MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

VITALIJUS LISOVSKIS

SKAITMENINIO TURINIO KIBERNETINIS SAUGUMAS- DDOS ATAKŲ PREVENCIJA IR APSAUGA SKAITMENINIO TURINIO PRIEINAMUMUI UŽTIKRINTI

Magistro baigiamasis darbas

Vadovas:

Prof. Dr. Mindaugas Kiškis

VILNIUS, 2023

MYKOLO ROMERIO UNIVERSITETAS

VIEŠOJO VALDYMO IR VERSLO FAKULTETAS

SKAITMENINIO TURINIO KIBERNETINIS SAUGUMAS - DDOS ATAKŲ PREVENCIJA IR APSAUGA SKAITMENINIO TURINIO PRIEINAMUMUI UŽTIKRINTI

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Studijų programa 6211LX066

VILNIUS, 2023

TURINYS

LENTELĖS ... 4

PAVEIKSLAI ... 5

ĮVADAS ... 6

1. SKAITMENINIO TURINIO KIBERNETINIO SAUGUMO TEORINIAI ASPEKTAI ... 8

1.1. Kibernetinio saugumo samprata ir pagrindiniai principai ... 8

1.2. DDoS atakų teorinė apžvalga ... 12

1.2.1. DDoS atakų samprata ... 12

1.2.2. DDoS atakų rūšys ... 12

1.3 DDoS atakų apsaugos technologijos ... 16

1.4. Kibernetinio saugumo programų Lietuvoje teisinis reglamentavimas ... 18

2. SKAITMENINIO TURINIO APSAUGA NUO DDOS ATAKŲ TELIA LIETUVA ĮMONĖJE ... 23

2.1. Tyrimo metodologija ... 24

2.2. Kokybinio tyrimo rezultatų analizė ... 29

2.2.1. DDos atakų mastas ir poveikis skaitmeniniui turiniui Telia Lietuva įmonėje ... 31

2.2.2. Esamų DDos atakų apsaugos priemonių apžvalga ... 31

2.3. Tyrimo rezultatų apibendrinimas ... 32

3. DDOS ATAKŲ APSAUGOS SKAITMENINIUI TURINIUI REKOMENDACINIS MODELIS ... 35

IŠVADOS ... 40

LITERATŪRA ... 41

ANOTACIJA ... 42

SANTRAUKA ... 44

SUMMARY ... 45

PRIEDAI ... 46

LENTELĖS

1 lentelė. Aplikacijų lygmuo (OSI) su galimų Dos/DDoS atakų tipais ir aptakų aprašymas tam tikrose sluoksniuos.
2 lentele. Kibernetinio saugumo architektūra Lietuvoje.
3 lentelė. Atvaizduojama tyrimo metodo struktūrą
4 lentelė. Tyrimo planas
5 lentelė. Tyrimo metodai
6 lentelė. DDoS atakų apsaugos rekomendacinis modelis

PAVEIKSLAI

1 pav. Kibernetinio saugumo santykis su “CIA Triada” Schou ir Hernandezo (2014)

2 pav. Dos atakos tipas

3 pav. DDos atakos tipas

ĮVADAS

Temos naujumas ir aktualumas. DDoS atakų prevencija ir apsauga nuo jų, siekiant užtikrinti skaitmeninio turinio prieinamumą, yra nauja ir aktuali mokslinių tyrimų tema dėl nuolat didėjančio skaitmeninio turinio kiekio ir nuolat besikeičiančių bei tobulėjančių atakų metodų. Ji taip pat aktuali telekomunikacijų bendrovių ir paslaugų kontekste, nes padeda užtikrinti klientų pasitenkinimą ir saugumą. Dėl vis didėjančio skaitmeninio turinio kiekio ir nuolat besikeičiančių bei stiprėjančių atakų metodų atsirado nauja aktuali tyrimų sritis, kurioje daugiausia dėmesio skiriama DDoS atakų prevencijai ir kovai su jomis, kad būtų užtikrintas skaitmeninio turinio prieinamumas. Tai taip pat ypač aktualu su ryšio paslaugas teikiančiomis telekomunikacijų bendrovėmis ir paslaugas jų paslaugas gaunančiais klientais, nes tai padeda užtikrinti klientų pasitenkinimą ir jų saugumą. Telia Lietuva buvo pasirinkta kaip šio tyrimo kontekstas dėl jos didelio klientų skaičiaus, išsamios paslaugų spektro, įskaitant ryšio, interneto, televizijos ir sprendimus įmonėms, bei jos patirties susiduriant su DDoS atakomis. Telia Lietuva yra viena didžiausių telekomunikacijų bendrovių Lietuvoje ir todėl yra labai aktualus tyrimo objektas.

Tyrimo problema ir problemos formulavimas. Skaitmeninio turinio prieinamumo užtikrinimas yra esminis uždavinys, susijęs su DDoS atakų prevencija ir apsauga nuo jų. DDoS atakos gali sukelti didelių nuostolių ir pakenkti reputacijai tiek skaitmeninio turinio teikėjams, tiek vartotojams. Šios problemos sprendimas yra labai svarbus. *Probleminis klausimas*: Kaip telekomunikacijų bendrovės ir paslaugų teikėjai gali veiksmingai apsisaugoti nuo DDoS atakų, kad užtikrintų skaitmeninio turinio prieinamumą ir kokybę?

Tyrimo objektas. DDoS atakų prevencija ir gynyba nuo jų siekiant užtikrinti skaitmeninio turinio prieinamumą.

Tyrimo tikslas. Išanalizuoti DDoS atakų prevencijos ir apsaugos nuo jų strategijas, metodikas ir geriausią praktiką, taikomą telekomunikacijų bendrovėse ir paslaugų teikėjams, atsižvelgiant į Telia Lietuva kontekstą.

Tyrimo uždaviniai:

1. Apžvelgti įvairias DDoS atakų kategorijas ir metodus bei jų poveikį skaitmeninio turinio prieinamumui.
2. Pateikti DDoS atakų pavyzdžių ir jų pasekmių skaitmeninio turinio teikėjams ir galutiniams naudotojams.
3. Išnagrinėti DDoS atakų prevencijos ir apsaugos nuo jų strategijas ir priemones, pavyzdžiui, tinklo architektūros optimizavimą, kibernetinio saugumo politiką ir apsaugos nuo DDoS atakų paslaugas bei technologijas.

4. Atlikti fokus grupės tyrimą su Telia Lietuva klientais, siekiant surinkti jų požiūrį, patirtį ir nuomonę apie skaitmeninio turinio kibernetinį saugumą ir DDoS atakų prevenciją bei apsaugą nuo jų.
5. Atlikti du skaitmeninio turinio teikėjo ar platformos, patyrusios DDoS atakas, ir įdiegtų apsaugos sprendimų atvejų tyrimus.
6. Atlikti pusiau struktūrizuotą interviu su divem Telia Lietuva ekspertais, siekiant gauti jų profesinę nuomonę, patirtį ir įžvalgas apie DDoS atakų prevenciją ir apsaugą, taikomą telekomunikacijų bendrovėje, bei aptarti galimus tobulinimo būdus ir strategijas.

Tyrimo metodai:

1. Literatūros analizė: Šiuo tyrimu siekiama išanalizuoti DDoS atakų sąvoką, tipus, metodus ir poveikį skaitmeninio turinio prieinamumui, atliekant išsamią mokslinės literatūros, straipsnių, tyrimų ir ataskaitų apžvalgą. Be to, šiame tyrime bus nagrinėjamos esamos prevencijos ir apsaugos strategijos bei priemonės. Minėta metodika gali turėti apribojimų, nes ji remiasi jau egzistuojančiomis žiniomis, o DDoS atakų prevencija ir apsauga nuo jų nuolat kinta. Nepaisant to, norint sukurti tvirtą teorinį pagrindą, būtina išsamiai išnagrinėti dabartinę mokslinę literatūrą.
2. Kokybinis tyrimas - fokus grupės metodas: Fokus grupės diskusija su 7-8 Telia klientais, siekiant gauti jų požiūrį, patirtį ir nuomones apie skaitmeninio turinio kibernetinį saugumą ir DDoS atakų prevenciją bei apsaugą. Diskusija vyks remiantis diskusijos gairėmis, apimant pagrindinius temos aspektus. Fokus grupės metodas gali būti ribotas dėl mažesnio kiekiu dalyvių, kurie gali būti paveikti pasirinkimo šališkumo, o taip pat dėl to, kad gauti duomenys yra subjektyvūs ir gali būti sunku juos abibendrinti.
3. Atvejo analizė – pusiau strūkturizuotas interviu su dviem ekspertais susijusiais su konkrečiais skaitmeninio turinio teikėjais ar platformomis, susidūrusiomis su DDoS atakomis, ir jų įgyvendintais apsaugos sprendimais. Atvejų analizės inerviu padės išsamiau suprasti praktinę DDoS atakų problemą ir efektyvius sprendimus. Atvejų tyrimų ribotumai yra susiję su tuo, kad jie analizuoja tik konkrečias situacijas, todėl išvadų abibendrinimas gali būti sunkus, ir kad analizuojant tik kelis atvejus gali būti praleisti kiti veiksniai, turintys įtakos DDoS atakų prevencijai ir apsaugai.

Šie tyrimo metodai kartu sudaro kombinuotą metodologiją, leidžiančią geriau suprasti ir įvertinti DDoS atakų problemą skaitmeninio turinio kontekste. Kombinuota metodologija leidžia sumažinti atskirų metodų ribotumų poveikį ir padeda gauti išsamesnę ir tikslesnę informaciją apie tiriamąją problemą.

Tačiau reikėtų nuolat aktualizuoti mokslinę literatūrą ir praktinę patirtį, kad būtų galima kuo tikslesnės ir išsamesnės išvados apie DDoS atakų prevenciją ir apsaugą skaitmeninio turinio kontekste.

1. SKAITMENINIO TURINIO KIBERNETINIO SAUGUMO TEORINIAI ASPEKTAI

1.1. Kibernetinio saugumo samprata ir pagrindiniai principai

Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti. Pasak Tarptautinės etikos, teisės ir technologijų bibliotekos (International Library of Ethics, Law and Technology, 2019), kibernetinis saugumas yra esminė sritis, kuria siekiama apsaugoti kompiuterių sistemas, tinklus ir duomenis nuo neteisėtos prieigos, vagystės, sugadinimo ar sunaikinimo. Pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (Nr. XII-1428, 2018) kibernetinis saugumas grindžiamas teisiniais, informacijos sklaidos, organizaciniais ir techniniais aspektais. Šie aspektai leidžia nustatyti, analizuoti ir reaguoti į kibernetinius incidentus, taip pat atkurti normalų elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veikimą.

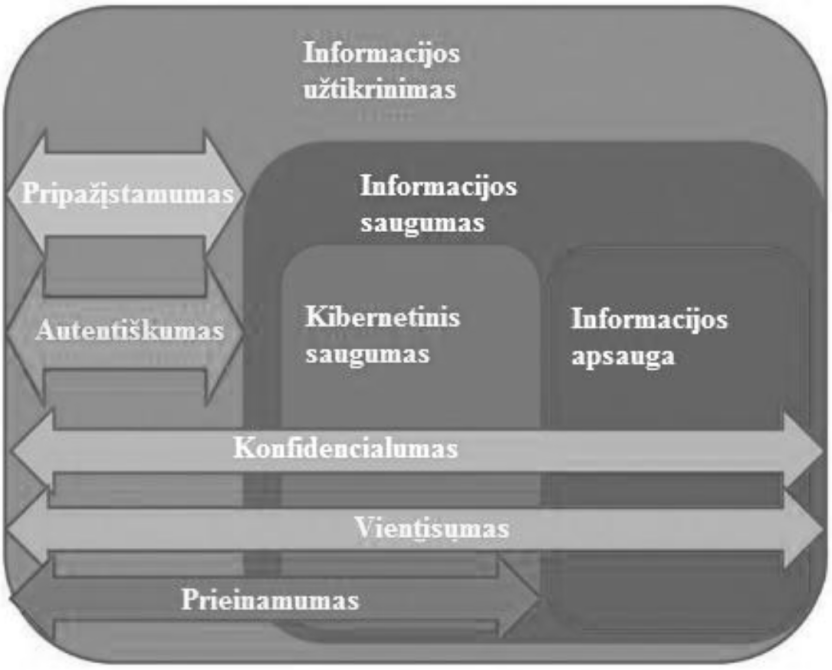
CIA triada, kurią sudaro konfidencialumas, vientisumas ir prieinamumas, yra vienos iš kibernetinio saugumo sričių, dar vadinamos informacijos saugumo pagrindas (Anderson, 1972). (Schou ir Hernandez, 2014) teigia, kad informacinių sistemų vientisumas priklauso nuo šių trijų veiksnių:

- Konfidencialumas reiškia duomenų saugumo lygį, kai prieiga prie duomenų suteikiama tik įgaliotiems asmenims. Jis užkerta kelią šnipinėjimui ir kitoms neteisėtos prieigos prie duomenų formoms. Konfidencialumas yra esminė kibernetinio saugumo dalis, apsauganti duomenis nuo nutekėjimo ar neįgaliotų asmenų peržiūros.
- Informacija saugoma vientisumo lygmeniu, ji apsaugoma nuo neleistinų pakeitimų ar ištrynimo ir visada yra naujausia bei išsami. Kad informacinės sistemos tinkamai veiktų, labai svarbu, kad visi duomenys būtų tikslūs ir išsamūs, todėl čia svarbus vientisumas.

- Kalbant apie duomenų saugumą, sąvoka "prieinamumas" reiškia, kiek įgalioti naudotojai visada gali pasiekti saugomus duomenis, kai jiems jų reikia. Prieinamumas yra labai svarbi kibernetinio saugumo dalis, nes padeda išvengti duomenų praradimo ir užtikrina, kad jie būtų prieinami visada, kai jų reikia.

Kaip autoriai (Schou ir Hernandez, 2014) teigia, kad kibernetinis saugumas siekia tų pačių tikslų kaip ir informacijos saugumas. Pateikia esminius kibernetinio saugumo ir informacijos saugos komponentus. 1 paveiksle pavaizduotas kibernetinio saugumo, informacijos saugumo ir informacijos užtikrinimo ryšys, santykis su konfidencialumu, vientisumu ir prieinamumu.

1 pav. Kibernetinio saugumo santykis su “CIA Triada” Schou ir Hernandezo (2014)



Anot Andersono (1972), informacijos konfidencialumo užtikrinimas padeda išvengti neteisėtos prieigos prie tos informacijos, duomenų vientisumo užtikrinimas padeda užkirsti kelią neteisėtam duomenų keitimui arba jį aptikti, o duomenų prieinamumo užtikrinimas padeda išvengti neteisėto ištrynimo ar nutraukimo. Remiantis "International Library of Ethics, Law and Technology, 2019", šie saugumo tikslai taikomi tiek ramybės būsenoje esantiems duomenims, t. y. kompiuteryje ar popieriuje saugomiems duomenims, tiek perduodamiems duomenims, t. y. tinklu siunčiamiems duomenims. Principai pagal Andersono (1972):

- Konfidencialumas: užkirsti kelią neteisėtai prieigai prie informacijos.
- Vientisumas: užkirsti kelią neleistinam duomenų keitimui arba jį nustatyti.
- Prieinamumas: apsaugoti nuo neleistino duomenų ištrynimo ar sutrikdymo.

Pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (Nr. XII-1428, 2018), “Kibernetinis saugumas - visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis

siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą.“

Analizuojant mokslinius šaltinius apie kibernetinį saugumą, galima pastebėti, kad trys svarbiausi informacijos saugumo aspektai yra prieinamumas, vientisumas ir konfidencialumas (dar vadinama "CIA triada") - tai pamatas, kuriais grindžiama duomenų apsauga. Sąvoka "vientisumas" reiškia gebėjimą išlaikyti informacijos tikslumą, patikimumą ir pagrįstumą per visą jos gyvavimo ciklą, o "prieinamumas" reiškia galimybę įgaliotiems darbuotojams gauti informaciją, kai tik jiems jos prireikia (Anderson, 1972). Konfidencialumas apsaugo informaciją nuo atskleidimo be leidimo.

Šiame straipsnyje daugiausia dėmesio skiriama strategijoms, kurios taikomos siekiant apsaugoti organizacijas nuo prieinamumo praradimo. Kai kurie iš šių būdų apima svarbiausių sistemų atnaujinimą, apsaugą nuo DDoS atakų, dubliavimą, ugniasienes ir tarpinius serverius, pakankamą pralaidumą ir prieigos kontrolę. Prieinamumas, vientisumas ir konfidencialumas vis dar plačiai taikomas vadovaujant viso pasaulio įmonių ir organizacijų informacijos saugumo veiklai, siekiant užtikrinti, kad jų vertingiausias turtas būtų veiksmingai apsaugotas. Pasak Schou ir Hernandezo (2014), organizacijos reikalavimai turėtų lemti informacijos prieinamumo, vientisumo ir slaptumo svarbos lygį.

Kibernetinio saugumo tikslai yra tapatūs informacijos saugumo tikslams. Tai 2014 m. įrodė (C. Schou ir S. Hernandez, 2014) Schou C., Hernandez S., Information Assurance Handbook: Efektyvaus kompiuterių saugumo ir rizikos valdymo strategijos kibernetinio saugumo, informacijos saugumo ir informacijos užtikrinimo ryšys, taip pat kaip jie susiję su konfidencialumu, vientisumu ir prieinamumu.

Apibendrinant kibernetinio saugumo samprata galima teigti, kad kibernetinis saugumas yra labai svarbi sritis, į kurią būtina atkreipti dėmesį siekiant užtikrinti informacijos saugumą įmonėse. "CIA triadą" sudaro konfidencialumas, vientisumas ir prieinamumas - tai pagrindiniai principai, kuriais grindžiamas kibernetinis saugumas. Šie pagrindiniai principai yra labai svarbūs įmonių informacijos saugumo veikloje ir padeda užtikrinti tinkamą duomenų apsaugą ir verslo veiklos tęstinumą.

Dėl šiuolaikinėje visuomenėje plačiai paplitusio informacinių technologijų naudojimo, kibernetinis saugumas tapo svarbia bet kurios šiuolaikinės įmonės sudedamąja dalimi. Dėl didėjančios priklausomybės nuo informacinių technologijų (IT) infrastruktūros ir interneto vis daugiau įmonių tampa atviros kibernetinių atakų galimybei, kuri gali turėti rimtų pasekmių ne tik jų verslo operacijoms, bet ir vartotojams bei verslo partneriams. (Agafonov, 2021)

Kibernetinio saugumo priemonės, kaip žinia, yra sudėtingos ir gali apimti daugybę atsakomųjų priemonių, skirtų apsaugoti organizaciją nuo įvairių galimų grėsmių. Antivirusinė programinė įranga, ugniasienės, šifravimo sistemos, duomenų atkūrimo sprendimai ir kitos prieigos kontrolės sistemos - tai

techninių apsaugos priemonių, kurios gali būti įdiegtos, pavyzdžiai. Informacijos saugumo politika, darbuotojų mokymas ir incidentų valdymo planai - tai galimų organizacinių priemonių pavyzdžiai. Be to, teisines priemones sudaro įstatymai, konvencijos ir politika, skirti kibernetiniam saugumui šalyje ar pramonės šakoje kontroliuoti. (Šidlauskas, 2018)

Kadangi kibernetinės grėsmės nuolat kinta ir tampa vis sudėtingesnės, įmonės ir organizacijos turi nuolat tobulinti savo kibernetinio saugumo sprendimus, kad apsaugotų savo informaciją ir infrastruktūrą nuo esamų ir dar tik atsirasiančių pavojų. Tai apima ne tik technologinių atnaujinimų diegimą, bet ir darbuotojų švietimą bei informavimą apie su kibernetiniu saugumu susijusias problemas.

Svarbu pabrėžti, kad IT skyrius yra atsakingas ne tik už kibernetinio saugumo užtikrinimą organizacijoje. Kadangi žmogaus klaidos ir neatsargumas yra pagrindinė daugelio saugumo pažeidimų priežastis, būtina, kad kiekvienas įmonės darbuotojas atliktų savo vaidmenį saugant jautrią informaciją. Dėl šios priežasties įmonės ir kitos organizacijos turi puoselėti kibernetinio saugumo kultūrą, kad kiekvienas darbuotojas žinotų savo vaidmenį ir atsakomybę, kurią jis prisiima saugodamas informacijos konfidencialumą. (Plečkaitis, 2016)

Kadangi technologijos ir internetas plačiai paplitę tiek asmeniniame, tiek profesiniame gyvenime, kibernetinio saugumo reikšmė įmonėms artimiausiais metais tik didės. Todėl kibernetinio saugumo funkcija taps dar svarbesnė, o įmonės turės skirti daugiau išteklių ir dėmesio šios srities tobulinimui.

Norint veiksmingai valdyti kibernetinį saugumą, būtina laikytis nuoseklaus ir integruoto požiūrio, apimančio įvairias sritis, įskaitant šias:

- Rizikos vertinimas: Įmonės ir kitos organizacijos privalo reguliariai atlikti rizikos vertinimą, kad galėtų atpažinti ir suvokti galimus pavojus ir silpnąsias vietas, esančias jų procesuose ir infrastruktūroje.
- Prevencinės priemonės: Tai apima tokius dalykus, kaip programinės ir techninės įrangos atnaujinimas, griežta saugumo politika ir tinkamas darbuotojų apmokymas.
- Aptikimas: Įmonės turėtų naudotis įvairiomis priemonėmis, kad laiku aptiktų kibernetinius įvykius. Tai leis joms reaguoti kuo greičiau.

Įgyvendinti veiksmingus incidentų valdymo ir atkūrimo planus yra svarbus žingsnis siekiant sušvelninti kibernetinio saugumo pažeidimo padarinius ir kuo greičiau atkurti įprastą verslo veiklą. Atsparumo didinimas apima investicijas į technologijas, procesus ir žmogiškuosius išteklius, siekiant sumažinti galimų incidentų, kurie gali įvykti ateityje, poveikį.

Kibernetinio saugumo neįmanoma užtikrinti be glaudaus daugelio įmonės padalinių, taip pat partnerių ir reguliavimo agentūrų bendradarbiavimo.

Apskritai kibernetinio saugumo idėja ir pagrindiniai principai, kuriais ji grindžiama, yra esminiai įmonių gebėjimo apsaugoti savo informaciją ir infrastruktūrą nuo vis sudėtingesnių kibernetinių atakų elementai. Norint veiksmingai valdyti kibernetinį saugumą, reikia laikytis visapusiško požiūrio,

apimančio ne tik technines ir organizacines atsargumo priemones, bet ir teisines apsaugos priemones bei darbuotojų švietimo ir sąmoningumo ugdymo programas. (Agafonov, 2021)

1.2. DDoS atakų teorinė apžvalga

1.2.1. DDoS atakų samprata

DDoS (angl. Distributed Denial of Service) atakos - tai piktavališki veiksmai, kai keli kompiuteriai, vadinamieji botnetai, naudoja bendrus išteklius, kad užvaldytų tikslinę sistemą ar tinklą ir priverstų jį tapti neprieinamu arba nereaguoti į teisėtus naudotojus (Zargar, 2013). Šios atakos formuojamos išnaudojant pažeidžiamas sistemas, pavyzdžiui, nesaugius daiktų interneto (IoT) įrenginius arba kenkėjiškomis programomis užkrėstus kompiuterius, siekiant surengti koordinuotą ataką prieš taikinį (Kreutz, 2015). DDoS išpuoliai gali turėti didelių pasekmių, įskaitant piniginius nuostolius, žalą reputacijai ir naudotojų pasitikėjimo sumažėjimą (Alrwais, 2016). Užpuolikas bando į sistemą, tinklą ar paslaugą siųsti tiek daug duomenų srauto, kad ji nepajėgtų apdoroti galiojančių užklausų. DDoS atakos gali turėti rimtų pasekmių, įskaitant paslaugų teikimo sutrikimus, finansinius nuostolius ir žalą reputacijai. Šioje teorinėje DDoS atakų apžvalgoje bus aptariamos pagrindinės sąvokos, įvairių tipų DDoS atakos ir paplitę jų mažinimo būdai.

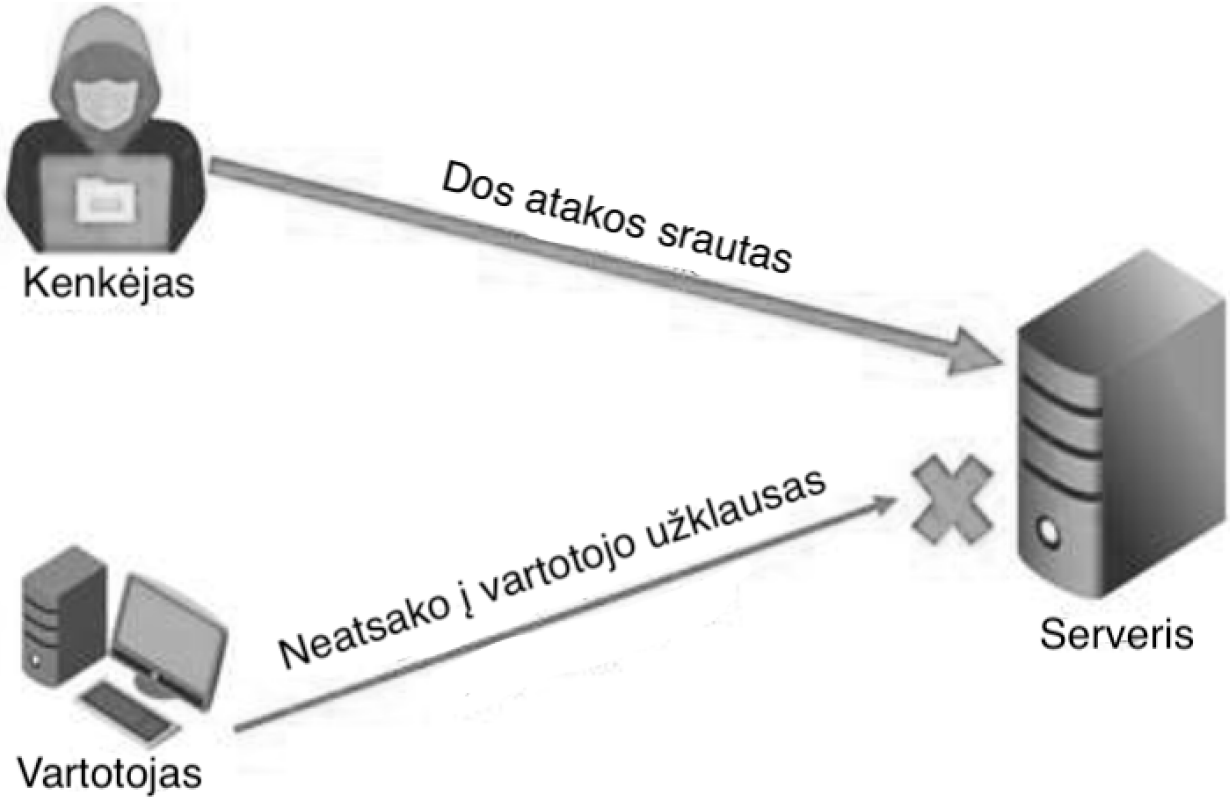
Pagrindinės sąvokos: DDoS atakoms būdingas duomenų srauto antplūdis, dėl kurio perkraunami tikslinės sistemos ištekliai, todėl ji sutrinka arba praranda reakciją. Užpuolikai dažnai naudoja botnetus - didelius užkrėstų įrenginių tinklus, kurie generuoja ir nukreipia srautą į taikinį. Kai kurioms DDoS atakoms sustiprinti naudojami stiprinimo būdai, kuriais pasinaudojant silpnais protokolais ar sistemomis sustiprinamas jų poveikis.

1.2.2. DDoS atakų rūšys

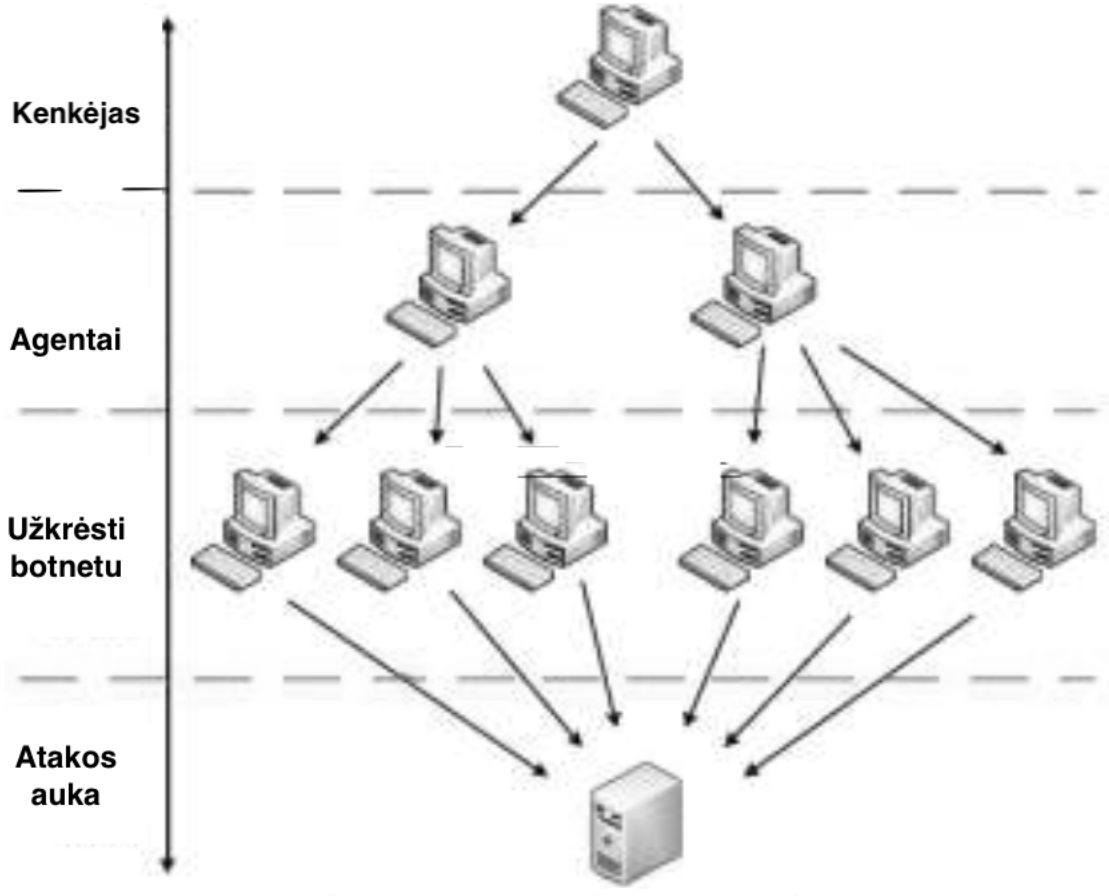
Iš įvairių internetinių atakų, keliančių grėsmę IT saugumui, didžiausią žalą daro atsisakymas teikti paslaugas (DoS) ir paskirstytas atsisakymas teikti paslaugas (DDoS). Be to, pastaruoju metu saugumo specialistams tenka daryti didžiulį spaudimą kuriant veiksmingas gynybos strategijas. DoS atakos gali būti vykdomos naudojant įvairius protokolus ir įrankius ir pradedamos iš įvairių OSI modelio sluoksnių. Šiame straipsnyje išsamiai apibrėžiamos DoS ir DDoS atakos ir paaiškinama, kaip įvairių tipų atakos gali būti įgyvendinamos ir paleidžiamos iš skirtingų OSI modelio sluoksnių. Jame siūloma giliau suprasti

šiuos vis dažniau pasitaikančius reiškinius, kad būtų galima sukurti veiksmingesnes atsakomąsias priemones (Hadeel, 2022).

2 pav. Dos atakos tipas



3 pav. DDos atakos tipas



DDoS atakų rūšys:

1. Užtvindymo atakos: Šių atakų tikslas - perkrauti taikinio pralaidumą siunčiant į jį didžiulius srautus. UDP ir ICMP protokolai yra užtvindymo pavyzdžiai.
2. Protokolų pagrindu vykdomos srautų atakos: Šios atakos naudoja protokolų pažeidžiamumą, kad išeikvotų tinklo išteklius ir sutrikdytų paslaugų teikimą. Du pavyzdžiai - SYN flood, kai išnaudojama TCP protokolų perdavimo procedūra, ir Ping of Death atakos, kai išnaudojamas ICMP protokolas.
3. Aplikacijų lygmens atakos: Šios atakos išnaudoja pažeidžiamumus arba išeikvoja sistemos išteklius, kad būtų nukreiptos į konkrečias taikomąsias programas ar paslaugas, veikiančias tikslinėje sistemoje. Pavyzdžiai peteikiami 1 letelėje.

1 Lentelė. Aplikacijų lygmuo (OSI) su galimų Dos/DDoS atakų tipais ir aptakų aprašymas tam tikrose sluoksniuos.

OSI sluoksnis	**Galimos Dos/DDOS atakos**	**Atakų aprašymas**

Taikymo	HTTP POST ir GET	Nukreipia didelį kiekį neteisėtų HTTP užklausų į serverį, sukuriant didelę apkrovą ir užkertant kelią teisėtoms užklausoms.
Pateikimas	Neformalūs SSL užklausos	Siunčia sugadintas SSL/TLS užklausas į serverį, siekiant sukelti klaidas ir perpildyti išteklius.
Seansas	Telnet DDOS	Naudoja Telnet protokolą, kad sukurtų daug neteisėtų seansų su serveriu, kuris pereikvoja sistemos išteklius ir gali sutrikdyti paslaugų teikimą.
Perdavimas	Smurf, SYN paketų srautas	Smurf ataka naudoja padirbtus ICMP paketus, o SYN srautas naudoja padirbtus SYN paketus, siekdami sukurti srautų ataką ir užkirsti kelią teisėtoms užklausoms vartotojui.
Tinklo	ICMP paketų srautas	Siunčia milžinišką kiekį neteisėtų ICMP paketų į serverį, sukeliant tinklo perdavimo perteklių ir trukdžius.
Duomenų ryšio	MAC paketų srautas	Perpildo komutatoriaus MAC adresų lentelę nukreipdami didelį kiekį padirbtų MAC adresų paketų, kurie trukdo normaliam tinklo veikimui.
Fizinis	Fizinio turto gedimai	Sutrikdo fizinį įrangos veikimą arba pertraukia ryšį, pvz., pertraukiant laidus, sugadinant įrenginius arba pakenkiant energetinėms sistemoms, siekiant nutraukti paslaugų teikimą.

1.3 DDoS atakų apsaugos technologijos

Apsaugai nuo įvairių DDoS atakų yra sukurta veiksmingų ir efektyvių technologijų. Tarp jų yra įsilaužimo aptikimo sistemos (IDS) ir įsilaužimo prevencijos sistemos (IPS), kurios stebi tinklo srautą ieškodamos DDoS atakų požymių ir automatiškai blokuoja arba filtruoja kenkėjišką srautą (Kumar, 2015). Taip pat yra srauto filtravimo ir greičio ribojimo technikos, kurios gali padėti nustatyti ir blokuoti kenkėjišką srautą, o teisėtą srautą praleisti (Zargar, 2013). Yra keletas technologijų, skirtų DDoS atakų prevencijai ir aptikimui, tarp jų:

- Rūšiavimo sienos (Rate Limiting) – srauto apribojimas, kuris leidžia nustatyti ateinančio srauto intensyvumą ir apribojimus. Viršijus leistiną ribą
- Aukšto balasto DNS (Highly Anycast DNS) – turint šią paslaugą serveriai yra pasiekiami net esant didelėms DDoS atakoms dėl daugybę geografiškai nutolusių DNS serverių;
- Įsilaužimo prevencijos sistemos (Intrusion Prevention System arba IPS) - įsilaužimo prevencijos sistemos. Ši sistema pasaugo nuo įsilaužimo į tinklą ir veikia analizuodama duomenų srautus. Nustačius įtartiną veiklą yra blokuojami srautai ir taip užtikrinamas tinklo saugumas.
- Įsilaužimo aptikimo sistemos (Intrusion Detection System arba IDS) - įsilaužimo aptikimo saugumo mechanizmas. Taip pat yra stebimi srautai, o jeigu aptinkamas bandymas įsilaužti į tinklą yra informuojamas administratorius, kad galėtų imtis veiksmų saugumui užtikrinti

Taip pat, svarbu turėti veiklos testinumo planą, kuriame būtų numatytos DDoS atakų apsaugos procedūros, incidentų valdymas ir atkūrimo veiksmai.

DDoS atakų aptikimas ir mažinimas realiuoju laiku naudojant mašininio mokymosi ir dirbtinio intelekto algoritmus (Jazi, 2017). Tinklo perteklius ir išteklių paskirstymas, kurie gali padėti užtikrinti, kad tikslinė sistema būtų pasiekiama net ir intensyvios atakos metu, gali padėti išlaikyti sistemą prisijungusią (Mirkovic, 2004). Kelios organizacijos dalijasi informacija apie vykstančius išpuolius ir koordinuoja savo atsakomuosius veiksmus vykdydamos bendras gynybos strategijas (Alrwais, 2016).

Apsaugos nuo DDoS atakų technologijų tobulinimas ir plėtra yra nuolatinis procesas, kadangi atakų metodai nuolat vystosi ir tampa sudėtingesni. Mokslininkai ir inžinieriai nuolat tyrinėja naujus būdus, kaip geriau apsaugoti sistemas nuo šių išpuolių, įskaitant naujų algoritmų, metodų ir technologijų kūrimą. Todėl svarbu nuolat stebėti DDoS atakų plėtrą ir mokytis iš pastarųjų atvejų, kad būtų galima kuo veiksmingiau apsaugoti savo sistemas ir infrastruktūrą nuo šių grėsmių.

Prevencijos būdai:

1. Perteklinis srauto rezervavimas: Vienas iš apsaugos nuo DDoS atakų būdų - užtikrinti, kad tikslinė sistema turėtų pakankamai išteklių ir pralaidumo, kad galėtų susidoroti su staigiais duomenų srauto šuoliais.

2. Srauto filtravimas: Kenkėjišką srautą galima nustatyti ir blokuoti prieš jam pasiekiant tikslinę sistemą taikant srauto filtravimo metodus. Tokių priemonių pavyzdžiai - nuodugnus paketų tikrinimas, IP filtravimas ir spartos ribojimas.
3. Turinio pristatymo tinklai (CDN): Tolygiai paskirstydami apkrovą keliems serveriams, turinio pristatymo tinklai (CDN) sumažina tikimybę, kad viena ataka užvaldys taikinį.
4. Įsilaužimo aptikimo ir prevencijos sistemos (IDPS): Šios priemonės stebi tinklo srautą ieškodamos kenkėjiškos veiklos požymių ir automatiškai blokuoja arba sumažina atakas realiuoju laiku.
5. DDoS poveikio mažinimo paslaugos: Šios paslaugos siūlo specializuotus metodus DDoS atakoms nustatyti ir atremti, paprastai nukreipdamos srautą per savo infrastruktūrą ir pašalindamos kenkėjišką srautą.

1.4. Kibernetinio saugumo programų Lietuvoje teisinis reglamentavimas

Remiantis Lietuvos kibernetinio saugumo politikos teisine baze ir šaltiniu "Kibernetinio saugumo mėnuo 2022" (https://kam.lt/kibernetinio-saugumo-menuo-2022/), kuriame pateikiama bendra informacija apie Lietuvos kibernetinio saugumo politikos gaires, nustatytos atsakingos institucijos ir subjektai. Pavyzdžiui, Lietuvos Respublikos Vyriausybė, tvirtindama ilgalaikius planus ar programas, nustato pirmines kibernetinio saugumo politikos gaires.

Krašto apsaugos ministerija yra atsakinga už kibernetinį saugumą reglamentuojančių teisės aktų, pavyzdžiui, Kibernetinio saugumo įstatymo, rengimą.

Kibernetinio saugumo taryba, sudaryta iš akademinės bendruomenės, viešojo ir privataus sektoriaus atstovų, teikia Krašto apsaugos ministerijai rekomendacijas ir pasiūlymus.

Krašto apsaugos ministerijos parengtų teisės aktų įgyvendinimą užtikrina Nacionalinio kibernetinio saugumo centro (atsakingo už kibernetinių incidentų valdymą Lietuvoje), Lietuvos policijos (atsakingos už kibernetinių nusikaltimų prevenciją, tyrimą ir užkardymą) ir Valstybinės duomenų apsaugos inspekcijos (atsakingos už kibernetinių incidentų, susijusių su asmens duomenų saugumo pažeidimais, tyrimą) bendradarbiavimas. Šios institucijos dalijasi informacija apie kibernetinių incidentų tendencijas ir grėsmes.

Lietuvoje kibernetinio saugumo subjektai apima tiek viešąsias, tiek privačias institucijas. Jos privalo įgyvendinti kibernetinį saugumą reglamentuojančių teisės aktų reikalavimus, įskaitant periodinį informacinių sistemų rizikos vertinimą, kibernetinio saugumo politikos ir jos įgyvendinimo dokumentų patvirtinimą bei tinkamų techninių saugumo priemonių įgyvendinimą. Administracinių nusižengimų kodekse numatytos nuobaudos už taikomų reikalavimų nesilaikymą kibernetinio saugumo subjektams.

Toliau pateiktoje lentelėje pateikiama informacija apie pagrindinius Lietuvos kibernetinio saugumo dalyvius, jų vaidmenis ir užduotis:

- Vyriausybė - nustato kibernetinio saugumo politikos gaires ir tvirtina ilgalaikius planus bei programas.
- Krašto apsaugos ministerija - rengia kibernetinio saugumo teisės aktus, pvz.
- Kibernetinio saugumo taryba - padeda Krašto apsaugos ministerijai teikdama rekomendacijas ir pasiūlymus.
- Nacionalinis kibernetinio saugumo centras - užtikrina teisės aktų įgyvendinimą ir valdo kibernetinius incidentus visoje Lietuvoje.
- Lietuvos policija - atsakinga už kibernetinių nusikaltimų prevenciją, tyrimą ir užkardymą.
- Valstybinė duomenų apsaugos inspekcija - tiria kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais.

- Kibernetinio saugumo subjektai - valstybės institucijos ir privačios organizacijos, įgyvendinančios kibernetinį saugumą reglamentuojančių teisės aktų reikalavimus, atliekančios rizikos vertinimą ir įgyvendinančios technines saugumo priemones. Už reikalavimų nesilaikymą baudžiama baudomis pagal Administracinių nusižengimų kodeksą.

2 lentele. Kibernetinio saugumo architektūra Lietuvoje.

Institucija / Organizacija	**Funkcija / Užduotis**
Vyriausybė	Nubrėžia svarbiausias Lietuvos kibernetinio saugumo politikos gaires, tvirtina ilgalaikius planus ir programas.
Krašto apsaugos ministerija	Rengia kibernetinio saugumo sritį reguliuojančius teisės aktus, pavyzdžiui, Kibernetinio saugumo įstatymą.
Kibernetinio saugumo taryba	Padeda Krašto apsaugos ministerijai savo rekomendacijomis ir pasiūlymais. Sudaryta iš mokslo, viešojo ir privataus sektorių atstovų.
Nacionalinis kibernetinio saugumo centras	Užtikrina Krašto apsaugos ministerijos parengtų teisės aktų įgyvendinimą. Atsakingas už kibernetinių incidentų valdymą visoje Lietuvoje.
Lietuvos policija	Atsakinga už kibernetinių nusikaltimų užkardymą, tyrimą ir prevenciją. Bendradarbiauja su kitomis institucijomis ir dalijasi informacija apie kibernetinių incidentų tendencijas ir grėsmes.
Valstybinė duomenų apsaugos inspekcija	Tiria kibernetinius incidentus, susijusius su asmens duomenų pažeidimais. Bendradarbiauja su kitomis institucijomis ir dalijasi informacija apie kibernetinių incidentų tendencijas ir grėsmes.
Kibernetinio saugumo subjektai	Lietuvoje veikiančios valstybės institucijos ir privačios organizacijos. Įgyvendina kibernetinio saugumo teisės aktų reikalavimus, atlieka informacinių sistemų rizikos vertinimą, pasitvirtina kibernetinio saugumo politikos ir įgyvendinimo dokumentus, įgyvendina technines saugumo priemones. Už nustatytų kibernetinio saugumo reikalavimų nevykdymą taikomos baudos pagal Administracinių nusižengimų kodeksą.

Šiame skyriuje nagrinėjama teisinė bazė, reglamentuojanti kibernetinio saugumo programas Lietuvoje, kuriomis siekiama apsaugoti skaitmeninį turinį nuo DDoS atakų. Svarbu suvokti taikomus teisės aktus, atsakingas institucijas ir jų vaidmenis šioje srityje.

Lietuvoje kibernetinio saugumo teisinę sistemą sudaro šie pagrindiniai teisiniai dokumentai ir taisyklės:

- Lietuvos Respublikos kibernetinio saugumo įstatymas (2018, Nr. XII-1428) reglamentuoja pagrindinius kibernetinio saugumo principus ir apibrėžia už kibernetinį saugumą atsakingas institucijas ir funkcijas.
- Nacionalinė kibernetinio saugumo strategija (2018, Nr. 13252) nustato pagrindinius kibernetinio saugumo tikslus, prioritetus, uždavinius ir veiksmų planą.
- Nacionalinis kibernetinių incidentų valdymo planas 2018, Nr. 13252) kuriame aprašomos valstybės ir organizacijų funkcijos ir atsakomybė, susijusios su kibernetinių incidentų prevencija, aptikimu, reagavimu ir atkūrimu, atsakingos institucijos ir jų pareigos

Apibendrinant įstatymine bazė pagrindinės institucijos, atsakingos už kibernetinio saugumo politikos įgyvendinimą Lietuvoje, yra šios:

- Nacionalinė kibernetinio saugumo centras kuris koordinuoja kibernetinio saugumo politiką ir priima sprendimus dėl kibernetinio saugumo strategijos įgyvendinimo.
- Nacionalinė kibernetinio saugumo centras ir kibernetinio saugumo kompetencijos centras atsakingas už kibernetinių incidentų valdymą, grėsmių ir atakų analizę ir koordinavimą su kitomis institucijomis.

Apsaugos nuo DDoS atakų Lietuvos kibernetinio saugumo programų teisinė struktūra apima apsaugą nuo DDoS atakų. Pagrindiniai su šia tema susiję dokumentai yra šie:

Nacionalinė kibernetinio saugumo centras [2] yra svarbus dokumentas, nustatantis kibernetinio saugumo politikos kryptį Lietuvoje. Strategijoje nurodomi pagrindiniai šalies kibernetinio saugumo tikslai, prioritetai, uždaviniai ir veiksmų planas. Strategijoje, be kita ko, aptariamos infrastruktūros apsaugos nuo kibernetinių atakų, įskaitant DDoS atakas, stiprinimo priemonės. Nacionalinė kibernetinio saugumo strategija padeda koordinuoti valstybės institucijų, organizacijų ir kitų suinteresuotųjų subjektų veiksmus siekiant užtikrinti skaitmeninio turinio saugumą ir prieinamumą.

Nacionalinė kibernetinio saugumo strategija [2] rodo Lietuvos Vyriausybės įsipareigojimą užtikrinti veiksmingą skaitmeninio turinio apsaugą ir stiprinti kibernetinį saugumą šalyje. Strategijoje taip pat pabrėžiama nacionalinio kibernetinio saugumo sektoriaus stiprinimo svarba siekiant veiksmingai kovoti su DDoS atakomis ir kitomis kibernetinėmis grėsmėmis.

Strategijos įgyvendinimas apima šiuos svarbius kriterijus:

Šiame etape valdžios institucijos rengia ir koordinuoja kibernetinio saugumo politikos dokumentų, pavyzdžiui, strategijų, planų ir rekomendacijų, įgyvendinimą.

Šiame etape įgyvendinamos prevencinės priemonės, kuriomis siekiama užkirsti kelią kibernetinėms atakoms, pavyzdžiui, DDoS atakoms, diegiant naujas technologijas, apsaugos mechanizmus ir pramonės standartus.

Kibernetinių incidentų valdymas: Šiame etape parengiamos procedūros ir gairės, kaip valdžios institucijos ir organizacijos turėtų reaguoti į kibernetinius incidentus, pavyzdžiui, DDoS atakas. Svarbūs šio etapo komponentai yra aptikimas, reagavimas, atkūrimas ir prevencinių priemonių tobulinimas.

Švietimas, mokymas ir gebėjimų stiprinimas: Kibernetinio saugumo švietimas ir informuotumo didinimas yra esminiai sėkmingo kibernetinio saugumo įgyvendinimo komponentai. Labai svarbu šviesti visuomenę, įmones ir institucijas apie kibernetinio saugumo svarbą ir skatinti kibernetinio saugumo kompetencijų ugdymą.

Kibernetinis saugumas yra pasaulinio masto problema, todėl būtina stiprinti tarptautinį bendradarbiavimą šioje srityje. Lietuva dalyvauja įvairiose tarptautinėse iniciatyvose ir projektuose, kuriais siekiama stiprinti kibernetinio saugumo politiką.

Nacionalinė kibernetinio saugumo strategija - tai Lietuvos Vyriausybės sukurtas dokumentas, kuriame apibrėžti šalies kibernetinio saugumo tikslai, principai ir veiksmai, kuriais siekiama apsaugoti šalies informacines sistemas, infrastruktūrą ir skaitmeninius išteklius. Strategijoje atsispindi valstybės kibernetinio saugumo prioritetai ir numatytos konkrečios priemonės, kaip šiuos prioritetus veiksmingai įgyvendinti.

Nacionalinė kibernetinio saugumo strategija grindžiama toliau išvardytais pagrindiniais principais:

- Prevencija. Labai svarbu užkirsti kelią kibernetinėms grėsmėms taikant nuoseklias ir veiksmingas prevencines priemones, pavyzdžiui, technologines naujoves, apsaugos mechanizmus, standartus ir gaires.
- Atsparumas. Lietuvos informacinės sistemos, infrastruktūra ir skaitmeniniai ištekliai turi būti atsparūs kibernetinėms grėsmėms ir gebėti greitai atsigauti po jų poveikio.
- Bendradarbiavimas. Veiksmingas kibernetinio saugumo įgyvendinimas reikalauja glaudaus valdžios institucijų, privataus sektoriaus, mokslo institucijų ir plačiosios visuomenės bendradarbiavimo. Kibernetinis saugumas yra globali problema, todėl būtina stiprinti tarptautinį bendradarbiavimą ir dalyvauti daugelyje tarptautinių iniciatyvų, siekiant užtikrinti saugią kibernetinės erdvės plėtrą.
- Mokymas. Švietimas ir gebėjimų stiprinimas kibernetinio saugumo švietimas ir informuotumo didinimas yra esminiai sėkmingo kibernetinio saugumo įgyvendinimo komponentai. Labai svarbu šviesti visuomenę, įmones ir institucijas apie kibernetinio saugumo svarbą ir skatinti kibernetinio saugumo kompetencijų ugdymą.

Nacionalinėje kibernetinio saugumo strategijoje nurodytos priemonės ir veiksmai, kurių imtasi šiems principams įgyvendinti, įskaitant politikos formavimą, prevenciją ir apsaugą, kibernetinių incidentų valdymą, švietimą, mokymą, kompetencijų ugdymą ir tarptautinį bendradarbiavimą. Toliau pateikiame keletą svarbiausių veiksmų ir priemonių.

Vyriausybė rengia ir koordinuoja kibernetinio saugumo politikos dokumentus, įskaitant strategijas, planus, rekomendacijas ir įstatymus. Taip užtikrinamas visapusiškas ir nuoseklus požiūris į kibernetinį saugumą:

- Prevencija ir apsauga - Siekiant užkirsti kelią kibernetinėms grėsmėms, įgyvendinamos prevencinės priemonės, pavyzdžiui, technologinės naujovės, apsaugos mechanizmai, standartai ir gairės. Tai apima investicijas į infrastruktūros atsparumo kūrimą ir kibernetinio saugumo technologijų diegimą.
- Kibernetinių incidentų valdymas - Kuriamos procedūros ir gairės, kaip valdžios institucijos ir organizacijos turėtų reaguoti į kibernetinius incidentus. Svarbūs šio etapo komponentai yra aptikimas, reagavimas, atkūrimas ir prevencinių priemonių stiprinimas. Tai apima bendradarbiavimą su nacionaliniais ir tarptautiniais partneriais siekiant greitai ir veiksmingai reaguoti į incidentus.
- Švietimas, mokymas ir gebėjimų stiprinimas - Siekiant veiksmingai įgyvendinti kibernetinį saugumą, būtina šviesti visuomenę, įmones ir institucijas apie kibernetinio saugumo svarbą. Tai apima informacinių kampanijų organizavimą, mokymų rengimą, švietimo programų kūrimą ir profesinių kompetencijų ugdymą.

Kibernetiniam saugumui gerinti labai svarbu dalyvauti tarptautinėse iniciatyvose, projektuose ir bendradarbiavimo programose. Tai apima bendradarbiavimą kibernetinio saugumo srityje su Europos Sąjunga, NATO ir kitomis tarptautinėmis organizacijomis, taip pat glaudžius ryšius su kitomis valstybėmis.

Nacionalinė kibernetinio saugumo strategijos yra veiksmingos kibernetinio saugumo strategijos pagrindas siekiant užtikrinti vyriausybės, privataus sektoriaus, mokslo institucijų ir pilietinės visuomenės bendradarbiavimą. Strategijoje ne tik pabrėžiama nacionalinio kibernetinio saugumo sektoriaus stiprinimo svarba, bet ir skatinama dalyvauti tarptautinėse kibernetinio saugumo iniciatyvose.

Įgyvendindama Nacionalinę kibernetinio saugumo strategiją, Lietuva siekia apsaugoti savo piliečių, įmonių ir valstybės institucijų skaitmeninę erdvę nuo kibernetinių grėsmių ir prisidėti prie pasaulinio kibernetinio saugumo gerinimo. Sėkmingas Strategijos įgyvendinimas leis Lietuvai pasiekti aukštesnį kibernetinio saugumo lygį, taip didinant šalies ekonominį konkurencingumą, užtikrinant nacionalinį saugumą ir skatinant visuomenės pasitikėjimą skaitmeninėmis technologijomis.

2. SKAITMENINIO TURINIO APSAUGA NUO DDOS ATAKŲ TELIA LIETUVA ĮMONĖJE

Telia Lietuva yra viena iš pirmaujančių telekomunikacijų įmonių Lietuvoje, teikianti interneto, televizijos, ryšio ir kitas paslaugas tiek privatiems, tiek verslo klientams. Dėl nuolat augančio skaitmeninio turinio svarbos bei kibernetinių grėsmių, tokių kaip DDoS atakos, įmonė yra įsipareigojusi užtikrinti aukšto lygio kibernetinį saugumą savo klientams.

DDoS atakos yra vienas iš labiausiai paplitusių ir kenksmingų kibernetinių nusikaltimų tipų, kurio metu užpultas tinklas ar serveris yra perkraunamas didžiuliu kiekiu netikrų užklausų, taip sutrikdydamas normalią veiklą ir prieigą prie skaitmeninio turinio. (Zargar, 2013). Telia Lietuva siekia apsaugoti savo klientų skaitmeninį turinį nuo šių atakų ir užtikrinti tinklo stabilumą, prieinamumą bei saugumą.

Toliau aprašomi keli pagrindiniai Telia Lietuva veiksmai skaitmeninio turinio apsaugai nuo DDoS atakų:

1. Prevencija: Telia Lietuva įdiegia ir nuolat atnaujina savo tinklo infrastruktūrą bei apsaugos priemones, siekdama užkirsti kelią DDoS atakoms dar prieš jas įvykdant. Tai apima įvairius filtravimo mechanizmus, tinklo segmentavimą ir kitus techninius sprendimus.
2. DDoS atakų aptikimas ir monitoringas: Telia Lietuva naudoja pažangias stebėjimo ir analizės sistemas, kurios padeda aptikti ir įvertinti galimas grėsmes realiu laiku. Tai leidžia reaguoti į atakas greitai ir efektyviai.
3. Incidentų valdymas: Esant DDoS atakai, Telia Lietuva turi paruoštą incidentų valdymo planą, kuris apima komunikaciją su klientais, atakos šaltinio identifikavimą, atakos pasekmių šalinimą ir atkūrimo veiksmus.
4. Klientų švietimas ir konsultavimas: Telia Lietuva teikia informaciją ir rekomendacijas savo klientams apie DDoS atakų prevenciją, apsaugą bei elgesį atakos metu. Tai apima klientų mokymus, renginius, seminarus, taip pat konsultacijas su klientais apie jų specifines situacijas ir galimus saugumo sprendimus.
5. Bendradarbiavimas su kitomis organizacijomis ir institucijomis: Telia Lietuva bendradarbiauja su kitomis telekomunikacijų įmonėmis, saugumo bendrovėmis, valdžios institucijomis ir tarptautinėmis organizacijomis, siekdama keistis informacija apie grėsmes, atakų tendencijas ir geriausias praktikas DDoS atakų prevencijai bei apsaugai.

Šie veiksmai padeda Telia Lietuva įmonėje užtikrinti aukštą skaitmeninio turinio apsaugos nuo DDoS atakų lygį. Tačiau svarbu pripažinti, kad DDoS atakos yra nuolat kintantis ir tobulėjantis fenomenas, todėl Telia Lietuva turi būti pasirengusi prisitaikyti prie naujų grėsmių ir toliau tobulinti savo apsaugos priemones, siekdama užtikrinti klientų skaitmeninio turinio saugumą ir prieinamumą.

2.1. Tyrimo metodologija

Darbo tyrimo metodologija grindžiama kokybiniu tyrimu, kurio pagrindiniai metodai yra fokus grupės ir atvejo analizės pusiau struktūrizuotas interviu. Kokybinis tyrimas buvo pasirinktas siekiant gauti gilesnį supratimą apie Telia Lietuva klientų nuomonę, jų patirtį susijusią su DDoS atakų prevencija, apsauga galimais tobulinimo būdais. Šios metodologijos pasirinkimas leidžia įvertinti ir aptarti skirtingas nuomones, taip pat gauti kokybišką informaciją, kuri gali būti naudinga tolesnei analizei ir tobulinimui.

Fokus grupės metodas: Šiame etape buvo atlikti pusiau struktūrizuoti interviu su Telia Lietuva klientais, siekiant gauti informaciją apie jų patirtį, nuomonę ir lūkesčius susijusius su DDoS atakų prevencija, apsauga bei galimais tobulinimo būdais. Fokus grupės metodas leido atlikti kokybišką tyrimą, kuriame dalyvavo skirtingų sričių klientai, susidūrę su skirtingais DDoS atakų aspektais.

Atvejo analizė – pusiau strūkturizuotas interviu su dviem ekspertais. Atvejo analizės metu buvo diskutuojama su dviem Telia Lietuva darbuotojais - tinklo inžinieriais, kurie atsakingi už DDoS atakų apsaugos priemonių diegimą ir palaikymą. Šie interviu leido gauti išsamų ir praktišką žinių apie esamas apsaugos priemones, jų veiksmingumą ir galimus tobulinimo būdus.

Tyrimo duomenys buvo analizuoti naudojant kokybinės analizės metodus, tokius kaip turinio analizė ir kodavimas. Duomenų analizė leido identifikuoti pagrindines problemas, tendencijas bei galimus tobulinimo būdus. Remiantis gautais rezultatais, buvo parengtos rekomendacijos ir išvados, skirtos DDoS atakų apsaugos priemonių tobulinimui Telia Lietuva įmonėje.

Tyrimo tikslingumo pagrindimas: Tyrimo tikslingumas yra pagrįstas tuo, kad DDoS atakų plitimas yra didelė problema visame pasaulyje, o šiuolaikinėje informacinėje visuomenėje ši problema tampa vis labiau aktualia. Dėl DDoS atakų prevencijos, aptikimo ir valdymo priemonių poreikio, būtina toliau tyrinėti ir kurti naujas apsaugos strategijas, kad būtų užtikrintas sklandus interneto veikimas.

Šis tyrimas yra tikslingas, nes jis siekia išsiaiškinti, kaip Telia Lietuva įmonė reaguoja į DDos atakas, kokį mastą ir poveikį jos sukelia, bei kokios apsaugos priemonės yra taikomos šioje konkrečioje įmonėje. Atsižvelgiant į minėtus autorius, šis tyrimas prisidės prie esamos mokslinės literatūros apie DDos atakas, padėsiantis įvertinti esamą situaciją ir galimus sprendimo būdus šioje srityje.

Be to, šis tyrimas yra svarbus norint suprasti DDoS atakų dinamiką ir rasti efektyvius būdus, kaip mažinti jų poveikį. Atliekant šį tyrimą, galime geriau suprasti DDoS atakų mechanizmus, jų plitimo tendencijas, taip pat tobulinti esamas ir kurti naujas apsaugos priemones. Taip pat šis tyrimas gali būti naudingas ne tik Telia Lietuva įmonei, bet ir kitoms telekomunikacijų įmonėms, susiduriančioms su panašiomis problemomis. Tai leis įmonėms geriau suprasti DDos atakų pavojus, poveikį verslui.

Tyrimo problema: Kokias technologijas ir strategijas galima taikyti efektyviai kovojant su DDoS atakomis ir kaip organizacijos gali bendradarbiauti šioje kovoje?

Tyrimo tikslas: Išsiaiškinti, kaip naujos technologijos ir bendradarbiavimas tarp organizacijų gali prisidėti prie efektyvios DDoS atakų prevencijos ir mažinimo.

Tyrimo uždaviniai:

1. Išanalizuoti DDoS atakų pobūdį ir jų keliamą grėsmę organizacijoms.
2. Aptarti, kaip naujos technologijos, tokios kaip dirbtinis intelektas ir debesų kompiuterija, gali padėti kovoti su DDoS atakomis.
3. Išanalizuoti, kaip tarporganizacinis bendradarbiavimas gali prisidėti prie DDoS atakų prevencijos ir mažinimo.
4. Pateikti rekomendacijas organizacijoms, kaip geriau apsisaugoti nuo DDoS atakų.

Tyrimo metodika: Šis tyrimas bus atliekamas kobinuotas tyrimas remiantis literatūros analize, fokus grupės apklausa ir pusiau struktūruotu interviu su Telia Lietuva ekspertais, kurie turi įtaką DDoS atakų prevencijai ir mažinimui.

Šio tyrimo metu bus identifikuotos technologijos ir strategijos, skirtos DDoS atakų prevencijai ir mažinimui, bei rekomendacijos, kaip organizacijos gali geriau apsisaugoti nuo šių atakų. Tyrimo struktūra pavaizduota 3 lentelėje.

3 lentelė. Tyrimo struktūrą

Tyrimo etapai	**Dimensija**	**Tyrimo kriterijai**	**Tyrimo metodai**
1-as etapas: Telia klientų nuomonės analizė	DDoS atakų poveikis skaitmeninio turinio prieinamumui	Klientų supratimas apie DDoS atakas, jų poveikį ir esamas apsaugos priemones	Fokus grupės apklausa su Telia klientais
2-as etapas: Ekspertų įžvalgų analizė	Efektyvios DDoS atakų prevencijos ir apsaugos strategijos	Ekspertų rekomendacijos, atpažinimo ir švelninimo strategijos, bendradarbiavimo svarba, naujų technologijų naudojimas	Pusiau struktūrizuoto interviu, atvejo analizės su dviem Telia ekspertais
3-ias etapas: Rekomendacijų ir išvadų formulavimas	DDoS atakų prevencijos ir	Klientų ir ekspertų nuomonės, galimi sprendimai,	Duomenų analizė ir sintezė, rekomendacijų ir

	apsaugos priemonių tobulinimas	tobulinimo galimybės	išvadų formulavimas

Tyrimo struktūrą:

1-as etapas: Telia klientų nuomonės analizė

1. Dimensija: DDoS atakų poveikis skaitmeninio turinio prieinamumui
2. Tyrimo kriterijai: klientų supratimas apie DDoS atakas, jų poveikį ir esamas apsaugos priemones
3. Tyrimo metodai: pusiau struktūrizuoti interviu su Telia klientais

2-as etapas: Ekspertų įžvalgų analizė

1. Dimensija: Efektyvios DDoS atakų prevencijos ir apsaugos strategijos
2. Tyrimo kriterijai: ekspertų rekomendacijos, atpažinimo ir švelninimo strategijos, bendradarbiavimo svarba, naujų technologijų naudojimas
3. Tyrimo metodai: Atvejo analizė – pusiau strūkturizuotas interviu su dviem ekspertais su 2 Telai Lietuva ekspertais.

3-ias etapas: Rekomendacijų ir išvadų formulavimas

1. Dimensija: DDoS atakų prevencijos ir apsaugos priemonių tobulinimas
2. Tyrimo kriterijai: klientų ir ekspertų nuomonės, galimi sprendimai, tobulinimo galimybės
3. Tyrimo metodai: duomenų analizė ir sintezė, rekomendacijų ir išvadų formulavimas

Ši struktūra leis atlikti kokybinį kombinuotą tyrimą, kuriame bus įvertinta Telia klientų nuomonė apie DDoS atakų poveikį skaitmeninio turinio prieinamumui bei efektyvias prevencijos ir apsaugos priemones pagal ekspertų patirtį ir žinias. Remiantis gautais rezultatais, galėsite parengti rekomendacijas ir išvadas, kaip tobulinti DDoS atakų prevenciją ir apsaugą.

Tyrimo planas, skirtas DDoS atakų prevencijai ir apsaugai nuo jų telekomunikacijų bendrovių ir paslaugų teikėjų kontekste atvaizduojamas 4 lentelėje Pagrindinis tyrimo tikslas yra išanalizuoti DDoS atakų prevenciją ir apsaugą siekiant užtikrinti skaitmeninio turinio prieinamumą.

4 lentelė. Tyrimo planas

Darbo dalis	**Aprašymas**
Temos aktualumas ir naujumas	DDoS atakų prevencija ir apsauga siekiant užtikrinti skaitmeninio turinio prieinamumą yra nauja ir aktuali tema dėl didėjančio skaitmeninio turinio kiekio ir besikeičiančių atakų metodų.

Tyrimo problema	Kaip telekomunikacijų bendrovės ir paslaugų teikėjai gali veiksmingai apsisaugoti nuo DDoS atakų, kad užtikrintų skaitmeninio turinio prieinamumą ir kokybę?
Tyrimo objektas	DDoS atakų prevencija ir gynyba nuo jų siekiant užtikrinti skaitmeninio turinio prieinamumą.
Tyrimo tikslas	Išanalizuoti DDoS atakų prevenciją ir apsaugą nuo jų siekiant užtikrinti skaitmeninio turinio prieinamumą telekomunikacijų bendrovių ir paslaugų kontekste.
Tyrimo uždaviniai	1. Apžvelgti DDoS atakų kategorijas, metodus ir poveikį skaitmeninio turinio prieinamumui. 2. Pateikti DDoS atakų pavyzdžių ir jų pasekmių. 3. Išnagrinėti DDoS atakų prevencijos ir apsaugos strategijas ir priemones. 4. Atlikti tyrimą su Telia Lietuva įmonės klientais. 5. Atlikti atvejo analizė – pusiau strūkturizuota interviu su dviem ekspertais. 6. Pateikti rekomendacijas ir aptarkite ateities perspektyvas.

Tyrimo metodai, aprašyti šiame darbe, yra:

1. Literatūros analizė: metodas, skirtas išanalizuoti DDoS atakų sąvoką, tipus, metodus, poveikį skaitmeninio turinio prieinamumui, ir esamas prevencijos bei apsaugos strategijas, remiantis mokslinės literatūros, straipsnių, tyrimų ir ataskaitų apžvalga.
2. Kokybinis tyrimas - fokus grupės metodas: metodas, kuriuo siekiama gauti Telia klientų požiūrį, patirtį ir nuomones apie skaitmeninio turinio kibernetinį saugumą ir DDoS atakų prevenciją bei apsaugą per fokus grupės diskusiją su 7-8 dalyviais.
3. Atvejo analizė: pusiau struktūrizuotas interviu metodas, skirtas atlikti 2-3 atvejų analizę, susijusią su konkrečiais skaitmeninio turinio teikėjais ar platformomis, susidūrusiais su DDoS

atakomis, ir jų įgyvendintais apsaugos sprendimais, siekiant išsamiau suprasti praktinę DDoS atakų problemą ir efektyvius sprendimus.

Šie metodai bus naudojami tyrimui atlikti ir vertingai informacijai gauti, susijusiai su DDoS atakų prevencija ir apsauga skaitmeninio turinio teikėjų ir platformų kontekste. 5 lentelėje atvaizduojami paminėti tyrimo metodai.

5 lentelė. Tyrimo metodai

Tyrimo metodai	**Aprašymas**
Literatūros analizė	Išanalizuoti DDoS atakų sąvoką, tipus, metodus, poveikį skaitmeninio turinio prieinamumui ir esamas prevencijos bei apsaugos strategijas, remiantis mokslinės literatūros, straipsnių, tyrimų ir ataskaitų apžvalga.
Fokus grupės metodas	Atlikti fokus grupės diskusiją su 7-8 Telia Lietuva klientais, siekiant gauti jų požiūrį, patirtį ir nuomones apie skaitmeninio turinio kibernetinį saugumą ir DDoS atakų prevenciją bei apsaugą. Diskusija vyks remiantis diskusijos gairėmis, apimant pagrindinius temos aspektus.
Kokybinis tyrimas, pusiau struktūrizuotas inerviu	Atlikti dvieju ekspertu apklausa apie atvejų analizę, susijusią su konkrečiais skaitmeninio turinio teikėjais ar platformomis, susidūrusiais su DDoS atakomis, ir jų įgyvendintais apsaugos sprendimais.

Šie trys tyrimo metodai sudaro kombinuotą metodologiją, leidžiančią geriau suprasti ir įvertinti DDoS atakų problemą skaitmeninio turinio kontekste. Kombinuota metodologija padeda sumažinti atskirų metodų ribotumų poveikį ir gauti išsamesnę ir tikslesnę informaciją apie tiriamąją problemą. Tačiau būtina nuolat aktualizuoti mokslinę literatūrą ir praktinę patirtį, kad būtų galima gauti kuo tikslesnes ir išsamesnes išvadas apie DDoS atakų prevenciją ir apsaugą skaitmeninio turinio kontekste.

2.2. Kokybinio tyrimo rezultatų analizė

Šiame skyriuje pateikiama kokybinio tyrimo rezultatų analizė, kurios metu buvo taikytas fokus grupės metodas ir pusiau struktūrizuoto interviu metodo atvejo analizė. Tyrimo metu buvo diskutuojama su dviem Telia Lietuva tinklo inžinieriais, siekiant gauti išsamesnę informaciją apie DDoS atakų apsaugos priemones ir galimus tobulinimus.

Fokus grupės metodas:

Fokus grupės metodu buvo siekiama išsiaiškinti Telia Lietuva klientų nuomonę apie DDoS atakų apsaugos priemones bei jų patirtį susidūrus su šiomis atakomis. Buvo sudaryta fokus grupė, sudaryta iš Telia Lietuva klientų, kurie savo veikloje naudoja skaitmeninį turinį ir yra susidūrę su DDoS atakomis.

Fokus grupės metu buvo aptariamos šios temos:

1. Klientų patirtis susidūrus su DDoS atakomis;
2. Esamų DDoS atakų apsaugos priemonių veiksmingumas;
3. Galimi DDoS atakų apsaugos tobulinimo būdai.

Pusiau struktūrizuoto interviu metu buvo atlikti interviu su dviem Telia Lietuva tinklo inžinieriais. Šio tyrimo tikslas buvo gauti specialistų nuomonę apie DDoS atakų apsaugos priemones, jų veiksmingumą ir galimus tobulinimus.

Pusiau struktūrizuoto interviu atvejo analizės metu buvo aptariamos šios temos:

1. Esamos DDoS atakų apsaugos technologijos ir jų veiksmingumas;
2. DDoS atakų prevencijos būdai ir strategijos;
3. Galimi DDoS atakų apsaugos tobulinimo būdai ir naujos technologijos.

Remiantis gautais tyrimo rezultatais, buvo nustatyta, kad klientai ir specialistai teigiamai vertina esamas DDoS atakų apsaugos priemones, tačiau pabrėžia, kad nuolat reikia tobulėti ir prisitaikyti prie kintančios situacijos. Taip pat buvo identifikuoti galimi tobulinimo būdai, kurie gali padėti užtikrinti geresnį skaitmeninio turinio apsaugą nuo DDoS atakų.

Ateityje reikėtų atlikti papildomus tyrimus, siekiant patikrinti siūlomų tobulinimo priemonių efektyvumą praktikoje. Tokiu būdu būtų galima užtikrinti, kad Telia Lietuva klientams suteikiamos aukštos kokybės DDoS atakų apsaugos paslaugos, prisitaikančios prie kintančios rinkos ir technologijų plėtros.

Kokybinio tyrimo rezultatų analizės išvados:

1. Telia Lietuva klientai yra patenkinti esamomis DDoS atakų apsaugos priemonėmis, tačiau jie pabrėžia, kad reikia nuolat tobulėti ir prisitaikyti prie kintančios situacijos.
2. Tinklo inžinieriai teigia, kad esamos DDoS atakų apsaugos technologijos yra veiksmingos, tačiau nuolatos reikia ieškoti naujų sprendimų ir technologijų, siekiant užtikrinti aukščiausią apsaugos lygį.

3. Tie klientai, kurie susidūrė su DDoS atakomis, patvirtino, kad Telia Lietuva suteikia pakankamą paramą atkuriant paslaugas ir mažinant atakų poveikį.

Remiantis šiame etape atliktos analizės rezultatais, bus parengtos rekomendacijos Telia Lietuva įmonei dėl DDoS atakų apsaugos priemonių tobulinimo, siekiant užtikrinti efektyvią skaitmeninio turinio apsaugą nuo šių atakų.

2.2.1. DDos atakų mastas ir poveikis skaitmeniniui turiniui Telia Lietuva įmonėje

Tyrimo metu buvo atlikta kokybinė analizė, siekiant išsiaiškinti DDoS atakų mastą ir poveikį skaitmeniniui turiniui Telia Lietuva įmonėje. Atliekant šį tyrimą, buvo naudojama fokus grupės apklausa ir pusiau struktūrizuotas interviu metodas, kurio metu buvo apklausti įmonės klientai ir specialistai. Tyrimo rezultatai parodė, kad DDoS atakos yra vienas iš pagrindinių kibernetinio saugumo iššūkių, su kuriais susiduria Telia Lietuva įmonė ir jos klientai.

DDoS atakų mastas įmonėje yra įvairaus pobūdžio - nuo smulkių ir trumpalaikių atakų iki didelių, ilgalaikių ir intensyvių atakų. Tokios atakos gali turėti įvairų poveikį įmonės veiklai ir klientų skaitmeniniam turiniui. Poveikis gali būti matuojamas paslaugų neprieinamumu, padidėjusiais resursų naudojimo kaštai, prastėjančia klientų patirtimi, taip pat galimais finansiniais nuostoliais.

Klientai ir specialistai pabrėžė, kad esamos DDoS atakų apsaugos priemonės yra veiksmingos, tačiau nuolat reikia tobulėti ir prisitaikyti prie kintančios situacijos. Tai reiškia, kad įmonė turėtų investuoti į naujausias technologijas, geriau apmokyti savo darbuotojus ir plėsti bendradarbiavimą su kitais paslaugų teikėjais bei ekspertais.

Remiantis šio tyrimo rezultatais, galima teigti, kad DDoS atakų mastas ir poveikis skaitmeniniui turiniui Telia Lietuva įmonėje yra aktualios problemos, kurios reikalauja nuolatinio dėmesio ir tobulinimo. Šiame darbe bus siūlomi būdai, kaip pagerinti esamas apsaugos priemones ir užtikrinti skaitmeninio turinio prieinamumą bei saugumą Telia Lietuva klientams.

2.2.2. Esamų DDos atakų apsaugos priemonių apžvalga

Telia Lietuva įmonėje naudojamos įvairios DDoS atakų apsaugos priemonės, įskaitant aukšto lygio algoritmus, mašininio mokymosi technologijas, tinkamą konfiguraciją bei nuolatinius saugumo patikrinimus. Įmonė taip pat bendradarbiauja su kitomis telekomunikacijų, saugumo įmonėmis ir saugumo ekspertais, kad geriau suprastų grėsmes ir tobulintų savo apsaugos sistemas. Šiame skyriuje bus aptariamos esamos DDoS atakų apsaugos priemonės ir jų veikimo principai. Taip pat bus nagrinėjamos Telia Lietuva įmonės taikomos saugumo priemonės bei klientų patirtis ir nuomonė šiuo klausimu.

DDoS atakų apsaugos priemonės yra suskirstytos į kelias kategorijas:

1. Apsaugos nuo DDoS atakų metodai:

1.1. DDoS atakų aptikimo ir prevencijos technologijos - šios technologijos padeda anksti aptikti DDoS atakas, analizuodami tinklo srautą ir ieškodami nenormalių modelių bei elgsenos. Tai apima srauto analizatorių, IDS/IPS sistemas ir anomalijų aptikimo sistemas.

1.2. Atakų šaltinio nustatymo ir blokavimo metodai - šie metodai padeda nustatyti atakos šaltinį ir blokuoti ataką. Tai apima "blackholing", "sinkholing" bei BGP (Border Gateway Protocol) ir DNS (Domain Name System) atakų šaltinio nustatymo metodus.

1.3. DDoS atakų mažinimo ir valdymo technologijos - šios technologijos apima saugumo priemones, kurios padeda mažinti atakos poveikį ir valdyti atakos metu vykstančius procesus. Tai apima srauto kiekio ribojimą, balansavimą tarp serverių, "scrubbing" centrus ir "clean pipe" technologiją.

1.4. Incidentų atsarginės kopijos ir atkūrimo strategijos - šios strategijos padeda įmonėms atkurti veiklą po DDoS atakos, apimant duomenų atkūrimą, tinklo infrastruktūros atkūrimą ir kritinių sistemos komponentų atkūrimą.

2. Telia Lietuva įmonės taikomos saugumo priemonės:

2.1. DDoS aptikimo ir filtravimo sistemą - Telia Lietuva taiko specializuotas sistemas, skirtas ankstyvam DDoS atakų aptikimui ir filtravimui, užkertant kelią atakoms prieš jas pasiekiant klientų infrastruktūrą.

2.2. Atakos šaltinio nustatymą ir bendradarbiavimą su kitais paslaugų teikėjais atakų mažinimui - Telia Lietuva bendradarbiauja su kitais paslaugų teikėjais, siekdama nustatyti ir blokuoti atakų šaltinius, taip pat keistis svarbia informacija apie atakas ir jų mažinimo būdus.

2.3. Ugniasienes, tinklo prieigos kontrolę ir kitas saugumo technologijas - Telia Lietuva taiko įvairias saugumo priemones, tokias kaip ugniasienės, VPN (Virtual Private Network) ir NAC (Network Access Control) sistemos, siekdama užtikrinti tinklo apsaugą ir saugumą. Be to, įmonė taiko apsaugos nuo kenkėjiškų programų ir el. pašto filtravimo sprendimus, kad apsaugotų savo klientus nuo įvairių grėsmių.

Esamų DDoS atakų apsaugos priemonių apžvalga parodė, kad Telia Lietuva įmonė taiko įvairias efektyvias saugumo priemones, skirtas užtikrinti skaitmeninio turinio apsaugą ir klientų patirties gerinimą. Tačiau, kaip parodė tyrimo rezultatai, visuomet reikia stebėti rinkos pokyčius ir technologijų plėtrą, kad būtų galima prisitaikyti prie naujų iššūkių ir efektyviai reaguoti į DDoS atakas.

Šiame skyriuje buvo aptartos esamos DDoS atakų apsaugos priemonės, jų veikimo principai bei Telia Lietuva įmonės taikomos saugumo priemonės. Tyrimo rezultatai rodo, kad klientai yra patenkinti dabartinėmis priemonėmis, tačiau pabrėžia, kad reikia nuolat tobulėti ir prisitaikyti prie kintančių sąlygų. Atsižvelgiant į šiuos aspektus, tolesniame darbe bus siūlomi tobulinimo sprendimai, skirti efektyviai apsaugoti Telia Lietuva klientų skaitmeninį turinį nuo DDoS atakų.

2.3. Tyrimo rezultatų apibendrinimas

Telia Lietuva įmonėje naudojamos įvairios DDoS atakų apsaugos priemonės, įskaitant aukšto lygio algoritmus, mašininio mokymosi technologijas ir tinkamą konfiguraciją bei nuolatinius saugumo

patikrinimus. Įmonė taip pat bendradarbiauja su kitomis telekomunikacijų, saugumo įmonėmis ir saugumo ekspertais, kad geriau suprastų grėsmes ir tobulintų savo apsaugos sistemas.

Tyrimo tikslas - išanalizuoti Telia Lietuva klientų nuomonę apie skaitmeninio turinio apsaugą nuo DDoS atakų ir identifikuoti galimus tobulinimo būdus šioje srityje. Tyrimo metodologija apima šiuos etapus:

1. Literatūros analizė: atlikta teorinė apžvalga apie DDoS atakas, jų rūšis, apsaugos technologijas ir Lietuvos teisinį reglamentavimą šioje srityje.
2. Kokybinis tyrimas: atlikti pusiau struktūrizuoti interviu su Telia Lietuva klientais. Interviu metu buvo užduoti klausimai, susiję su DDoS atakų poveikiu, esamomis apsaugos priemonėmis ir galimomis tobulinimo priemonėmis.
3. Duomenų analizė: atliktas gautų interviu duomenų apibendrinimas, kategorizavimas ir analizė, siekiant atskleisti klientų nuomonę ir patirtį.

Tyrimo rezultatai:

1. DDoS atakų poveikis skaitmeniniam turiniui: klientai supranta DDoS atakų pavojų ir jų poveikį skaitmeninio turinio prieinamumui, paminėta, kad DDoS atakos gali sukelti svetainių neveikimą, sutrikimus paslaugų veikime ir finansinius nuostolius.
2. Esamos DDoS atakų apsaugos priemonės: klientai yra patenkinti dabartinėmis Telia Lietuva taikomomis DDoS atakų apsaugos priemonėmis, tačiau pabrėžia, kad visada yra vietos tobulėjimui ir inovacijoms. Galimi tobulinimo būdai: klientai siūlo investuoti į naujas technologijas, stiprinti bendradarbiavimą su kitais paslaugų teikėjais ir organizacijomis, taip pat geriau apmokyti personalą ir klientus.

Išvados ir rekomendacijos. Atsižvelgiant į tyrimo rezultatus, galima teigti, kad Telia Lietuva klientai yra patenkinti dabartine DDoS atakų apsauga, tačiau turi kelis pasiūlymus dėl tobulinimo priemonių. Rekomenduojama investuoti į naujas technologijas, bendradarbiauti su kitais paslaugų teikėjais ir organizacijomis, geriau apmokyti personalą ir klientus bei nuolat sekti kibernetinio saugumo tendencijas. Taip pat, svarbu atkreipti dėmesį į klientų informavimą apie DDoS atakų prevenciją ir apsaugos būdus, kad būtų galima bendromis pastangomis sumažinti DDoS atakų keliamą grėsmę skaitmeniniam turiniui.

Toliau pateikiamos konkrečios rekomendacijos, pagrįstos tyrimo rezultatais:

1. Investuoti į pažangias DDoS atakų aptikimo ir prevencijos technologijas, kurios padėtų veiksmingai atpažinti ir neutralizuoti atakas.

2. Skatinti bendradarbiavimą tarp skirtingų paslaugų teikėjų ir suinteresuotų šalių, siekiant keistis informacija apie atakas, jų šaltinius ir apsaugos būdus.
3. Įdiegti nuolatinius mokymus ir seminarus Telia Lietuva personalui, kad jie būtų geriau informuoti apie naujausias DDoS atakų tendencijas ir galėtų teikti kvalifikuotą pagalbą klientams.
4. Organizuoti informavimo kampanijas ir renginius klientams, kad jie būtų geriau informuoti apie DDoS atakų prevenciją ir apsaugos būdus.
5. Nuolat stebėti kibernetinio saugumo situaciją ir reaguoti į naujas grėsmes bei tendencijas, tobulinant esamas apsaugos priemones ir diegiant naujas.

Atsižvelgiant į tyrimo rezultatus, galima teigti, kad Telia Lietuva klientai yra patenkinti dabartine DDoS atakų apsauga, tačiau turi kelis pasiūlymus dėl tobulinimo priemonių. Rekomenduojama investuoti į naujas technologijas, bendradarbiauti su kitais paslaugų teikėjais ir organizacijomis, geriau apmokyti personalą ir klientus bei nuolat sekti kibernetinio saugumo tendencijas. Taip pat, svarbu atkreipti dėmesį į klientų informavimą apie DDoS atakų prevenciją ir apsaugos būdus, kad būtų galima bendromis pastangomis sumažinti DDoS atakų keliamą grėsmę skaitmeniniam turiniui.

Toliau pateikiamos konkrečios rekomendacijos, pagrįstos tyrimo rezultatais:

1. Investuoti į pažangias DDoS atakų aptikimo ir prevencijos technologijas, kurios padėtų veiksmingai atpažinti ir neutralizuoti atakas.
2. Skatinti bendradarbiavimą tarp skirtingų paslaugų teikėjų ir suinteresuotų šalių, siekiant keistis informacija apie atakas, jų šaltinius ir apsaugos būdus.
3. Įdiegti nuolatinius mokymus ir seminarus Telia Lietuva personalui, kad jie būtų geriau informuoti apie naujausias DDoS atakų tendencijas ir galėtų teikti kvalifikuotą pagalbą klientams.
4. Organizuoti informavimo kampanijas ir renginius klientams, kad jie būtų geriau informuoti apie DDoS atakų prevenciją ir apsaugos būdus.
5. Nuolat stebėti kibernetinio saugumo situaciją ir reaguoti į naujas grėsmes bei tendencijas, tobulinant esamas apsaugos priemones ir diegiant naujas.

Atsižvelgiant į visus tyrimo rezultatus ir rekomendacijas, Telia Lietuva galės stiprinti savo skaitmeninio turinio apsaugą nuo DDoS atakų ir užtikrinti aukštesnį klientų pasitenkinimą bei pasitikėjimą savo paslaugomis.

1. DDOS ATAKŲ APSAUGOS SKAITMENINIUI TURINIUI REKOMENDACINIS MODELIS

Šiame rekomendacinio modelio skyriuje pateikiamos pagrindinės DDoS atakų prevencijos ir apsaugos priemonės, skirtos skaitmeniniam turiniui apsaugoti Telia Lietuva įmonėje. Modelis grindžiamas gautais tyrimo rezultatais, klientų ir ekspertų nuomonėmis, taip pat analizuojant šiuolaikines DDoS atakų prevencijos ir apsaugos praktikas.

Rekomendacinis modelis susideda iš kelių pagrindinių komponentų:

1. Infrastruktūros apsauga:

1.1. Apsaugoti kritinę infrastruktūrą, naudojant fizinės ir virtualios apsaugos priemones.

1.2. Įgyvendinti tinklo segmentavimą, kad sumažinti atakų poveikį.

1.3. Taikyti griežtesnę prieigos kontrolę ir autentifikaciją, siekiant sumažinti neautorizuoto naudojimo riziką.

1.4. Naudoti DDoS atakų aptikimo ir filtravimo sistemą, kad greitai aptiktumėte ir neutralizuotumėte atakas.

2. Bendradarbiavimo stiprinimas:

2.1. Stiprinti bendradarbiavimą tarp paslaugų teikėjų, siekiant efektyviau keistis informacija apie DDoS atakas ir jų prevenciją bei apsaugą.

2.2. Sudalyvauti nacionaliniuose ir tarptautiniuose kibernetinio saugumo forumuose, kad būtų galima keistis žiniomis ir patirtimi su kitais sektoriaus veikėjais.

3. Technologijų atnaujinimas ir nuolatinė tobulinimas:

3.1. Investuoti į naujas ir pažangias DDoS atakų prevencijos bei apsaugos technologijas.

3.2. Nuolat tobulinti esamą DDoS atakų aptikimo ir apsaugos sistemą, atsižvelgiant į naujausius grėsmių modelius ir kibernetinio saugumo tendencijas.

4. Personalui ir klientams skirtas švietimas:

4.1. Mokyti personalą apie DDoS atakų prevenciją, apsaugą ir poveikį skaitmeniniam turiniui, kad jie galėtų efektyviau padėti klientams.

4.2. Organizuoti švietimo sesijas klientams, siekiant juos informuoti apie DDoS atakų rizikas, prevencijos priemones ir kaip elgtis atakos metu.

4.3. Skatinti ir palaikyti sąmoningumo kėlimą apie kibernetinį saugumą visuomenėje, kad mažėtų galimybė DDoS atakoms pasinaudoti neinformuotais asmenimis.

5. Incidentų valdymas ir ataskaitos:

5.1. Sukurti ir tobulinti incidentų valdymo procedūras, skirtas greitai ir efektyviai reaguoti į DDoS atakas.

5.2. Nustatyti atsakomybes ir komunikacijos kanalus tarp skirtingų įmonės padalinių ir personalo, kad užtikrintumėte sklandų incidentų valdymą.

5.3. Parengti reguliarias ataskaitas apie DDoS atakas, jų prevenciją ir apsaugą, kad būtų galima nuolat stebėti situaciją ir priimti sprendimus, kaip geriau apsaugoti skaitmeninį turinį.

Toliau pateikiamos rekomendacijos gali padėti Telia Lietuva įmonėje efektyviau spręsti DDoS atakų klausimus ir užtikrinti skaitmeninio turinio apsaugą. Siekiant nuolat tobulinti šį rekomendacinį modelį, svarbu stebėti kibernetinio saugumo tendencijas, naujas technologijas ir praktikas, bei konsultuotis su ekspertais ir klientais.

Rekomendacinis modelis yra grindžiamas klientų ir ekspertų nuomonėmis, gautais tyrimo rezultatais, taip pat analizuojant šiuolaikines DDoS atakų prevencijos ir apsaugos praktikas. Modelis siūlo integruotą požiūrį į DDoS atakų apsaugą, apimant infrastruktūros apsaugą, bendradarbiavimo stiprinimą, technologijų atnaujinimą ir nuolatinį tobulinimą, personalo ir klientų švietimą bei incidentų valdymą ir ataskaitas. Šis rekomendacinis modelis gali būti naudingas Telia Lietuva įmonei ir kitoms paslaugų teikėjams, siekiant tobulinti skaitmeninio turinio apsaugą nuo DDoS atakų.

6 lentelė. DDoS atakų apsaugos rekomendacinis modelis

Nr.	**Sritis**	**Rekomendacijos**
1.	Infrastruktūros apsauga	1.1 Patobulinti ir nuolat atnaujinti DDoS atakų apsaugos sistemas
		1.2 Įdiegti naujausias apsaugos technologijas ir sprendimus
		1.3 Reguliariai atlikti saugumo auditą ir testus
2.	Bendradarbiavimas	2.1 Stiprinti bendradarbiavimą su kitais paslaugų teikėjais ir organizacijomis
		2.2 Dalyvauti saugumo forumuose, konferencijose ir mokymuose
3.	Technologijų atnaujinimas	3.1 Investuoti į naujausias DDoS atakų prevencijos ir apsaugos technologijas
		3.2 Stebėti rinką ir naujoves, siekiant užtikrinti geriausią įmanomą apsaugą
4.	Personalo ir klientų švietimas	4.1 Mokyti ir tobulinti darbuotojų kompetencijas DDoS atakų apsaugos srityje
		4.2 Organizuoti švietimo sesijas klientams
		4.3 Skatinti sąmoningumo kėlimą apie kibernetinį saugumą visuomenėje
5.		5.1 Sukurti ir tobulinti incidentų valdymo procedūras

	Incidentų valdymas ir ataskaitos	5.2 Nustatyti atsakomybes ir komunikacijos kanalus tarp skirtingų įmonės padalinių ir personalo
		5.3 Parengti reguliarias ataskaitas apie DDoS atakas, jų prevenciją ir apsaugą

Ši lentelė vaizduoja rekomendacinį modelį, skirtą tobulinti skaitmeninio turinio apsaugą nuo DDoS atakų Telia Lietuva įmonėje. Modelis apima infrastruktūros apsaugą, bendradarbiavimą, technologijų atnaujinimą, personalo ir klientų švietimą, bei incidentų valdymą ir ataskaitas.

Galimų tobulinimo priemonių analizė

1. Įvadas

Analizuojamos galimos tobulinimo priemonės, susijusios su DDoS atakų prevencija ir apsauga, remiantis klientų ir ekspertų nuomonėmis. Skyriuje bus aptariamos skirtingos strategijos, technologijos ir metodai, leidžiantys efektyviau mažinti DDoS atakų poveikį skaitmeninio turinio prieinamumui.

2. Strategijų tobulinimas

2.1 Paslaugų teikėjų bendradarbiavimas: stiprinti bendradarbiavimą tarp Telia Lietuva ir kitų paslaugų teikėjų, keistis informacija apie atakas, jų šaltinius ir taikomas apsaugos priemones.

2.2 Incidentų ataskaitos: kurti išsamesnes ataskaitas apie DDoS atakas, leidžiančias klientams ir kitoms šalims geriau suprasti atakų pobūdį ir veiksmingai reaguoti į jas.

3. Technologijų tobulinimas

3.1 Naujų technologijų integravimas: investuoti į naujas ir pažangias DDoS atakų prevencijos bei apsaugos technologijas, padedančias efektyviau aptikti, filtruoti ir neutralizuoti atakas.

3.2 Apsaugos nuo DDoS atakų sistemos nuolatinis tobulinimas: nuolat atnaujinti ir gerinti esamą DDoS atakų aptikimo ir apsaugos sistemą, atsižvelgdama į naujausius grėsmių modelius ir kibernetinio saugumo tendencijas.

4. Metodų tobulinimas

4.1 Personalo mokymas: užtikrinti, kad Telia Lietuva personalas nuolat būtų mokomas ir informuojamas apie naujausias DDoS atakų prevencijos ir apsaugos priemones bei praktikas.

4.2 Klientų švietimas: sukurti klientams skirtą informacinę medžiagą ir renginius, suteikiant naudingą informaciją apie DDoS atakų prevenciją ir apsaugą, taip pat jų poveikį skaitmeninio turinio prieinamumui.

5. Išvados

Tobulinimo priemonės grindžiamos klientų ir ekspertų nuomonėmis bei šiuolaikinėmis DDoS atakų prevencijos ir apsaugos praktikomis. Svarbu suprasti, kad kibernetinio saugumo srityje nuolat kinta grėsmių vaizdas, todėl reikia prisitaikyti prie naujų iššūkių ir nuolat ieškoti geresnių sprendimų. Telia Lietuva turėtų įgyvendinti šias strategijas, technologijas ir metodus, siekdama užtikrinti aukštesnį savo klientų skaitmeninio turinio prieinamumo saugumo lygį. Taip pat svarbu atsižvelgti į bendradarbiavimo su kitais sektoriaus dalyviais svarbą, kad būtų galima efektyviau spręsti kibernetinio saugumo iššūkius ir sumažinti DDoS atakų poveikį.

Toliau pateikiamos pagrindinės išvados:

1. Stiprinti bendradarbiavimą tarp paslaugų teikėjų, siekiant efektyviau keistis informacija apie DDoS atakas ir jų prevenciją bei apsaugą.
2. Sudaryti išsamesnes DDoS atakų ataskaitas, kurios padėtų geriau suprasti atakų pobūdį ir reaguoti į jas.
3. Investuoti į naujas ir pažangias DDoS atakų prevencijos bei apsaugos technologijas, kurios padėtų efektyviau aptikti, filtruoti ir neutralizuoti atakas.
4. Nuolat tobulinti esamą DDoS atakų aptikimo ir apsaugos sistemą, atsižvelgiant į naujausius grėsmių modelius ir kibernetinio saugumo tendencijas.
5. Mokyti personalą ir informuoti klientus apie DDoS atakų prevenciją ir apsaugą, taip pat jų poveikį skaitmeninio turinio prieinamumui.

Toliau rekomenduojama Telia Lietuva įmonėje pritaikyti šias tobulinimo priemones, siekiant užtikrinti aukštesnį skaitmeninio turinio kibernetinio saugumo lygį ir pagerinti klientų patirtį. Taip pat svarbu nuolat stebėti kibernetinio saugumo tendencijas ir atlikti periodinius tyrimus, kad būtų galima laiku nustatyti naujas grėsmes ir įvertinti esamų apsaugos priemonių efektyvumą.

Rekomendacijų ir išvadų formulavimas

Remiantis anksčiau atliktų tyrimų gautais rezultatais ir analize siekiama pateikti konkrečias rekomendacijas ir išvadas, kurios padėtų Telia Lietuva įmonei tobulinti DDoS atakų prevenciją ir apsaugą skaitmeninio turinio kontekste.

Dimensija: DDoS atakų prevencijos ir apsaugos priemonių tobulinimas

Tyrimo kriterijai: klientų ir ekspertų nuomonės, galimi sprendimai, tobulinimo galimybės

Tyrimo metodai: duomenų analizė ir sintezė, rekomendacijų ir išvadų formulavimas

Pagrindinės rekomendacijos, remiantis tyrimu, yra šios:

1. Investuoti į naujas technologijas, skirtas DDoS atakų prevencijai ir apsaugai, kad būtų galima efektyviau atpažinti ir neutralizuoti atakas.
2. Skatinti bendradarbiavimą tarp paslaugų teikėjų, siekiant bendromis pastangomis mažinti DDoS atakų sukeltą poveikį skaitmeninio turinio prieinamumui.
3. Mokyti klientus apie DDoS atakas, jų poveikį ir būdus, kaip jų išvengti, kad būtų galima sumažinti atakų poveikį ir padėti klientams apsaugoti savo skaitmeninį turinį.
4. Apmokyti įmonės darbuotojus, ypač klientų aptarnavimo personalą, atpažinti ir efektyviai spręsti su DDoS atakomis susijusias problemas.
5. Užtikrinti, kad teisinis reglamentavimas būtų nuoseklus ir veiksmingas, siekiant suteikti reikalingą pagrindą DDoS atakų prevencijai ir apsaugai.

Išvados:

1. DDoS atakos turi reikšmingą poveikį skaitmeninio turinio prieinamumui ir gali sukelti finansinių nuostolių bei reputacijos praradimą.
2. Telia Lietuva klientai yra patenkinti esamomis DDoS atakų prevencijos ir apsaugos priemonėmis, tačiau reikia nuolat tobulėti ir prisitaikyti prie kintančios kibernetinio saugumo aplinkos ir DDoS atakų raidos.
3. Norint efektyviai mažinti DDoS atakų poveikį skaitmeninio turinio prieinamumui, būtina investuoti į naujas technologijas, gerinti bendradarbiavimą tarp paslaugų teikėjų ir užtikrinti nuolatinį personalo bei klientų mokymą.
4. Teisinis reglamentavimas Lietuvoje yra svarbus veiksnys, leidžiantis efektyviai spręsti su DDoS atakų prevencija ir apsauga susijusias problemas.
5. Telia Lietuva turėtų imtis konkrečių veiksmų, pagrįstų šio tyrimo rezultatais ir rekomendacijomis, siekiant tobulinti DDoS atakų prevenciją ir apsaugą skaitmeninio turinio prieinamumo kontekste.

Ateityje reikėtų atlikti panašius tyrimus, kad būtų galima stebėti DDoS atakų prevencijos ir apsaugos priemonių veiksmingumą bei tobulinimo galimybes. Taip pat būtų naudinga įvertinti kitų šaltinių, pvz., ekspertų ar pramonės atstovų, nuomones ir patirtis, siekiant gauti išsamesnę ir platesnę analizę apie DDoS atakų prevenciją ir apsaugą.

IŠVADOS

Remiantis atliktu tyrimu, darbo išvadose pateikiami pagrindiniai rezultatai, susiję su skaitmeninio turinio apsauga nuo DDoS atakų Telia Lietuva įmonėje:

1. DDoS atakos yra vienas iš pagrindinių skaitmeninio turinio kibernetinio saugumo iššūkių, turintis tiesioginį poveikį skaitmeninio turinio prieinamumui ir paslaugų veikimui. Atakos gali sukelti svetainių nepasiekiamumą, paslaugų trikdžius ir finansinius nuostolius tiek paslaugų teikėjams, tiek klientams.
2. Telia Lietuva įmonėje taikomos DDoS atakų prevencijos ir apsaugos priemonės yra vertinamos kaip gana efektyvios, tačiau klientai ir ekspertai pabrėžia, kad reikia nuolat tobulėti ir prisitaikyti prie kintančios kibernetinio saugumo situacijos.
3. DDoS atakų prevencijos ir apsaugos priemonių tobulinimas turėtų apimti investicijas į naujas technologijas, darbuotojų mokymą, bendradarbiavimą su kitais paslaugų teikėjais ir kibernetinio saugumo ekspertais, taip pat klientų informavimą ir sąmoningumo ugdymą.
4. Šio darbo metu parengtas DDoS atakų apsaugos skaitmeniniam turiniui rekomendacinis modelis gali padėti Telia Lietuva įmonei užtikrinti aukštesnį skaitmeninio turinio prieinamumo lygį, sumažinant DDoS atakų poveikį.
5. Ateityje reikėtų atlikti daugiau tyrimų, susijusių su DDoS atakų prevencija ir apsauga, kad būtų galima nuolat tobulinti strategijas ir technologijas bei užtikrinti skaitmeninio turinio prieinamumą ir kokybę.

Šios išvados atspindi svarbiausius šio darbo rezultatus ir pateikia vertingų įžvalgų apie skaitmeninio turinio apsaugą nuo DDoS atakų. Jie gali būti naudingi ne tik Telia Lietuva įmonėje, bet ir kitose įmonėse, susiduriančiose su panašiais iššūkiais.

LITERATŪRA

1. Agafonov, K. (2021). Kibernetinio saugumo valdymo modelis elektroniniams rinkimams įgyvendinti. Mykolo Romerio universitetas. https://repository.mruni.eu/handle/007/17825
2. Anderson, R. (1972). Security Engineering: A Guide to Building Dependable Distributed Systems.
3. Cloudflare. (2022). What is a DDoS attack? https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/
4. ES kibernetinio saugumo erdvės kūrimas: poveikio Lietuvai analizė. (2016). https://gs.elaba.lt/object/elaba:15149593
5. International Library of Ethics, Law and Technology. (2020). https://link.springer.com/10.1007/978-3-030-29053-5_2
6. Kaspersky. (2022). What is a DDoS attack? https://www.kaspersky.com/resource-center/threats/ddos-attacks
7. KIBERNETINIO SAUGUMO APLINKA LIETUVOJE. (2015 m. gruodžio 9 d. Nr. VA-P-90-4-16). https://www.valstybeskontrole.lt/LT/Product/23587
8. Kibernetinio saugumo sąvokos apibrėžimas. XII-1428 (2014). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee
9. Nacionalinis kibernetinio saugumo centras (2022). https://www.nksc.lt/aktualu.html
10. Lietuvos Respublikos kibernetinio saugumo įstatymas. (2018). Nr. XII-1428. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/KFZyEPUCbf
11. Lietuvos Respublikos Vyriausybės nutarimas "Dėl Nacionalinės kibernetinio saugumo strategijos patvirtinimo". (2018). Nr. 13252. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595
12. Norton. (2021). What is a DDoS Attack? https://us.norton.com/blog/privacy/what-is-a-ddos-attack
13. Radware. (2022) What Is a DDoS Attack? https://www.radware.com/cyberpedia/ddospedia/ddos-meaning-what-is-ddos-attack/
14. Schou, C., & Hernandez, S. (2014). Information Assurance Handbook: Effective computer security and risk management strategies. McGraw-Hill Osborne Media.
15. Šidlauskas, A. (2018). Vartotojų elektroninių duomenų apsaugos duomenų ypatumai. Mykolo Romerio universitetas. https://vb.mruni.eu/object/elaba:25184230/ 17. https://www.sciencedirect.com/science/article/abs/pii/S1389128617301172
18. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-alrwais.pdf
19. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. (2017). https://www.sciencedirect.com/science/article/pii/S1389128617301172
20. http://ieeexplore.ieee.org/document/6994333/
21. https://www.researchgate.net/publication/2879658_A_taxonomy_of_DDoS_attack_and_DDoS_Defense_mechanisms
22. http://ijmrap.com/wp-content/uploads/2020/01/IJMRAP-V2N7P59Y20.pdf
23. Kibernetinio saugumo mėnuo 2022. (2022). https://kam.lt/kibernetinio-saugumo-menuo-2022
24. Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimas. (2018). Nr. 13252. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f/asr#part_5a4a17b82cc64cf4ba1dc41021eada4d

ANOTACIJA

Magistro darbo pavadinimas: Skaitmeninio turinio apsauga nuo DDoS atakų Telia Lietuva įmonėje. Šio magistro darbo tikslas - išanalizuoti skaitmeninio turinio apsaugos nuo DDoS atakų aspektus Telia Lietuva įmonėje ir pateikti rekomendacijas esamoms apsaugos priemonėms tobulinti. Darbą sudaro išsamus teorinis DDoS atakų ir apsaugos technologijų tyrimas, kibernetinės saugos teisinio reglamentavimo Lietuvoje analizė ir kokybinis tyrimas, kurio metu buvo atlikti pusiau struktūruoti interviu su Telia Lietuva klientais. Tyrimo rezultatai parodė, kad DDoS atakos gali turėti reikšmingą poveikį skaitmeninio turinio prieinamumui ir verslo funkcijoms. Nepaisant to, kad Telia Lietuva klientai iš esmės yra patenkinti teikiamomis saugumo priemonėmis, tyrimas atskleidė, kad, atsižvelgiant į nuolat besikeičiančią kibernetinio saugumo aplinką, būtina nuolat tobulėti. Investicijos į naujas technologijas, bendradarbiavimas su kitais paslaugų teikėjais, klientų švietimas ir darbuotojų mokymas - tai vienos iš rekomendacijų, į kurias atkreiptas dėmesys šiame dokumente. Be to, dokumente pabrėžiama, kad teisinis reguliavimas yra svarbus veiksnys užtikrinant veiksmingą prevenciją ir apsaugą nuo DDoS atakų, todėl būtina reguliariai peržiūrėti ir atnaujinti teisines nuostatas. Šiame dokumente pateikiama vertingų įžvalgų apie DDoS atakų prevenciją ir apsaugą nuo jų skaitmeninio turinio erdvėje, kurios gali būti naudingos Telia Lietuva ir kitoms su panašiais iššūkiais susiduriančioms organizacijoms.

Raktiniai žodžiai: skaitmeninis turinys, kibernetinis saugumas, DDoS atakos, saugumo priemonės, Telia Lietuva, klientų nuomonė, rekomendacijos.

ABSTRACT

The title of the Master's thesis is Protection of digital content against DDoS attacks in Telia Lietuva company.
The aim of this Master's thesis is to analyse the aspects of digital content protection against DDoS attacks in Telia Lietuva company and to provide recommendations for improving the existing protection measures. The thesis consists of a detailed theoretical study of DDoS attacks and protection technologies, an analysis of the legal regulation of cyber security in Lithuania and a qualitative study, which included semi-structured interviews with Telia Lietuva customers. The results of the research showed that DDoS attacks can have a significant impact on the availability of digital content and business functions. Despite the fact that Telia Lietuva's customers are generally satisfied with the security measures provided, the study revealed that the ever-changing cybersecurity landscape requires continuous improvement. Investment in new technologies, cooperation with other service providers, customer education and staff training are some of the recommendations addressed in this document. The document also stresses that the legal framework is an important factor in ensuring effective prevention and protection against DDoS attacks, and that it is therefore necessary to regularly review and update legal provisions. This paper provides valuable insights into the prevention and protection against DDoS attacks in the digital content space, which may be useful for Telia Lietuva and other organisations facing similar challenges.

Keywords: digital content, cybersecurity, DDoS attacks, security measures, Telia Lietuva, customer opinion, recommendations.

SANTRAUKA

Šiame magistro darbe nagrinėjama skaitmeninio turinio apsauga nuo DDos atakų Telia Lietuva įmonėje.
Tyrimo tikslas - įvertinti esamas apsaugos priemones ir pateikti pasiūlymus dėl jų tobulinimo. Atliktas išsamus teorinis tyrimas apie DDoS atakas ir apsaugos technologijas, teisinį kibernetinio saugumo reglamentavimą Lietuvoje ir kokybinis tyrimas, kurio metu atlikti pusiau struktūruoti interviu su Telia Lietuva klientais. Remiantis išvadomis, DDoS atakos daro didelę įtaką skaitmeninio turinio prieinamumui ir įmonių veiklos rezultatams. Nors klientai iš esmės yra patenkinti esamomis saugumo priemonėmis, tyrimas atskleidė, kad jas reikia nuolat tobulinti ir gebėti prisitaikyti prie nuolat besikeičiančios kibernetinio saugumo aplinkos. Tarp svarbių pasiūlymų - investicijos į naujas technologijas, bendradarbiavimas su kitais paslaugų teikėjais, klientų švietimas ir darbuotojų mokymas. Taip pat pabrėžiama teisinės sistemos svarba veiksmingai DDoS atakų prevencijai ir apsaugai nuo jų. Šiame darbe pateikiama vertingų įžvalgų apie DDoS atakų prevenciją ir apsaugą skaitmeninio turinio erdvėje, kurios gali būti vertingos Telia Lietuva ir kitoms su panašiais iššūkiais susiduriančioms organizacijoms.

Reikšminiai žodžiai: skaitmeninis turinys, kibernetinis saugumas, DDoS atakos, saugumo priemonės, Telia Lietuva, klientų atsiliepimai, rekomendacijos.

SUMMARY

This thesis focuses on the protection of digital content against DDos attacks in Telia Lietuva. The aim of the study is to evaluate the existing protection measures and to provide suggestions for their improvement. A comprehensive theoretical study on DDoS attacks and protection technologies, legal regulation of cyber security in Lithuania and a qualitative study with semi-structured interviews with Telia Lietuva customers were conducted. According to the findings, DDoS attacks have a significant impact on the availability of digital content and the performance of companies. While customers are generally satisfied with their existing security measures, the research revealed that they need to be continuously improved and able to adapt to the ever-changing cyber security environment. Important suggestions include investment in new technologies, cooperation with other service providers, customer education and staff training. The importance of the legal framework to effectively prevent and protect against DDoS attacks is also highlighted. This paper provides valuable insights into the prevention and protection of DDoS attacks in the digital content space, which may be of value to Telia Lietuva and other organisations facing similar challenges.

Keywords: digital content, cybersecurity, DDoS attacks, security measures, Telia Lietuva, customer feedback, recommendations.

PRIEDAI

Priedas1Tyrimo instrumentarijus

Priedas2 Fokus grupės apklausos analizės transkribcija

Priedas3 Kokybinio tyrimo – pusiau struktūrizuoto interviu su ekspertais analizės transkribcija