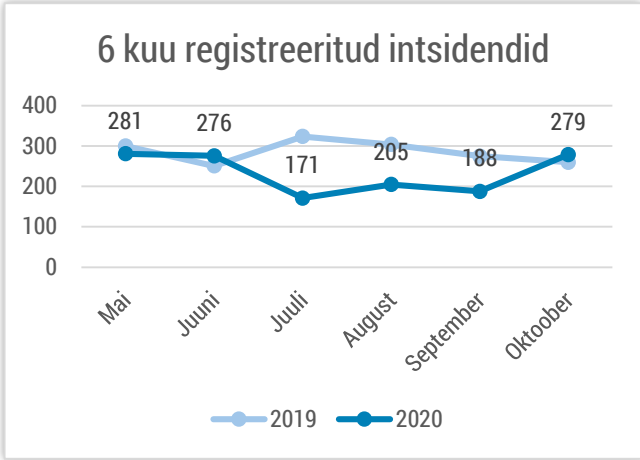
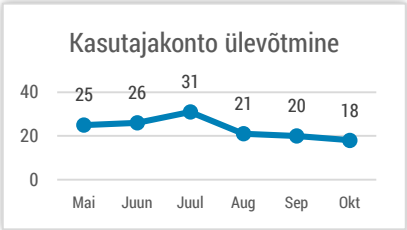
# Olukord küberruumis – oktoober 2020

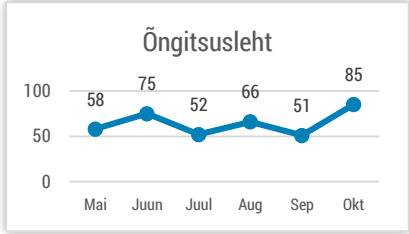
- Oktoobris registreerisime 279 intsidenti. Märkimisväärse tõusu taga on Emoteti pahavara suuremahuline levik.
- Emoteti pahavara levib lainetena ning selle tagajärgi asutustele võime näha alles pikema aja jooksul.
- Eestis asuvat kompromiteeritud serverit kasutati ähvardavate kirjade saatmiseks USA valijatele.
- Oktoobris tähistas Euroopa küberturvalisuse kuud.
- USA ja Euroopa liit omistasid taaskord varasemaid küberrünnakuid Venemaa sõjaväeluureametnikele.
- Maailmas jätkuvad suure mõjuga lunavararünnakud.




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




*Teated kontode ülevõtmisest on aasta jooksul stabiliseerunud.*




*Õngitsuslehtede hulk tõusis aasta kõrgeimale tasemel. Õngitsetakse nii kontoandmeid, kui ka petetakse välja raha.*

# Olukord Eesti küberruumis

**20. oktoobril saadeti USA Demokraatliku erakonna liikmetele kahes osariigis kümneid tuhandeid e-kirju** pealkirjaga „Vote for Trump or else!", milles väideti, et saatja teab, kelle poolt valija hääletas ja nõuti, et peab minema uuesti hääletama. Näiliselt tulid need aadressilt info@officialproudboys.com (mis viitab kohalikule äärmusparempoolsele neofašistlikule grupeeringule Proud Boys), kuid metaandmetest selgus, et kirjade saatmiseks kasutati Koolibri kirjastuse serverit Eestis. See tähendab, et ründajad kasutasid ära Elkdata serveris majutatud Koolibri kodulehe haavatavust, lisades lehele pahatahtliku koodi, mille abil need kirjad välja saata.

Koolibri ja Elkdata tegid intsidendi asjaolude selgitamiseks igakülgset koostööd CERT-EE-ga. RIA suhtles operatiivselt partneritega USA küberturvalisuse agentuurist CISA. Päev hiljem teatas USA föderaalne juurdlusbüroo, et kirjade taga on Iraani päritolu tegutseja.

**Septembrikuus kirjutasime teenustõkestusrünnakutest kahe kommertspanga vastu.** Sarnase käekirjaga rünnakud (väljapressimiskiri, näidisrünnak ja hoiatus, et raha maksmata jätmisel rünnatakse uuesti) toimusid 8. oktoobril taas ühe Eesti finantsasutuse vastu, kelle osad teenused olid häiritud või katkesid mitme tunni jooksul. Sarnaseid väljapressimiskirju said Eesti ettevõtted oktoobris veel, kuid enamasti ei kaasnenud nendega enam isegi näidisrünnakut. Seega võib hinnata, et kõnealused kurjategijad üritavad imiteerida suuri panku rünnanud kurjategijaid (kes omakorda imiteerivad riiklikke kinnisründe ehk APT gruppe).

**Emoteti pahavara levib jätkuvalt lainetena.** Oktoobris saime teada mitmekümnest Eesti asutusest, mille arvutid olid nakatunud – hotellidest projekteerimisfirmade, erameditsiinipakkujatest kohalike omavalitsuste asutusteni. Oleme nakatunud seadmete omanikke teavitanud, kuid soovime rõhutada, et taolistest nakatumistest võivad alguse saada palju suuremad intsidendid nagu andmelekked või lunavararünnakud.

**Riigivõrgu töö oli oktoobris häiritud mitmel korral.** 10. oktoobri tööpäeva lõpus jäi seadme rikke tõttu kolmandik Narva piirkonna klientidest võrguühenduseta, enamus neist taastati südaööks. Hooldustööde tõttu oli 12. oktoobril kahe tunni jooksul häireid ja katkestusi Lääne-Tallinna Keskhaigla, PERHi psühhiaatriakliiniku ja Tallinna kainestusmaja võrgus.

**29. ja 30. oktoobril nägime taas näiliselt SEB Panga nimel saadetud petukirju,** mille kaudu püüti ligi pääseda inimeste pangakontodele ja varastada neilt raha. Intsidendid näitavad, et PIN-koodide väljapetmise abil raha varastamise skeem ei kadunud pärast septembrikuist politsei küberkuritegude üksuse töövõitu Rumeenias.

# Tegevused küberturvalisuse parandamisel Eestis

**Oktoobris tähistati juba kaheksandat aastat üle-euroopalist küberturvalisuse teadlikkuse kuud,** mille eesmärk on suurendada Euroopa Liidu liikmesriikide elanike inimeste teadlikkust võrguturvalisusest. Seda kampaaniat korraldavad ELi liikmesriikide ja enam kui 300 partneri (valitsused, ülikoolid, mõttekojad, valitsusvälised organisatsioonid, kutseliidud, erasektori ettevõtted) toetusel Euroopa Liidu Küberturvalisuse Amet (ENISA) ja Euroopa Komisjon.

**Küberturvalisuse kuu Eestis keskendus tänavu IT-vaatliku kampaaniaga ettevõtete küberturvalisusele** – lisaks reklaamikampaaniatele käisime küberhügieenist rääkimas ettevõtlusüritustel üle Eesti. Mitmed meie töötajad ja koostööpartnerid (Helen Evert, Peeter Marvet, Hans Lõugas, Mai Kraft) osalesid kas füüsiliselt või virtuaalselt Tallinnas, Tartus, Viljandis, Narvas ja Võrumaal toimunud üritustel. Aitäh kõigile panustajatele!

**30. oktoobril toimus Tallinnas Kultuurikatlas Euroopa Liidu kübervõrgustiku EU CyberNet esimene aastakonverents.** Ühendades klassikalist küberturvalisuse konverentsi internetis üle kantud virtuaalüritusega arutleti Euroopa Liidu küberarenguabi projektide üle, räägiti võimalustest seda abi koordineeritumalt ning tõhusamalt pakkuda ning ennustati, milline saab olema EU CyberNeti roll nendes tegevustes. Konverentsi avas Euroopa Komisjoni rahvusvahelise partnerluse volinik Jutta Urpilainen, sõna võtsid teiste hulgas Eesti välisminister Urmas Reinsalu, Riigi Infosüsteemi Ameti peadirektor Margus Noormaa, Eesti küberjulgeoleku erivolitustega diplomaatilise esindaja Heli Tiirmaa-Klaar. Konverents on järelevaadatav EU CyberNet kodulehel: https://www.eucybernet.eu/live/

**Tellisime ITvaatlik.ee eraisikutele mõeldud kodulehekülje jaoks koolitusvideod vene keeles,** mis aitaksid eakamatel elanikel õppida, kuidas teha elementaarseid küberhügieeni tegevusi. Videod on vaid osa materjalidest, mis sel sügisel vene keelt kõnelevatele elanikele plaanis on – lisaks koolitasime ka vene emakeelega raamatukogude töötajaid, et nad saaksid paremini oma kliente toetada.

# Rahvusvaheline keskkond

**USA justiitsiministeerium esitas süüdistused kuuele Venemaa luureameti GRU ametnikule mitmete suuremahuliste küberrünnakute läbi viimise eest** – sh. NotPetya kampaania, Prantsusmaa 2017. aasta presidendivalimiste mõjutamine, rünnakud olümpiamängude vastu. Eesti Välisministeerium toetas USA otsust. Oktoobris kehtestas sanktsioonid Vene luurajatele (kaasa arvatud GRU direktorile) ka Euroopa Liit – seda täpsemalt 2015. aasta Saksa parlamendi ja kantsleri suunal tehtud küberrünnaku eest.

**USA julgeolekuasutused hoiatasid oktoobris lunavararünnakute märgatava sagenemise eest haiglate ja muude terviseasutuste vastu.** USAs sattus üheks selliseks sihtmärgiks New Jersey haigla, kes maksis andmete lekitamise vältimiseks 670 tuhat dollarit lunaraha. **Juba aastaid varem lunavararünnaku ohvriks langenud Soome Vastaamo psühhiaatriakliinik** aga ei maksnud. 2018. aastal kliinikust lekkinud andmeid kasutati aga oktoobris väljapressimiseks – mitte enam kliinikult, vaid patsientidelt.

**Lunavararünnakute laine maailmas aga jätkub:** maailma suurim kruiisikorraldamise ettevõte Carnival teavitas, et sai augustis pihta lunavararünnakuga, mille tõttu varastati suures mahus klientide, töötajate ning laevameeskonna liikmete isikuandmeid. Lunavararünnakud tabasid ka Montreali ühistranspordisüsteemi ning Saksa tarkvarafirma AG.

**Oktoobris täheldasime, et sagenes rünnakumall, mille kohaselt sooritatakse üha enam lunavaraga nakatunutele lisaks ka ummistusründeid,** et sundida ohvreid kurjategijatele lunaraha maksma.

**Iraani valitsusega seostatud rühmitus Silent Librarian taaskäivitas rünnakutelaine ülikoolide vastu**, kelle teaduslikule infole üritatakse õngitsuskirjade toel ligi pääseda.

**Rootsi kindlustusfirmat Folksam tabas andmeleke,** mille tõttu said mitmed veebiplatvormid, sh Facebook ja Google, ligipääsu umbkaudu ühe miljoni Rootsi elaniku tundlikele isikuandmetele – ehk andmetele, mida Rootsi kodanikud olid otsinud Folksami kodulehel.

**Oktoobris selgus, et kevadel Rootsi turvafirmasse Gunnebo süsteemidesse pääsenud kurjategijad** suutsid kätte saada mitmete erinevate firmade (võimalik, et pankade, lennujaamade, aga ka tuumajaamade, kelle turvalisuse eest Gunnebo vastutab) ja riigiasutuste tehnilised joonised.

**USA valimiste taustal** varastasid küberkurjategijad tõenäoliselt õngitsuskirjast alguse saanud rünnaku toel USA Vabariikliku Partei Wisconsini harult 2,3 miljonit dollarit.