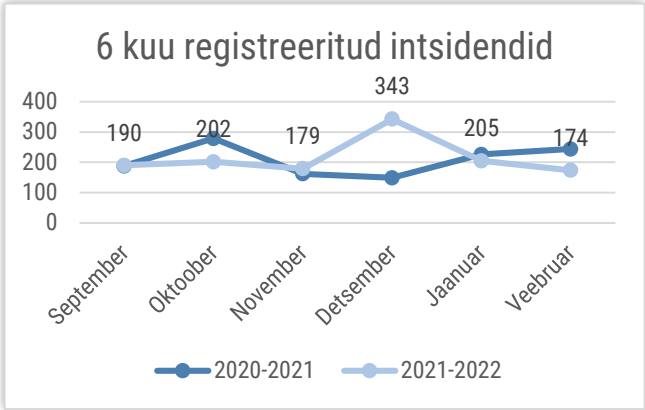
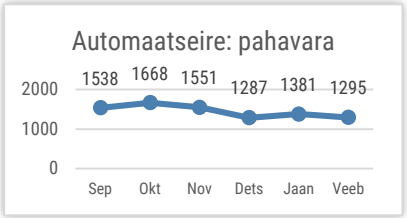
Olukord küberruumis – veebruar 2022

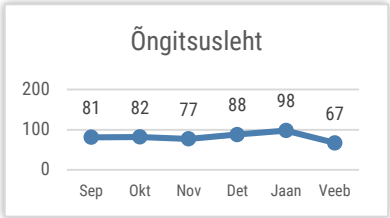
- Veebruaris registreerisime 174 mõjuga intsidenti, mis on aasta keskmisest veidi madalam näitaja.
- Veebruaris toimus keskmisest enam teenuste katkestusi ja neist kõige suurema mõjuga oli kuu keskpaigas toimunud Telia ulatuslik kõneside- ja M2M-teenuste rike.
- Avaldasime RIA küberturvalisuse aastaraamatu, kus kirjutasime eelmisel aastal Eesti ettevõtteid ja asutusi mõjutanud olulistest turvanõrkustest.
- Jätkusid küberrünnakud Ukraina vastu, esines nii teenustõkestusründeid kui ka pahavara levitamist.



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

Veebruaris nägime keskmiselt rohkem erinevate **teenuste katkestusi**. Üldjuhul oli nende põhjuseks kas tarkvara või riistvara rike, aga esines ka teenus-tõkestusründeid. Kõige suurema mõjuga oli Telia ulatuslik kõneside- ja M2M-teenuste rike, mis kestis alates 15.02 hilisõhtust kuni 16.02 õhtuni. M2M teenuseid kasutatakse näiteks kontroll- ja juhtimis-seadmetes värava avamiseks või m-parkimise alustamiseks. Katkestus mõjutas kõnesid hädaabi-numbrile 112, probleeme esines ka riigiinfo telefonile 1247 ja perearsti nõuandeliinile 1220 helistamisel.

Nii 9. veebruaril kui ka 22. veebruaril ei olnud võimalik kasutada digiretsepti, kindlustatuse kontrolli ega teisi avalikke Haigekaasa teenuseid. Mobiil-ID kasutamine ei olnud võimalik kokku neljal korral. Maksu- ja Tolliameti veebilehel tekkis 7.veebruaril kell 12.45 kuni 14.52 katkestus seoses protsessori ülekoormusega. 17.veebruaril katkes ajavahemikuks 14.23 kuni 15.00 rahvastikuregistri töö. 24.veebruaril ajavahemikul 18.08 kuni 19.15 ei olnud andmebaasi tõrke tõttu võimalik vormistada isikute ega sõidukite piiriületusi.

Mitmed riigiametite veebilehed olid **skaneeringust põhjustatud häirete** tõttu kättesaamatud. 20. veebruaril toimus riigiportaali eesti.ee töös seitse lühiajalist katkestust. Sotsiaalministeeriumi veebilehe töö oli häiritud 22.veebruaril ja Sotsiaalkindlustusameti avalik veeb ei olnud kättesaadav 24.veebruari öösel.

Veebruaris toimusid **teenustõkestusrünnakud (DDoS) nii koolide, haridusteenuste kui ka ERR vastu**. 4., 5. ja 22. veebruaril rünnati kolme erinevat Lõuna-Eesti kooli. Kahel korral rünnati ka õppeinfosüsteemi Tahvel. 7. veebruaril ajavahemikul 10.11 kuni 10.18 sooritati teenusetõkestusrünne Eesti Rahvusringhäälingu vastu, mistõttu oli portaalide töö häiritud kuni 11.00.

Sagenesid **kasutajakontode ülevõtmised**, millest anti teada 30 korda. Meid teavitati nii kompromiteeritud sotsiaalmeedia kui ka e-posti kontodest. Üldjuhul võeti kasutajatel mitu kontot korraga üle, esmalt saadi ligipääs näiteks Gmaili kontole ja selle kaudu vahetati ka teiste keskkondade paroolid ära. Soovitame igas keskkonnas kasutada erinevat tugevat salasõna ja võimalusel kahetasemelist autentimist, nii on võimalik kaitsta end olukorra eest, kus paroolide lekke korral saavad kõik salasõnad korraga teatavaks. Samuti soovitame salasõnu regulaarselt uuendada.

Veebruaris märkasime sagenenud teavitusi näiliselt **Linkedin'i poolt saadetud õngitsuskirjadest**, mis suunavad kasutaja mobiiltelefoni loosimise lehele. Kirjades väidetakse, et lingile vajutades on võimalik teada saada millised ettevõtted on kasutaja profiili vaadanud. Soovitame alati enne lingi avamist selle poolt viidatud aadressi (URL-i) üle kontrollida, seda saab teha kursoriga lingile liikudes. Kui see aadress ei esine korrektsel kujul, näiteks linkedin.com, on väga tõenäoliselt tegemist õngitsuskirjaga

Tegevused küberturvalisuse parandamisel Eestis

Saime valmis **RIA küberturvalisuse aastaraamatu**, kus kirjutame eelmisel aastal avalikuks saanud turvanõrkustest, mis põhjustasid pahandust nii Eestis kui ka mujal maailmas. Raamatus on juttu nii Microsoft Exchange'i, Atlassian Confluence kui ka Log4j haavatavustest, mis kõik mõjutasid eelmisel aastal Eesti ettevõtteid ja asutusi. Turvanõrkuste kõrval on aastaraamatus juttu finantspettustest, ummistusrünnakutest, RIA suvistest küberintsidentidest, lunavararünnakutest, suurema kahjuta jäänud potentsiaalselt ulatuslikest intsidentidest, taakvarast, valimistest ja paljust muust.

Avaldasime **täiendatud ohuhinnangu** Ukraina vastastest küberrünnakutest ning nende võimalikest mõjudest Eestis. Pöörame tähelepanu kahele peamisele ründevektorile ehk rünnetele teenusepakkuja ja lõppkasutaja kaudu, mida Ukrainas kasutati. Ohuhinnangus andsime konkreetsed soovitused asutuste ja ettevõtete infoturbejuhtidele.

Jätkusid **koolitused tulevastele Eesti infoturbestandardi rakendajatele**, mille eesmärgiks on anda oskused ja teadmised uue E-ITS standardi rakendamiseks. Neid koolitusi oleme korraldanud regulaarselt alates 2021.aastast.

Veebruaris **lõpetasime järelevalvemenetlused kolme ettevõtte** osas ning hindasime nende küberturvalisuse seaduse kohustuste täitmist piisavaks. RIA kontrollib turvameetmete rakendamist nii riigi ja kohaliku omavalitsuse asutuste kui ka olulise ja elutähtsa teenuse osutaja infosüsteemides.

Kohtusime virtuaalselt Eesti Panga ja Eesti kommertspankade juhtidega, rääkisime neile küberruumi hetkeolukorrast Eestis, meid varitsevatest ohtudest ning leppisime kokku edasised koostöövõimalused.

Teavitasime nii ettevõtteid kui riigiasutusi **kriitilistest turvanõrkustest** nende veebides või kasutuses olevas tarkvaras. Taolisi teavitusi teeme regulaarselt, kui antakse välja kriitilisi turvauuendusi Eestis kasutuses olevale tarkvarale.

Avaldasime RIA veebilehel olulisemad viited ja soovitused, kuidas olla kursis viimaste kübersündmustega ja kuidas end ja enda asutust teatud ohtude eest paremini kaitsta seoses julgeolekuolukorraga Euroopas.

Rahvusvaheline keskkond

Veebruaris tabasid Ukrainat nii enne kui ka pärast sõjaseisukorra väljakuulutamist mitmed küber-rünnakud. Näiteks kuu alguses hoiatas Microsoft Gamaredoni-nimelise häkkerite rühmituse eest, mis juba mitu kuud oli Ukraina organisatsioone järjepidevalt õngitsuskirjadega sihtinud. Kuu vältel olid Ukraina pankade, riigiasutuste, relvajõudude ja teiste organisatsioonide veebilehed ja –teenused sageli teenusetõkestusrünnete tõttu maas. Mitmed riigid (sh Eesti) on osad neist rünnetest omistanud Vene sõjaväeluurele GRU.

Lisaks teatas CERT-UA, et nende **relvajõudude personali isiklike e-maili kontodele saadetakse massiliselt õngitsuskirju**. Õngituskampaania omistati rühmitusele UNC1151 (*Ghostwriter*), mida on seostatud nii Venemaa kui Valgevenega. Sealjuures on käimas ka õngitsused, milles kasutatakse Ukraina relvajõudude liikme kompromiteeritud e-maili, et sihtida Euroopa riikide ametnikke, kes tegelevad Ukraina sõjapõgenike logistikaga.

Seoses sõjaga Ukrainas aktiveerusid ka mitmed rahvusvaheliselt tuntud kuritegelikud küberrühmitused ja häktivistid. Näiteks teatas Venemaa pinnal tegutsev Conti lunavararühmitus, et toetab täielikult Venemaa presidenti ning ähvardas rünnata Kremli vaenlaseid. Peale seda tekkis rühmituse sees lõhestumine, kus arvatavalt Ukraina päritolu rühmituse liige avaldas sisemised vestlused.

Vastukaaluks on aktiivse rolli võtnud ka häktivistide küberrühmitus Anonymous, mis näiteks ründas Venemaa kaitseministeeriumit ja lekitas infot selle töötajate kohta. Rühmitus on teatanud ka näiteks Valge-vene raudteesüsteemi ja Vene riiklike telekanalite ründamisest.

Ukraina olukorra kõrval oli veebruaris ka teisi mõjukaid küberründeid. Näiteks kuu alguses said Lääne-Euroopa naftaga tegelevad üksused pihta lunavaraga, mistõttu oli nende töö häiritud. Sihtmärkide seas olid näiteks Saksamaa ettevõtted Oiltanking ja Mabanaf. Rünnete taga olevat rühmitus BlackCat. Sama rühmitus ründas ka lennujaamasid teenindavat ettevõtet Swissport, mistõttu hilinesid mitmed lennud.

Veebruaris sai teatavaks ka küberrünne USA meediaettevõtte News Corp suunal, mille tulemusel said arvatavasti Hiina riikliku taustaga häkkerid ligi aja-kirjanike ja teiste töötajate e-kirjadele ning dokumentidele. USA-s viis küberrünnak rivist välja logistikahiiglase Expeditors International, mille tegevused üle maailma olid häiritud. Lisaks sai lunavaraga pihta USA kiibitootja Nvidia.

Ka Euroopa sideettevõtted puutusid küberrünnetega kokku. Näiteks Vodafone Portugal sai pihta jõulise küberrünnakuga, mistõttu katkes 4G ja 5G võrkude töö. Nii Nvidia kui ka Vodafone rünnakute taga võis olla Lapsus$ häkkerite rühmitus.