsusid Bloombergi üles lausa artiklit tagasi võtma.

USA kaitseminister James Mattis ütles oktoobri alguses toimunud NATO kaitseministrite kohtumisel, et **USA on valmis aitama NATO liitlasi kübervõimetega**. See on osa septembris avaldatud uuest USA küberstrateegiast.

Hollandi, Suurbritannia ja USA **omistasid Venemaa sõjaväeluurele (GRU) terve hulga varasemate aastate küberrünnakuid**, sealhulgas rünnakud dopinguvastase agentuuri WADA, keemiarelvade keelustamise organisatsiooni OPCW, USA demokraatide partei ja üht Briti telekanali vastu.

USA valimiste eel avalikustas sotsiaalvõrgustik Twitter massiivse hulga võltskontode poolt loodud sisu (10 miljonit säutsu ja nendega kaasnenud pilte), millega Venemaa ja Iraani trollide võrgustikud püüdsid mõjutada USA avalikku diskussiooni. Venemaal St. Peterburis asuva Internet Research Agency (IRA) nimelise ettevõtte võrgustikust tuvastas Twitter 3841 kontot, lisaks leidsid nad 770 Iraani taustaga kontot. **USA justiitsministeerium esitas oktoobris kriminaalsüüdistuse ühele Venemaa kodanikule**, kes IRA kaudu juhtis kampaaniat USA valimiste diskrediteerimiseks.

Tšehhi julgeolekuagentuur BIS võttis maha serverid, mida Liibanonis tegutseva grupeeringu Hezbollah agendid kasutasid Facebooki kasutajatele pahavara levitamiseks.