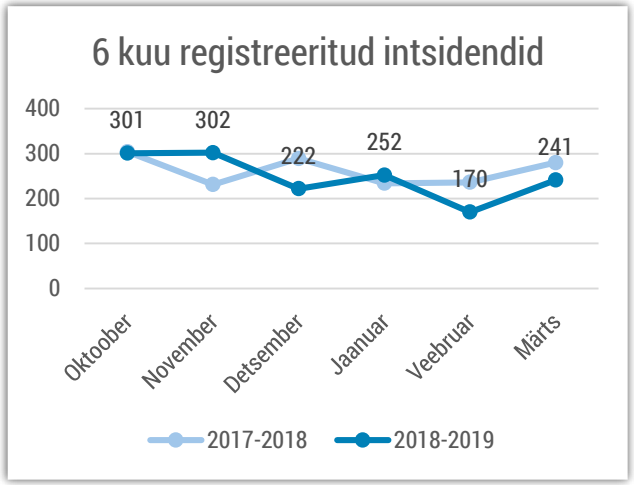
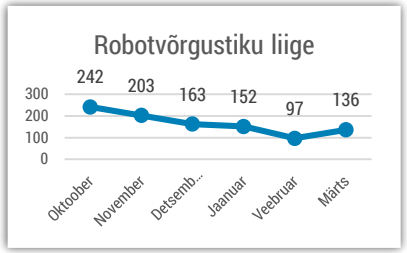
Olukord küberruumis – märts 2019

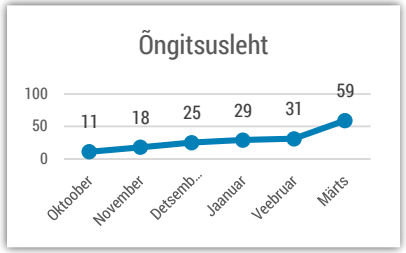
- Märtsis registreerisime 241 intsidenti, mida oli märkimisväärselt rohkem kui veebruaris, kuid samas siiski vähem kui mullu samal ajal.
- Eesti ettevõtted said märtsis taas 80 000 eurot kahju pettuste kaudu, mis said alguse meilikontode kompromiteerumisest.
- Kirjutasime valmis küberturvalisuse ülevaate 2018. aasta kohta.
- Maailma üks suurimaid alumiiniumitootjaid sai pihta laiaulatusliku lunavararünnakuga.



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



Kõige rohkem saame teateid robotvõrgustikuga nakatunud arvutitest Eesti küberruumis. Viimasel poolaastal on nende teadete hulk aga langustrendis.



Üha enam tuvastame õngitsuslehti, mille eesmärgiks on kätte saada kasutaja erinevaid andmeid.

Olukord Eesti küberruumis

Meilikontode kompromiteerimisest alguse saanud finantspettused tõid ligi 80 000 eurot kahju. Märtsis teavitati taaskord Eesti ettevõtetest, mis langesid finantspettuste ohvriks – ühe kahju oli 70 000 eurot, teisel pea 13 000 eurot. Mõlemal juhul olid kurjategijad kompromiteerinud ettevõtete meilivestlused välisriikidest pärit koostööpartneritega ning hetkel, kui oli vaja teha pangaülekanne, saadeti ettevõtetele kurjategijate valduses olevate pangakontode andmed.

Möödunud kuul esines **ligi kahe tunni jooksul tõrkeid mobiil-ID kasutamises**. Tõrgete ajavahemikul ebaõnnestusid kuni 80% ulatuses mobiil-ID teenuse päringud. Probleem lahenes pärast ajutist teenuse kasutamise piiramist. Esialgse hinnangu kohaselt ei pidanud teenuse süsteemikomponent koormusele vastu ning kuna kasutajad üritasid pärast ebaõnnestumist teenust kohe uuesti kasutada, siis tekkisidki häired.

Märtsis täheldasime pahavara lainet, mis saadeti paari transpordiettevõtete meilidomeeni ära kasutades. Tegu oli nn meiliteesklusega (*email spoofing*), mille käigus valiti ühe töötaja email jäljendamiseks. Ärakasutamist võimaldas asjaolu, et ettevõtete meilidomeenidel puudusid meiliteeskluse vastased kaitsemeetmed (SPF, DKIM ja DMARC). Näiteks DMARC lubab teistel meiliserveritel kontrollida, kas asutuse nimel saadetud kiri saabus tegelikult selle asutuse poolt volitatud serverist või mitte.

***Muudatus intsidentide taksonoomias**

Kuukokkuvõtte graafikutel olevate intsidentide nimetused (robotvõrgustiku liige, õngitsusleht) võivad erineda nimetustest, mida kasutasime varasematel kuudel. Tegemist on pikemalt planeeritud intsidentide taksonoomia korrastamisega, mis peaks edaspidi tagama selgema ja järjepidevama ülevaate küberintsidentide liikidest.

Tegevused küberturvalisuse parandamisel Eestis

Kirjutasime valmis ülevaate Eesti küberruumist 2018. aastal. Räägime selles Eesti küberturvalisuse aastaraamatus mullu kõige enam kahju tekitanud intsidentidest, kuidas me Eesti küberturvalisust paremaks teeme ja kuidas küberturvalisuse nimel teiste asutustega koostöö käib. Ülevaatega saab tutvuda siin.

Märtsikuus korraldasime kohalikele omavalitsuste töötajatele üle kahekümne küberhügieeni koolituse ja arutasime linnade-valdade juhtidega nende omavalitsuse küberturvalisuse küsimuste üle. Külastasime näiteks Lääne-Harju, Haljala, Rakvere, Jõelähtme, Viru-Nigula, Vinni, Tapa, Väike-Maarja, Järva, Lääne-Nigula, Märjamaa, Türi, Põhja-Pärnumaa, Kehtna, Põhja-Sakala, Kadrina, Kohila, Rae ja Harku valda, linnadest veel Raplat, Loksat ja Rakveret. Jätkame taoliste külaskäikudega ka aprillis ja mais.

Korraldasime ühisõppuse Soome kolleegidega, kus harjutasime mõlema riigi energiasektorit puudutanud küberintsidendi lahendamist. Õppuse legendi kohaselt nõudsid kurjategijad mõlemas riigis elektrivarustuse teenuste säilitamise eest lunaraha. Seetõttu pidid kahe riigi küberintsidentide käsitlemise meeskonnad omavahel infot vahetama ja koostööd tegema. Taolised õppused aitavad meil naabritega valmistuda sellisteks olukordadeks, kus mõni küberintsident mõjutab mõlemat riiki ning kus koos tegutsemine aitab kriise kiiremini lahendada.

Tellisime järjekordse krüptograafiauuringu, mis sel korral pöörab tähelepanu kvantarvuti-kindlatele krüptograafia algoritmidele. Kuna kvantarvutite arenguga võib tekkida oht, et praegu kasutatavad krütoalgorütmid ei ole enam piisavalt turvalised, tuleb juba praegu teha otsuseid, milliseid krüptograafilisi lahendusi tuleks hakata arendama näiteks elektroonilise identiteedi valdkonnas. Uuring ise on kättesaadav siit:

20. märtsil **esitles siseministeerium käsiraamatut „Käitumisjuhised kriisiolukordadeks“,** milles erinevate valdkondade eksperdid on kirjeldanud erinevaid kriisiolukordi ning lisanud iga peatüki juurde tegutsemisjuhendi. RIA annab käsiraamatus nõu, milliste küberjuhtumitega inimesed oma igapäevaelus kõige sagedamini kokku puutuvad ning jagame soovitusi, kuidas ennast intsidentide eest kaitsta ja mida teha siis, kui midagi on juba juhtunud.

Rahvusvaheline keskkond

Üks maailma suurimaid alumiiniumitoodete- ja taastuvenergiatootjaid Norsk Hydro sattus lunavararünnaku ohvriks. Intsident sai alguse USAs asuvast tehasest ning levis Norsk Hydro ülemaailmse võrgu kaudu teistesse tehastesse. Rünnak mõjutas tehaseid, mis valmistavad alumiiniumist lõpptooteid ning eriti oluliselt olid mõjutatud kontoriarvutid ja tehaste võimekus saada operatiivselt informatsiooni tellimuste kohta. Intsident ei mõjutanud Hydro energiatootmist. **LockerGoga nimelise lunavara** leviku peatamiseks ja süsteemide taastamiseks tuli eraldada kõik tehased ülemaailmsest võrgust. Samuti vähendati tehastes automatiseerimist ja kasutati rohkem inimtööjõudu. Ettevõttel olid andmed varundatud ning lunaraha ei plaanita maksta. Esialgse hinnangu kohaselt ulatuvad kahjud ca 30-35 miljoni euroni.

BEC-ründed (*business email compromise*) liiguvad mobiili. Kui varasemalt püüti meilikontot kompromiteerida ainult meili vahendusel, siis nüüd saadetakse enne õngitsuskiri, milles küsitakse ohvri telefoninumbrit ning seejärel palutakse täita mingit ülesannet SMS'i teel. Ründes kasutatakse ära ka selliseid internetiteenuseid, mis pakuvad telefoninumbreid ilma, et oleks vaja füüsilist SIM-kaarti, mis teeb kurjategija kättesaamise veelgi keerulisemaks. Ettevõtte meilikontode kompromiteerumisest alguse saanud finantspettused on ka Eesti ettevõtetele suurt kahju tekitanud.

Marriott'i andmeleke on seni maksma läinud 28 miljonit dollarit. Möödunud aasta novembris teavitas hotellikett Marriott andmelekkest, kus esialgsete andmete järgi sattus küberkurjategijate kätte ligikaudu 500 miljoni kliendiandmeid, sh nimed, elukoha aadressid, sünnikuupäevad, telefoninumbrid, meiliaadressid, passinumbrid, broneeringuandmed ja mõnel juhul ka krediitkaardiandmed. Nii investorid, kui ka mõned kliendid on Marriottile esitanud hagi leides, et hotell ei teinud piisavalt, et leket takistada või tuvastada.

Huawei esitas hagi USA valitsuse vastu seoses keeluga kasutada Huawei tooteid föderaalametites. USA on toonud keelu põhjuseks julgeolekuohu ning kutsub üles ka oma liitlasi loobuma Huawei toodete kasutamisest. Lisaks on USA hoiatanud, et kui seda soovitust kuulda ei võeta, siis ei pruugita jagada enam nende riikidega luureteavet. Ehitavates 5G võrkudes Huawei seadmete kasutamise üle on arutelud julgeolekuaspektist toimunud mitu kuud juba. Sealhulgas teavitas märtsis ka NATO, et hakkab analüüsima Hiina toodetega seotud riske.