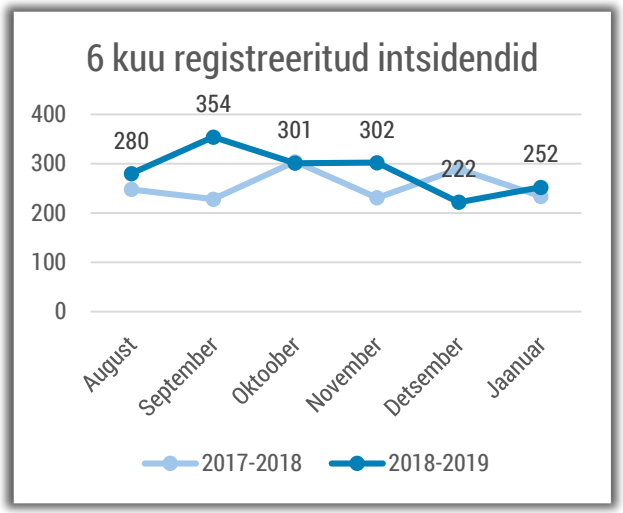
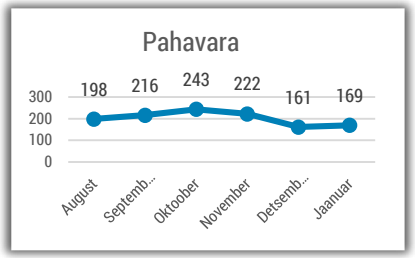
Olukord küberruumis – jaanuar 2019

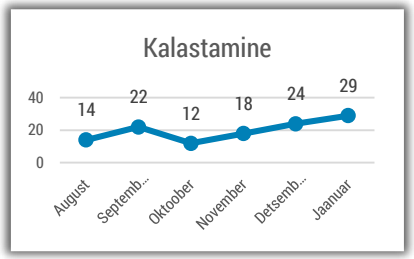
- Jaanuaris registreerisime 252 intsidenti, mida on rohkem kui eelmisel kuul ning mullu samal ajal.
- Aasta algas suure andmelekke kogumi avalikustamisega, milles leidunud Eestiga seonduvatest andmetest oli ligi kolmandik lekkinud juba varem.
- RIA pädevuses on usaldusteenuste järelevalve.
- Jaanuaris algatas RIA järelevalvemenetlused kohalikes omavalitsustes.
- Prantsusmaa sõjavägi kavatseb kasutada küberrelvi nagu traditsioonilisi relvi, sh rünnakule vastamiseks.
- Apple'i videokõneteenuses FaceTime tuvastati oluline turvaviga, mis seab ohtu kasutajate turvalisuse ja konfidentsiaalsuse.



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



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



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

Olukord Eesti küberruumis

Jaanuaris avalikustati kasutajaandmeid sisaldavad andmelekke kogumid, milles on **ligikaudu 460 000 Eesti domeeniga (.ee lõpuga) meiliaadressi**, neist umbes 180 000 on levinud juba varasemate lekete kaudu. Uusi meiliaadresse on ligikaudu 280 000, millest enamik lekkis koos parooliga. Lekkinud paroolide abil on võimalik kurjategijatel ligi pääseda meilivestlustele ning seda on võimalik omakorda enda huvides mitmel moel ära kasutada. Näiteks edastada pahavara või õngitsuskirju, lootuses, et konto omaniku tuttavad lähevad kergemini õnge ja avavad kirjaga kaasas olevaid manuseid. Ühtlasi võib e-posti lekete korral suureneda finantspettuste arv, kuna kurjategijad otsivad üles arvete maksmisega seonduvad meilivestluseid ning edastavad enda kontonumbri, kuhu ohver pahaaimamatult ülekande teeb.

Kasvanud on teated sekspressimiskirjadest, kus ohvrid saavad kirju justkui nende endi meilikontolt. Tegelikkuses kasutavad küberkurjategijad ära nõrgalt kaitstud infosüsteeme, kus meiliserver ei kontrolli, kas kuvatav aadress ühtib selle aadressiga, millelt kiri tegelikult saadeti. Kirjeldatud võttega püütakse luua ohvrites veendumust, et kurjategija on pääsenud ligi kasutaja meilikontole, kuigi tegelikult ei ole. Soovitame kurjategijatele mitte maksta ning pöörduda teenusepakkuja poole palvega rakendada SPF, DKIM ja DMARC reeglid ning reeglistikule vastav kontroll.

Kuressaare elektrikatkestusele järgnesid teenusekatkestused. Jaanuaris katkes õhuliini rikke tõttu Elektrilevi elektrivarustus Kuressaare lähedal, mõjutades algselt kuni 14 000 klienti. Ajakirjanduse andmetel olid elektrivarustuse katkemise tõttu lühiajaliselt häiritud ka mobiilioperaatori mobiilside ja kaabelvõrgu kasutamine. Kuu lõpus toimus õhtusel ajal järjekordne ligi kolmetunnine elektrikatkestus liigniiskuse tõttu. Juhtum näitas hästi Eesti teenuste tegelikku ristsõltuvust üksteisest ja varulahenduste vajalikkust. Konkurentsiamet on algatanud juhtunuga seoses Elektrilevi suhtes järelevalvemenetluse.

Tegevused küberturvalisuse parandamisel Eestis

Korraldasime rahvusvahelise CERTide võrgustiku TF-CSIRT kohtumise ja Euroopa regioonile suunatud sümpoosioni FIRST. Ürituste eesmärk oli tuua kokku erinevate riikide CERTide tehnilisi inimesi, jagada infot uute riskide kohta ja vahetada kübervaldkonnas õpitud kogemusi. TF-CSIRT (Task-Force on Computer Security Incident Response Team) koondab Euroopa küberintsidentide käsitlemise meeskondi (CERTe) ning kohtub korrapäraselt Euroopa eri paigus. FIRST on globaalne CERTide foorum, kus arutatakse küberintsidentide käsitlemisega seotud teemadel.

Suurest huvist tingituna korraldasime jaanuaris kaks täiendavat **IT-riskide hindamiskoolitust**. Soovitame tutvuda ka varasemalt koostatud abistavate juhendmaterjalidega, mis selgitavad riskianalüüsi koostamist. IT riskianalüüsi koostamise kohustus tuleneb küberturvalisuse seadusest.

Aasta alguses **uuendasime** välise ja kõigile ligipääsetava IT-spetsialistidele mõeldud **failide analüüsimise tööriista Cuckoo**, mis annab senisest rohkem informatsiooni pahavara käitumise kohta. Tööriist võimaldab asutuse IT-spetsialistil kontrollida, kas fail sisaldab pahavara või mitte ning seeläbi säästa aega pahavara kontrollimisel.

Alates jaanuarist teostame **järelevalvet usaldusteenuse üle**. Meie kohustus on usaldusteenuste jaoks anda välja tegevuslube, kvalifitseeritud staatusi, hallata usaldusnimekirja ning teha järelevalvet teenuse osutamise üle. Kolm põhilist usaldusteenust on digitaalne allkirja teenus, aja- ja digitempli teenus. Eestis pakub usaldusteenuseid SK ID Solutions ja ajatempli teenust osutab veel GuardTime.

Jaanuaris algatasime järelevalvemenetlused mitme kohaliku omavalitsuse üle, kus kontrollime infosüsteemide turvameetmete rakendamist tulenevalt avaliku teabe seadusest. Kohalikes omavalitsustes ei ole infoturbe olukord ülemäära hea ning seetõttu oleme suunanud sinna rohkem teadlikkuse tõstmise kui järelevalve ressursse. Eesmärk on infoturbe meetmete rakendamise abil luua eeldused võimaliku kahju ärahoidmiseks või leevendamiseks.

Rahvusvaheline keskkond

Ameerika Ühendriikide julgeolekuasutuste raportis sedastatakse, et Hiina, Venemaa, Iraan ja Põhja-Korea kasutavad küberoperatsioone poliitilise, sõjalise ja majandusliku edu saavutamiseks. Näiteks kasutavad USA rivaalid küberruumi demokraatlike institutsioonide õõnestamiseks, liitlaste ja partnerite alavääristamiseks ning poliitiliste tulemuste kujundamiseks endale soodsas suunas.

Prantsusmaa kaitseminister deklareeris rahvusvahelisel küberjulgeoleku foorumil, et kübersõda on alanud ning **Prantsusmaa sõjavägi kavatseb kasutada küberrelvi nagu igat teist traditsioonilist relva – sh vastamaks rünnakule**. Samuti kuulutati välja haavatavuste otsimise programm (*bug-bounty program*) „Yes We Hack", mille raames otsivad häkkerid kaitsevaldkonna infosüsteemides haavatavusi.

USA justiitsministeerium **esitas Huaweile 23 süüdistust ärisaladuste varastamises, pettustes ja õiguse mõistmise takistamises** ning eraldi süüdistuse ka Huawei finantsjuhile Meng Wanzhoule **Iraani sanktsioonide rikkumises**. Lisaks USA-le on ka **Poola esitanud süüdistuse ühele Huawei töötajale** ja endisele Poola julgeolekutöötajale – mehi kahtlustatakse Hiina kasuks **spioneerimises** Poola riigi vastu.

Viimastel kuudel on mitmed **riigid loobunud või kaaluvad loobuda Huawei toodetest** julgeolekuohu ettekäändel, sh Jaapan, Tšehhi, Poola jt.

Näiteks muutis Tšehhi maksuamet riigihanke tingimusi selliselt, et Huawei ja ZTE jäävad osalusest välja, kuna neid peetakse julgeolekuohuks. **Eesti** saab siinkohal toetuda üksnes partnerriikide hinnangutele, sest meil puudub eraldi võime sertifitseerida kahtlusega toodete turule lubamist või keelamist. Taolise sertifitseerimis-skeemi loomine üksnes Eesti-suuruse turu jaoks oleks liialt kulukas ning ebaotstarbekas.

Küberturvalisusega tegeleva ettevõtte Avast uuringust selgus, et **kasutajad teevad ise end küberohtudele haavatamaks**, sest ei uuenda oma seadmete ja programmide tarkvara. 55 protsenti ülemaailmselt kasutatavatest programmidest on uuendamata, sealjuures paistavad vananenud tarkvara poolest eriti silma populaarsed programmid nagu Adobe, VLC ja Skype.

Jaanuaris avalikustati meedias, et **Apple'i videokõneteenuses FaceTime on tuvastatud turvaviga, mis seab ohtu kasutajate turvalisuse ja konfidentsiaalsuse**. Turvaviga ära kasutades oli võimalik kuulata kõnesaaja audiot ja videopilti ilma, et ta oleks kõne vastu võtnud. Pärast vea avalikuks tulekut keelas Apple turvaviga võimaldava grupikõnede kasutamise. Soovitame kõigil hoida oma tarkvara uuendatuna, et selliseid ohte minimeerida.