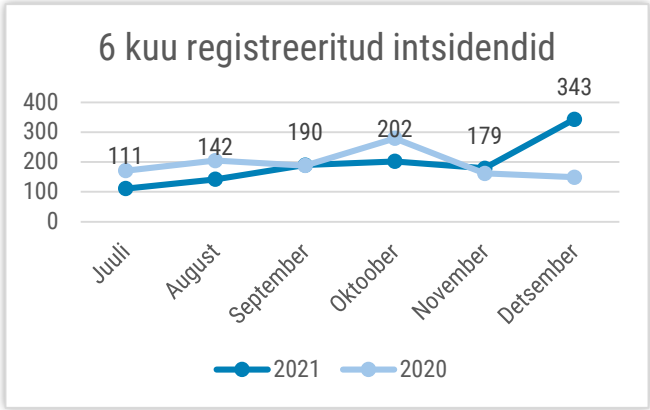
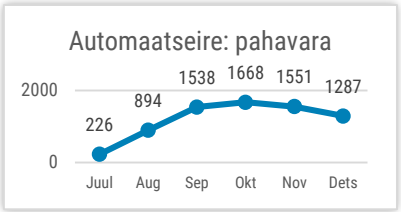
Olukord küberruumis – detsember 2021

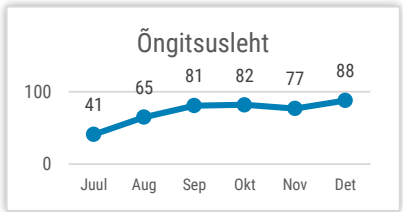
- Detsembris registreerisime 343 mõjuga intsidenti. Keskmisest palju kõrgem näitaja tuli tänu avastatud kompromiteeritud Eesti veebilehtedele.
- Turvanõrkus Java programmeerimiskeele logimisfunktsioonis Log4j pani IT- ja infoturbemeeskonnad palavikuliselt uuendusi tegema.
- Korraldasime RIA koostööpartneritele mõeldud veebikonverentsi „Olukorrast digiriigis 2021“.
- Venemaaga seostatud lunavararühmitus Conti ründas Austraalias mitut ettevõtet



CERT-EE-le teavitatud intsidendid, millel oli mõju andmete või infosüsteemide konfidentsiaalsusele, terviklusele või käideldavusele.



Automaatseire käigus tuvastatud seadmed Eesti küberruumis, mis on pahavaraga nakatunud. CERT-EE teavitab nakatumistest võrkude omanikke.



Õngitsuslehed moodustavad jätkuvalt kõige suurema osa CERT-EE registreeritud intsidentidest

Olukord Eesti küberruumis

Nii nagu mujal maailmas, möödus detsembrikuu küberturvalisuse valdkonnas ühe suure turvanõrkuse paikamise tähe all. 9. detsembril avaldati programmeerimiskeele Java logimisfunktsioonis Log4j kriitiline turvanõrkus, mille kaudu sai ründaja saata serverile pahatahtliku koodi ning võtta serveri üle. Turvanõrkus tähendas, et üle maailma olid kokku sajad miljonid seadmed või süsteemid ründajate poolt ülevõtmise ohus, sealhulgas Eesti e-riigi teenused ja neid toetavad seadmed.

Samal ajal, kui võtsime oma teenustes kasutusele uue Log4j versiooni paigaldamiseks või siis meetmeid ohu vähendamiseks, töötasime ühiselt ka koos Eesti IT-majadega, suhtlesime avaliku sektori turvajuhtidega, teavitasime elutähtsa teenuse osutajaid ja avaldasime pressiteate turvanõrkuse kohta. Pikemalt saab lugeda RIA blogist.

Log4j turvanõrkuse tõttu ei ole veel täheldatud edukaid rünnakuid, üksikutes süsteemides suutsid ründajad turvanõrkuse abil jooksutada krüptoraha kaevandamise pahavara. Kuid kuna rahvusvaheliselt on tulnud üksikuid teateid ründajatest, kes on suutnud turvanõrkust ära kasutada, oleme jätkuvalt valvel. Info õnnestunud rünnakute kohta võib ilmuda ka (palju) hiljem.

Nimetatud turvanõrkuse kõrval tuvastasime detsembri keskel 160 kompromiteeritud Eestiga seotud veebilehte, mis olid ründajate poolt ümber suunatud. Aegunud või paikamata veebiteenuste komponente ära kasutades olid need suunatud domeenidele, mis näiteks teavitas kasutajat nutitelefoni võitmisest ja sundis kasutajat avama reklaame ning hüpikaknaid. Teavitasime leidudest kõigi domeenide haldajaid koos soovitusega oma võrguseaded üle vaadata.

Jõulude eel hakkas taas levima tegevjuhi petuskeem, kus raamatupidaja või mõni teine arvete tasumise eest vastutav inimene saab e-kirja, mille saatjaks on näiliselt sama ettevõtte tegevjuht. Kirjas palutakse kiirelt tasuda lisatud arve, milles märgitud arvelduskonto on petturite kontrolli all. Saime detsembris tosinal korral teada ebaõnnestunud katsetest, kuid üks kord läks petturitel ka õnneks. Detsembri keskel teatas üks ettevõte ligi 15 000 euro saatmisest välisriigi pangakontole just sellise pettuse järel. Paar päeva hiljem tegi pettur sama ettevõtte suunas uue katse, kuid sel korral ebaõnnestus.

Jätkuvalt on teenustõkestusründed häirimas Eesti inimeste elu. Detsembri lõpus toimus kaks hajutatud teenustõkestusrünnakut (DDoS) rünnakut ühe Eesti kommertspanga suunas. Lühiajalised rünnakud häirisid interneti- ja mobiilipanka sisenemist ning kaardimakseid.

Palju lihtsamalt häiriti ühe telekomiettevõtte veebilehe toimimist, kus ründaja laadis ettevõtte veebivormi suure hulga faile ja tekitas sellega tõrkeid veebiilehe töös – leht hangus või ei olnud ajutiselt kättesaadav.

Tegevused küberturvalisuse parandamisel Eestis

9. detsembril avalikustatud Log4j turvanõrkuse järel töötasime koos kõikvõimalike partneritega nii Eestis kui väljapool, et teenused saaksid võimalikult kiiresti paigatud ja rünnakukatsed tuvastatud. Infoturbe- ja IT-spetsialistid tegid üle maailma koostööd haavatavate süsteemide ja seadmete tuvastamiseks, et võimalikult kiiresti vähendada rünnakuvõimalusi. Tõenäoliselt tähendas see paljude asutuste infoturbe- ja IT-spetsialistidele magamata öid ja ületunde, selle pingutuse eest oleme neile igati tänulikud.

Korraldasime 7. ja 8. detsembril koostööpartneritele suunatud veebikonverentsi "Olukorrast digiriigis 2021". Rääkisime koos teiste asutuste ekspertidega küberturvalisusest, valimistest, värskest Eesti infoturbestandardist ja paljust muust. Veebikonverentsi esimese päeva ülekanne on järelvaadatav siin ja teise päeva ülekanne siin RIA Facebooki leheküljel.

Eesti infoturbestandardi ehk E-ITSi uus versioon sai valmis ning avalikustatakse peagi E-ITS portaalis. Standardit kehtestav küberturvalisuse seaduse muutmise eelnõu läbis vajalikud kooskõlastusringid.

Alustasime kolme elutähtsa teenuse osutaja (ETO) suhtes järelevalvemenetlused, mille käigus kontrollime küberturvalisuse seaduse nõuete täitmist. Järelevalvemenetluse eesmärgiks on kontrollida ETO organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamist ja nende piisavust teenuse osutamiseks kasutatava võrgu- ja infosüsteemide küberintsidentide ennetamiseks, teavitamiseks ning lahendamiseks.

Kriitilise informatsiooni infrastruktuuri kaitse osakond (KIIK) kohtus erinevate organisatsioonidega tuleviku koostöö eesmärgil, sealhulgas ka Eesti Panga ja Teliaga. Lisaks avaldati artikkel perearstikeskuste küberturvalisuse parandamisest ajakirjas "Perearst"

Rahvusvaheline keskkond

Nii nagu Eestis, röövis Log4Shell turvanõrkus unetunde paljudelt IT-ekspertidelt üle maailma. Seega tuli paljudel ettevõtetel kiiresti välja töötada parandused ja need sisse viia, sest võidu tuli joosta nii kurjategijate kui ka riiklike sidemetega küberrühmitustega, kes hakkasid kohe turvanõrkust aktiivselt ära kasutama.

Kuu alguses hoiatas Apple 11 USA välisministeeriumi töötajat, et nende iPhone'id on nakatatud Pegasuse nuhkvaraga. Pegasus kuulub Iisraeli ettevõttele NSO, mille klientideks on paljud riigid. Pegasusega nakatudes saab käivitada sihtmärgi telefoni kaamera ja mikrofoni, samuti pääseb ligi kogu telefoni sisule.

Prantsuse küberamet ANSSI teatas, et Vene välisluureteenistuse küberrühmitus APT29 (tuntud ka kui Nobelium) on aasta vältel rünnanud paljusid Prantsuse organisatsioone. ANSSI teatel on rühmitus kompromiteerinud mitme organisatsiooni e-maili aadresse ja saatnud nende alt välja pahavara sisaldavaid kirju välismaistele institutsioonidele.

Pead tõstis ka Conti lunavara, millega sai pihta Austraalia elektriettevõte CS Energy. Ettevõte varustab elektriga miljoneid majapidamisi ning neil on suured kliendid kaubandusest ja tööstusest. Ettevõtte sõnul ühendati kompromiteeritud seadmed kiiresti lahti ülejäänud võrgust. Nii ei saanud ka elektri tootmine ja pakkumine rünnaku tõttu mõjutatud.

Contiga on seostatud ka teist Austraaliat tabanud hoopi. Nimelt ilmusid tumeveebi müüki 38 000 Lõuna-Austraalia avaliku sektori töötaja andmed. Lekkisid näiteks töötajate ees- ja perekonnanimi, sünnipäev, kodune aadress, pangakonto andmed, töötasu, maksuinfo. Põhjuseks oli avalikule sektorile tarkvara pakkunud ettevõtet Frontier Software tabanud lunavararünnak.

Turvaspetsialistide hinnangul on Contil ka juba selge, kuidas ära kasutada Log4Shell turvanõrkust, et saada esialgne ligipääs teatud tarkvara kasutajate võrkudesse.

Ka Brasiilia tervishoiuministeerium teavitas, et neid tabas ulatuslik lunavararünnak. Miljonite kodanike COVID-19 vaktsineerimisandmed muutusid kättesaamatuks. Samuti kukkusid maha kõik tervishoiuministeeriumi veebilehed. Rünnaku eest võttis vastutuse rühmitus Lapsus$.

Ent detsember tõi ka häid uudiseid. Ukraina õiguskaitseorganid arreteerisid 51 inimest, keda kahtlustatakse häkkerite foorumites varastatud andmete müümises. Arestiti umbes 100 andmebaasi, mis sisaldasid tundlikku infot sadade miljonite inimeste kohta. Lisaks võtsid Ukraina võimud maha ühe suurima andmemüügi platvormi, kus müüdi inimeste nimesid, telefoninumbreid, aadresse ja mõnel juhul ka sõidukiinfot.