EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2021 M. ENISA GRĖSMIŲ APLINKA

2020 m. balandžio mėn.–2021 m. liepos mėn. vidurys

2021 M. SPALIO MĖN.

APIE ENISA

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) yra Sąjungos agentūra, kurios tikslas – siekti aukšto bendro kibernetinio saugumo lygio visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įkurta 2004 m. ir sustiprinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų, kuriuose naudojamos kibernetinio saugumo sertifikavimo schemos, patikimumą, bendradarbiauja su valstybėmis narėmis ir ES įstaigomis ir padeda Europai pasirengti būsimiems kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra dirba kartu su savo pagrindiniais suinteresuotaisiais subjektais, siekdama stiprinti pasitikėjimą susietąja ekonomika, didinti Sąjungos infrastruktūros atsparumą, užtikrinti Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos apie ENISA ir jos darbą galima rasti čia: www.enisa.europa.eu.

KONTAKTINIAI DUOMENYS
Su dokumento rengėjais galima susisiekti adresu etl@enisa.europa.eu.
Žiniasklaidos atstovų užklausas dėl šio dokumento galima teikti adresu press@enisa.europa.eu.

REDAKTORIAI
Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras – Europos Sąjungos kibernetinio saugumo agentūra

DUOMENŲ TEIKĖJAI
Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

PADĖKA
Norėtume padėkoti ENISA *ad hoc* darbo grupės kibernetinių grėsmių aplinkos klausimais nariams ir stebėtojams už jų vertingą grįžtamąją informaciją bei pastabas tvirtinant šią ataskaitą. Taip pat norėtume padėkoti ENISA patariamajai grupei ir nacionalinių ryšių palaikymo pareigūnų tinklui už jų vertingą grįžtamąją informaciją.
Taip pat norėtume padėkoti ENISA informuotumo apie padėtį ir pranešimo apie incidentus grupėms už jų aktyvų indėlį ir paramą apibendrinant įvairią informaciją ir rengiant grėsmių aplinkos ataskaitą.

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

TURINYS

SANTRAUKA

Tai devintoji ENISA grėsmių aplinkos (angl. *ENISA Threat Landscape*, ETL) ataskaita, t. y. metinė ataskaita apie kibernetinių grėsmių aplinką, kurioje įvardijamos pagrindinės grėsmės, svarbiausios pastebėtos tendencijos, susijusios su grėsmėmis, grėsmės subjektai ir išpuolių metodai, taip pat aprašomos atitinkamos rizikos mažinimo priemonės. Grėsmių aplinkos ataskaitų rengimo metodika nuolat tobulinama ir šiais metais ataskaitą padėjo parengti naujai sudaryta ENISA *ad hoc* darbo grupė kibernetinių grėsmių aplinkos klausimais.

2021 m. ETL ataskaita apima 2020 m. balandžio mėn.–2021 m. liepos mėn. – tai ataskaitoje aptariamas ataskaitinis laikotarpis. Ataskaitiniu laikotarpiu nustatytos šios pagrindinės grėsmės:

- **Išpirkos reikalavimo programinė įranga**
- **Kenkimo programinė įranga**
- **Išnaudojamoji kriptovaliutos gavyba**
- **Su e. laiškais susijusios grėsmės**
- **Grėsmės duomenims**
- **Grėsmės prieinamumui ir vientisumui**
- **Dezinformacija ir klaidinga informacija**
- **Nekenkėjiško pobūdžio grėsmės**
- **Išpuoliai prieš tiekimo grandinę**

Šioje ataskaitoje aptariame pirmąsias 8 kibernetinių grėsmių kategorijas. 9-oji kategorija „grėsmės tiekimo grandinei“ dėl jos ypatingos svarbos buvo išsamiai išanalizuota specialioje ENISA ataskaitoje „ENISA išpuolių prieš tiekimo grandinę grėsmių aplinka“ [1].

Dėl kiekvienos nustatytos grėsmės kategorijos aptariami išpuolių metodai, žinomi incidentai ir tendencijos, įskaitant pasiūlytas rizikos mažinimo priemones. Ataskaitiniu laikotarpiu nustatėme toliau išvardytas tendencijas.

- **Išpirkos reikalavimo programinė įranga** įvertinta kaip **pagrindinė grėsmė 2020–2021 m.**
- **Vyriausybinės organizacijos ėmėsi veiksmų** nacionaliniu ir tarptautiniu lygmenimis.
- **Kibernetinių nusikaltėlių motyvu vis dažniau tampa** jų veiklos **monetizacija,** pvz., išpirkos reikalavimo programinė įranga. **Kriptovaliutos** išlieka pagrindine išmokos grėsmės subjektams išmokėjimo priemone.
- 2020 m. pastebėta **mažėjanti kenkimo programinės įrangos** naudojimo tendencija išliko nepakitusi 2021 m. 2021 m. pastebėjome, kad grėsmės subjektai naudoja santykinai naujas arba neįprastas programavimo kalbas, kad perkeltų savo kodą.
- 2021 m. pirmąjį ketvirtį **išnaudojamosios kriptovaliutos gavybos užkratų skaičius** buvo **kaip niekad didelis**, palyginti su pastaraisiais metais. **Finansinė nauda**, susijusi su išnaudojamąja kriptovaliutos gavyba, tapo paskata grėsmės subjektams vykdyti šiuos išpuolius.
- **COVID-19 vis dar yra pagrindinė pagunda rengti** išpuolių per e. paštą **kampanijas**.
- **Sveikatos priežiūros sektoriuje taip pat padaugėjo duomenų saugumo pažeidimų**.
- **Tradicinės DDoS (paskirstytojo paslaugos trikdymo) atakos** 2021 m. tapo tikslingesnės, pastovesnės ir vis labiau įvairialypės. **IoT (daiktų internetas)** kartu su **mobiliojo ryšio tinklais** prisideda prie naujos DDoS atakų bangos.
- 2020 ir 2021 m. pastebime **nekenkėjiško pobūdžio incidentų skaičiaus augimą**, nes COVID-19 pandemija tapo daugybės **žmogaus klaidų** ir **netinkamo sistemų konfigūravimo** priežastimi ir galiausiai 2020 m. dauguma pažeidimų buvo padaryti dėl klaidų.

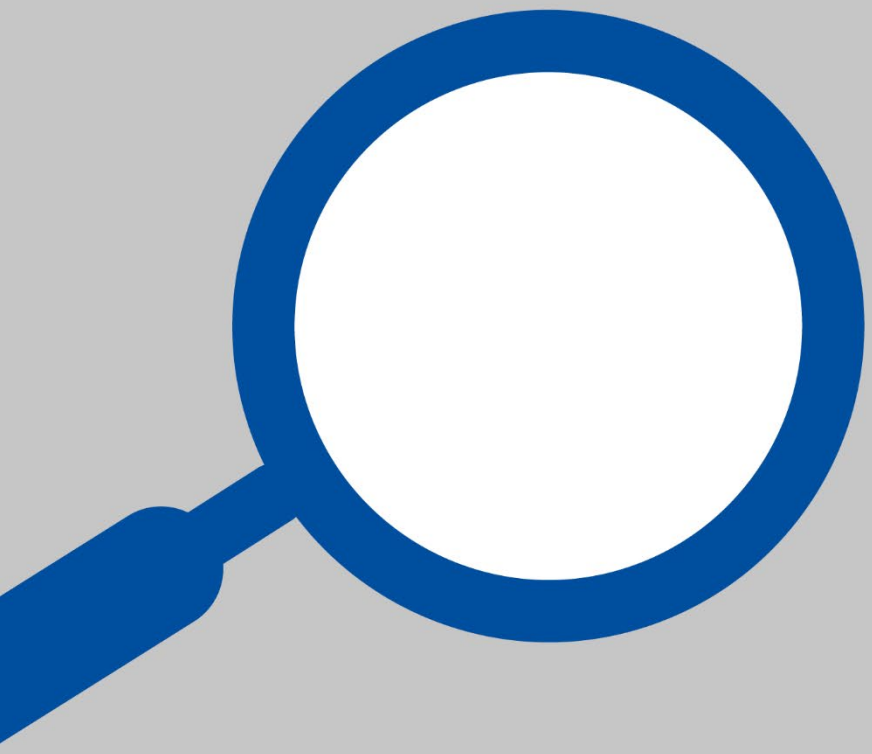
Su grėsmės subjektais, jų motyvais ir taikiniais susijusių tendencijų supratimas iš esmės padeda planuoti kibernetinio saugumo gynybos priemones ir rizikos mažinimo strategijas. Tai yra sudedamoji mūsų bendro grėsmių vertinimo dalis, nes taip sudaromos sąlygos nustatyti prioritetines saugumo kontrolės priemones ir, remiantis

[1] ENISA išpuolių prieš tiekimo grandinę grėsmių aplinka, 2021 m. liepos mėn. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

galimu grėsmių pasireiškimo poveikiu ir tikimybe, parengti specialią strategiją. Atsižvelgiant į tai ir rengiant 2021 m. ETL ataskaitą, išnagrinėtos šios keturios kibernetinių grėsmių subjektų kategorijos:

- **Valstybės remiami subjektai**
- **Kibernetinių nusikaltimų subjektai**
- **Samdomi įsilaužėliai**
- **Įsilaužėliai aktyvistai**

Atlikdama nuolatinę analizę, ENISA nustatė kiekvienos 2021 m. ETL pateiktos pagrindinės grėsmės tendencijas ir nagrinėtinus aspektus. Pagrindinės išvados ir sprendimai, pateikti šiame vertinime, pagrįsti įvairiais ir viešai prieinamais ištekliais, kurie pateikiami literatūros, naudotos rengiant šį dokumentą, sąraše. Ataskaita iš esmės skirta strateginių sprendimų priėmėjams ir strateginės politikos formuotojams, tačiau ji taip pat bus naudinga techninei kibernetinio saugumo bendruomenei.



GRĖSMIŲ APLINKOS APŽVALGA

Devintojoje ENISA grėsmių aplinkos (ETL) ataskaitoje pateikiama bendra kibernetinių grėsmių aplinkos apžvalga. ETL ataskaitą sudaro strateginė ir techninė dalys, įskaitant techninių žinių turintiems ir neturintiems skaitytojams svarbią informaciją. Šiais metais darbą padėjo atlikti nauja ENISA *ad hoc* darbo grupė grėsmių kibernetiniam saugumui aplinkos klausimais[2].

2020 ir 2021 m. didėjo ne tik kibernetinio saugumo išpuolių vektorių ir išpuolių skaičius, bet ir jų poveikis. Kaip ir tikėtasi, COVID-19 pandemija taip pat turėjo poveikį kibernetinių grėsmių aplinkai. Viena iš pastovesnių tendencijų, kurią sukėlė COVID-19 pandemija, yra ilgalaikis perėjimas prie mišraus darbo biure. Todėl kibernetinės grėsmės, susijusios su pandemija, ir „naujos kasdienybės“ išnaudojimas tampa įprastu reiškiniu. Dėl šios priežasties padaugėjo galimybių rengti išpuolius, todėl pastebime, kad vis daugiau kibernetinių išpuolių į organizacijas ir įmones nukreipiama pasinaudojant nuotoliniu darbu namuose[3].

Apskritai kibernetinių grėsmių daugėja. Vis daugiau veiklos vykdoma internete, tradicinė infrastruktūra perkeliama į internetą ir debesija grindžiamas priemones, vis didesnis junglumas ir vis plačiau naudojamos naujos technologijos, pvz., dirbtinis intelektas (DI)[4][5], todėl kibernetinio saugumo aplinka išsiplėtė – išpuoliai tapo sudėtingesni, painesni, jų poveikis didesnis. Visų pirma grėsmė tiekimo grandinėms ir jų reikšmė dėl galimo katastrofiško grandininio poveikio tapo viena svarbiausių didžiausių grėsmių, tokia svarbi, kad ENISA parengė specialią šios grėsmės aplinkos apžvalgą[6].

Verta pažymėti, kad šioje ENISA grėsmių aplinkos ataskaitoje ypatingas dėmesys skiriamas kibernetinių grėsmių poveikiui įvairiuose sektoriuose, įskaitant Tinklų ir informacinių sistemų saugumo direktyvoje (TISD) išvardytus sektorius. Atsižvelgiant į kiekvieno sektoriaus ypatumus, galima padaryti įdomią įžvalgą, kai kalbama apie grėsmių aplinką, taip pat potencialią tarpusavio priklausomybę ir reikšmingas sritis. Atitinkamai sektorinių grėsmių aplinkai reikia skirti daugiau dėmesio.

Šiais metais kibernetinės bendruomenės gynėjai, kaip ir politikos formuotojai, taip pat ėmėsi svarbių veiksmų. Pasaulio bendruomenė pradėjo suprasti komunikacijos ir bendradarbiavimo svarbą išaiškinant ir atsekant kibernetinius nusikaltėlius, naudojančius išpirkos reikalavimo programinę įrangą (didžiausia grėsmė 2021 m. ETL ataskaitiniu laikotarpiu), visų pirma tai tapo pagrindiniu pasaulio lyderių strateginių susitikimų darbotvarkių klausimu.

Ankstesnių 2021 m. ETL versijų skaitytojai pastebės, kad pagrindinių grėsmių struktūra yra kitokia. Šiais metais ENISA žengė žingsnį atgal ir apibendrino grėsmių kategorijas siekdama sugrupuoti panašias grėsmes ir užtikrinti geresnį jų reprezentatyvumą. Tai dalis nuolatinių pastangų peržiūrėti grėsmių taksonomiją. Tai padės metodiškai nustatyti artimiausių kelerių metų tendencijas.

2021 m. ETL yra pagrįsta įvairia atvirųjų šaltinių informacija ir kibernetinių grėsmių žvalgybos šaltiniais. Joje nustatytos pagrindinės grėsmės, tendencijos ir išvados, ir pateikiama atitinkama aukšto lygio rizikos mažinimo strategija. ENISA dabar dirba siekdama sukurti patikimesnę pranešimo apie grėsmių aplinką metodiką ir taip skatinti skaidrų ir nuoseklų darbą.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – 2020 m. išlaidų dėl duomenų pažeidimų ataskaita - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA „Dirbtinio intelekto grėsmių aplinka“: 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 išpuolių prieš tiekimo grandinę grėsmių aplinka, 2021 m. liepos mėn. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. PAGRINDINĖS GRĖSMĖS

2020 ir 2021 m. atsirado ir pasireiškė įvairių naujų kibernetinių grėsmių. Remiantis šioje ataskaitoje pateikta analize, 2021 m. ENISA grėsmių aplinkos apžvalgoje nustatytos šios 8 pagrindinės grėsmių grupės, kurioms ir skiriama daugiausia dėmesio (žr.Figure 1). Šios 8 grėsmių grupės išskiriamos dėl jų reikšmės ataskaitiniu laikotarpiu, populiarumo ir poveikio, kuris buvo padarytas pasireiškus šioms grėsmėms.

- **Išpirkos reikalavimo programinė įranga**
  Išpirkos reikalavimo programinė įranga – tai kenkėjiško išpuolio rūšis, kai išpuolio rengėjai užšifruoja organizacijos duomenis ir už atkurtą prieigą reikalauja atlygio. Išpirkos reikalavimo programinė įranga yra pagrindinė grėsmė ataskaitiniu laikotarpiu, įskaitant keletą ypač žinomų ir plačiai pagarsėjusių incidentų. Išpirkos reikalavimo programinės įrangos keliamos grėsmės reikšmę ir poveikį taip pat patvirtina įvairios Europos Sąjungoje (ES) ir visame pasaulyje įgyvendinamos susijusios politinės iniciatyvos.

- **Kenkimo programinė įranga**
  Kenkimo programinė įranga – tai programinė arba programinė aparatinė įranga, skirta neteisėtiems procesams atlikti, kurie turi neigiamą poveikį sistemos konfidencialumui, vientisumui arba prieinamumui. Daugybę metų kenkimo programinės įrangos grėsmė buvo labai didelė, nors 2021 m. ENISA grėsmių aplinkos ataskaitiniu laikotarpiu šios grėsmės rodiklis mažėjo. Naujų išpuolių metodų naudojimas ir kai kurios svarbios teisėsaugos bendruomenės pergalės turėjo įtakos atitinkamų grėsmės subjektų operacijoms.

- **Išnaudojamoji kriptovaliutos gavyba**
  Išnaudojamoji kriptovaliutos gavyba – tai kibernetinis nusikaltimas, kurį darydamas nusikaltėlis slapta naudoja aukos kompiuterio galią kriptovaliutos gavybai. Plintant kriptovaliutoms ir atsižvelgiant į vis dažnesnį jų naudojimą platesnėje visuomenės dalyje, pastebėta, kad daugėja atitinkamų kibernetinio saugumo incidentų.

- **Su e. laiškais susijusios grėsmės**
  Su e. laiškais susiję išpuoliai – tai pačios įvairiausios grėsmės, susijusios veikiau su žmogaus psichologinėmis ir kasdienių įpročių silpnybėmis, o ne techniniais informacinių sistemų pažeidžiamumo aspektais. Įdomu tai, kad, nepaisant daugybės informuotumo didinimo ir švietimo kampanijų apie šios rūšies išpuolius, grėsmė išlieka labai aktuali. Paminėtina, kad vis dažniau įsilaužiama į verslo e. laiškus ir naudojami pažangūs sudėtingi metodai piniginei vertei išgauti.

- **Grėsmės duomenims**
  Ši kategorija apima duomenų saugumo pažeidimus / duomenų nutekinimą. Duomenų saugumo pažeidimas arba duomenų nutekinimas – tai neskelbtinų, konfidencialių arba saugomų duomenų atskleidimas nepatikimoje aplinkoje. Duomenų saugumo pažeidimai gali būti padaromi dėl kibernetinio išpuolio, darbuotojo, kuris naudojasi viešai neatskleista informacija, netyčinio duomenų praradimo arba atskleidimo. Grėsmė išlieka didelė, nes prieiga prie duomenų yra pagrindinis išpuolio rengėjų tikslas dėl įvairių priežasčių, pvz., turto prievartavimo, išpirkos, šmeižto, klaidingos informacijos ir pan.

- **Grėsmės prieinamumui ir vientisumui**
  Prieinamumas ir vientisumas yra pačių įvairiausių grėsmių ir išpuolių tikslas, tarp kurių išsiskiria paskirstytojo paslaugos trikdymo (DoS) ir internetinių išpuolių grupė. DDoS išpuoliai vykdomi išimtinai internete ir yra pagrindinės grėsmės IT sistemoms, siekiant apriboti jų prieinamumą išnaudojant visus jų pajėgumus, taip sukeliant veikimo sutrikimus, duomenų praradimą ir paslaugų teikimo nutraukimą. Grėsmė ENISA grėsmių aplinkos ataskaitoje nuolat vertinama kaip aukšta dėl jos apraiškų faktiniuose incidentuose ir galimo didelio poveikio.

- **Dezinformacija ir klaidinga informacija**
  Vis daugiau rengiama dezinformacijos ir klaidingos informacijos kampanijų, kurias paskatino dažniau naudojamos socialinių tinklų platformos ir internetinė žiniasklaida, taip pat intensyvesnis žmonių naudojimasis internetu per COVID-19 pandemiją. Ši grėsmių grupė pirmą kartą įvardijama ETL; tačiau jos svarba kibernetiniame pasaulyje yra didelė. Dezinformacijos ir klaidingos informacijos kampanijos dažnai naudojamos vykdant hibridinius išpuolius, siekiant sumažinti bendrą pasitikėjimą, t. y. pagrindinis kibernetinio saugumo aspektas.

- **Nekenkėjiško pobūdžio grėsmės**

Grėsmės paprastai laikomos savanoriška ir kenkėjiška veikla, vykdoma priešiškų šalių, kurios kai kuriais atžvilgiais yra suinteresuotos vykdyti išpuolį prieš konkretų taikinį. Šiai kategorijai priskiriame grėsmes, kurių kenkėjiškas pobūdis nėra aiškus. Dažniausiai tai atvejai, susiję su žmogaus klaidomis ir netinkamu sistemos konfigūravimu, tačiau tai gali būti ir fizinės nelaimės, nuo kurių nukenčia IT infrastruktūra. Be to, šios grėsmės, atsižvelgiant į jų pobūdį, nuolat aptariamos metinėje grėsmių aplinkos ataskaitoje ir jos yra pagrindinis susirūpinimą keliantis veiksnys vertinant riziką.

1 diagrama. 2021 m. ENISA grėsmių aplinka. Pagrindinės grėsmės

Pažymėtina, kad pirmiau minėtos grėsmės apima grėsmių kategorijas ir apibendrinimą nustatant aštuonias pirmiau išvardytas kategorijas. Kiekviena iš grėsmių grupių toliau analizuojama specialiame šios ataskaitos skyriuje, kuriame išsamiau aptariami jų ypatumai ir pateikiama konkretesnė informacija, išvados, tendencijos, išpuolių metodai ir rizikos švelninimo kryptys.

1.2. PAGRINDINĖS TENDENCIJOS

Toliau pateiktame sąraše apibendrinamos pagrindinės ataskaitiniu laikotarpiu pastebėtos kibernetinių grėsmių aplinkos tendencijos. Jos taip pat išsamiai peržiūrėtos įvairiuose 2021 m. ENISA grėsmių aplinkos ataskaitos skyriuose.

- **Ypač sudėtingų ir didelį poveikį turinčių tiekimo grandinės pažeidimų** daugėjo, kaip tai matyti iš specialios ENISA grėsmių aplinkos tiekimo grandinėje ataskaitos. **Valdomų paslaugų teikėjai** yra ypač vertinami taikiniai tarp kibernetinių nusikaltėlių.
- **Per COVID-19 pandemiją išplito kibernetinio šnipinėjimo** užduočių vykdymas ir atsirado **galimybės veikti kibernetiniams nusikaltėliams**.

- **Vyriausybinės organizacijos ėmėsi veiksmų** nacionaliniu ir tarptautiniu lygmeniu. Pastebėta, kad vyriausybės labiau stengiasi siekdamos išardyti valstybės remiamų grėsmės subjektų veiklą ir imtis prieš juos teisinių veiksmų.
- **Kibernetinių nusikaltėlių motyvu vis dažniau tampa** jų veiklos **monetizacija,** pvz., išpirkos reikalavimo programinė įranga. **Kriptovaliutos** išlieka pagrindine išmokos grėsmės subjektams sumokėjimo priemone.
- Kibernetinių nusikaltimų metu vykdomi išpuoliai **vis dažniau būna nukreipti į ypatingos svarbos infrastruktūrą kartu ją sugadinant**.
- **Kenkimas naudojant e. laiškus, kuriais stengiamasi išvilioti duomenis, ir nuotolinio darbalaukio tarnybų (RDP) kontrolės perėmimas** yra du dažniausiai pasitaikantys **užkrato naudojant išpirkos reikalavimo programinę įrangą vektoriai**.
- 2021 m. vis labiau buvo domimasi **išpirkos reikalavimo programinės įrangos, kaip paslaugos rūšies (RaaS), verslo modelių tipu,** todėl tapo sudėtinga tinkamai atpažinti pavienius grėsmės subjektus.
- **Trigubo poveikio išpirkos reikalavimo programinės įrangos** schemų atvejų skaičius 2021 m. gerokai padidėjo.
- 2020 m. pastebėta **mažėjanti kenkimo programinės įrangos** naudojimo tendencija išliko nepakitusi 2021 m. 2021 m. pastebėjome, kad grėsmės subjektai naudoja santykinai naujas arba neįprastas programavimo kalbas savo kodui prijungti.
- **Kenkimo programinė įranga, nukreipta į konteinerių aplinką**, naudojama vis dažniau, įskaitant tokias naujoves, kaip antai, iš atminties vykdoma kenkimo programinė įranga nenaudojant failų.
- Kenkimo programinės įrangos kūrėjai toliau ieško būdų, kaip **apsunkinti apgrąžos inžineriją ir dinaminę analizę**.
- 2021 m. pirmąjį ketvirtį **išnaudojamosios kriptovaliutos gavybos užkratų skaičius** buvo **kaip niekad didelis**, palyginti su pastaraisiais keleriais metais. **Finansinė nauda**, susijusi su išnaudojamąja kriptovaliutos gavyba, tapo paskata grėsmės subjektams vykdyti šiuos išpuolius.
- **2021 m. kriptovaliutos gavybos ir išnaudojamosios kriptovaliutos gavybos veikla buvo kaip niekad intensyvi**.
- Galime matyti, kad **pereinama nuo išnaudojamosios kriptovaliutos gavybos naršyklėje prie išnaudojamosios kriptovaliutos gavybos naudojant failus**.
- **COVID-19 vis dar yra pagrindinė pagunda rengti** išpuolių per e. paštą **kampanijas**.
- **Verslo e. laiškų perėmimo (BEC)** atvejų **padaugėjo**, jie tapo **sudėtingesni** ir **tikslingesni**.
- Vis labiau plinta **duomenų viliojimo kaip paslaugos (PhaaS)** verslo modelis.
- Grėsmės subjektai, atsižvelgdami į grėsmes duomenims ir informacijai, savo dėmesį nukreipė į **informaciją apie skiepus**.
- **Sveikatos priežiūros sektoriuje taip pat padaugėjo duomenų saugumo pažeidimų**.
- Tradiciniai DDoS (paskirstytojo paslaugos trikdymo) išpuoliai vis dažniau vykdomi **mobiliojo ryšio tinkluose ir IoT (daiktų internete).**
- **Paslaugos trikdymas reikalaujant išpirkos (RDoS)** yra nauja su paslaugų trikdymu susijusių išpuolių rūšis.
- **Dalijimasis ištekliais virtualioje aplinkoje** veikia kaip paskata rengti DDoS išpuolius.
- 2021 m. **DDoS kampanijos** tapo tikslingesnės ir daug dažnesnės bei vis labiau įvairialypės.
- **Dirbtiniu intelektu (DI) grindžiama dezinformacija** padeda išpuolių vykdytojams vykdyti savo išpuolius.
- **Duomenų viliojimas yra dezinformacijos išpuolių epicentre** ir šiuo atveju išnaudojami žmonių įsitikinimai.
- **Klaidinga informacija ir dezinformacija** yra kibernetinės nusikalstamos veiklos epicentre ir ji plinta precedento neturinčiais tempais.
- **Dezinformacijos kaip paslaugos (DaaS) verslo modelis** gerokai išplito ir taip atsitiko dėl didėjančio COVID-19 pandemijos poveikio ir poreikio turėti daugiau informacijos.
- 2020 ir 2021 m. pastebėjome **nekenkėjiško pobūdžio incidentų skaičiaus augimą**, COVID-19 pandemija tapo daugybės **žmogaus klaidų** ir **netinkamo sistemų konfigūravimo** atvejų priežastimi, ir 2020 m. dauguma pažeidimų buvo padaryti dėl klaidų.
- **Padaugėjo su debesijos saugumu susijusių nekenkėjiško pobūdžio incidentų**.

1.3. PAGRINDINIŲ GRĖSMIŲ ARTUMAS ES ATŽVILGIU

Svarbus aspektas, į kurį reikia atsižvelgti ENISA grėsmių aplinkos ataskaitoje, susijęs su kibernetinės grėsmės artumu Europos Sąjungos (ES) atžvilgiu. Tai ypač svarbu siekiant padėti įvertinti kibernetinių grėsmių reikšmę, susieti jas su potencialiais grėsmės subjektais ir vektoriais, ir net padėti atrinkti tinkamus tikslingus rizikos mažinimo vektorius. Laikydamiesi pagal ES bendrą saugumo ir gynybos politiką (BSGP)[7] pasiūlytos klasifikacijos, kibernetines grėsmes klasifikuojame į keturias kategorijas, kaip parodyta Table 1.

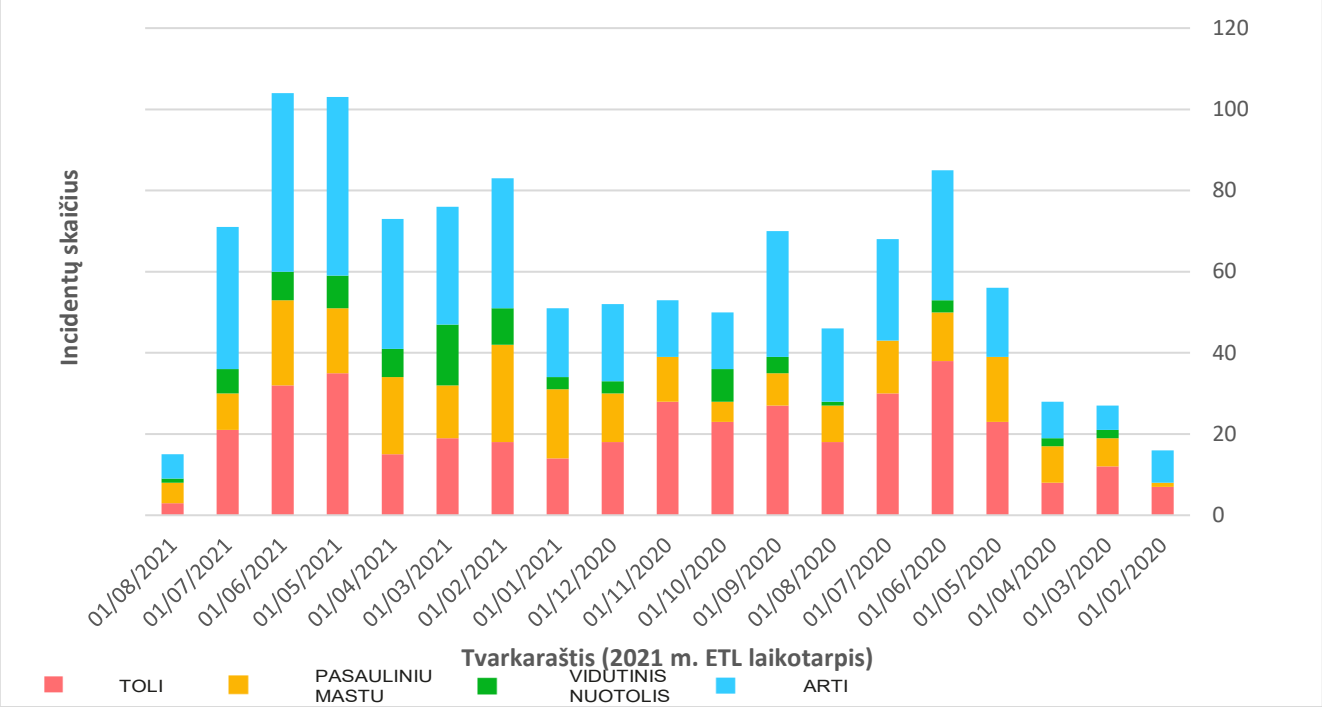
1 lentelė. Kibernetinių grėsmių artumo klasifikacija

Artumas	Problemos
ARTI	Nukentėję tinklai, sistemos, kontroliuojamos ir užtikrinamos ES viduje. Nukentėję gyventojai ES viduje.
VIDUTINIS NUOTOLIS	Tinklai ir sistemos laikomi gyvybiškai svarbiais veiklos tikslams pasiekti ES bendrojoje skaitmeninėje rinkoje ir TISD sektoriuose, tačiau už jų kontrolę ir patikinimą atsako ne ES institucijos arba valstybių narių viešosios arba privačiosios valdžios institucijos. Nukenčia geografinių teritorijų, esančių netoli ES sienų, gyventojai.
TOLI	Tinklai ir sistemos, kurios, jei joms bus padaryta įtaka, turės kritinį poveikį veiklos tikslams pasiekti ES bendrojoje skaitmeninėje rinkoje ir TISD sektoriuose. Šių tinklų ir sistemų kontrolė ir patikinimas nepriklauso ES institucijoms arba valstybių narių viešosioms arba privačiosioms institucijoms. Nukenčia geografinių teritorijų, esančių toli nuo ES sienų, gyventojai.
PASAULINIU MASTU	Visose išvardytose srityse

Figure 2 parodytas incidentų, susijusių su pagrindinėmis grėsmių kategorijomis, apie kurias pranešta 2021 m. ETL, tvarkaraštis. Reikėtų pažymėti, kad diagramoje pateikta informacija pagrįsta OSINT (atvirųjų šaltinių žvalgybos informacija) ir tai yra ENISA darbo informuotumo apie padėtį srityje rezultatas[8].

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Pagal ES kibernetinio saugumo akto 7 straipsnio 6 dalį https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

2 diagrama. Pastebėtų incidentų, susijusių su pagrindinėmis ETL grėsmėmis (OSINT pagrįstas informuotumas apie padėtį) tvarkaraštis atsižvelgiant į jų artumą.



Kaip matyti iš pirmiau pateiktos diagramos, 2021 m. incidentų buvo daugiau nei 2020 m. Visų pirma kategorijoje „ARTI“ nuolat daugėjo pastebėtų incidentų, susijusių su pagrindinėmis grėsmėmis, o tai reiškia, kad ES lygmeniu jie yra reikšmingi. Nieko stebėtino, kad mėnesinės tendencijos (kurios diagramoje nepavaizduotos dėl informacijos glaustumo), susijusios su skirtingomis klasifikacijomis, yra gana panašios, nes kibernetinis saugumas yra tarpvalstybinio pobūdžio ir dažniausiai grėsmės pasireiškia visais artumo lygmenimis. Verta pažymėti, kad per paskutinius 2021 m. ETL ataskaitinio laikotarpio mėnesius pastebėtas didesnis kategorijos „ES ARTI“ artumas, t. y. tendencija, kurią ENISA toliau stebės siekdama išsiaiškinti, kaip ji vystosi ir koks jos ryšys su grėsmės subjektų veikla bei nuolatinių grėsmių vektoriais.

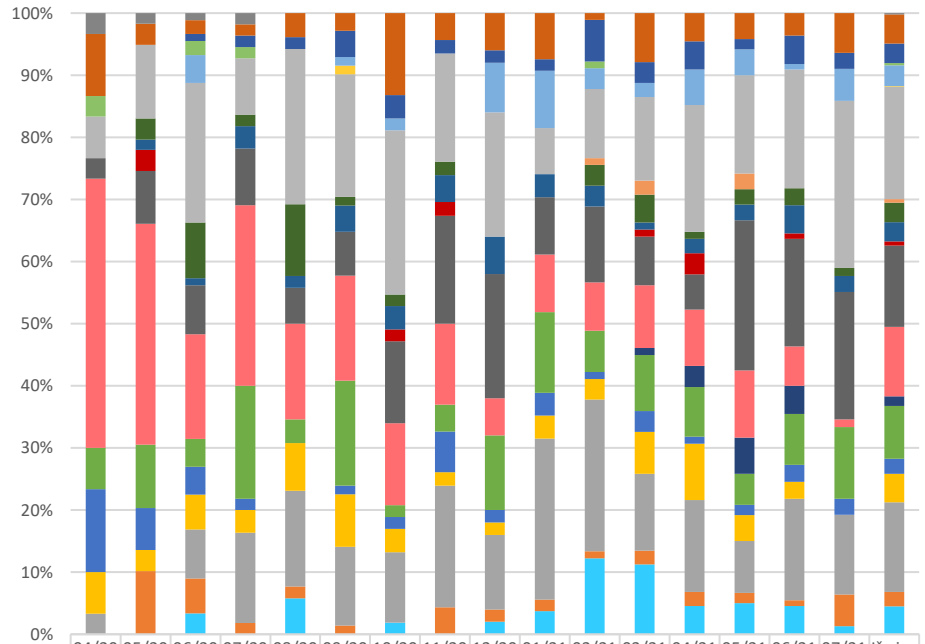
1.4. PAGRINDINĖS GRĖSMĖS PAGAL SEKTORIUS

Kibernetinės grėsmės paprastai nėra būdingos vienam konkrečiam sektoriui ir dažniausiai daro poveikį daugiau nei vienam sektoriui. Iš tiesų taip ir yra, nes daugeliu atvejų grėsmės pasireiškia dėl pagrindinių IRT sistemų, naudojamų įvairiuose sektoriuose, trūkumų išnaudojimo. Tačiau tikslingi išpuoliai, taip pat išpuoliai, kurių metu išnaudojami kibernetinio saugumo brandos skirtumai įvairiuose sektoriuose ir tam tikrų sektorių populiarumas / žinomumas, yra veiksniai, į kuriuos reikia atsižvelgti. Šie veiksniai prisideda prie grėsmių, kurios pasireiškia kaip incidentai konkrečiuose sektoriuose, būtent todėl svarbu atidžiai išnagrinėti pastebėtų incidentų ir grėsmių sektoriaus aspektus. Be to, kiekviename sektoriuje pastebėtos tendencijos ir sektorių tarpusavio priklausomybė – tai pastebėjimai, kuriuos galima nustatyti atliekant tokią analizę.

3 ir 4 diagramose pateikta informacija apie nuo pastebėtų incidentų nukentėjusius sektorius, remiantis OSINT (vieši žvalgybinės informacijos šaltiniai) ir tai yra ENISA darbo informuotumo apie padėtį srityje rezultatas[9]. Diagramose pateikta informacija apie incidentus, susijusius su 2021 m. ETL pagrindinėmis grėsmėmis. Tai pirmasis ENISA bandymas nustatyti konkrečiuose sektoriuose kylančias grėsmes. Artimiausiu metų ir būsimose grėsmių aplinkos leidiniuose bus stengiamasi sektorius suderinti su Tinklo ir informacinių sistemų saugumo direktyvoje (TISD) ir pasiūlyme dėl jos peržiūros (TISD 2.0) išvardytais sektoriais.

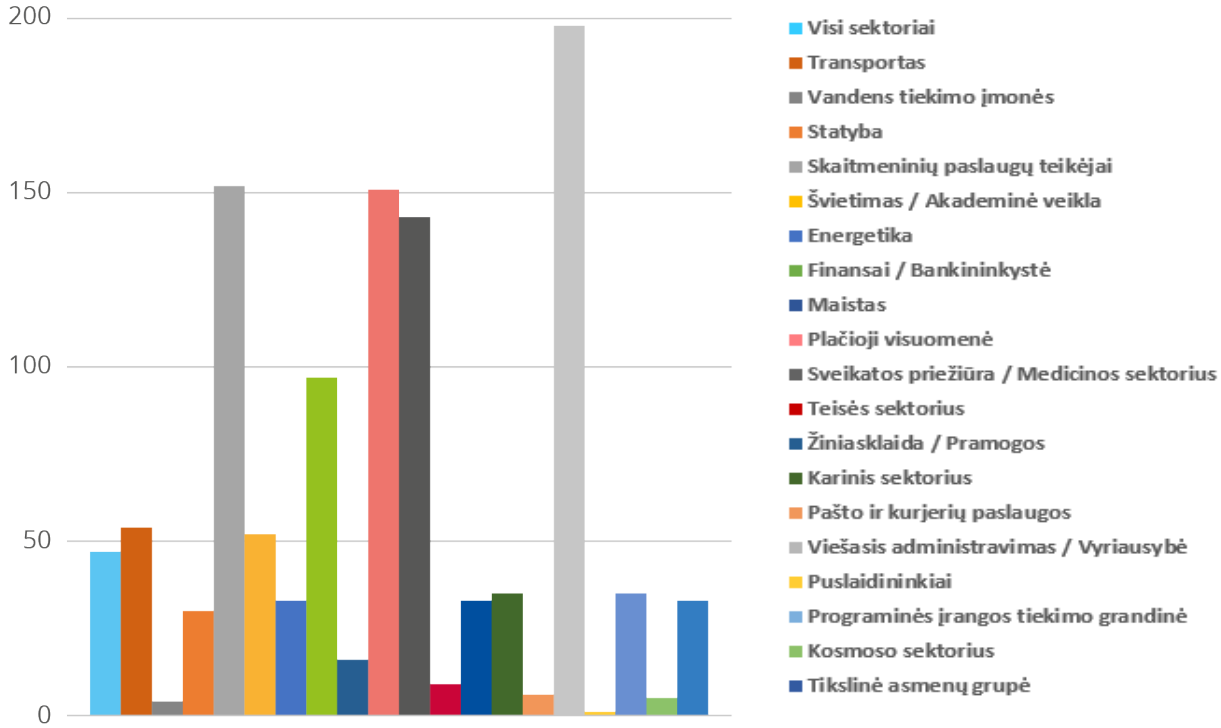
[9] Pagal ES kibernetinio saugumo akto 7 straipsnio 6 dalį (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

3 diagrama. Pastebėtų incidentų, susijusių su ETL pagrindinėmis grėsmėmis, tvarkaraštis pagal nukentėjusį sektorių.



	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	Iš viso
Vandens tiekimo įmonės	1	1	1	1													2
Transportas	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Tikslinė asmenų grupė			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Kosmoso sektorius	1		2	1							1						4
Programinės įrangos tiekimo grandinė			4			1	1		4	5	3	2	5	5	1	4	35
Puslaidininkiai						1											1
Viešasis administravimas / Vyriausybė	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Pašto ir kurjerių paslaugos											1	2		3			6
Karinis sektorius		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Žiniasklaida / Pramogos		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Teisės sektorius		2					1	1				1	3		1		7
Sveikatos priežiūra / Medicinos sektorius	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Plačioji visuomenė	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Maistas												1	3	7	5		16
Finansai / Bankininkystė	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energetika	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Švietimas / Akademinė veikla	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Skaitmeninių paslaugų teikėjai	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Statyba		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Visi sektoriai			3		3		1		1	2	11	10	4	6	5	1	47

4 diagrama. Sektoriai, kuriuose buvo įvykdyti išpuoliai, pagal incidentų skaičių (2020 m. balandžio mėn.–2021 m. liepos mėn.)



Šiuo ataskaitiniu laikotarpiu daugybė incidentų buvo nukreipti į viešojo administravimo ir valdžios institucijas ir skaitmeninių paslaugų teikėjus. To ir galima tikėtis atsižvelgiant į horizontalųjį paslaugų teikimą šiame sektoriuje, taigi ir poveikį daugybei kitų sektorių. Taip pat pastebėjome, kad nemažai incidentų yra nukreipti į galutinius naudotojus ir nebūtinai į konkretų sektorių. Nemažai išpuolių surengta sveikatos sektoriuje ir pastebėti šios veiklos intensyvėjimo ženklai per paskutinius keletą ataskaitinio laikotarpio mėnesių (2021 m. gegužės–liepos mėn.). Įdomu tai, kad finansų sektoriuje ištisus metus įvyksta pastovus skaičius incidentų. Iš programinės įrangos tiekimo grandinės taip pat matyti, kad 2021 m. incidentų skaičius padidėjo ir ši aplinkybė patvirtinta ENISA grėsmių aplinkos tiekimo grandinėje ataskaitoje[10].

1.5. METODIKA

2021 m. ENISA grėsmių aplinkos (ETL) ataskaita pagrįsta atviruosiuose šaltiniuose prieinama informacija, kuri iš esmės yra strateginio pobūdžio, ir pačios ENISA žvalgybos apie kibernetines grėsmes pajėgumais, ir apima daugiau nei vieną sektorių, technologiją ir kontekstą. Stengiamasi, kad ataskaita būtų suprantama pramonei ir prekiautojams, visame jos tekste įvairiose išnašose pateikiant nuorodas arba cituojant įvairių saugumo tyrėjų darbus, saugumo tinklaraščius ir naujienų žiniasklaidos straipsnius. 2021 m. ETL ataskaita apima 2020 m. balandžio mėn.–2021 m. liepos mėn. – tai ataskaitoje aptariamas ataskaitinis laikotarpis.

Rengiant 2021 m. ETL ataskaitą buvo naudotas toliau aprašytas metodas. Aptariamu laikotarpiu ENISA, pasinaudodama informuotumu apie padėtį, parengė pagrindinių incidentų, apie kuriuos buvo pateikta informacija atviruosiuose šaltiniuose, sąrašą. Šis sąrašas buvo naudojamas kaip pagrindas parengiant pagrindinių grėsmių sąrašą, taip pat kaip kelių ataskaitoje aprašytų tendencijų ir pateiktų statistinių duomenų šaltinis.

Paskui ENISA ir išorės ekspertai atliko išsamią literatūros, prieinamos atviruosiuose šaltiniuose, pvz., naujienų žiniasklaidos straipsnių, ekspertų nuomonių, žvalgybos ataskaitų, incidentų analizės ir saugumo tyrimo ataskaitų, analizę. Atlikdama nuolatinę analizę, ENISA nustatė kiekvienos 2021 m. ETL pateiktos pagrindinės grėsmės

[10] ENISA išpuolių prieš tiekimo grandinę grėsmių aplinka, 2021 m. liepos mėn. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

tendencijas ir nagrinėtinus aspektus. Pagrindinės išvados ir sprendimai, pateikti šiame vertinime, pagrįsti įvairiais ir viešai prieinamais ištekliais, kurie pateikiami literatūros, naudotos rengiant šį dokumentą, sąraše.

Ataskaitoje bandome daryti skirtumą tarp šaltinių, kuriais rėmėmės, ir mūsų atlikto vertinimo. (Tai darome sąmoningai vartodami frazę „mūsų vertinime“). Galiausiai, atlikdami vertinimą, tikimybę įvertiname vartodami žodžius, kuriais išreiškiamas tikimybės įvertis (pvz., tikėtina, labai tikėtina, neabejotinai)[11].

Šioje ataskaitoje panaudota MITRE ATT&CK® sistema[12] siekiant atkreipti dėmesį į išpuolių taktiką ir metodus, susijusius su atitinkama grėsme (žr. A priedą). Dėl kiekvienos ATT&CK® taktikos rūšies pateikiama informacija apie priešiškos šalies naudotus metodus. Šiuo atveju galima parengti taikytiną ATT&CK rizikos mažinimo[13] sąrašą. MITRE ATT&CK® – tai žinių bazė, bendra rungimosi taktikos ir metodų kalba, pagrįsta realaus pasaulio pastebėjimais. MITRE ATT&CK® žinių bazė naudojama kaip konkrečių grėsmių modelių ir metodikos privačiajame sektoriuje, vyriausybėje ir kibernetinio saugumo produktų ir paslaugų bendruomenėje rengimo pagrindas.

Ataskaitą patvirtino 2021 m. balandžio mėn. sudaryta ENISA *ad hoc* darbo grupė kibernetinių grėsmių aplinkos klausimais[14], kurią sudaro Europos ir tarptautinių viešojo ir privačiojo sektoriaus subjektai.

Atsižvelgdama į būsimas grėsmių aplinkos ataskaitas, ENISA rengia oficialią naują metodiką, siekdama skatinti skaidrumą ir nustatyti struktūrizuoto ir tinkamai suderintų procesų pagrindus. Šiuo tikslu grėsmių aplinkos metodika kartu su peržiūrėta grėsmių taksonomija ateityje bus paskelbta viešai.

1.6. ATASKAITOS STRUKTŪRA

2021 m. ENISA grėsmių aplinkos (ETL) ataskaitos struktūra išliko kaip ir ankstesniais metais, 2021 m. pasinaudojant panašia struktūra pagrindinėms kibernetinėms grėsmėms aptarti. Ankstesnių ataskaitų skaitytojai pastebės, kad grėsmių kategorijos buvo konsoliduotos atsižvelgiant į tai, kad ateityje bus naudojama nauja kibernetinių grėsmių taksonomija.

Šios ataskaitos struktūra yra tokia:

2 skyriuje nagrinėjamos su grėsmės subjektais susijusios tendencijos (t. y. valstybės remiami subjektai, kibernetinių nusikaltimų subjektai, samdomi įsilaužėliai ir įsilaužėliai aktyvistai).
3 skyriuje aptariamos pagrindinės išvados, incidentai ir tendencijos, susijusios su išpirkos reikalavimo programine įranga.
4 skyriuje pateikiamos pagrindinės išvados, incidentai ir tendencijos, susijusios su kenkimo programine įranga.
5 skyriuje aprašomos pagrindinės išvados, incidentai ir tendencijos, susijusios su išnaudojamąja kriptovaliutos gavyba.
6 skyriuje pateikiamos pagrindinės išvados, incidentai ir tendencijos, susijusios su e. pašte kylančiomis grėsmėmis.
7 skyriuje aptariamos pagrindinės išvados, incidentai ir tendencijos, susijusios su grėsmėmis duomenims.
8 skyriuje pateikiamos pagrindinės išvados, incidentai ir tendencijos, susijusios su grėsmėmis prieinamumui ir vientisumui.
9 skyriuje pabrėžiama hibridinių grėsmių svarba ir aprašomos pagrindinės išvados, incidentai ir tendencijos, susijusios su dezinformacija ir klaidinga informacija.
10 skyriuje aptariamos pagrindinės išvados, incidentai ir tendencijos, susijusios su nekenkėjiško pobūdžio grėsmėmis.
A priede pateikiami metodai, kurie paprastai naudojami rengiant su kiekviena grėsme susijusį išpuolį, remiantis MITRE ATT&CK® sistema.
B priede pateikiami su kiekviena grėsme susiję žinomi incidentai, apie kuriuos buvo pranešta ataskaitiniu laikotarpiu.

[11] CIA - Tikimybės įverčio žodžiai 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