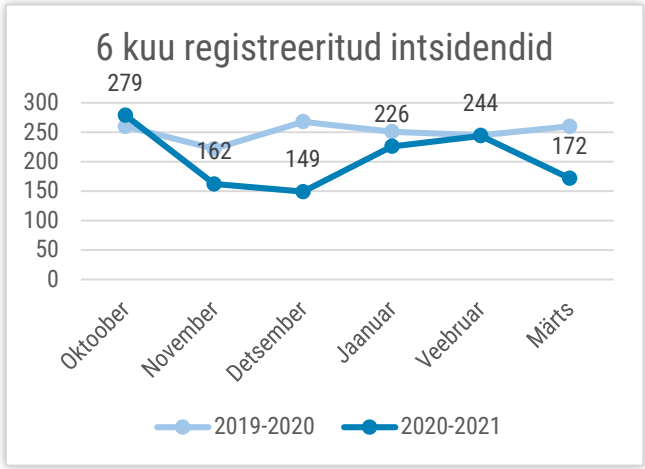
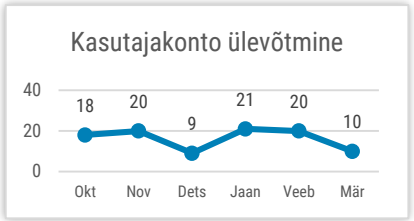
Olukord küberruumis – märts 2021

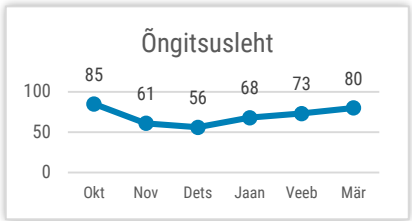
- Märtsis registreerisime 172 intsidenti, mis on keskmisest madalam hulk.
- Eesti ja maailma küberruumi häiris Microsofti meiliserverite turvanõrkuste järel alanud kompromiteerimiste laine.
- Avaldasime mitu aastat töös olnud uue Eesti infosturbestandardi E-ITS, mis hakkab asendama ISKE standardit.
- RIA uueks küberturvalisuse teenistuse juhiks valiti Eesti esinduse asejuht ÜRO juures Gert Auväärt.



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



Meilikontode ja sotsiaalmeedia-kontode ülevõtmine on jätkuvalt päevakajaline.



Õngitsuslehtede hulk on püsivalt kõrgel tasemel ja tõusutrendis. Eelkõige õngitsetakse kontoandmeid.

Olukord Eesti küberruumis

Olukorda Eesti küberruumis mõjutas rahvusvaheline intsident, kui Microsoft avalikustas 2. märtsil neli nullpäeva haavatavust oma meiliserverite tarkvaras, mille kaudu said ründajad laiaulatusliku ligipääsu kogu serverile, sealhulgas e-kirjadele ja salasõnadele. Teavituste järel ehitasid ründajad kiiresti tööriistad, mis hakkasid otsima veel uuendamata ja seega haavatavaid Exchange'i servereid üle terve maailma, leidmise korral need kompromiteeriti ja nakatati pahavaraga. 3. märtsil tuvastasime Eestist 80 mainitud haavatavustega meiliserverit. Teavitasime nende omanikke nii otse kui ka sideteenuse pakkuja kaudu.

Lisaks informeerisime avaliku sektori turvajuhte ning elutähtsa ja olulise teenuse osutajaid uuendamise vajadusest. Kui 10. märtsil seiret kordasime, oli kaks kolmandikku nendest serveritest endiselt paikamata ning seetõttu rünnakutele avatud. Ka mitmed avaliku sektori asutused või avalikke teenuseid pakkuvad asutused, näiteks kohalikud omavalitsused, haridus- ja tervishoiuasutused, leidsid oma hallatavatest serveritest jälgi sama haavatavuse kaudu kompromiteerimisest, rünnakukatsetest ja tagaustest.

Pikemalt kirjutame Exchange'i intsidendist oma värskes 2021. aasta esimese kvartali ülevaates.

Märtsis teavitati meid kahest suuremast lunavarajuhtumist. 24. märtsil tabas lunavararünnak üht elektritöödega tegelevat ettevõtet, krüpteerides kahes serveris olevad failid ning takistas rohkem kui saja inimese tööd. Teine intsident toimus juba veebruaris, kui ühe energia ja veetöötluse valdkonna ettevõtte failiserverid, meiliserverid ja varukoopiad krüpteeriti. Tõenäoliselt saadi ettevõttele ligi läbi tavakasutajate muu pahavaraga nakatunud arvutite.

Märtsis teavitas haridus- ja noorteamet (Harno) meid kahel korral teenustõkestusründest – 22. ja 26. märtsil. Esimesel päeval toimus rünnak mitme lainena paari tunni jooksul pärast tööpäeva lõppu, mistõttu ei mõjutanud see lõppkasutajaid märkimisväärselt. Teisel korral sooritati rünnak keset päeva, kuid vaid paarikümne minuti jooksul.

Ära tuleks märkida ka Eesti ehitusmasinatega tegeleva ettevõtte-suunaline arvepettus. E-posti kompromiteerimise tõttu vahetas ründaja ära nende poolt äripartnerile saadetud arvel arvenumbri, mistõttu maksis partner ca 35 000 eurose arve petturite arvele.

Tegevused küberturvalisuse parandamisel Eestis

RIA uueks küberturvalisuse teenistuse juhiks valiti avalikul konkursil Gert Auväärt, kes praegu töötab asejuhina Eesti alalises esinduses ÜRO juures. Pikaajalise rahvusvahelise kogemusega ning ka varem põgusalt RIA ridadesse kuulunud Auväärt alustab tööd 15. juulil. Tema hinnangul on oluline, et et Eesti püsiks maailma TOP 5 riigi hulgas, kelle poole liitlased küberturvalisuse teemadel pöörduvad ning oleks selge ja häälekas kõneisik küberturvalisuse teadlikkuse tõstmisel ja ohtude ennetamisel. Seni teenistust vedanud Lauri Aasmann jätkab teenistust peadirektori nõunikuna.

Märtsis avalikustasime mitu aastat töös olnud uue Eesti infosturbestandardi (E-ITS), mis vahetab pika üleminekuperioodi jooksul 2024. aastaks välja seni kasutusel olnud ISKE. Uus infoturbestandard on eelkõige avalikule sektorile loodud tööriist, millega tagatakse, et kõigis avalikke ülesandeid täitvates asutustes (nt kohalikus omavalitsuses) käidaks andmetega ja süsteemidega ümber turvaliselt.

Turvameetmete süsteem vajas värskendust, sest 2004. aastast kehtiv ja ligi 5000 lehekülge mahukas ISKE oli paljude jaoks sisuliselt hoomamatu ja tekitas turvalisuse asemel mitmete asutuste silmis pelgalt palju paberimajandust. 2018. aastal ISKE uuendamine peatati, anti alternatiivina võimalus rakendada rahvusvaheliselt tunnustatud standardit ISO/IEC 27001 ning alustati uue standardi väljatöötamist. Äsja valminud E-ITS pakub asutustele jõukohast eestikeelset ja Eesti õigusruumile sobivat alust infoturbe käsitlemiseks. E-ITS vastab rahvusvahelistele standarditele, pakkudes infoturbe tagamiseks etalonmeetmeid ja nende rakendamise süsteemi. Sellele vundamendile saab iga asutus vajaduse ja soovi korral lisada ka oma turvameetmeid. Avaliku sektori töötajatele peaks E-ITSi kasutamine saama tööprotsessi loomulikuks osaks. E-ITSiga seonduvad materjalid on koondatud veebilehele eits.ria.ee.

Teavitasime enam kui 6000 isikut, kelle arvuti brauserisse salvestatud paroolid olid lekkinud Emoteti pahavaraga nakatumise tõttu. Märtsi alguses informeerisime kõiki teadaolevaid ohvreid ja teenusepakkujaid. Üheks ohtlikumaks pahavaraks peetav troojalane Emotet jõudis viimase suurema lainena Eestisse eelmisel aastal, ent õnneks ei kujuta see enam aktiivset ohtu, sest on õiguskaitseasutuste poolt kahjutuks tehtud.

Märtsi keskpaigas lansseeriti RIA poolt veetava Euroopa Liidu kübervõrgustiku EU CyberNet tehniline platvorm CynAct. See hakkab ühendama kübervaldkonna organisatsioone selle ala ekspertidega üle terve Euroopa. Võrgustiku esimesel virtuaalsel üritusel tutvustati platvormi võimalusi ja kasutamist. Märtsi lõpuks oli võrgustikuga liitunud 15 asutust erinevatest Euroopa riikidest.

Rahvusvaheline keskkond

Nagu Eesti ülevaates märgitud, mõjutas maailma küberruumi Microsoft Exchange'i haavatavused, mille ekspluateerimiseks hakkasid ründajad kiiresti tööriistu ehitama. Need kompromiteerimised päädisid üle maailma eri tüüpi rünnakutega – näiteks Black Kingdomi nimeline lunavara krüpteeris vähemalt 1500 Microsoft Exchange'i serverit.

Samuti teatati Exchange rünnaku tagajärjel toimunud Norra parlamenti puudutanud andmevargusest. Kuu jooksul ilmes ka muud teavet infot riiklike parlamentide vastu suunatud rünnakute kohta, mille taga olid tõenäoliselt riikliku taustaga ohustajad: **Saksa parlamendi liikmeid tabas harpuunimisrünnak** (ehk väga täpselt sihitud õngitsusrünnak), mida seostatakse Vene sõjaväeluure GhostWriteri-nimelise küberrühmitusega. Viimastel kuudel aset leidnud uurimine viitab, et eelmisel aastal toimunud **rünnakus Soome Parlamendi vastu kahtlustatakse Hiinaga seotud APT31 rühmitust,** tuntud ka Zirconiumi nime all.

Märkimisväärseteks lunavara ohvriteks langesid märtsikuus haridusega tegelev Suurbritannia heategevusorganisatsioon Harris Federation, kelle töö halvati pea täielikult. Sarnane rünnak tabas ka USA IT-teenusepakkujat CompuComi, kelle rünnakust tulnud kahjusid hinnatakse 20 miljonile eurole ning Taiwani arvutitootjat Acerit, kellelt nõutakse andmete taastamise nimel 50 miljonit dollarit lunaraha. Ühe populaarseima teenusena pakutava Ryuk lunavaraga rünnati ligi 700 Hispaania riigisektori üksust.

Lunavaraga seotud arengutest vajab äramärkimist Clop-nimelise lunavararühmituse uus meetod, kus ärgitatakse ohvriks sattunud ettevõtte kliente ettevõtet survestama lunaraha ära maksma. Kübereksperdid märkasid huvitavat rünnaku mustrit, mille kohaselt sihib üks aktiivsemaid lunavararühmitusi REvil küberkindlustust omavaid ohverid.

Möödunud kuul avastati uudne Androidi nuhkvara, mis peibutas kasutajaid süsteemiuuendusena – troojaviirusena süsteemis leviv nuhkvara on ringluses vaid mitteametlikes kanalites ehk et ametlikust Google Play poest seda ei leidunud.

Facebook teatas Hiina valitsusega seotud kontode blokeerimisest, kuna neid kasutati aktivistide, ajakirjanike ja dissidentide seadmete pahavaraga nakatamiseks.

Märtsikuus nägime ka varasemate kuude rünnete tagajärgi, kus näiteks eelmises kuuülevaates mainitud Accelioni intsidendi tagajärjel lekitati naftatootmiskontserni Shelliga seotud teavet, sealhulgas isikuandmeid.