EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA OHTUDE KAARDISTAMISE ARUANNE 2021

Aprillist 2020 juuli keskpaigani 2021

OKTOOBER 2021

ENISA

Euroopa Liidu Küberturvalisuse Amet (ENISA) on Euroopa Liidu asutus, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu Euroopas. 2004. aastal asutatud ning ELi küberturvalisuse määrusega tugevdatud Euroopa Liidu Küberturvalisuse Amet osaleb ELi küberpoliitikas, suurendab IKT-toodete, -teenuste ja -protsesside usaldusväärsust küberturvalisuse sertifitseerimiskavade abil, teeb koostööd liikmesriikide ja ELi organitega ning aitab Euroopal valmistuda tuleviku küberprobleemideks. Teadmisi jagades, võimekust arendades ja teadlikkust suurendades teeb amet koostööd peamiste sidusrühmadega, et tugevdada usaldust sidusa majanduse vastu, edendada Euroopa Liidu taristu säilenõtkust ning tagada kokkuvõttes Euroopa ühiskonna ja kodanike digitaalne turvalisus. ENISA ja tema tegevuse lisateave on aadressil www.enisa.europa.eu.

KONTAKTANDMED
Autorite kontaktaadress: etl@enisa.europa.eu.
Dokumendiga seotud meediapäringud: press@enisa.europa.eu.

TOIMETAJAD
Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Euroopa Liidu Küberturvalisuse Amet

KOOSTAJAD
Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

TÄNUAVALDUS
Soovime tänada ENISA küberohtude kaardistamise ajutise töörühma liikmeid ja vaatlejaid käesoleva aruande kinnitamisel antud väärtusliku tagasiside ja kommentaaride eest. Ühtlasi soovime tänada ENISA nõuanderühma ja riikide kontaktametnike võrgustikku väärtusliku tagasiside eest.
Samuti soovime tänada ENISA olukorrateadlikkuse ja intsidentidest teatamise töörühmi nende aktiivse panuse ja toe eest teabeosade koondamisel ohtude kaardistamise aruandeks.

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

SISUKORD

KOMMENTEERITUD KOKKUVÕTE

See on ENISA ohtude kaardistamise aruande üheksas väljaanne – aastaaruanne, milles käsitletakse küberturbeohtude kaardistamise olukorda ja tuvastatakse peamised ohud, ohtudega seoses täheldatud peamised suundumused, ohusubjektid ja ründemeetodid ning kirjeldatakse asjakohaseid leevendusmeetmeid. Ohtude kaardistamise aruannete koostamismetoodika pideval täiustamisel toetas käesoleva aasta tööd ENISA äsja moodustatud küberohtude kaardistamise ajutine töörühm.

ENISA ohtude kaardistamise 2021. aasta aruanne hõlmab ajavahemikku 2020. aasta aprillist kuni 2021. aasta juulini, mida nimetatakse aruandes aruandeperioodiks. Aruandeperioodil tuvastatud peamised ohud on muu hulgas järgmised.

- **Lunavara**
- **Kahjurvara**
- **Kaevekaaperdus**
- **E-postiga seotud ohud**
- **Andmevastased ohud**
- **Kättesaadavuse ja tervikluse vastased ohud**
- **Väär- ja eksiteave**
- **Mittekuritahtlikud ohud**
- **Tarneahelaründed**

Käesolevas aruandes käsitleme 8 esimest küberohukategooriat. 9. kategooria ohte (tarneahelaohud) analüüsiti üksikasjalikult nende erilise tähtsuse tõttu ENISA tarneahelarünnetega seotud ohtude kaardistamise aruandes[1].

Iga tuvastatud ohu korral käsitletakse ründemeetodeid, märkimisväärseid intsidente ja suundumusi ning leevendusmeetmete ettepanekuid. Suundumuste osas tõstame aruandeperioodil esile järgmist.

- **Lunavara** peetakse **aastatel 2020–2021 peamiseks ohuks.**
- **Valitsusorganisatsioonid on suurendanud tegevust** nii riigi kui ka rahvusvahelisel tasandil.
- **Küberkurjategijaid motiveerib üha enam** oma tegevuse **rahaks muutmine**, näiteks lunavaraga. **Krüptovaluuta** on endiselt kõige tavalisem ohusubjektide kasutatav väljamaksemeetod.
- 2020. aastal täheldatud **kahjurvara kasutamise vähenemine** jätkub 2021. aastal. 2021. aastal täheldasime nende ohusubjektide arvu suurenemist, kes kasutasid oma koodi portimiseks võrdlemisi uusi või tundmatuid programmeerimiskeeli.
- Võrreldes eelmiste aastatega oli **kaevekaaperdusrünnete** arv 2021. aasta I kvartalis **enneolematult suur**. Ohusubjekte innustas neid ründeid tegema kaevekaaperdusega kaasnev **rahaline kasu**.
- **COVID-19 on seniajani valdav peibutusvahend** e-posti rünnete kampaaniates.
- Esines **tervishoiuandmetega seotud rikkumiste järsk kasv**.
- **Tavapärased hajusate ummistusrünnete kampaaniad** on 2021. aastal suunatumad, püsivamad ja üha enamate vektoritega. **Esemevõrk (IoT)** koos **mobiilsidevõrkudega** on toonud kaasa hajusate ummistusrünnete uue laine.
- 2020. ja 2021. aastal täheldame **mittekuritahtlike intsidentide arvu järsku kasvu**, sest COVID-19 pandeemia tõttu mitmekordistus **inimlike vigade** ja **süsteemide konfiguratsioonivigade arv** kuni selleni, et 2020. aastal oli enamik andmerikkumistest tingitud vigadest.

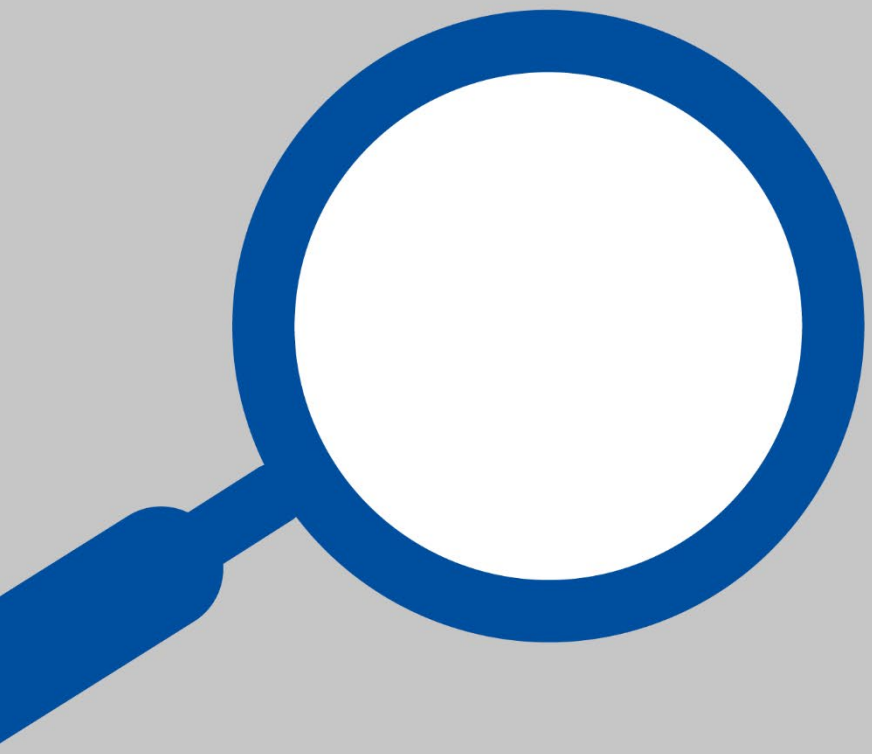
Ohusubjektidega seotud suundumuste, nende motivatsiooni ja sihtmärkide mõistmine aitab suuresti kavandada küberturvalisuse kaitsemeetmeid ja leevendusstrateegiaid. See on meie üldise ohuhinnangu lahutamatu osa, sest

[1] ENISA tarneahelarünnetega seotud ohtude kaardistamise aruanne, juuli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

võimaldab ohu realiseerumise võimaliku mõju ja tõenäolisuse alusel prioriseerida turbekontrollimeetmeid ning välja töötada sihtotstarbelise strateegia. Seda silmas pidades käsitletakse ENISA ohtude kaardistamise 2021. aasta aruandes nelja küberturvalisuse ohusubjektide kategooriat.

- **Riigijõud**
- **Küberkurjategijad**
- **Palgatud häkkerid**
- **Häktivistid**

Pideva analüüsi abil tuletas ENISA oma ohtude kaardistamise 2021. aasta aruandes iga peamise ohuga seotud suundumused ja huvipunktid. Siin hinnangus esitatud põhilised tähelepanekud ja otsused on tehtud mitme avalikult kättesaadava allika põhjal, mis on lisatud käesoleva dokumendi koostamise allikaviidetele. Aruanne on peamiselt suunatud strateegilistele otsustajatele ja poliitikakujundajatele, kuid pakub huvi ka tehnilisele küberturbe kogukonnale.



1. OHUSPEKTRI ÜLEVAADE

ENISA ohtude kaardistamise aruande üheksandas väljaandes on küberturbeohtude ülevaade. Ohtude kaardistamise aruanne on osaliselt strateegiline ja osaliselt tehniline ning sisaldab teavet nii tehnilise kui ka mittetehnilise valdkonna lugejatele. Käesoleva aasta tegevust toetas ENISA äsja asutatud küberohtude kaardistamise ajutine töörühm[2].

Küberturberünded on kogu 2020. ja 2021. aasta vältel pidevalt kasvanud peale vektorite ja arvude ka mõju mõistes. Ootuspäraselt on küberturbeohte mõjutanud ka COVID-19 pandeemia. Üks COVID-19 pandeemia püsivamaid arengusuundi on kestev üleminek hübriidkontori mudelile. See tähendab, et pandeemiaga seotud küberturbeohud ja „uue normaalsuse“ kasutamine on muutumas tavapäraseks. See suundumus on suurendanud rünnete toetuspinda, mille tulemusena oleme näinud organisatsioonidele ja ettevõtetele kodukontorite kaudu tehtavate küberrünnete arvu suurenemist[3]

Küberturbeohud on üldiselt sagenemas. Ajendatuna üha suuremast kohalolekust veebis, tavapäraste taristute üleminekust veebi- ja pilvepõhistele lahendustele, paremast võrguühendusest ning kujunemisjärgus tehnoloogiate (nt tehisintellekt[4][5]) uute funktsioonide kasutamisest on küberturbemaastikul suurenenud rünnete komplekssus, keerukus ja mõju. Eelkõige on oht tarneahelatele ja nende olulisus võimaliku katastroofilise doominoefekti tõttu saavutanud peamiste ohtude seas esikoha, mistõttu koostas ENISA selle ohukategooria kohta ohtude kaardistamise eriaruande[6].

Tuleb märkida, et käesolevas ajakohastatud ENISA ohtude kaardistamise aruandes on erilise tähelepanu all küberohtude mõju eri valdkondadele, sealhulgas küberturvalisuse direktiivis loetletutele. Ohuspektrit arvestades võib teha huvitavaid tähelepanekuid iga valdkonna eripära, potentsiaalsete vastastiksõltuvuste ja oluliste teemade kohta. Valdkondlikud ohuspektrid väärivad seega rohkem tähelepanu.

Samuti on nii küberkogukonna kaitsjad kui ka poliitikakujundajad astunud sel aastal märkimisväärseid samme. Ülemaailmne kogukond on hakanud mõistma teabevahetuse ja koostöö olulisust küberkurjategijate uurimisel ja jälitamisel ning just lunavarast (kõige tähtsam oht ENISA ohtude kaardistamise 2021. aasta aruande aruandeperioodil) on saanud üheks peamiseks ülemaailmsete juhtide strateegiakohtumiste päevakorrapunktiks.

ENISA ohtude kaardistamise 2021. aasta aruande varasemate väljaannete tähelepanelikud lugejad märkavad erinevusi peamiste ohtude kaardistamisel. Sel aastal astus ENISA sammu tagasi ja koondas ohukategooriad nii, et sarnased ohud oleksid lõimitud ja esindatud paremini. See on osa toimuvast tegevusest muudetud ohutaksonoomia suunas ja aitab lähiaastatel käsitleda suundumusi metodoloogiliselt.

ENISA ohtude kaardistamise 2021. aasta aruanne põhineb mitmesugusel avalikest allikatest pärit teabel ja küberohtude luureteabe allikatel. Aruanne tuvastab peamised ohud, suundumused ja tähelepanekud ning esitab asjakohased kõrgetasemelised leevendusstrateegiad. Praegu tõhustab ENISA ohtude kaardistamise aruandluse metoodikat, et edendada läbipaistvust ja järjepidevust.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – „Andmerikkekulude 2020. aasta aruanne“ – https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA tehisintellektiohtude kaardistamise aruanne: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISA tarneahelarünnetega seotud ohtude kaardistamise aruanne, juuli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. PEAMISED OHUD

2020. ja 2021. aasta jooksul ilmnes ja materialiseerus mitu küberohtu. Käesolevas aruandes olevale analüüsile tuginedes tuvastatakse ENISA ohtude kaardistamise 2021. aasta aruandes järgmised 8 peamist ohurühma ja keskendutakse nendele (vt **Joonis 1**). Nende 8 ohurühma esiletõstmisel arvestati nende olulisust aruandeperioodil, populaarsust ja nende materialiseerumise mõju.

- **Lunavara**
  Lunavara on kuritahtliku ründe liik, kus ründajad krüptivad organisatsiooni andmed ja nõuavad juurdepääsu taastamiseks lunaraha. Lunavara oli mitme kõrgetasemelise ja suurt meediakajastust saanud intsidendi tõttu aruandeperioodil peamine oht. Lunavaraga ohu raskust ja mõju näitab ka mitu seonduvat Euroopa Liidu (EL) ja ülemaailmset poliitikaalgatust.

- **Kahjurvara**
  Kahjurvara on tarkvara või riistvara, mille eesmärk on teha volitamata protsesse, mis kahjustavad süsteemi konfidentsiaalsust, terviklust või käideldavust. Kahjurvaraohtu on vaatamata ENISA ohtude kaardistamise 2021. aasta aruande aruandeperioodil esinenud intsidentide vähenemisele peetud püsivalt suureks. Uute ründemeetodite kasutamine ja õiguskaitsekogukonna saavutatud olulised saavutused on mõjutanud asjaomaste ohusubjektide tegevust.

- **Kaevekaaperdus**
  Kaevekaaperdus ehk peidetud krüptorahakaeve on küberkuritegevuse liik, kus kurjategija kasutab krüptovaluuta loomiseks salaja ohvri andmetöötlusvõimsust. Tänu krüptovaluuta levikule ja sellele, et laiem avalikkus kasutab krüptovaluutat üha rohkem, on täheldatud vastavate küberturbeintsidentide sagenemist.

- **E-postiga seotud ohud**
  E-postiga seotud ründed on hulk ohte, kus kasutatakse ära pigem inimpsüühika ja argiharjumustega seotud haavatavust kui infosüsteemide tehnilisi haavatavusi. Vaatamata paljudele seda liiki rünnete teadvustamis- ja teabekampaaniatele tuleb siiski tõdeda, et märkimisväärne oht püsib. Eelkõige on sagenemas meilipetted ja keerukate meetodite kasutamine rahalise kasu saamiseks.

- **Andmevastased ohud**
  Siia kategooriasse kuuluvad andmerikkumised (andmelekked). Andmerikkumine ehk andmeleke on tundlike, konfidentsiaalsete või kaitstud andmete levitamine ebausaldusväärsesse keskkonda. Andmerikkumine võib toimuda küberründe, siseteabe väärkasutamise, tahtmatu andmekao või andmete avaldamise tulemusena. Oht on jätkuvalt suur, sest juurdepääs andmetele on ründajate üks peamisi sihtmärke mitmel põhjusel, näiteks väljapressimine, lunaraha, laimamine, eksiteave jne.

- **Kättesaadavuse ja tervikluse vastased ohud**
  Kättesaadavus ja terviklus on sihtmärgiks arvukates ohtudes ja rünnetes, eelkõige ummistus- ja veebirünnete rühmades. Hajus ummistusrünne, mis on rangelt seotud veebipõhiste rünnetega, on üks kõige kriitilisema tähtsusega ohtudest IT-süsteemidele ja kahjustab nende käideldavust, ammendades ressursse, põhjustades jõudluse vähenemist, andmekadu ja teenusekatkestusi. Oht on ENISA ohtude kaardistamise aruandes järjepidevalt kõrgel kohal nii selle esinemise tõttu reaalsetes intsidentides kui ka võimaliku suure mõju tõttu.

- **Väär- ja eksiteave**
  Väär- ja eksiteabe levitamise kampaaniad sagenevad, sest ühismeediaplatvorme ja veebimeediat kasutatakse üha rohkem, samuti seepärast, et inimeste veebikohalolek on COVID-19 pandeemia tõttu üha suurem. Kuigi seda ohurühma mainitakse siinses ENISA ohtude kaardistamise aruandes esimest korda, on see kübermaailmas väga oluline. Väär- ja eksiteabe levitamise kampaaniaid kasutatakse sageli hübriidrünnetes, et vähendada usalduse kui küberturbe kui ühe põhikomponendi üldist tajumist.

- **Mittekuritahtlikud ohud**
  Ohtudeks loetakse üldiselt ohusubjektide vabatahtlikke ja kuritahtlikke tegevusi, millel on teatud stiimuleid rünnata konkreetset sihtmärki. See kategooria hõlmab ohte, kus kuritahtlik kavatsus ei ole ilmne. Need ohud on peamiselt tingitud inimlikest vigadest ja süsteemi konfiguratsioonivigadest, kuid need võivad hõlmata ka füüsilisi katastroofe, mis on suunatud IT-taristu vastu. Ka olemuse tõttu on need ohud ohtude kaardistamise aastaaruandes pidevalt olemas ja riskihinnangutes olulisel kohal.

Joonis 1. ENISA ohtude kaardistamise 2021. aasta aruanne – peamised ohud

Tuleb märkida, et eespool nimetatud ohud hõlmavad kategooriaid ja ohukogumeid, mis on koondatud kaheksasse eespool mainitud valdkonda. Iga ohurühma analüüsitakse põhjalikumalt käesoleva aruande vastavas peatükis, milles käsitletakse ohurühma eripära ning esitatakse täpsem teave, tähelepanekud, suundumused, ründemeetodid ja leevendusvektorid.

1.2. PEAMISED SUUNDUMUSED

Alljärgnevas loetelus on kokkuvõte aruandeperioodil küberohtude spektris täheldatud peamised suundumused. Neid analüüsitakse üksikasjalikult ka ENISA ohtude kaardistamise 2021. aasta aruande eri peatükkides.

- Vastavasisulises ENISA tarneahelarünnetega seotud ohtude kaardistamise aruandes rõhutatakse **tarneahelate väga keerukate ja mõjusate turberikkumiste** suurt sagedust. **Hallatud teenuste osutajad** on küberkurjategijate jaoks väärtuslikud sihtmärgid.
- **COVID-19 pandeemia ajendas küberspionaaži** ja tekitas **küberkurjategijatele võimalusi**.
- **Valitsusorganisatsioonid on suurendanud tegevust** nii riigi kui ka rahvusvahelisel tasandil. Valitsusasutused teevad senisest rohkem riiklike ohujõudude tegevuse katkestamiseks ja nende vastu õiguslike meetmete võtmiseks.
- **Küberkurjategijaid motiveerib üha enam** oma tegevuse **rahaks muutmine**, näiteks lunavaraga. **Krüptovaluuta** on endiselt kõige tavalisem ohusubjektide kasutatav väljamaksemeetod.
- Küberkuritegevuse ründed **on üha enam suunatud elutähtsa taristu vastu ja avaldavad neile suuremat mõju**.
- **Ohustamine e-posti kaudu toimuva andmepüügiga ning kaugtöölauateenuste jõurünne** on jätkuvalt kaks kõige tavalisemat **lunavara nakkusvektorit**.
- Keskendumine **lunavara kui teenuse tüüpi ärimudelitele** on 2021. aasta jooksul suurenenud, mis raskendab ohusubjektide individuaalset tuvastamist.

- **Kolmekordse väljapressimise lunavara** skeemide esinemissagedus on 2021. aasta jooksul jõudsalt kasvanud.
- 2020. aastal täheldatud **kahjurvara kasutamise vähenemine** jätkub 2021. aastal. 2021. aastal täheldasime nende ohusubjektide arvu suurenemist, kes kasutasid oma koodi portimiseks võrdlemisi uusi või tundmatuid programmeerimiskeeli.
- Sagenenud on **konteinerkeskkondadele suunatud kahjurvara** kasutamine, kus kasutatakse selliseid uudseid täiustusi nagu mälu kaudu käivitatav failideta kahjurvara.
- Kahjurvara arendajad leiavad pidevalt võimalusi, kuidas **raskendada pöördprojekteerimist ja dünaamilist analüüsi**.
- Võrreldes eelmiste aastatega oli **kaevekaaperdusrünnete** arv 2021. aasta esimesel veerandil **rekordiliselt suur**. Ohusubjekte innustas neid ründeid sooritama kaevekaaperdusega kaasnev **rahaline kasu**.
- **Krüptorahakaeve ja kaevekaaperdustegevuse maht on 2021. aastal rekordiliselt suur**.
- Märgatav on **üleminek brauseripõhiselt kaevekaaperduselt failipõhisele**.
- **COVID-19 on seniajani valdav peibutusvahend** e-posti rünnete kampaaniates.
- **Meilipetted** on **sagenenud** ning muutunud **keerukamaks** ja **suunatumaks**.
- **Teenusena toimuva andmepüügi** ärimudel on üha sagedam.
- Ohusubjektid pöörasid andmete ja teabe ohustamisega seoses oma tähelepanu **vaktsiiniteabele**.
- Esines **tervishoiuandmetega seotud rikkumiste järsk kasv**.
- Tavapärased hajusad ummistusründed liiguvad **mobiilsidevõrkudesse ja esemevõrku**.
- **Lunarahanõudega ummistusrünne** on ummistusrünnete seas uus nähtus.
- **Ressursside jagamine virtuaalkeskkonnas** võimendab hajusaid ummistusründeid.
- **Hajusate ummistusrünnete kampaaniad** on 2021. aastal suunatumad, palju püsivamad ja üha enamate vektoritega.
- **Tehisintellektivõimeline väärteave** toetab ründajaid rünnete sooritamisel.
- **Väärteaberünnete keskmes on andmepüük**, mille kaudu kuritarvitatakse jõuliselt inimeste uskumusi.
- **Väär- ja eksiteave** on küberkuritegevuse keskmes ning kasvab enneolematu kiirusega.
- **Väärteabe kui teenuse ärimudel** on oluliselt kasvanud, mida soodustab COVID-19 pandeemia üha suurenev mõju ja vajadus saada rohkem teavet.
- 2020. ja 2021. aastal täheldasime **mittekuritahtlike intsidentide arvu järsku suurenemist**, sest COVID-19 pandeemia tõttu mitmekordistus **inimlike vigade** ja **süsteemi konfiguratsioonivigade arv** kuni selleni, et 2020. aastal oli enamik andmerikkumisi tingitud vigadest.
- **Pilveturbega seotud mittekuritahtlike intsidentide arv on järsult kasvanud**.

1.3. PEAMISTE OHTUDE LÄHEDUS ELILE

ENISA ohtude kaardistamise aruande kontekstis on oluline kaalutleda küberohtude lähedust Euroopa Liidule (EL). See on eriti tähtis, et aidata analüütikutel hinnata küberohtude olulisust, seostada neid võimalike ohusubjektide ja vektoritega ning isegi aidata valida asjakohaseid suunatud leevendusvektoreid. Vastavalt ELi ühise julgeoleku- ja kaitsepoliitika jaoks kavandatud klassifikatsioonile[7] klassifitseerime küberohud nelja kategooriasse (**Tabel 1**).

Tabel 1. Küberohtude läheduse klassifikatsioon

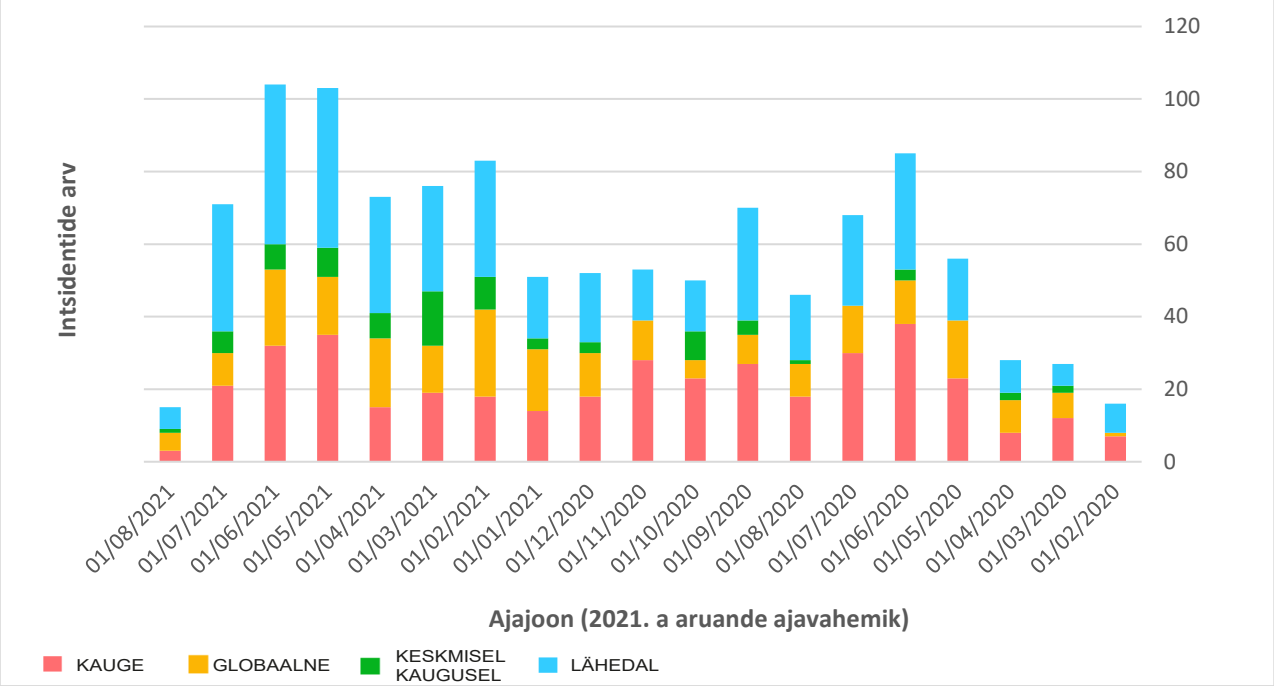
Lähedus	Probleemid
Lähedal	Mõjutab võrke, süsteeme ELis, juhitakse ja tagatakse EList. Mõjutab elanikke ELi piires.
Keskmisel kaugusel	Võrgud ja süsteemid, mida peetakse elutähtsaks tegevuseesmärkide saavutamiseks ELi digitaalsel ühtsel turul ning küberturvalisuse direktiivi kohaldamisala valdkondades, kuid mille juhtimine ja tagamine sõltub ELi-välistest institutsioonilistest asutustest või liikmesriikide avaliku või erasektori asutustest. Mõjutab elanikke geograafilistes piirkondades ELi piiri lähedal.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Lähedus	Probleemid
Kaugel	Võrgud ja süsteemid, millel on sekkumise korral määrav mõju tegevuseesmärkide saavutamisele ELi digitaalsel ühtsel turul ning küberturvalisuse direktiivi kohaldamisala valdkondades. Nende võrkude ja süsteemide juhtimine ja tagamine toimub kaugemalt kui ELi institutsioonilistest asutustest või liikmesriikide avaliku või erasektori asutustest. Mõjutab elanikke geograafilistes piirkondades EList kaugel.
Globaalne	Kõik eespool nimetatud piirkonnad

Joonis 2 kujutab ENISA ohtude kaardistamise 2021. aasta aruandes esitatud peamiste ohukategooriatega seotud intsidentide ajajoont. Juhime tähelepanu, et joonise teave põhineb avalikest allikatest pärit luureandmetel allikast ja see on ohuteadlikkuse valdkonnas[8] tehtud ENISA töö tulemus.

Joonis 2. ENISA ohtude kaardistamise aruandes esitatud peamiste ohtudega seotud intsidentide ajajoon (avalikust allikast saadud luureandmetel põhinev ohuteadlikkus), arvestades nende lähedust.



Eelmiselt jooniselt nähtub, et 2021. aasta intsidentide arv on suurem kui 2020. aastal. Peamiste ohtudega seotud intsidentide arvu kasvu võib täheldada eelkõige kategoorias „lähedal“, mis näitab nende olulisust ELi kontekstis. Ei ole üllatav, et igakuised suundumused (mida joonisel kokkuvõtlikkuse huvides ei ole) on eri kategooriates üsna sarnased, sest küberturvalisus ei tunne piire ja ohud materialiseeruvad enamasti kõigil lähedustasanditel. Tuleb märkida, et viimastel ENISA ohtude kaardistamise 2021. aasta aruandega hõlmatud kuudel võib ELi läheduse tasandil „lähedal“ täheldada suuremat intsidentide arvu. ENISA jätkab selle suundumuse jälgimist, et näha, kuidas olukord areneb ja kuidas see seostub ohusubjektide tegevustega ning praeguste ohuvektoritega.

1.4. PEAMISED OHUD VALDKONDADE JÄRGI

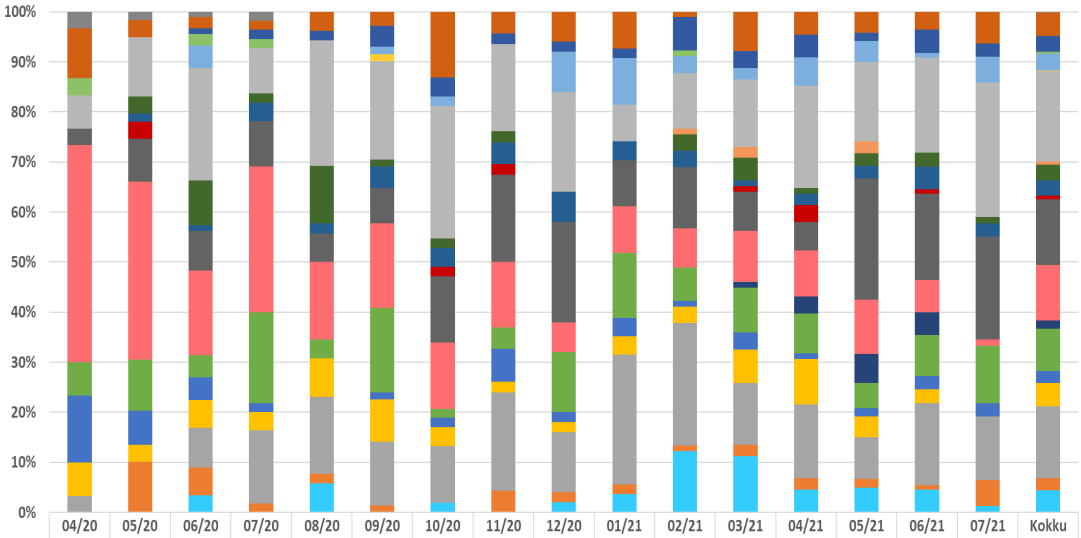
Küberohud ei piirdu tavaliselt ühe konkreetse valdkonnaga ja enamasti mõjutavad mitut. Põhjus on, et sageli seisnevad ohud valdkonna IKT-alussüsteemide haavatavuste ärakasutamises. Samas tuleb arvestada ka selliseid

[8] Vastavalt ELi küberturvalisust käsitleva õigusakti artikli 7 lõikele 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

tegureid nagu suunatud ründed ja ründed, mis kasutavad ära küberturbeküpsuse erinevusi eri valdkondades ja teatud valdkondade populaarsust/olulisust. Need asjaolud aitavad kaasa konkreetsetes valdkondade intsidentidele, mistõttu tuleb hoolikalt analüüsida täheldatud intsidentide ja ohtude valdkonnapõhiseid asjaolusid. Sellisest analüüsist nähtuvad näiteks suundumused igas valdkonnas ja valdkonnaülene sõltuvus.

Joonistel 3 ja 4 on mõjutatud valdkonnad, mis on seotud intsidentidega, mida täheldati avalikust allikast pärit luureandmete alusel ja on ENISA poolt ohuteadlikkuse valdkonnas[9] tehtud töö tulemus. Joonised kujutavad intsidente, mis on seotud ENISA ohtude kaardistamise 2021. aasta aruandes esitatud peamiste ohtudega. See on ENISA esimene katse kaardistada ohtude mõju konkreetsetele valdkondadele. Lähiaastatel ja edaspidi ajakohastatavates ENISA ohtude kaardistamise aruannetes püütakse kooskõlastada valdkonnad küberturvalisuse direktiivis ja selle läbivaatamise ettepanekus (küberturvalisuse direktiiv 2.0) loetletud valdkondadega.

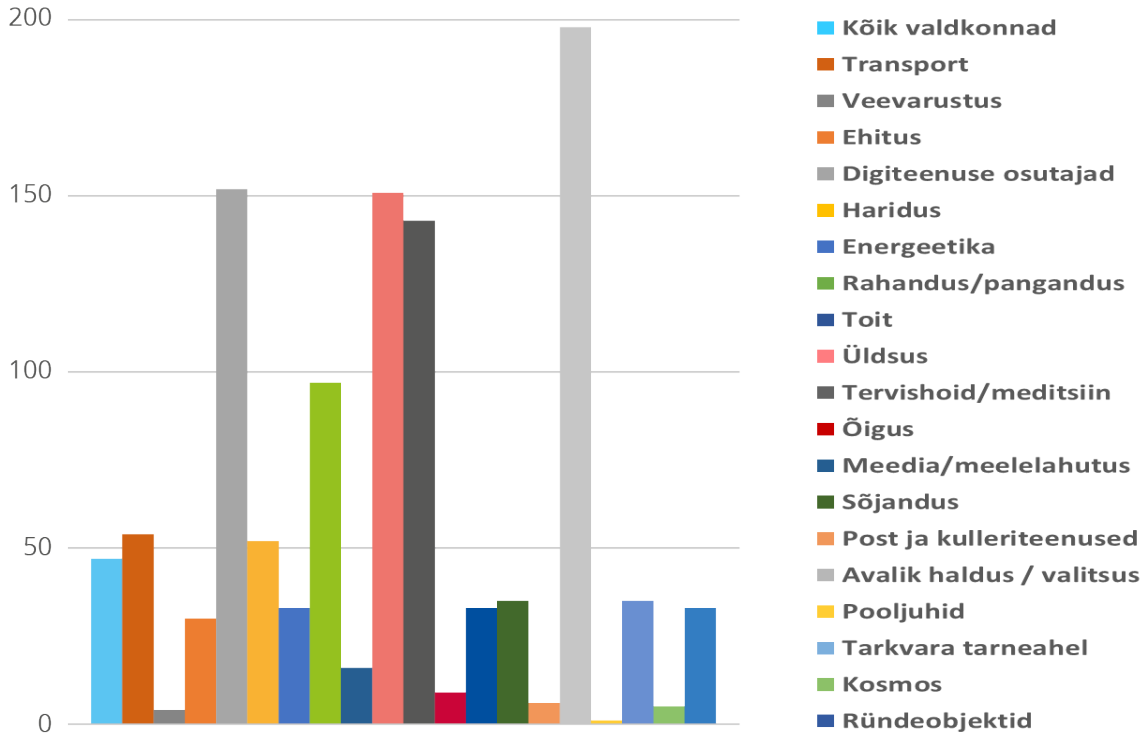
Joonis 3. ENISA ohtude kaardistamise 2021. aasta aruandes esitatud peamiste ohtudega seotud intsidentide ajajoon mõjutatud valdkonna kaupa.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	Kokku
Veevarustus	1	1	1	1													2
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Ründeobjektid			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Kosmos	1		2	1							1						4
Tarkvara tarneahel			4			1	1		4	5	3	2	5	5	1	4	35
Pooljuhid						1											1
Avalik haldus / valitsus	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Post ja kulleriteenused											1	2		3			6
Sõjandus		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Meedia/meelelahutus		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Õigus		2					1	1				1	3		1		7
Tervishoid/meditsiin	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Üldsus	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Toit												1	3	7	5		16
Rahandus/pangandus	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energeetika	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Haridus	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digiteenuse osutajad	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Ehitus		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Kõik valdkonnad			3		3		1		1	2	11	10	4	6	5	1	47

[9] Vastavalt ELi küberturvalisust käsitleva õigusakti artikli 7 lõikele 6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Joonis 4. Sihtsektorid intsidentide arvu järgi (aprill 2020 – juuli 2021)



Sellel aruandeperioodil oli palju intsidente suunatud avaliku halduse ja valitsuse ning digiteenuse osutajate vastu. Viimane on ootuspärane, arvestades teenuste horisontaalset pakkumist valdkonnas ja seega selle mõju paljudele muudele valdkondadele. Ühtlasi täheldasime suurt arvu intsidente, mis ei olnud suunatud konkreetse valdkonna, vaid pigem lõppkasutajate vastu. Ka tervishoiuvaldkonna vastu suunatud intsidente oli oluliselt palju ja see tegevus sageneb aruandeperioodi viimastel kuudel (mai–juuli 2021). Huvitav on tõdeda, et intsidentide arv rahandussektoris on aasta lõikes ühetaoline. Ka tarkvara tarneahelas võib 2021. aastal täheldada intsidentide arvu suurenemist. Sama tähelepanek on ka ENISA tarneahelarünnetega seotud ohtude kaardistamise aruandes[10].

1.5. METOODIKA

ENISA ohtude kaardistamise 2021. aasta aruande aluseks on avalikest allikatest pärit teave (peamiselt strateegilise olemusega) ja ENISA enda küberohuteadmuse allikad ning see hõlmab mitut valdkonda, tehnoloogiat ja konteksti. Aruanne püüab olla tööstusest ja müüjatest sõltumatu ning selle tekstis on läbivalt mitmes allmärkuses viidatud eri julgeolekuteadlaste uuringutele, julgeolekublogidele ja ajakirjandusartiklitele. ENISA ohtude kaardistamise 2021. aasta aruanne hõlmab ajavahemikku 2020. aasta aprillist kuni 2021. aasta juulini, mida nimetatakse aruandes aruandeperioodiks.

ENISA ohtude kaardistamise 2021. aasta aruande koostamisel kasutati järgmist käsitlusviisi. ENISA koostas vaatlusaluse perioodi vältel olukorrast ülevaate saamiseks oluliste intsidentide loetelu vastavalt nende kajastamisele avalikes allikates. Sellest loetelust lähtuti peamiste ohtude loetelu koostamisel ning seda kasutati ka aruandes kirjeldatud suundumuste ja statistika allikmaterjalina.

Seejärel analüüsisid ENISA ja väliseksperdid põhjalikult avalikest allikatest kättesaadavat kirjandust, näiteks ajakirjandusartikleid, eksperdiarvamusi, luurearuandeid, intsidendianalüüse ning julgeoleku-uuringute aruandeid. ENISA tuletas pideva analüüsimise abil oma ohtude kaardistamise 2021. aasta aruandes esitatud iga peamise

[10] ENISA tarneahelarünnetega seotud ohtude kaardistamise aruanne, juuli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ohuga seotud suundumused ja huvipunktid. Siin hinnangus esitatud põhilised tähelepanekud ja otsused on tehtud mitme avalikult kättesaadava allika põhjal, mis on lisatud käesoleva dokumendi koostamise allikaviidetele.

Püüame aruandes eristada allikatest pärit teavet ja meie hinnanguid. (Selleks kasutame aruandes väljendit „meie hinnangul“.) Hindamisel kasutamine tõenäosuse väljendamiseks sõnastust, mis väljendab hinnangulist tõenäosust (nt tõenäoliselt, väga tõenäoliselt, kindlasti)[11].

MITRE ATT&CK® raamistikku[12] kasutati käesolevas aruandes ohu jaoks kasutatavate ründetaktikate ja -meetodite esiletõstmiseks (vt A lisa). Iga ATT&CK®-taktika korral on esitatud tegijate kasutatud meetodid. See võib viia rakendatavate ATT&CK-leevendusmeetmete[13] loeteluni. MITRE ATT&CK® on teadmusbaas, tegelikel tähelepanekutel tuginevate võistlevate taktikate ja meetodite korral kasutatav ühine keel. Teadmusbaasi MITRE ATT&CK® kasutatakse erasektoris, valitsuses ning küberturvalisuse toodete ja teenuste kogukonnas konkreetsete ohumudelite ning meetodite väljatöötamiseks.

Aruande kinnitas 2021. aasta aprillis moodustatud ENISA küberohtude kaardistamise ajutine töörühm,[14] mis koosneb Euroopa ja rahvusvaheliste avaliku ja erasektori asutuste ekspertidest.

ENISA arendab ohtude kaardistamise aruannete koostamise uut metoodikat, et edendada läbipaistvust ning võimaldada liigendatud ja hästi kooskõlas protsesse. Selle saavutamiseks on kavas tulevikus avalikustada ohtude kaardistamise metoodika koos läbivaadatud ohutaksonoomiaga.

1.6. ARUANDE ÜLESEHITUS

ENISA ohtude kaardistamise 2021. aasta aruandes kasutatakse sama ülesehitust kui varasemates, kasutades 2021. aasta peamiste küberohtude rõhutamiseks sarnast ülesehitust. Varasemate väljaannete lugejad märkavad, et ohukategooriate koondamisel on lähtutud sellest, et tulevikus on kavas võtta kasutusele uus küberturbeohtude taksonoomia.

Käesoleva aruande ülesehitus on järgmine.

2. peatükis uuritakse suundumusi, mis on seotud ohusubjektidega (st riigijõud, küberkurjategijad, palgatud häkkerid ja häktivistid).
3. peatükis käsitletakse lunavaraga seotud peamisi tähelepanekuid, intsidente ja suundumusi.
4. peatükis käsitletakse kahjurvaraga seotud peamisi tähelepanekuid, intsidente ja suundumusi.
5. peatükis käsitletakse kaevekaaperdusega seotud peamisi tähelepanekuid, intsidente ja suundumusi.
6. peatükis käsitletakse e-postiga seotud ohtudega seotud peamisi tähelepanekuid, intsidente ja suundumusi.
7. peatükis käsitletakse andmeohtudega seotud peamisi tähelepanekuid, intsidente ja suundumusi.
8. peatükis käsitletakse kättesaadavuse ja tervikluse vastaste ohtudega seotud peamisi tähelepanekuid, intsidente ning suundumusi.
9. peatükis rõhutatakse hübriidohtude tähtsust ja kirjeldatakse väär- ja eksiteabega seotud peamisi tähelepanekuid, intsidente ja suundumusi.
10. peatükis käsitletakse mittekuritahtlike ohtudega seotud peamisi tähelepanekuid, intsidente ja suundumusi.
A lisas esitatakse iga ohu kohta tavalised meetodid vastavalt MITRE ATT&CK®-raamistikule.
B lisa hõlmab iga ohu kohta aruandeperioodil esinenud märkimisväärseid intsidente.

[11] CIA – Hinnangulise tõenäosuse väljendamise sõnad https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK® , https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes