VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

Erika Juknevičiūtė

KOMPIUTERIŲ TINKLŲ SAUGOS UŽTIKRINIMO METODIKOS KŪRIMAS

DEVELOPMENT OF COMPUTER NETWORK SECURITY ASSURANCE METHODOLOGY

Baigiamasis magistro darbas

Informacijos ir informacinių technologijų saugos studijų programa, valstybinis kodas

621E14007

Informatikos inžinerija

Informacinės sistemos

Vilnius, 2014

Vilniaus Gedimino technikos universitetas

Fundamentinių mokslų fakultetas

Informacinių technologijų katedra

ISBN ISSN

Egz. sk. …….

Kalba

x lietuvių

užsienio

Informacijos ir informacinių technologijų saugos studijų programos baigiamasis magistro darbas

Pavadinimas **Kompiuterių tinklų saugos užtikrinimo metodikos kūrimas**

Autorius **Erika Juknevičiūtė** Vadovas doc. dr. Nikolaj Goranin

Anotacija

Magistrinio darbe apibrėžiamos tinklo saugos savybės - daugiausia žemesniųjų TCP/IP modelio lygmenų, suderintos su ISO/IEC 27002 ir ISO/IEC 27033:1 standartais. Šias savybes darbe siekiama pritaikyti organizacijoms pagal jų dydį ir veiklos sektorių. Šiuo tikslu pateikta CVSS v2 balo modifikacija. Kitas darbe pasiūlytas sprendimas yra rizikos skaičiavimo modelis, kuris apima organizacijos dydžio ir veiklos sektoriaus parametrus. Rizikos vertės yra apibūdinamos kaip incidento tikimybės ir poveikio turtui skaičiavimo rezultatas. Sprendimo medžio modelis yra pateiktas kaip supaprastintas tinklo saugos savybių rekomendacijos vertinimo vaizdas organizacijoms pagal jų dydį ir veiklos sektorių. Toks sprendimo medis gali praversti organizacijos darbuotojams, kurie neturi reikalingų techninių žinių, taip pat pat gali būti panaudotas kaip žinių bazė ekspertinėms sistemoms.

Prasminiai žodžiai: Kompiuterių tinklų saugos užtikrinimo metodika, ISO/IEC 27033:1, ISO/IEC 27002, rizikos nustatymas, CVSS v2, sprendimo medžiai.

Vilnius Gediminas Technical University

Fundamental sciences faculty

Information systems department

ISBN ISSN

Copies No. ……..

Information and information technology security study programme bachelor (master) thesis.

Title: **Development of computer network security assurance methodology**

Author **Erika Juknevičiūtė** Academic supervisor **doc. dr. Nikolaj Goranin**

Thesis language

[ ] Lithuanian

[x] Foreign (English)

Annotation

The aim of this thesis is adaptation of network security measures based on organization size and sector. Therefore fundamental network security features compatible with ISO/IEC 27002 and ISO/IEC 27033:1 standards have been identified and adoption model of lower TCP/IP security features to unique organization environment is demonstrated. For this reason the calculations of CVSS v2 had to be modified. Another solution proposed to achieve the aim is risk calculation model based on organization size and sector. The risk values are described as calculation result of incident probability and impact to asset. The probability is calculated from statistical data. The most needed network security features to organization environment are chosen by calculated risk values. Decision tree model gives simple view to organization network security needs, therefore it could by used by employees without good technical skill on this area. Also decision tree model could be used later acknowledge database for expert system.

Keywords: Computer network security assurance methodology, ISO/IEC 27033:1, ISO/IEC 27002, risk assessment, CVSS v2, decision trees.

Turinys

1. Įvadas 9
1.1. Tyrimo objektas 10
1.2. Darbo tikslas ir uždaviniai 10
1.3. Temos naujumas 11
1.4. Temos aktualumas 11
1.5. Tyrimo metodika 12
1.6. Darbo rezultatai 12
1.7. Darbo struktūra 12
2. Egzistuojančių metodikų ir tyrimų analizė 14
2.1. Sąsaja tarp standartų ir metodikų 14
2.2. Kriterijai metodikai 14
2.3. Šiuolaikinių metodikų apžvalga 16
2.4. ISO/IEC saugos standartai 29
2.5. ISO/IEC 27033-1:2009 29
2.6. ISO/IEC 27002:2005 29
2.7. Kompiuterių tinklų saugos rizikos mažinimo priemonės 29
3. Tinklo saugos užtikrinimo priemonių parinkimas pagal organizacijų riziką 36
3.1. Ekspertinės sistemos 41
3.2. Sprendimų medžiai 43
3.3. Sprendimo medžių taikymas sudarytai metodikai 45
3.4. CVSS v2 pritaikymas rizikos vertinimui pagal organizacijos aplinką 45
3.5. Sprendimų medžių realizacija su „WEKA“ programinė įranga. 63
4. Išvados 66
Literatūra 67

Paveikslų sąrašas

2.2.1 pav. CIA triada

2.3.1 pav. Ataka išnaudojant ARP protokolą

2.3.2 pav. DHCP atakos modelis

2.3.3 pav. DHCP atakos modelis

3.1 pav. Veiksniai, lemiantys saugaus tinklo projektavimą

3.1.1 pav. Ekspertinės sistemos architektūra

3.2.1 pav. Sprendimų medžių mokymosi įėjimas ir išėjimas

3.4.1 pav. Procentinis pažaidų pasiskirstymas L2, L3 ir L4 protokolams

3.4.2 pav. Tinklo saugos pažaidų išnaudojimo poveikio vertinimo informacijos kubas

3.4.3 pav. Tinklo saugos rizikos nustatymo ir valdymo procesai

3.5.1 pav. Sprendimo medžio dinaminės ARP inspekcijos rekomendacijai fragmentas

Lentelių sąrašas

2.3.1 lentelė. Tinklų tipai ir jiems būdingos atakos

2.3.2 lentelė. Metodikų palyginimas

2.7.1 lentelė. Saugos grėsmių mažinimo priemonių parinkimas pagal informacijos technologijos saugos standartus

3.1 lentelė. Rizikos priklausomybė nuo organizacijos dydžio

3.2 lentelė. Rizikos įvertinimas, atsižvelgus į tikimybę ir poveikį

3.4.1 lentelė. Triados reikalavimų pažaidos

3.4.2 lentelė. CVSS Bazinės metrikos

3.4.3 lentelė. Atviro teksto autentifikacijos protokolų naudojimo SCADA CVSS v2 bendri rezultatai

3.4.4 lentelė. ICT-CERT kibernetinių incidentų statistiniai duomenys pagal veiklos sektorių

3.4.5 lentelė. ICT-CERT kibernetinių incidentų statistinių duomenų vidurkiai pagal veiklos sektorių

3.4.6 lentelė. „Achiles“ atliktų saugos pažeidimų testų skirtingiems pramonės sektoriams rezultatai

3.4.7 lentelė. Tikimybei skaičiuoti naudojama metinė pažaidų statistika

3.4.8 lentelė. Pažaidų poveikiui skaičiuoti naudojami CVSS atributai

3.4.9 lentelė. Pažaidų poveikiui skaičiuoti naudojami CVSS atributai

Santrumpos

ACL – Access Control List – Prieigos Kontrolės Sąrašas

ARP - Address Resolution Protocol – Adreso Keitimo Protokolas

BGP - Border Gateway Protocol – Kraštinio Maršruto Parinktuvo Protokolas

CIA - Confidentiality, Integrity and Availability – Konfidencialumas, Integralumas ir Prieinamumas

CVSS - Common Vulnerability Scoring System – Bendra Pažaidų Vertinimo Sistema

EAP – Extensible Authentication Protocol – Išplėstas Autentifikacijos Protokolas

HTTPS - Hypertext Transfer Protocol Secure - Saugus Hiperteksto Protokolas

ICMP - Internet Control Message Protocol – Interneto Žinučių Kontrolės Protokolas

IP – Internet Protocol – Interneto Protokolas

IPS – Intrusion Prevention System – Įsibrovimų Prevencijos Sistema

IDS – Intrusion Detection System – Įsibrovimų Aptikimo Sistema

IOS - Internetwork Operating System – Tarptinklinė Operacinė Sistema

LAN – Local Aera Network – Lokalus Tinklas

MAC - Media Access Control – Prieigos Valdymas

MiTM – Man in the middle – Tarpininko ataka

OSPF protokolas - Open Shortest Path First – Trumpiausio kelio protokolas

TCP - Transmission Control Protocol – Perdavimo Valdymo Protokolas

UDP – User Datagram Protocol – Vartotojo Duomenų Protokolas

L – Layer – Lygmuo

L2 – Layer 2 – Antras lygmuo

L3 – Layer 3 – Trečias lygmuo

L4 – Layer 4 – Ketvirtas lygmuo

SNMP – Simple Network Management Protocol – Paprastas Tinklo Valdymo Protokolas

SSH - Secure Shell – Saugus nuotolinio prisijungimo protokolas

VLAN - Virtual Local Area Network – Virtualus Lokalus Tinklas

VPN – Virtual Private Network – Virtualus Privatus Tinklas

1. Įvadas

Kompiuterių tinklai yra komunikacinė infrastruktūra, skirta perduoti duomenis tarp mazgų. Taikomosios programos perduodami duomenys turi būti paruošti transportavimui, galiausiai būna paverčiami elektrinių arba optinių signalų seka, kuri pasiekusi gavėją vėl atvaizduojama taikomosios programos [44]. Kiekvienas šio perdavimo etapas yra rizikingas saugos atžvilgiu ir turi būdingas pažaidas, kurios išnaudojami incidentų metu. Informacija internete keliauja protokolų pagalba, kurių rinkinys sudaro TCP/IP (Transmission Control Protocol/Internet Protocol) protokų dėklą, susidedantį iš 4-ių lygmenų. Norint apsaugoti informaciją nuo pažaidų išnaudojimo, reikia rūpintis kiekvieno TCP/IP lygmens sauga. Tai reiškia, kad jei vienas lygmuo yra pažeistas, komunikacija yra sutrikdyta, net jei kituose lygmenyse dar nėra neigiamų rezultatų. ISO/IEC 27033-1 standarte tinklo sauga yra apibrėžiama kaip įrenginių, jų valdymo veiklų, taikomųjų programų/paslaugų ir galinių naudotojų sauga, taip pat komunikacinėmis linijomis perduodamos informacijos sauga. Galima sakyti, kad sauga yra tiek stipri, kiek yra stiprus silpniausias lygis. Kalbant apie tinklą, 2-asis (angl. Layer 2 – L2) TCP/IP lygmuo gali būti labai silpnas. Šiame darbe daugiausia nagrinėjamas 2-asis ir 3-iasis (angl. Layer 3 – L3) TCP/IP lygmuo ir tam tikrų aukštesniųjų lygmenų tinklo paslaugų sauga.

Svarbu, kad incidentų metu būtų pakenkta kuo mažesnei infrastruktūros daliai. Jeigu įsivaizduoti organizaciją iš įsibrovėlio, turinčio blogų kėslų pusės, galima būtų ją suskirstyti į atskirus elementus, kurie sudaro taikinio modelį. Toks modelis apimtų serveriuose įdiegtų operacinių sistemų, tinklų įrangos, vidinių ir išorinių vartotojų saugą [37]. Kiekvienas už savo taikinio modelio elementą/us atsakingas asmuo turi užtikrinti maksimalią saugą, tačiau ne visi specialistai dėl vienokių ar kitokių priežasčių yra pakankamai skiriantys tam dėmesio ar yra atitinkamos kvalifikacijos. Atliktas tyrimas parodė, kad informacijos saugos specialistai apytiksliai 2.21h skiria informacijos saugos tema paieškai [33]. Tokiu atveju naudinga turėti praktines gaires, kuriomis galima būtų vadovautis. Kadangi pastaruoju metu organizacijos vis dažniau stengiasi vadovautis tarptautiniais standartais, gairės turėtų būti suderintos su standartų rekomendacijomis.

Dėl informacinių technologijų vystymosi (angl. information technology – IT) ir naudojimo sektorių įvairovės ši sritis tampa tokia pati reikli saugos užtikrinimui kaip ir pinigai. Daugumai situacijų informacijos turtą net ir galima įvertinti pinigų matu.

Vyriausybinės, karinės, finansinės institucijos, ligoninės ir privatus verslas kaupia didelį kiekį konfidencialios informacijos apie jų darbuotojus, klientus, produktus, tyrimus ir finansinį statusą. Dauguma šios informcijos surenkama, apdorojama ir saugoma elektroniniu formatu IT įrangoje ir perduodama kompiuterių tinklu. Per pastaruosius metus informacijos saugos sritis pastebimai išaugo ir išsivystė, o tuo pačiu išryškėjo ir specializacijos: tinklų ir infrastruktūros sauga, taikomųjų programų ir duomenų bazių sauga, saugos testavimas, informacinių sistemų auditas, verslo tęstinumo planavimas ir elektroninių nusikaltimų tyrimas. Kiekvienai organizacijai svarbu užsitikrinti saugą visose srityse, kuri susijusi su rizika pagal organizacijos parametrus, o esant investicijų klausimui, įsivertinti svarbiausius poreikius.

1.1. Tyrimo objektas

Tyrimo objektas – kompiuterių tinklų saugos metodikos ir pagrįstų saugos priemonių parinkimas pagal organizacijos aplinkos parametrus.

1.2. Darbo tikslas ir uždaviniai

Baigiamojo magistro darbo tikslas – paruošti kompiuterių tinklų saugos užtikrinimo metodiką, suderintą su parinktais tarptautiniais ISO/IEC standartais ir pritaikyti tinklo saugos priemonių poreikio vertinimą pagal organizacijos aplinkos parametrus. Tikslui pasiekti atliekami uždaviniai:

1. Išanalizuoti esamus kompiuterių tinklų saugos standartus.
2. Išanalizuoti esamas saugos užtikrinimo metodikas.
3. Remiantis išanalizuotais standartais ir metodikomis nustatyti reikalavimus, kurie būtini siekiant užtikrinti bazinę kompiuterių tinklų saugą.
4. Sudaryti modelį, kuriuo galima vadovautis parenkant tinklo saugos priemones ir jas taikant pagal organizacijos aplinką.

1.3. Temos naujumas

Esamos tinklo saugos užtikrinimo metodikos skirtos vienai tinklo saugos sričiai, dažniausiai bevieliam tinklui, saugos testavimui. Daugiausia informacijos susijusios su baziniu tinklo saugos užtikrinimu yra pateiktos įrangos, produktų gamintojų, pvz., Cisco, HP, SAN. Trūksta metodikų, kuriomis galima būti vadovautis praktiškai realizuojant tarptautinių standartų rekomendacijas.

Publikacijose retai bandoma pateikti konkrečių L2, L3 lygmenų tinklo saugos priemonių pritaikymo būdą pagal konkrečius organizacijos parametrus. Reikalingas mechanizmas, kurio pagalba būtų galima įvertinti tam tikros tinklo saugos priemonės reikalingumą.

1.4. Temos aktualumas

Vis dažniau užtikrinant saugą organizacijose vadovaujamasi tarptautiniais standartais. Kad būtų tinkamai jais vadovaujamasi pravartu turėti praktines priemones jų rekomendacijų realizacijai. Magistrinio darbe siekiame susieti tarptautinių standartų reikalavimus su pasiūlytomis saugos užtikrinimo priemonėmis.

Nėra metodų parinkti tinklo saugos užtikrinimo priemones pagal konkrečius organizacijos parametrus, kas lemia, kad saugos užtikrinimo procesas yra komplikuotas, nes dažnai nesuprantama poreikių ir prioritetų. Turint saugos priemonių vertinimo modelį kompiuterių tinklų saugos metodika leistų realizuoti saugų tinklą atsižvelgiant į objekto parametrus, reikalingus numatyti labiausiai rekomenduotinas ir priimtinas saugos priemones. Modeliu galima būtų naudotis, kai vertinamas saugos lygis arba norima jį pakelti, praktiškai realizuoti saugos standartų rekomendacijas.

Pritaikyti sprendimų medžiai suteiktų konstruktyvų ir greitą saugos priemonių rekomenduotinumo vaizdą, paremtą praktiniais rodikliais.

1.5. Tyrimo metodika

Analitinėje darbo dalyje atliekama šiuolaikinių kompiuterių tinklų saugos užtikrinimo metodikų bibliotekinis tyrimas ir pasinaudojus lyginamuoju analizės metodu išskiriami aptariamų metodikų bendri bruožai ir trūkumai. Pasinaudojus loginės indukcijos metodu formuojama nauja kompiuterių tinklų saugos užtikrinimo metodika. Metodikos pritaikymo modeliui kurti pasinaudojama koncepcinio modeliavimo technika.

1.6. Darbo rezultatai

Kompiuterių tinklų saugos užtikrinimo metodika suderinta su tarptautinių standartų rekomendacijomis rizikai mažinti.

Tinklo saugos priemonių vertinimo modelis pagal organizacijos dydį ir veiklos sektorių.

1.7. Darbo struktūra

Baigiamasis magistro darbas sudarytas iš trijų skyrių.

Pirmame skyriuje apibrėžiamas tyrimo objektas, nustatomi tikslai ir uždaviniai, pagrindžiamas darbo aktualumas ir naujumas, pateikiama tyrimo metodika, laukiami rezultatai ir struktūra.

Antrame skyriuje apžvelgiamos esamos metodikos bei pateikiama atrinktų standartų ISO/IEC 27033-1:2009 ir ISO/IEC 27002:2005 analizė. Standartai lyginami tarpusavyje ir ieškoma bendrų saugos užtikrinimo rekomendacijų, apsaugančių nuo labiausiai paplitusių grėsmių. Toks palyginimas svarbus formuluojant kertinį tinklų saugos užtikrinimo pagrindą. Taip pat skyriuje apžvelgiamos kitų autorių parengtos ir publikuojamos metodikos. Metodikų apžvalga leidžia daryti išvadas, ko trūksta atliktiems darbams nagrinėjama tema ir tuo pačiu, ką reiktų pateikti rengiamoje metodikoje.Taip pat apibūdinama parengta metodika baziniam kompiuterių tinklų saugos užtikrinimui pagal tyrimo rezultatus.

Trečiame skyriuje kalbama apie poreikį tinklų saugos savybių parinkimo modeliui pagal rizikos analizės išvadas. Toks modelis padėtų parinkti saugos priemones,

kurios yra būtinos užtikrinti priimtiną saugos riziką. Skyriuje aprašomi praktikoje jau taikomi pažaidų vertinimo būdai, kurie gali būti adaptuojami. Pasiūlomas priimtiniausias tinklo saugos savybių poreikio organizacijai pagal jos veiklos sritį ir dydį vertinimo modelis.

2. Egzistuojančių metodikų ir tyrimų analizė

2.1. Sąsaja tarp standartų ir metodikų

Kalbant apie kompiuterių tinklų saugą svarbu tinkamai apsibrėžti ir suvokti sąvokas ir ryšį tarp standartų ir metodikų. Tai tampa itin aktualu, kai pagal poreikį bandoma parinkti teorinę arba praktinę kompiuterių tinklo saugos užtikrinimo pagalbinę priemonę, pagal kurią vadovaujamasi nustatant, diegiant ar tobulinant saugą tinkluose.

Standartas yra nusistovėjusių, įvertinamų, pasiekiamų, įgyvendinamų ir suprantamų teiginių arba kriterijų rinkinys. Tai žinių rinkinys, kuris yra laikomas gera praktika. Gretinant su nuostatais (angl. policy), kurie nurodo kas turi būti padaryti, bet nenusako kokiu būdu, standartas yra kaip etalonas pamatavimui, stebėjimui ir palyginimui, taigi pagal jį gali būti vertinamas saugos lygis. Atotrūkio nuo teorijos atžvilgiu standartas yra artimesnis praktikai nei nuostatai.

Metodika yra metodų, procesų ir praktikų rinkinys, kurie yra kartojami daug kartų. Apibendrintai galima sakyti, kad standartas yra pateikta geriausia saugos praktika, o metodika yra procesai kaip tą praktiką realizuoti. Taigi metodika turi daugiausiai praktinės saugos įgyvendinimo vertės nei standartai ir dar labiau nei strategijos.

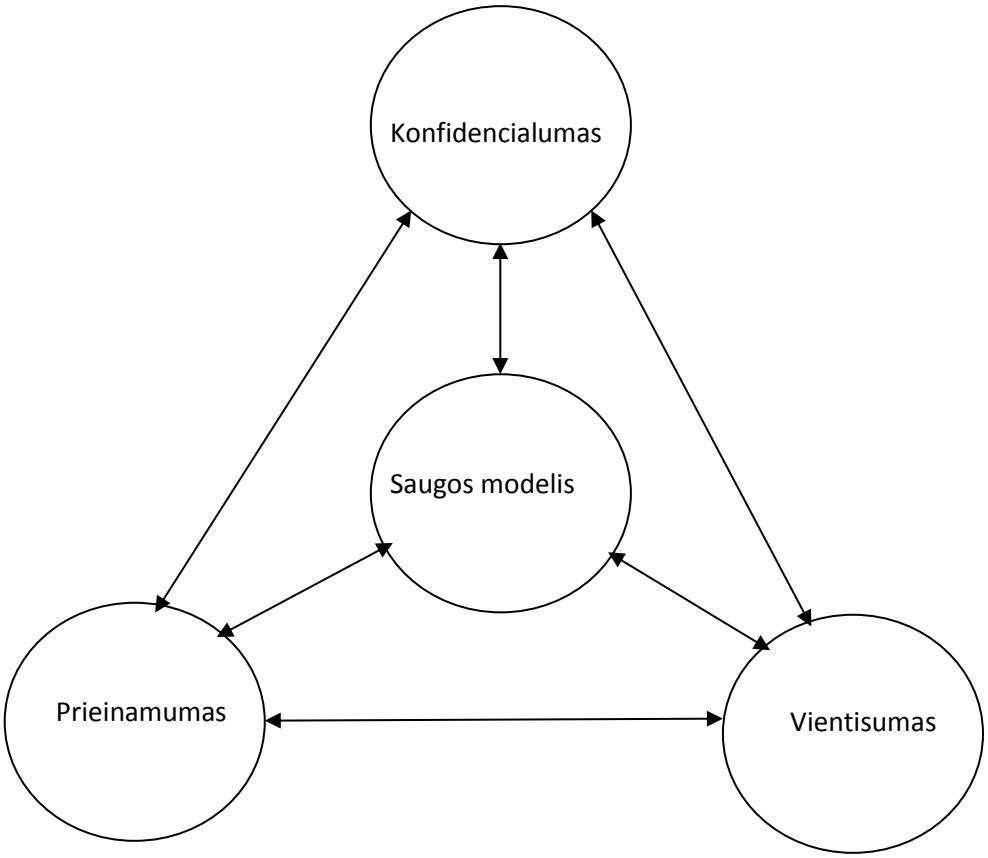
2.2. Kriterijai metodikai

Metodikos realizavimas pagal informacijos technologijos saugos standartus užtikrintų produktų ar paslaugų kokybę, saugą, patikimumą, efektyvumą ir suderinamumą [41]. Vadovaujantis metodika turėtų būti įgyvendinama CIA triada (4.1 pav.), pagal kurią saugiose sistemose turėtų būti užtikrinta:

Konfidencialumas (ang. Confidentiality) – užtikrinti, kad informaciją peržiūrės tik autorizuoti asmenys.

Integralumas (ang. Integrity) – užtikrinimas, kad duomenis pasiekts gavėją nepakeisti ir tokia tvarka kokia buvo perduoti siuntėjo.

Prieinamumas (angl. Availability) – informacija yra pasiekiama autorizuotų naudotojų tada, kada reikia.



2.2.1 pav. CIA triada [6]

Užtikrinant tinklų saugą reikia įtraukti prevencijos (angl. prevention), aptikimo (angl. detection) ir atsako (angl. response) mechanizmus. Kadangi nėra tobulų prevencijos priemonių, nuošalyje negali būti palikti kiti paminėtieji mechanizmų tipai [2].

Dėl įvairaus ir masinio atakų skaičiaus įmonės ir organizacijos vis dažniau nusprendžia pasirūpinti sauga pasiremdamos rekomendacinio pobūdžio tarptautiniais informacinių technologijų saugos ISO/IEC standartais. Tarptautinė standartizacijos organizacija (ISO - the International Organization for Standartization) ir Tarptautinė elektrotechnikos komisija (IEC – the International Electrotechnical Commision) sudaro specializuotą pasaulinę standartizacijos sistemą [15].

Norint remtis tam tikru standartu/ais išryškėja atotrūkis tarp teorinio pateikimo ir praktinio taikymo. Šiuo metu trūksta praktinių metodikų, kurios apibrėžtų, kas turi būti atlikta, kad galima būtų sumažinti tam tikrą riziką. Dažnai standartai naudojami ne prieš realizuojant saugos užtikrinimą, o po to, kai jis vertinamas ar tobulinamas. Nuo pat saugos užtikrinimo pradžios taikomi metodai padėtų įvertinti standartų taikymo įtaką organizacinės

vertės kūrimui ir taip lemtų standartų atnaujinimo procesus bei leistų daryti kitas saugos srities išvadas.

Sudaryta metodika turėtų būti adaptuojama prie unikalios organizacijos aplinkos. Tinklo saugos ypatybių parinkimui, kaip saugos valdymo daliai, reikalingas įvertinimas arba metrikos. Tokios metrikos turėtų leistų objektyviai įvertinti, kurios tinklo saugos ypatybės turi aukščiausią prioritetą, o kurios žemiausią.

Sudarant metodiką svarbu nubrėžti ribą tarp to, kas yra bazinės kompiuterių tinklo saugos priemonės, o kas gali būti priskirta sudėtingesniam lygiui. Bazines kompiuterių tinklų saugos priemones atskirti nuo sudėtingesnio lygio realizacijų galima pasinaudojus tinklų projektavime naudojamais funkciniais elementais, išskiriant skirtingo sudėtingumo grupes:

- Bazinės – realizuota paprasta technologija, pvz., prieigos kontrolės sąrašai (angl. access control lists - ACLs).
- Patobulintos – dažnai kitos technologijos pagrindu įgyvendinta saugos priemonė, pav. elektroninis parašas. Patobulintos priemonės taip pat yra vienos funkcijos, bet lyginant su bazinėmis daug sudėtingesnės.
- Integruotos – mišrus bazinės ir patobulintos grupių junginys veikimui su keliais funkciniais elementais.

2.3. Šiuolaikinių metodikų apžvalga

Dauguma suformuluotų saugos procedūrų yra skirtos TCP/IP taikomajam lygmeniui, dėl to yra poreikis transporto ir tarptinklinio lygmens metodikai. Vieninga tinklo saugos metodika užtikrintų kritinių saugos grėsmių likvidavimą, tačiau turėtų išlaikyti komunikacijos poreikius tenkinantį funkcionalumą. Tokio tipo metodika turėtų sumažinti tinklo saugos pažaidas, kurias galima skirstyti į [2]:

- Technologines - tinklo įrangos technologijos turi būdingas spragas.
- Konfigūravimo - tam tikri tinklo įrangos nuostačiai neapgalvoti, taip pat paliekamos saugos spragos, kurios sukelia didelę atakų riziką.
- Saugos politikos - apibrėžiama, kas prie ko turi priėjimą, ir kokius

veiksmus gali daryti.

Publikacijose ir kituose šaltiniuose pabrėžiama tinklo skaidymo į zonas svarba. Tinklo zonos atskiriamos užkardomis. Vienas iš saugaus tinklo organizavimo būdų yra vidinio, kaip patikimo, tinklo atskyrimas nuo išorinio. Tinklo sluoksnių saugos koncepcija leidžia sumažinti incidento žalos dydį [37].

Doug White ir Alan Rea sudarytos sričių paradigmos esmę sudaro tinklo skaidymas į vidinį, perimetro kraštinį (angl. border) ir išorinį. Tokių sluoksnių sauga neatsiejama nuo įvykių žurnalų (angl. logs) saugojimo. Kuo išsamesni įvykių žurnalai, tuo lengvesnis incidentų priežasčių nagrinėjimas. Tačiau reikia atsižvelgti, kad įvykių žurnalai užima daug vietos ir yra problemiškas jų saugojimas ir peržiūrėjimas. Įvykių žurnalai turi būti saugomi atskiruose įrenginiuose apsaugotose zonose.

Publikacijoje akcentuojama informacijos perėmimo (angl. interception) grėsmė jai keliaujant išoriniu tinklu, esančiu už įmonės ar organizacijos kontrolės ribų. Informacijos mainų išoriniu tinklu kontrolei ir šifravimui naudojama VPN tinklas, kuris gali būti realizuojamas IPSec protokolu. IPSec protokolas yra skirtas išoriniu tinklu siunčiamiems paketams apsaugoti, palaiko šifravimo savybę, vientisumo užtikrinimą ir autentifikavimą. Realizuotas IPSec protokolas laikomas saugiu tuneliu tarp dviejų mazgų. IPSec apima du pagrindinius protokolus. Pirmąjį galima paminėti raktų apsikeitimo internetu (angl. Internet Key Exchange – IKE) protokolą, kuris skirtas kontroliuoti simetrinių raktų padalijiimą tarp įrenginių, kuriuose veikia IPSec. IPSec yra efektyvus būdas apsisaugoti nuo neautorizuotų įrenginių įterptos klaidingos maršruto parinkimo informacijos. Kita IPSec dalis yra ESP/AH – saugi įdėta įkrova (angl. Encapsulated Security Payload) užtikrina IP paketų šifravimą ir vientisumą ir AH (angl. Authentication header) - tik vientisumą [44].

Organizuojant suskirstyto į zonas tinklo saugą išskiriami keli saugos lygiai ir naudojamos atitinkamo tipo užkardos: paketų filtravimas, taikomojo lygmens tarpininkas ir personalinės. Paketų filtravimo užkardos naudojamos apsaugoti žemo lygio atakas, nukreiptas į demilitarizuotą (angl. demilitarized – DMZ) zoną. Taikomojo lygmens užkarda tinkama naudoti prieš vidinį tinklą. Tokia užkarda labiausiai gali apsaugoti vidinį tinklą ir nesukelia vadinamojo butelio kaklelio efekto, nes tikėtina, kad srautas į vidinį tinklą yra mažas. Vidinio tinklo galiniai įrenginiai įprastai saugomi ir personaline užkarda. Pabrėžiama, kad tolimiausiame tinklo krašto taške turi būti apribotas tiek įeinantis, tiek išeinantis srautas ir taip užtikrinant dvikryptę saugą [44]. Užkardos taisyklės išeinančiam srautui turi būti sudarytos taip, kad iš organizacijos tinklo vidaus nebūtų atakuojami išoriniai tinklai. Anksčiau tinklo

perimetrui apsaugoti naudotas statinio paketų filtravimo užkardos, galinčias filtruoti paketus pagal tinklo lygmenį, pakeitė išsamios analizės užkardos (ang. stateful packet inspection - SPI) [24]. SPI užkardos, galinčios fiksuoti pastovias TCP ir UDP jungtis. Statinė paketų užkarda praleis ateinantį srautą tik į tuos aukštos numeracijos (1024-65535) prievadus, kurie apibrėžti užkardos lentelėje, nes tokie prievadai generuojami automatiškai ir yra tik laikinai paskirti TCP jungties metu, kai tuo tarpu 0-1024 prievadai priskiriami tam tikrai paslaugai (pvz., 25-asis SMTP).

Be minėtųjų tinklo dalių, dar išskiriama DMZ – sritis, kurioje patalpinti serveriai, kuriems reikalingas ryšys su išore [44]. Saugaus tinklo architektūrai nepakanka turėti atskiras saugos zonas. Kitas etapas yra virtualių tinklų (angl. Virtual Local Area Networks - VLANs) sukūrimas. Nepatikimi virtualūs tinklai galėtų būti kuriami viename komutatoriuje, DMZ skirti kitame, o dar viename patikimieji, kurių tikėtina yra daugiausia [42]. DMZ zoną taip pat rekomenduojama skirstyti į atskirus potinklius, kad pavyzdžiui atakos vykdomos prieš žiniatinklio serverius neturėtų neigiamo poveikio pašto serveriams.

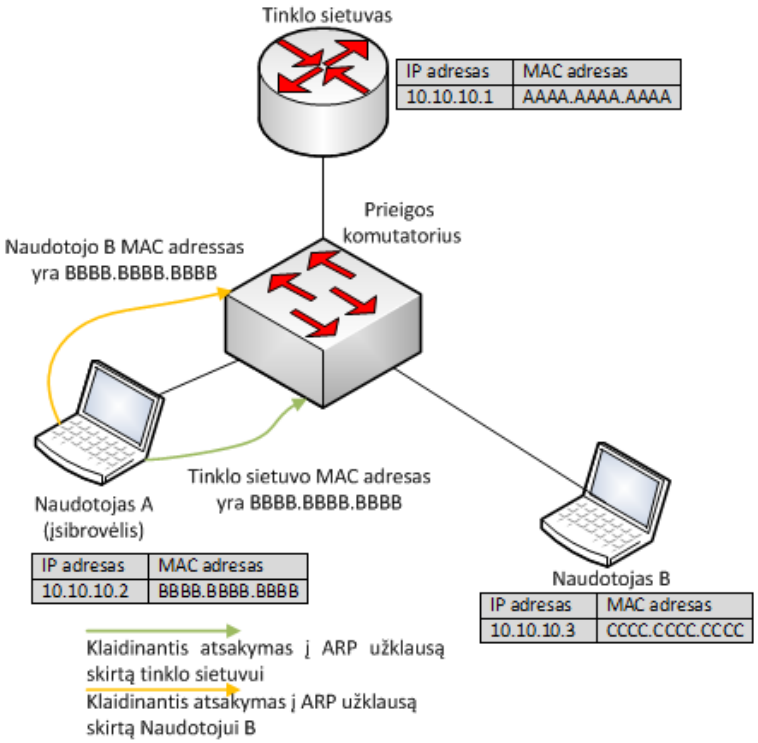
E. Garla, V. Duboskaja akcentuoja, kad projektuojant tinklus dažniausiai siekiama įdiegti šiuos saugos sprendimus ir technologijas:

- Filtrus arba prieigos sąrašus.
- Tinklo adresų transliavimą (angl. Network Address Translation - NAT).
- Loginį ir fizinį tinklo segmentavimą.
- Užkardą.
- Tinklo prieigos kontrolę.
- Įsilaužimų prevencijos sistemą (angl. Intrusion Prevention System - IPS).
- VPN.

Sistemingą tinklų saugojimą CERT (Computer Emergency Response Team) 2002-ais metais apibrėžė SkiP (Security Knowledge in Practice) metodu. Vadovaujantis juo tinkle turi būti imtasi priemonių, sunkinančių įsilaužimų vykdymą, turi būti pranešta apie sistemų anomalijas ir akcentuojamas analizavimo poreikis, siekiant numatyti galimas problemas, taip pat įtraukiant įsibrovimų požymių turinčių anomalijų prevenciją. SkiP taip pat apima ir atsaką į įsibrovimus, praktikų ir metodų tobulinimą atnaujinus sistemą [35].

TCP/IP tinklo sauga gali būti ir yra dažnai nagrinėjama pavienių įrenginių ribose, atsižvelgiant į jiems būdingas grėsmes ir priemones mažininti. SUN Wei-ja ir CAI Hao [43] pateiktos eksperimentais pagrįstos komutatorių perdavimo ir išmokimo (angl. self-learning) algoritmo veikimo saugos rizikos, kurios negali būti sumažintos užkarda arba antivirusine programa.

Publikacijoje tiriama komutatorių nuodijimo ataka realizuojama, kai komutatoriaus adresų lentelėje (Content addressable Memory – CAM) yra įrašomi įsibrovėlio siųsti suklastoti MAC adresai. Jie įrašomi CAM lentelėje, kai atakuojamajam siunčiamas ARP užklausos atsakymas su įsibrovėlio MAC adresu vietoj legalaus [29]. Įsibrovėlis siunčia tokį kiekį duomenų kadrų su klaidingais MAC adresais, kad užsipildo CAM lentelė. Tai lemia tai, kad komutatorius visus paketus, kuriuos jis gauna, ištransliuoja per visus prievadus, išskyrus tuos per kuriuos gavo duomenis. Tokių sąlygų pakanka, kad kenkėjas galėtų šnipinėti komutuojamą LAN tinklą [43].



2.3.1 pav. Ataka išnaudojant ARP protokolą

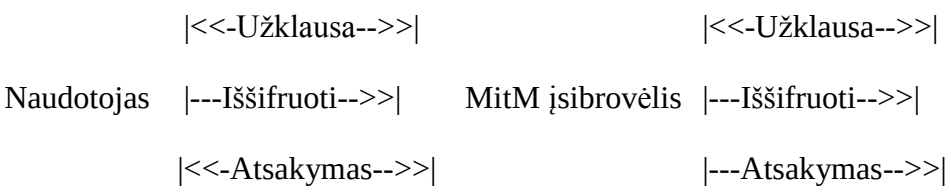
Kita nagrinėjama klaidingai perduodamų duomenų ataka įvykdoma, kai įsibrovėlis suklaidina ARP užklausą, apsimesdamas, kad jis turi IP adresą, kurio klausiama ir įsirašo savo MAC adresą. Grįžtant ARP užklausai pagal išmokimo algoritmą komutatorius

teisingą prievadą pakeičia suklastotu. Tokiomis sąlygomis įsibrovėlis gali įvairiai pasinaudoti duomenimis: juos surinkti, kai duomenų kadrai nebėra perduodami teisėtam gavėjui, vykdyti tarpininko (angl. Man-in-The-Middle - MiTM) ataką nepakeistus duomenis siųsdamas gavėjui ir taip pasyviai šnipinėdamas, perduoti pakeistus duomenis ir vykdyti kitą kenkėjišką veiklą.

Straipsnyje apibrėžta komutatorių saugos strategija, kuri sudaryta iš:

- Apsisaugojimui nuo apnuodijimo atakų prievadui ribojamas transliavimo individualiems ir grupiniams adresams kadrų su nežinomu MAC adresu skaičius.
- Dar vienas metodas apsisaugoti nuo apnuodijimo atakų yra apriboti komutatoriaus įsirašomus MAC adresus vienam prievadui.
- Maksimalaus skaičiaus duomenų transliavimo individualiems, grupiniams arba visiems adresams kadrų ribojimas per tam tikrą laiko vienetą (dažniausiai sekundę). Taip pat pagalbai nuo apsinuodijimo atakos, kad būtų išvengta MAC adreso suklastojimo, prievadui nurodomas tik vienas galimas MAC adresas. Papildomai tai apsaugo nuo MAC adresų dubliavimosi.

Publikacijose aptariami ir kiti atakos modeliai. Bendras MitM atakos scenarijus yra užpuoliko įsiterpimasį kliento ir serverio komunikaciją. Tokio scenarijaus metu įsibrovėlis perduoda klaidingas žinutes sukurdamas saugaus komunikavimą įvaizdį tarp kliento ir serverio, taip atrodydamas kaip serveris klientui arba klientas serveriui. Techniškai užpuolikas gali naudoti programą, kuri atrodo kaip serverio klientas arba atvirkščiai. Pavykus atakai galimas perduodamų paketų šnipinėjimas, autentifikuotų sesijų perimimas, paketų įterpimas arba komandų siuntimas serveriui ir siunčiant suklastotus atsakymus naudotojui. MitM atakomis siekiama jautrios ir vertingos informacijos. MitM atakomis gali būti siekiama suklaidinti komunikaciją naudotojo arba serverio pusėje ir perimti informaciją (pvz.,. identitetą, adresą, slaptažodį ar kitą konfidencialią informaciją, kuri būtų panaudota kenkėjiškais tikslais) ir taip pat tuo pačiu metu pakeisti perdavimą. Naudotojo - serverio scenarijus gali būti atvaizduotas taip:



DHCP klaidinimo atakos metu įsibrovėlis pateikia save kaip DHCP serveris ir atsako į DHCP užklausimus su klaidingu IP ir MAC adresu.

DHCP apsimetimo atakos scenarijus:

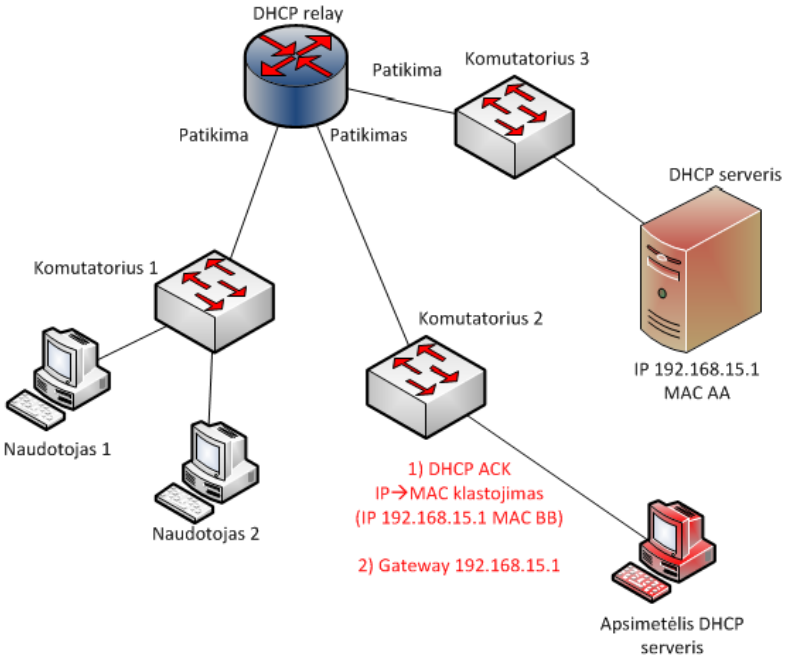
1) Įsibrovėlis paleidžia DHCP serverį, kuris siunčia įsibrovėlio IP adresą kaip numatytą tinklo sietuvo IP adresą.

2) Auka jungiasi į tinklą ir turi gauti IP adresą per DHCP.

3) Įsibrovėlis aplenkia tikrą DHCP serverį ir siunčia suklastotą DHCP patvirtinimą aukai ir taip tapdamas aukos tinklo sietuvu.

4) Auka gauna įsibrovėlio IP adresą kaip savo numatytąjį tinklo sietuvą DHCP atsakymo žinutėje.

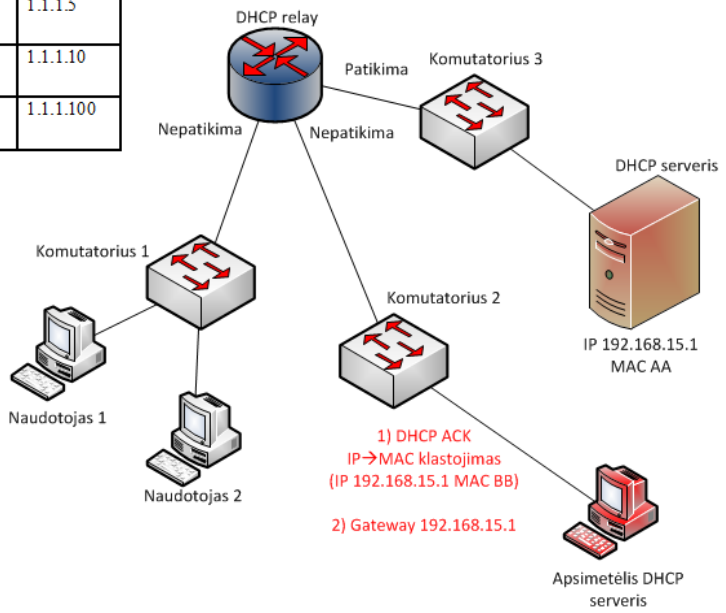
5) Įsibrovėlis turi sąlygas įsiterpti į persiunčiamus IP paketus.



2.3.2 pav. DHCP atakos modelis

DHCP sąsajų lentelė

Prievadas	MAC	IP
1/1	AA	1.1.1.5
1/2	DD	1.1.1.10
1/3	EE	1.1.1.100



2.3.3 pav. DHCP atakos modelis

Prevencinė priemonė nuo tokios atakos yra tikrinimas, ar iš to prievado galima gauti atsakymą į DHCP užklausą. Taigi jeigu bus gaunamas atsakymas iš nepatikimo

prievado, tai jis bus atmetamas. Tikrinama pagal dinaminių ARP įrašų lentelę. Plačiau apie šios priemonės taikymą aprašyta A priede pateiktoje metodikoje.

Daug testuojamų modelių yra pagrįsti įsibrovimu iš tinklo vidaus. Pagal CSI/FBI atliktą tyrimą tik 32 % apklaustųjų mano, kad niekada nėra atakuoti iš vidinio tinklo. Tyrimai parodo, kad darbdaviai atakuojami dėl paprasčiausios priežasties – jau turima prieiga prie tinklo [8]. Taip pat net 15% atakų yra vidinių darbuotojų neautorizuota prieiga ir privilegijų ribų nepaisymas.

2.3.1 lentelė. Tinklų tipai ir jiems būdingos atakos

Saugos zonų skaičius	**Naudotojų grupių skaičius**	**Komutatorių skaičius**	**Atakos**
1	Viena	Vienas	MAC klastojimas CAM lentelės perpildymas
1	Viena	Daugiau nei 1	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN STP atakos
1	Daugiau nei 1	Vienas	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN
1	Daugiau nei 1	Daugiau nei 1	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN STP atakos

Daugiau nei 1	Viena	Vienas	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN
Daugiau nei 1	Viena	Daugiau nei 1	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN
Daugiau nei 1	Daugiau nei 1	Vienas	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN Privataus VLAN atakos
Daugiau nei 1	Daugiau nei 1	Daugiau nei 1	MAC klastojimas CAM lentelės perpildymas Peršokimas per VLAN Privataus VLAN atakos

Rečiau publikacijose yra minimos maršruto parinktuvų grėsmės: neautorizuota prieiga, sesijos perėmimas, maršrutų nukreipimas, paslaugų trikdymas (angl. Denial of Service - DoS), slaptas pasiklausymas ir informacijos vagystės [3]. Užtikrinant maršruto parinktuvų saugą, be visiems tinklo įrenginiams aktualių saugos nustatymų, reikia skirti dėmesio saugių maršruto parinkimo protokolų realizavimui, pavyzdžiui BGP maršruto parinkimo protokolui galima nustatyti MD5 autentifikaciją [29]. TCP sujungimui tarp dviejų mazgų. MD5 autentifikavimas nėra tik paprastas slaptažodžio siuntinėjimas atnaujinimų metu [30]. MD5 raktas naudojamas suskaičiuoti atnaujinimų metu siunčiamais duomenimis

paremtą parašą. MD5 algoritmas, kaip ir IPSec protokolu realizuotas VPN, leidžia apsisaugoti nuo maršruto parinkimo informacijos pakeitimo.

S. Alabady pateikia procesų rinkinį, skirtą maršruto parinktuvų ir užkardų saugos užtikrinimui, tokių kaip nuotoliniu būdu prijungiančių prie įrenginio autorizavimas, nuotolinio valdymo ir stebėjimo protokolų (pvz., SNMP) ribojimas, prieigos kontrolės sąrašų nustatymą kenksmingo srauto nufiltravimui ir kt.

Norėdami įsitikinti komutatorių, maršruto parinktuvų pažaidomis kaip kurie autoriai pateikia testavimo pavyzdžius, pasinaudoję programomis:

- Nessus – programinė įranga, skirta nuskaityti tinklo pažaidas. Nessus parodo, kokios paslaugos ir procesai yra leidžiami tinkle. Pasinaudojus tokia informacija galima įvertinti tinklo saugą arba išnaudoti spragas kenkėjiškai veiklai.
- Dsniff – gali būti panaudotas ARP klastojimui, ir jei ataka sėkminga, įsibrovėlis gali stebėti duomenų srautą.
- Ethereal – atakų metu būtų naudojamas tinklo srauto analizei. Simuliuojant atakas galima bandyti surinkti informaciją apie slaptažodžius, CAM ir maršruto parinkimo lenteles [2].
- Nmap - programa nuskenuoja atvirus maršruto parinktuvo arba užkardos TCP ir UDP portus.
- Macof – galima panaudoti atakoms prieš komutatorius: MAC suklastojimui ir CAM perpildymui [2].

Kad įvertinti suformuluotą metodiką sudaroma lentelė jos palyginimui su anksčiau publikuotomis ir darbe aptartomis tinklo saugos užtikrinimo procedūromis:

2.3.2 lentelė. Metodikų palyginimas

Tinklo saugos užtikrinimo priemonės	**Doug White ir Alan Rea metodika**	**SUN Wei-ja ir CAI Hao metodika**	**S. Alabady metodika**	***Allied Telesis* (įrangos gamintojas) metodika**	**Suformuluota metodika**
Slaptažodis fiziniam sąrankos prievadui (angl. console)					+
Slaptažodis SSH v3 prisijungimui			+		+
Prieigos sąrašai SSH v3 prisijungimo ribojimui	+			+	+
TELNET prisijungimo išjungimas			+		+
Hiperteksto protokolo (angl. Hypertext Transfer Protocol Secure – HTTP) išjungimas			+		+
Dinaminis ARP tikrinimas		+			+
ARP galiojimo laiko nustatymas					+
Maksimalaus perduodamų transliavimo individualiais adresais (angl. unicast), transliavimo grupiniais adresais (angl. multicast) ir transliavimo (angl. broadcast) tipo kadrų		+			+

skaičiaus per laiko vienetą apibrėžimas					
Nežinomam MAC adresui perduodamų transliavimo individualiais adresais, transliavimo grupiniais adresais kadrų skaičiaus ribojimas		+			
MAC adresų ribojimas prievadui		+	+	+	+
Šaltinio IP tikrinimas				+	+
LLDP išjungimas arba apribojimas			+		+
Tiesioginių transliavimo paketų išjungimas			+		
STP įjungimas				+	+
STP pagrindinio komutatoriaus tikrinimas (angl. root guard)				+	+
STP BPDU kadrų tikrinimas				+	+
Kelių virtualių tinklų praleidimo per vieną kanalą protokolo slaptažodis					+
Tinklo skaidymas į virtualius tinklus					+
Privačių tinklų kūrimas				+	+
Nenaudojamų prievadų saugi konfigūracija			+		+
Prieigos prievadų				+	+

nustatymas praleisti tik vieną virtualų tinklą					
OSPF kaimynystės autentifikacija MD5 algoritmu koduotu slaptažodžiu					+
BGP prieigos sąrašai					+
BGP MD5 autentifikacija					+
BGP kaimynų įvykių žurnalų vedimas					+
SNMP protokolo sauga			+	+	+
Saugomi žunalo įrašai	+			+	+
Stebimas pralaidumas	+				+
Įsibrovimų aptikimo sistemos (angl. Intrusion detection systems – IDS)		+	+		+
Įsibrovimų prevencijos sistemos (angl. Intrusion prevention systems – IPS)					+
Pagrįstas skirstymas į saugos zonas	+				+
Slaptažodžiai konfigūracijose saugomi šifruoti					+
Autentifikacijos serveris	+		+	+	+
VPN IPsec	+				+

Sudarant metodiką buvo atsižvelgta į šiuolaikinių metodikų trūkumus. Magistrinio darbe sudaryta metodika apima TCP/IP L2 ir L3 lygmenų saugą, architektūrinius reikalavimus, prieigos kontrolę, nėra pritaikyta konkrečiam gamintojui, išlaiko universalumą. Kuriamą metodiką siekiama suderinti su tarptautiniais ISO/IEC standartais.

2.4. ISO/IEC saugos standartai

Aktualiausi standartai norint išvengti kompiuterių tinklų saugos rizikos atrinkti ISO/IEC 27002:2005 (Informacijos technologija. Saugos metodai. Informacijos saugos valdymo praktikos kodeksas) bei ISO/IEC 27033-1:2009 (Informacijos technologija. Saugos metodai. Tinklo sauga.).

2.5. ISO/IEC 27033-1:2009

ISO/IEC 27033-1 standartas apžvelgia rizikos, projektavimo ir kontrolės aspektus tam tikram tinklo tipui ar situacijai: bevielis tinklas, virtualūs privatūs tinklai, tinklo segmentavimas ir t.t. [15].

Standartu galima vadovautis rizikos identifikavimui ir analizei, o tokios analizės rezultatai leidžia apibrėžti tinklo saugos reikalavimus. Pateikiama techninės arba kitokio tipo tinklo saugos kontrolės apžvalgos.

Standartas klasikinį CIA saugos modelį papildo negalėjimas atsisakyti (angl. non-repudation) ir patikimimo (angl. reliability) reikalavimais.

2.6. ISO/IEC 27002:2005

ISO/IEC 27002:2005 informacijos saugos valdymo praktikos kodekse yra suformuluoti reikalavimai prieigos kontrolei, tokie kaip nuosekli prieigos prie tinklų valdymo politika ir naudotojų profilių kūrimas, privilegijų valdymui pabrėžiant, kad asmenims nebūtų suteikta daugiau teisių nei reikia jų funkcijoms atlikti.

2.7. Kompiuterių tinklų saugos rizikos mažinimo priemonės

Tinklo saugos klausimas neatsiejamas nuo grėsmių, kurių apibrėžimas aktualus suvokiant standartų rekomendacijų ir pagal juos parengtų procesų rinkinio naudą. Kad būtų išskirtos saugos priemonės tokių grėsmių mažinimui ieškoma ankstesniame skyriuje apibrėžtų

standartų bendrumų. Atsižvelgiant į standartų rekomendacijas, kurias galima realizuoti kompiuterių tinklų saugai, parenkamos saugos užtikrinimo priemonės:

2.7.1 lentelė. Saugos grėsmių mažinimo priemonių parinkimas pagal informacijos technologijos saugos standartus

ISO/IEC 27002	**ISO/IEC 27033-1**	**Sudaryta metodika (A priedas)**
10.4.1 Apsaugos nuo kenkimo programų valdymo priemonės.	8.5 Tinklo audito žurnalo įrašai ir stebėjimas. 8.6 Įsibrovimų apsauga ir prevencija. 8.7 Apsauga nuo kenkimo programų.	27. Įsibrovimų aptikimo sistema (angl. Intrusion Detection System – IDS). Įsibrovimų prevencijos sistema (angl. Intrusion Prevention System - IPS).
8.3.3 Pasibaigus darbuotojo, rangovo ir trečiosios šalies atstovo darbo, samdos sutarties ar susitarimo galiojimo laikui, visos jiems anksčiau suteiktos prieigos ar informacijos apdorojimo priemonių teisės turėtų būti panaikintos arba pritaikytos naujai prie naujų pareigų.		11. IEEE 802.1x protokolo naudojimas.
	8.5 Tinklo audito žurnalo įrašai ir stebėjimas.	22. Maršruto parinkimo kaimynų įvykių žurnalai. 26. Žurnalų įrašų serverio konfigūravimas tinklo įrenginiuose. 23. Paprasto tinklo valdymo

		protokolo (angl Simple Network Management Protocol – SNMP) saugus konfigūravimas.
10.2.2 Trečiosios šalies teikiamos paslaugos, ataskaitos ir kiti dokumentai turėtų būti nuolat stebimi ir tikrinami, turėtų būti reguliariai atliekamas auditas. 10.6.2 Tinklo paslaugų saugumas.	8.2.4 Tinklo srauto stebėjimas. 8.5 Tinklo audito žurnalo įrašai ir stebėjimas.	23. Saugus SNMP protokolo naudojimas. 25. Tinklo srauto stebėjimas.
10.6.2 Tinklo paslaugų saugumas. 11.4.7 Tinklo maršrutų valdymas. 12.2 Kriptografinė kontrolė.	8.8 Kriptografija paremtos paslaugos.	5. Saugus nuotolinio prisijungimo (angl. Secure Shell - SSH) trečiosios versijos protokolo naudojimas. 8. Saugus hiperteksto protokolo (angl. Hypertext Transfer Protocol Secure – HTTPS) protokolo naudojimas jungiantis per žiniatinklį. 12. VTP (Virtual Trunking Protocol) slaptažodžio konfigūravimas. 18. Trumpiausio kelio (angl. Open Shortest Path First – OSPF) maršruto parinkimo protokolo kaimynų autentifikacija. 19. OSPF maršruto parinkimo protokolo kaimynų prieigos sąrašai. 20. Kraštinio maršruto parinkimo (angl. Border Gateway Protocol - BGP) maršruto parinkimo protokolo

		kaimynų autentifikacija. 21. BGP maršruto parinkimo protokolo kaimynų prieigos sąrašai 24. Slaptažodžių šifravimas.
10.1.3 Siekiant sumažinti galimybę nesankcionuotai ir netyčia pakeisti arba piktnaudžiauti organizacijos turtu, turėtų būti aiškiai atskirtos pareigos ir numatytos atsakomybės sritys. 11.6.1 Informacijos prieigos ribojimas. 10.6.2 Tinklo paslaugų saugumas. 11.2.2 Privilegijų valdymas. 11.4.1 Naudotojai turi prieigą tik prie tų paslaugų, kuriomis jiems buvo suteikta teisė naudotis. 11.4.2 Naudotojo autentifikavimas išoriniamas prisijungimams. 11.5.2 Naudotojo identifikavimas ir	8.2.2.2 Tinklo saugos taisyklės. 8.4 Identifikacija ir autorizacija.	6. Apibrėžti SSH v3 prisijungimo prieigos sąrašai. 7. HTTP išjungimas. 8. Apibrėžti HTTPS prisijungimo prieigos sąrašai. 11. IEEE 802.1x protokolo naudojimas.

autentifikavimas. 12.5.4 Turėtų būti apsisaugota nuo galimo informacijos nutekėjimo.		
11.4.4 Turi būti kontroliuojamas fizinis ir loginis priėjimas prie diagnostinių ir sąrangų prievadų. 11.5.1 Saugios prisijungimo procedūros.		4. Fiziniam sąrankų prievadui prisijungimui naudojamas slaptažodis. 5. Saugus nuotolinio prisijungimo (angl. Secure Shell - SSH) trečios versijos protokolo naudojimas. 6. Apibrėžti SSH v3 prisijungimo prieigos sąrašai. 7. Saugus hiperteksto protokolo naudojimas jungiantis per žiniatinklį. 8. Apibrėžti HTTPS prisijungimo prieigos sąrašai. 15. Nenaudojamų prievadų saugus virtualių tinklų konfigūravimas.
11.4.5 Tinkluose turėtų būti atskiros informacijos paslaugų, naudotojų ir informacijos sistemų grupės.	9.2 Saugi tinklo architektūra/dizainas.	29. Tinklo skaidymas į zonas.
11.4.6 Naudotojų galimybės prisijungti prie bendro naudojimo tinklų, ypač išplėstų už organizacijos ribų, turėtų būti apribotos,	8.8 Kriptografija paremtos paslaugos. 9.2 Saugi tinklo architektūra/dizainas. 10.9 Tinklo palaikymas	28. VPN IPSec konfigūravimas.

atsižvelgaint į prieigos valdymo politiką ir į veiklos reikalavimus.	keliaujantiems naudotojams. 10.10 Tinklo palaikymas namų ir mažo verslo padaliniams.	
9.6 Kritinės ir jautrios informacijos apdorojimo priemonėms sukurti tinkami saugos barjerai. 10.6.2 Tinklo paslaugų saugumas. 12.5.4 Turėtų būti apsisaugota nuo galimo informacijos nutekėjimo.	8.2 Tinklo saugos valdymas.	1. Dinaminio adreso keitimosi protokolo (angl. Address Resolution Protocol – ARP) inspekcijos ir DHCP sąsajų bazės naudojimas. 2. ARP atsakymų dažnio limito nustatymas. 3. Statinių prieigos valdymo (angl. Media Access Control – MAC) adresų aprašymas. 9. LLDP (Link Layer Discovery Protocol) išjungimas. 10. LLDP konfigūravimas reikiamiems prievadams. 16. Tinkamo režimo parinkimas prievadui. 17. IP šaltinio tikrinimas. 13. Svarbiausio STP komutatoriaus apsauga. 14. STP BPDU apsauga.
10.6.2 Tinklo paslaugų saugumas.	8.2 Tinklo saugos valdymas.	18. OSPF maršruto parinkimo protokolo kaimynų autentifikacija. 19. OSPF maršruto parinkimo protokolo kaimynų prieigos sąrašai.

		20. BGP maršruto parinkimo protokolo kaimynų autentifikacija. 21. BGP maršruto parinkimo protokolo kaimynų prieigos sąrašai.

Aptariamų standartų lyginimas ieškant priemonių mažinti tam tikras grėsmes ir riziką išskiria bendras aktualiausias saugos priemones, kurios privalomos norint užtikrinti kompiuterių tinklų saugą.

3. Tinklo saugos užtikrinimo priemonių parinkimas pagal organizacijų riziką

Daugiau kaip 150 ekspertų iš vyriausybinių, privačių ir akademinių organizacijų apibrėžė saugos išvadas ir praktines metrikas, kurios apimė taikomojo lygmens saugą, finansinius aspektus, incidentų, pakitimų ir pažaidų valdymą. Buvo aptarti du finansiniai aspektai: informacijos saugos kaip IT biudžeto dalis procentais ir informacijos saugos biudžeto skirstymas [39]. Organizacija, planuodama tinklo saugos užtikrinimą, turi būti numačiusi, kokio dydžio biudžetas jai skiriamas, atsižvelgiant į finansus tinklo įrangai įsigyti, specialisto darbo užmokesčiui ir kt. Investicijos saugai turi būti suderintos su galimais praradimais, kadangi dėl lėšų skyrimo saugai ir todėl padidėjusios produkto arba paslaugos kainos, organizacijos gali būti išstumtos iš verslo. Taigi investicijos saugai susijusios su verslo principais, kai tiek sauga tiek finansiniai aspektai vaidina svarbų vaidmenį. Analitikai nustatė, kad viena valanda tinklo neveikimo didžiausioms pasaulinėms kompaninjoms gali būti įvertintas keletu šimtu tūkstančių dolerių nuostoliu ir maždaug 5% rinkos sumažėjimo, o vidutinė programos neveikimo kaina visiems pramonės sektoriams siekia šimtą tūkstančių dolerių ir vis dar didėja. Tokiems sektoriams kaip finansų paslaugos, finansinės poveikis per valandą gali būti keli milijonai dolerių [19]. Saugos valdymo procesas iš esmės yra rizikos skaičiavimas, reikalaujantis pasikartojančio vertinimo užtikrinant išlaidų, laiko ir išteklių efektyvumą. Rizikos dydis yra potencialaus incidento, dažnai apibūdinamo kaip saugos grėmė arba piknaudžiavimas, dažnio ir poveikio derinys. Atsižvelgiant į tai, kad sauga reikalauja tam tikrų finansinių ir žmogiškųjų resursų, metodikai reikalingas modelis, kuriuo vadovaujantis pagal turimus organizacijos kriterijus galima būtų įvertinti tinklo saugos priemonės reikalingumą. Svarbu nustatyti, kokio lygio sauga reikalinga informacijai, o tuo pačiu ir kompiuterių tinklams, kad užtikrinti tinkamą organizacijos valdymą šiuo klausimu. Taigi reikalingos tinklo saugos priemonių identifikavimas ir analizavimas kad būtų sumažinta tinklo saugos rizika. Šitie aspektai leistų realizuoti ir palaikyti saugų ir funkcionalų tinklą, kuris šiomis dienomis yra kritiškas veiksnys kiekvieno verslo operacijoms [15] [34]. Siekiant sukurti modelį, kuriuo galima būtų vadovautis organizacijoms, kurių tinklo saugos valdymas nėra užtikrinamas arba pradinio lygio, reikalingi organizacijų aplinkos parametrai, šiame darbe apibrėžiami organizacijos dydžiu ir veiklos sritimi. Skirtingo dydžio organizacijų yra

nevienoda informacinių technologijų aplinka, o tuo pačiu ir rizikingumas:

3.1 lentelė. Rizikos priklausomybė nuo organizacijos dydžio

Mažo dydžio organizacijos apibūdinimas	**Vidutinio dydžio organizacijos apibūdinimas**	**Didelės organizacijos apibūdinimas**
Mažas kompleksiškumas	Vidutinio dydžio kompleksiškumas	Kompleksiška
Nedidelis srautas	Talpina dešimtis serverių, įvairių gamintojų techninę įrangą ir programinės įrangos platformas bei įvairias taikomąsias programas.	Aukšti pralaidumo reikalavimai
Keli saugomi informacijos turto tipai (pvz., serveriai, duomenų bazės, taikomosios programos)	Skirtingo tipo informacinis turtas	Daug informacijos turto tipų
		Didelis skaičius nutolusių padalinių ir nuotoliniu būdu dirbančių darbuotojų
Minimali su turtu siejama rizika	*Įvairaus lygio rizikos siejamas su turtu*	*Aukšta rizika*

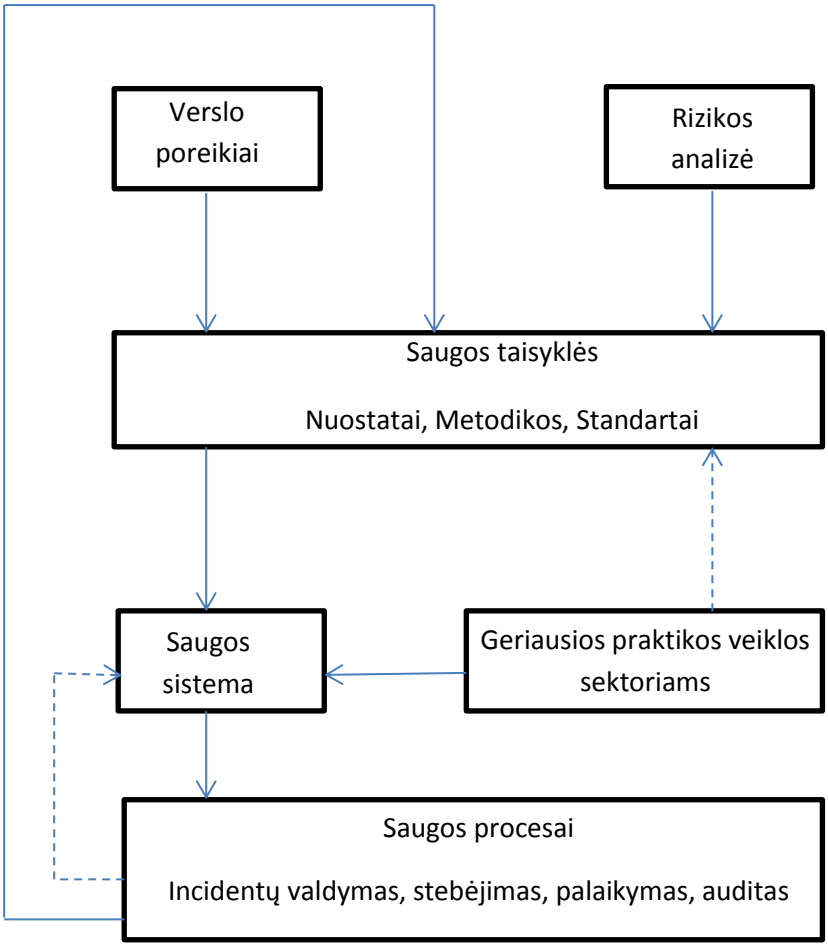
Metodikai reikalingas modelis, kurio pagalba būtų galima klasifikuoti surinktus pažaidų duomenis suskirstant, kokią potencialią žalą gali turėti saugos spraga tam tikro dydžio ir veiklos sektoriaus organizacijai, ir pagal tai leistų spręsti, ar tam tikra saugos priemonė yra pagrįsta. Techninės saugos metrikos leidžia įvertinti ir taip užtikrinti techninio saugos valdymo arba įrenginių/objektų, naudojamų informacinių sistemų saugai, veiksmingumą. Publikacijose pateikiama techninės saugos matavimo modeliai, užtikrinantys veiksmingą tinklo saugos valdymą. Tai gali būti tinklo saugos veiksmingumo matavimas: įrenginių, tokių kaip užkarda, IDS ir IPS sistemos, komutatoriai, bevielės prieigos stotelės, bevieliai valdikliai, tinklo architektūra, bei tinklo paslaugų, tokių kaip saugus hiperteksto protokolas ir

virtualus privatus tinklas [15]. Šiame darbe formuluojamas tinklos saugos priemonių poreikio matavimas prieš įgyvendinant tinklo įrenginių arba tinklo paslaugų saugos savybes.

Vienas iš būdų skaičiuoti organizacijos riziką arba pažaidos lygį yra pasinaudojant CVSS v2 balą. Saugos rizikos valdymo įmonės, skaičiuodamos organizacijos rizikos arba grėsmės lygį, kaip komponentę naudoja CVSS v2 balą. Tokios įmonės naudoja programinę įrangą, kuri gali integruoti organizacijos tinko topologiją, pažaidų duomenis ir turto duomenų bazę, kurie panaudojami kliento informavimui apie galimą rizikos lygį. CVSS v2 gali būti panaudotas pažaidos rizikos skaičiavimui, bet yra nesusietas su unikalia organizacijos aplinka, pateiktas tik skaičiavimo mechanizmas, kuris leidžia įtraukti aplinkos parametrus. Kiekviena organizacija, kuri nori įsivertinti, turėtų žinoti savo reikalavimus konfidencialumui, prieinamumui ir integralumui. Trūksta bendro modelio, kuriuo galima būtų vadovautis, jei jos to negali padaryti. Taip pat trūksta atsižvelgimo į incidento tikimybę konkrečiam veiklos sektoriui. Taip pat CVSS v2 balą reiktų atsieti nuo konkrečioss pažaidos ir panaudoti grėsmės tikimybę atvejams, kai reikia įvertinti darbe siūlomų ar kitame šaltinyje apibrėžtų saugos priemonių parinkimą

Kitas mechanizmas, kuriuo galima vadovautis parenkant tinklo saugo savybes, yra rizikos vertinimo duomenys. Įvykis, kuris identifikuojamas kaip potencialiai galints sutrukdyti pasiekti organizacijos tikslus, yra laikomas rizika, ir turi būti vertinamas pasiremiant įvykio tikimybe ir poveikio tikslams svarbos lygiu.

Rizikos analizės duomenys gali būti panaudoti priimant sprendimą, kurie rizikos veiksniai ir kaip labai gali paveikti organizacijos procesus ir tuo pačiu veiklos rezultatus. Rizikos, kurių gali tikėtis organzacija yra apibūdinamos poveikio ir tikimybės terminais [4]. Poveikio vertės turi atspindėti matavimo vienetus, naudojamus organizacijos tikslams, skirtingus poveikio tipus, tokius kaip finansai, žmonės, reputacija ir t.t. Atitinkamai įvertintos rizikos tikimybės laiko intervalas turi būti suderintas su užsibrėžtu tikslų laiko intervalu. Rizikos valdymas apima grėsmių identifikavimą, įvertinant grėsmių įvykio tikimybę iš jau įvykusių incidentų duomenų ir jų metu paveiktas turtines vertybes. Taip galima pamatuoti galimus praradimus, bei identifikuoti, kurių veiksmų galima imtis mažinant riziką atsižvelgiant, kad investicijos yra pagrįstos. Taip pat turrėtų būti dokumentuoti rezultatai ir įgyvendimo planas valdymo tikslais [26]. Taigi rizikos analizė yra dalis saugaus tinklo užtikrinimo proceso dalis:



3.1 pav. Veiksniai, lemiantys saugaus tinklo projektavimą [25]

Rizikos nustatymas organizacijoje gali būti atliekamas siekiant įvarių tikslų, taigi ir įvarių tipų: strateginis, vidinio audito, vartotojų, tiekimo grandinės, rinkos ir kt. Šiame darbe siekiami tikslai yra susiję su :

- Saugos rizikos vertinimu – galimų pažaidų organizacijos fiziniam turtui ir informacijos saugai vertinimas. Toks vertinimas apima infrastruktūrą, taikomasias programas ir įprastai yra vykdomas žmonių, kurie atlieka organizacijos informacijos saugos funkcijas [4].
- Informacinių technologijų saugos vertinimas – galimų techninių sistemos nesklandumų vertinimas ir informacinių technologijų investicijų saugai grąžos vertinimas. Informacinių technologijų rizikos vertinimas turi apžvelgti vidinius veiksnius, tokius kaip sistemos neveikimo dažnį ir

trukmę, darbuotojų prieigos valdymą, konfidencialių duomenų ir informacijos saugą, bei išorinius, tokius kaip naujos programinės ir techninės įrangos įdiegimą ir kibernetinių nusikaltimų incidentus per praėjusius metus.

Pagal Ahmad R., Azuwa M.P. ir Sahibri rizikos įvertinimas reikalingas įvykdyti ISO/IEC 27001 standarto reikalavimą, kuris apibrėžiamas:

„10.6.1 Tinklo valdymo priemonės. Valdymas. Tinklai turėtų būti tinkamai valdomi ir prižiūrimi, siekiant apsaugoti juos nuo grėsmių bei užtikrinti nuo tinklo priklausomų sistemų, taikomųjų programų ir jais perduodamos informacijos saugumą.“

Publikacijoje apibrėžta rekomendacija, išpildanti standarto reikalavimą, apibrėžiama kaip tinkamo rizikos lygio palaikymas, kad būtų realizuotas tinklo ir saugos valdymas, užtikrinantis informacijos saugą. Rizika vertinama kaip dydis, priklausantis nuo turto vertės, grėsmės ir pažaidos.

Rizikos vertinimo skalė įprastai yra seka verčių pagal svarbą (pvz., žema, vidutinė ir aukšta) bei turi skaitinius atitikmenis (pvz., 1 atitinka žemiausią vertę, 2 – vidutinę, o 3 – aukščiausią). Rizikos vertinimo skalės pasirinkimas gali tikti vienu atveju ir netikti kitu. Skalė turi būti tinkamai apibrėžta suteikiant prasmingą įvertinimą ir parodanti identifikuotos rizikos prioritetus, bei ja turi būti galima vadovautis skiriant organizacijos resursus. Šis vertinimas apžvelgia tokius veiksnius kaip procesų veiksnumą, prieigos kontrolę, duomenų saugą ir kibernetinius nusikaltimus. Toks vertinimas įprastai vykdomas organizacijos informacinių technologijų rizikos specialistų ir valdžios atstovų [4].

3.2 lentelė. Rizikos įvertinimas, atsižvelgus į tikimybę ir poveikį

Tikimybė	**Apibrėžimas**	**Aprašymas**
1	Mažai tikėtina	Mažai tikėtina, kad įvyks incidentas per tikslui apibrėžtą laiko intervalą
2	Tikėtina	Tikėtina, kad įvyks incidentas per tikslui apibrėžtą laiko intervalą
3	Tikrai įvyks	Prognozuojama, kad incidentas tikrai įvyks per tikslui apibrėžtą laiko intervalą

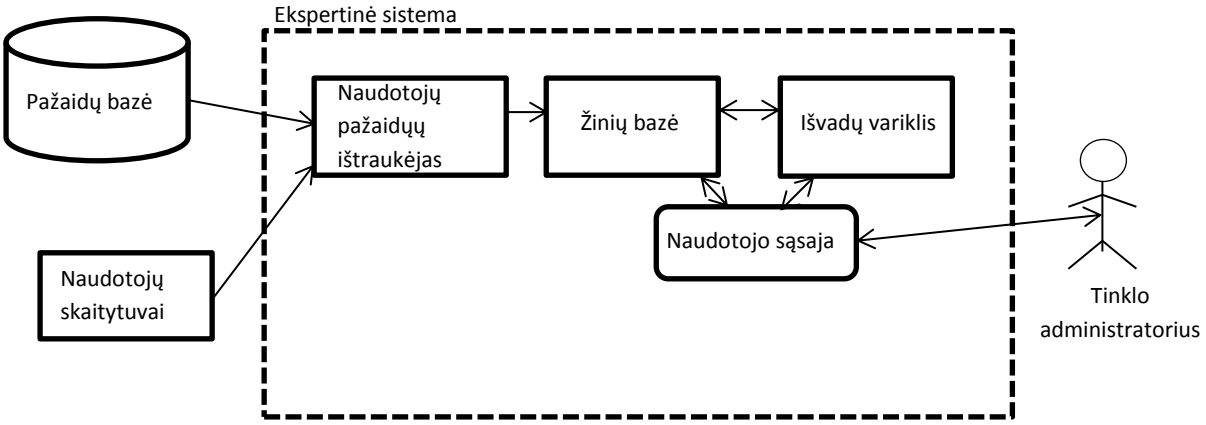
Įvertinus riziką galimiems incidentams, organizacija gali nuspręsti į kuriuos saugos incidentus suteikti didžiausią prioritetą ir parinkti atsakomąsias priemones.

3.1. Ekspertinės sistemos

Ekspertinė sistema yra kompiuterinė programa, vykdanti užduotį, kurią kitais atvejais atliktų žmogus. Ekpertinė sistema yra dirbtinio intelekto (angl. artificial intelligence – AI) šaka ir pirmą kartą buvo pateikta Edward Feigenbaum, dabar laikomu šių sistemų pradininku, kuris kartu su kolegomis 6-ajame dešimtmetyje Standfordo universitete sėkmingai sukūrė pirmąją ekspertinę sistemą [28]. Ekspertinės sistemos galėtų būti pritaikytos parinkti tinklo saugos užtikrinimo priemones pagal organizacijos veiklos sektorių ir aplinką

Tikriausiai dažniausiai pasitaikantis ekspertinių sistemų taikymas tinklo saugos srityje yra įsibrovimų aptikimui [36]. Yra is sudėtingesnių publikacijose pateikiamų ekspertinių sistemų taikymo pavyzdžių, tokių kaip kompleksinės kelių fazių atakos (Shahriari *et al* 2008). Tokioms atakoms pritaikomi atakų scenarijai. Toks pritaikymas praplečia tipinę pažaidų analizę, kai nuskaitomi individualūs įrenginiai, nes daugumos atakų scenarijų atveju kenkėjai išnaudoja ne vieno įrenginio, o kelių ir daugiau pažaidų, kad pasiektų savo tikslus.

Projektuojant ekspertinę sistemą, reikalingas žinių inžinierius, kuris gilinasi į tai, kaip žmogus priima sprendimus ir paverčia taisykles kompiuteriams suprantamais terminais. Žinių inžinierius turi užtikrinti, kad kompiuteris turi visas žinias reikalingas problemai išspręsti. Jis taip pat turi užtikrinti, kad kompiuteris gali panaudoti žinias efektyviai išrenkant iš keleto motyvuotų metodų.



3.1.1 pav. Ekspertinės sistemos architektūra [19]

Komponentės pažaidos ištraukėjas gauna įvestis iš dviejų šaltinių: pažaidų duomenų bazės ir įrenginio skaitytuvo (pav. programa *Nessus*). Įrenginio skaitytuvai ieško žinomų pažaidų pavieniuose įrenginiuose ir siunčia rezultatus ištraukėjui, kuris kitu etapu ieško, kuriai klasei priklauso pažaida duomenų bazėje. Toliau ištraukėjas formuluoja atitinkamus faktus ir išsiunčia juos žinių bazei. Pavyzdžiui, paleidus *Nessus* pažaidų skaitytuvą gaunama ataskaita, kad įrenginys *h1* turi Telnet paslaugos pažaidą, kurio kodas CVE-2001-0554. Ištraukėjas siunčia šią informaciją į Nacionalinę pažaidų bazę (angl. National Vulnerabilities Database – NVD) ir reikalauja reikalingos informacijos apie pažaidą. Apdorojus užklausą paaiškėja, kad tai yra buferio perpildymo pažaida, kuri gali būti išnaudojama ir kenkėjui suteikia galimybę įgyti aukščiausias privilegijas įrenginyje. Taigi į žinių bazę saugojimui nusiunčiamas įrašas *PaslaugaPažaida (Telnet, h1)*.

Informacija, esanti žinių bazėje, talpina žinomų faktų rinkinį, taisykles ir kitą įgytą informaciją, kuria vadovaujantis faktams galima priskirti „jei-tada“ (angl. „if-then“) sprendimą [10].

Galima sakyti, kad išvadų variklis yra bendras valdymo mechanizmas, kuris taiko žinių bazės žinias tam tikrai specifinei užduočiai spręsti, išvadai padaryti [40]. Žinių bazė yra žmogui perskaitomas taisyklių rinkinys. Tai duomenų saugykla, skirta informacijos surinkimui, saugojimui, organizavimui ir paieškai. Ekspertinė sistema gali užsikrauti taisykles į darbinę atmintį ir bandyti jas pritaikyti duomenims, įvestiems per naudotojų sąsają [20].

Pavyzdžiui publikacijoje siūlomas daugiapakopis atakų ekspertinės sistemos modelis gali turėti tris pagrindines komponentes [36]. Pirma komponentė yra rinkinys

pradinių faktų, aprašančių tinklo pradinę topologiją ir konfigūraciją. Antras tai rinkinys taisyklių, kurios gali būti panaudojamos kaip papildanti informacija apie įrenginių sujungimą tinkle ir prieinamumą prie jų. Trečia – rinkinys pažaidų modelių, apimančių sąlygas prieš pažaidas ir po jų. Taigi jos nurodo, kokioms sąlygoms esant sistema gali būti pažeista, ir kokios sąlygos bus tam įvykus. Toks modelis, turintis pradinių faktų ir taisyklių rinkinį, gali būti realizuotas kaip ekspertinė sistema.

Kitas dažnas ekspertinių sistemų taikymas tinklų srityje yra sprendimuose, skirtuose tinklo problemoms spręsti. Tokiuose sprendimuose visada yra analizuojamas tinklo srautas, o galiausiai ekspertinės analizės metu sistema palygina esančias tinklo problemas su informacija, esančia žinių bazėje.

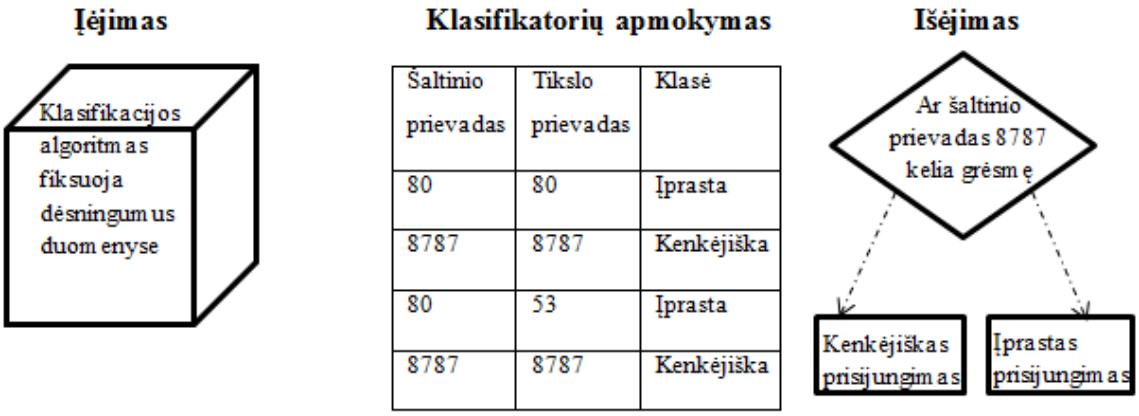
Kuriamos metodikos tinklų saugos priemonių parinkimui reikalingas įrankis, kuriuo naudotis nereiktų specialių žinių ir gebėjimų, metodika galėtų būti lengvai plečiama, adaptuojant rekomenduotinas saugos priemones pagal organizacijų aplinkos parametrus. Panašus į aptartus ekspertinių sistemų naudojimo atvejus tinklo saugos priemonių parinkimui galėtų būti taikomas tolesniame etape. Norint ateityje pritaikyti ekspertinę sistemą tinklo saugos priemonių parinkimui, pirma reiktų suformuluoti faktus, kuriais galėtų pasinaudoti išvadų variklis. Kadangi vienas iš šio darbo tikslų yra tinklo saugos priemonių parinkimas pagal individualią organizacijos aplinką, apibrėžiamą jos dydžiu ir veiklos sektoriumi, pirma reikia rasti būdą kaip įvertinti saugos priemonės reikalingumą. Ekspertinės sitemos atžvilgiu, toks vertinimas ir galėtų būti kaip faktai, vėliau panaudojami ekspertinės sistemos išvadų variklyje.

3.2. Sprendimų medžiai

Sprendimų medžiai yra vienas iš klasifikacijos algoritmų pavyzdžių. Klasifikacijos algoritmai, identifikuodami esamų duomenų dėsningumą, kuria sprendimų medžius. Klasifikacija yra duomenų mainų technika kuri priskiria objektus į vieną iš kelių apibrėžtų kategorijų [38]. Sprendimų medis gali būti apibrėžtas kaip numatymui skirta modeliavimo technika, kuri kuria paprastą medžio tipo struktūrą vyraujančio dėsningumo modeliavimui [27]. Dauguma pateikiama duomenų mainų mokslinių publikacijų yra apie duomenų mainų algoritmus, techniką ir terminologiją. Šiame darbe nėra išsamiai gilinamasis į sprendimų medžių technologiją ir jie taikomi saugos sprendimams nustatyti, kurie būtų

praktiškai realizuoti. Magistrinio darbe sprendimų medžiai yra panaudojami kaip apibendrinanti duomenų masyvą priemonė, kuri automatiškai skirsto duomenis. Turint sprendimo medį būtų galima lengvai įskaityti rezultatus, pvz., tam tikros saugos priemonės rekomenduotinumą tam tikro veiklos sektoriaus ir dydžio organizacijai.

Daugelis darbų aprašo sprendimų medžius kaip duomenų mainų temą įsibrovimams aptikti nuo jų sudarymo iš taip vadinamų medaus puodynių (angl. honeypot) duomenų (Gregio et al. 2007) iki grėsmių klasifikavimo realiu laiku (Sangkatsanee et at. 2009). Paplitusiu atveju sprendimų medžiai gali padėti nuspręsti, kuriuos IDS parašus įrašyti, kurias užkardos taisykles nustatyti ir kokio tipo tinklo žymes nustatyti tolesnei analizei. Sprendimų logika išryškina kenksmingą veiklą, taigi gali būti naudojama kartu su realaus laiko įrankiais imantis atsakomųjų veiksmų prieš kibernetines atakas. Iš įsibrovimų aptikimo perspektyvos, pasinaudojant klasifikuojančiais algoritmais tinklo veikla gali būti charakterizuojama kaip kenksminga, įprasta, nuskaitomojo pobūdžio arba pagal tam tikrą informaciją, tokią kaip šaltinio/tikslo prievadai, IP adresai ir prisijungimo metu persiųstų duomenų kiekis. Toks sprendimų medžių taikymas daugelyje mokslinių publikacijų yra įprastas. Paprastas sprendimų medžio pavyzdys, paremtas viena sprendimo taisykle, yra žinomo prievado 8787, dažnai panaudojamo kenkėjiškai veiklai, vertinimas [31]:



3.2.1 pav. Sprendimų medžių mokymosi įėjimas ir išėjimas

Tokie taikymo būdai leidžia sprendimų medžius panaudoti einamo laiko taikymui [31]. Šiame darbe nebus kalbama apie sprendimo medžių naudojimą einamojo laiko įrankiuose. Darbe sprendimo medžiai pasirinkti kaip priemonė skirstanti arba klasifikuojanti

turimus duomenis siekiant supaprastintai atvaizduoti tinklo saugos priemonės pasirinkimo pagal organizacijos aplinką duomenis.

3.3. Sprendimo medžių taikymas sudarytai metodikai

Kai kurie tyrėjai sėkmingai sukūrė sprendimo medžių klasifikatorius pasinaudodami vadinama medaus puodynių technologija, nuskaitymo dažniu, IDS pranešimais arba įprastiniais tinklo darbo duomenimis. Metodikos taikymui reikalingas lankstus įrankis, kuris leistų parinkti saugos priemones tiek naudojantis rizikos analizės išvadomis, tiek jų neturint. Taikant sprendimo medžių koncepciją kuriamai metodikai siekiama turėti rekomenduotinų saugos priemonių nustatymo ir atvaizdavimo būdą organizacijoms pagal jų veiklos sritį, riziką, o tuo pačiu ir galimų atakų pobūdį. Gauti rezultatai turėtų palengvinti sprendimo priėmimą organizacijoms pasirenkant tam tikrą saugos priemonę. Tokiu būdu technologijų parinkimas yra pritaikomas pagal tam tikrus įvesties duomenis, nėra nepagrįstas. Reikalinga suvestų duomenų apibendrinimo funkcionalumą turinti priemonė, teikianti reikalingas išdavas. Būtent sprendimo medžiai suteikia reikiamą lankstumą. Darbe panaudojami realūs statistiniai pažaidų kiekio kiekvienam apibrėžtam organizacijos veiklos sektoriui duomenys bei pavyzdiniai poveikio duomenys.

3.4. CVSS v2 pritaikymas rizikos vertinimui pagal organizacijos aplinką

Sudaroma metodika turi padėti organizacijoms įvykdyti CIA triados reikalavimus, todėl rekomenduojamos saugos priemonės ir galimos žalos jų nerealizavus gali būti vertinamos pagal tai, kaip labai yra pažeisti triados reikalavimai. Sprendimų medžiuose turi būti CIA triados įvykdymo vertinimo kriterijus. Su tikslu, kad tolesnėje darbo eigoje sprendimų medžiais atvaizduotas klasifikavimo modelis taptų praktiniu taikymo įrankiu, reikalingi audito metu arba realiomis sąlygomis surinkti statistiniai duomenys, apimantys organizaciją apibūdinančius duomenis, atakos tipus, žalą ir kt. 3.5.1 lentelė parodo, kaip gali būti pažeisti CIA triados reikalavimai:

3.4.1 lentelė. Triados reikalavimų pažaidos

Konfidencialumas	**Vientisumas**	**Prieinamumas**
Minimalus nejautrių duomenų atskleidimas	Minimalus kiekis menkai sugadintų	Minimaliai sutrikdytos antrinės svarbos paslaugos
Minimalus kritinių duomenų atskleidimas	Minimalus kiekis labai sugadintų	Minimaliai sutrikdytos pirminės svarbos paslaugos
Platus nejautrių duomenų atskleidimas	Didelis kiekis menkai sugadintų	Labai sutrikdytos pirminės svarbos paslaugos
Platus kritinių duomenų atskleidimas	Didelis kiekis labai sugadintų	Labai sutrikdytos antrinės svarbos paslaugos
Visų duomenų atskleidimas	Visi duomenys visiškai sugadinti	Visos paslaugos neveikia

Bendra pažaidų vertinimo sistema (angl. CVSS – Common Vulnerability Scoring System) yra standartizuotas pažaidų vertinimo metodas [21]. CVSS v2 vertinimo sistema yra kibernetinės saugos industrijos standartas, kuris leidžia prioritizuoti pažaidas pagal konkrečią riziką, keliamą organizacijai. Pažaidų rizikai vertinti kiekvienu atveju reikalinga metrika. Būtent metrika leidžia metodiškai vertinti riziką susijusią su pažaida. CVSS metrikomis perteikiama sistema, kuri susieja IT pažaidų charakteristikas su poveikiu [21].

CVSS balas yra dešimtainis skaičius intervale [0.0, 10.0] ir yra sudarytas iš trijų metrikų grupių: bazinės, laikinosios ir aplinkos [25]. CVSS bazinės metrikos naudojamos įvertinti potencialioms pasekmėms, kai pažeidžiamas konfidencialumas, integralumas ir prieinamumas. Šios metrikos charakterizuoja tiesioginį poveikį IT turtui, kai yra išnaudojamos pažaidos ir yra apibrėžiami kaip konfidencialumo, integralumo ir prieinamumo praradimo laipsnis.

3.4.2 lentelė. CVSS Bazinės metrikos

Bazinės metrikos	**Nustatymo kriterijus**	**Balas**
Prieigos vektorius	Kaip yra išnaudojama pažaida	Kuo labiau nutolęs įsilaužėlis gali būti nuo taikinio, tuo aukštesnis pažaidos balas
Prieigos komplikuotumas	Atakos, išnaudojančios pažaidą, sudėtingumas, kai įsibrovėlis jau turi prieigą prie taikinio	Kuo mažesnis sudėtingumas, tuo aukštesnė pažaidos vertė
Autentifikacija	Kiek kartų įsilaužėlis turėjo autentifikuotis, kad įvykdytų sėkmingą ataką	Kuo mažiau autentifikacijos tipų yra reikalaujama, tuo aukštesnis pažaidos balas
Poveikis konfidencialumui	Poveikis konfidencialumui, kai sėkmingai išnaudojama pažaidą	Padidėjęs poveikis konfidencialumui padidina pažaidos vertę
Poveikis integralumui	Poveikis integralumui, kai sėkmingai išnaudojama pažaida	Padidėjęs poveikis integralumui padidina pažaidos balą
Poveikis prieinamumui	Poveikis prieinamumui, kai sėkmingai išnaudojama pažaida	Padidėjęs poveikis prieinamumui padidina pažaidos balą

CVSS nuo 2004 metų, nuo tada, kai buvo sudarytas, pritaikytas kelių gamintojų, panaudotas pažaidos įrankiams bei saugumo bilietams. Kaip pavyzdys gali būti techninės ir programinės įrangos gamintojai, tokie kaip IBM, HP ir skenavimų įrankių gamintojai, tokie kaip *Nessus* ir *Qualys* bei JAV Nacionalinio standartų ir technologijų instituto (angl. National Institute of Standart and Technology – NIST) organizacija, kuri palaiko NVD duomenų bazę, pagrindinę žinomų pažaidų talpyklą. Beveik visos žinomos pažaidos yra įtrauktos į Nacionalinę pažaidų bazę (angl. National Vulnerability Database – NVD), kuri yra publikuojama NIST. Taigi dauguma žinomų pažaidų yra laisvai prieinamos. CVSS v2

pagalba buvo stengiamasi sukurti universalią ir nuo gamintojų nepriklausomą pažaidų vertinimo sistema. Šiuo metu yra antroji versija, kuri palaikoma FIRST organizacijos. CVSS v2 nekategorizuoja atakų taip pat ir nepateikia bendro modelio vertinant rizikos lymenį. CVSS tik pateikia informaciją apie pažaidas operaciniame lygmenyje ir yra paliekama gamintojams, kurie papildo savo produktų informacija, ir naudotojams įvertinti informaciją konkretaus taikinio perspektyvoje. Pavyzdžiui pažaida CVE-1999-0196 turi bazinį vektorių [AV:N/AC:L/Au:N/C:P/I:N/A:N], apibrėžiantį bazinį balą 5, lemiamą pažaidos išnaudojamumo balo, kurio vertė 10.0 ir poveikio balo - 2.9. Bazininių metrikų komponentės yra:

AV:N (Acces vector:None) - Prieigos vektorius:Nėra.

AC:L (Autentification Complex:Low) - Prieigos Komplikuotumas:Žemas.

Au:N (Autentification:None) - Autentifikacija:Nėra.

C:P (Confidenciality:Partial) - Poveikis Konfidencialumui:Dalinis.

I:N (Integrity:None) - Poveikis Integralumui:Nėra.

A:N (Availability:none) - Poveikis Prieinamumui:Nėra.

Kitos metrikų grupės, laikinoji ir aplinkos, yra priklausomos arba nuo laiko arba nuo aplinkos, todėl neaprašomos NVD bazėjė. Būtent aplinkos vertės darbe yra siekiama apibrėžti iš duomenų rastų publikacijose, kad būtų įvykdyti reikalavimai, keliami tinklo saugos priemonių parinkimui. Šiame darbe siekiama turėti bendrą modelį pažaidoms vertinti pagal organizacijos sektorių ir dydį konkrečiai tinklo atakai. Būtent turint aplinkos metrikas gali tiksliau numatyti potencialą grėsmę ir sudaryi bendrą modelį jos įvertinimui pagal pramonės sektorių.

Jungtinių valstijų Energetikos departamento elektros tiekimo ir energijos patikimumo biuras įgyvendino projektą, kurio tikslas buvo padidinti nacionalinės energetikos infrastruktūros patikimumą ir sugebėjimą atkurti procesus sumažinant energijos sutrikimo riziką kibernetinių atakų metu [21]. Pagrindinė projekto dalis buvo SCADA (National Supervisory Control and Data Acguisition) sistemų pažaidų analizė, kurią atlikus identifikuojamos pažaidos, kurie gali sukelti sistemai riziką. Kitu etapu buvo pateikiamos rizikos mažinimo priemonės. Projekte buvo įvertintas kiekvienas iš dešimties SANS (sistemų administravimo, audito, tinklų administravimo ir saugos instituto) aprašytos bendros pažaidos įvertintų pagal CVSS v2. Nors SCADA sistemos skiriasi nuo kitų IT sistemų, tačiau saugos atžvilgiu bendros IP ir eterneto technologijos, CIA triados reikalavimai. Pagal pažaidų,

tenkančių konkretiems SCADA sistemos komponentams statistiką, tinklo įrangai priskiriama 5% aptinkamų pažaidų, lygiai tiek pat ir užkardoms, kurių pažaidos nurodomos kaip klaidos taisyklėse [21].

SSH rizikai vertinti pagal organizacijos duomenis naudojama SCADA tyrimo rezultatai atviro teksto autentifikacijos pažaidai pagal CVSS v2. Duomenys pateikiami lentelėje skaičiavimui naudojamoms metrikoms ir jų vertėms parodyti

3.4.3 lentelė. Atviro teksto autentifikacijos protokolų naudojimo SCADA CVSS v2 bendri rezultatai [21]

Metrika	**Vertė**
Bazinė metrika	
Prieigos vektorius	Tinklas
Prieigos komplikuotumas	Aukštas
Autentifikacija	Nėra
Poveikis konfidencialumui	Visiškas
Poveikis integralumui	Visiškas
Poveikis prieinamumui	Visiškas
Bazinis rezultatas	7,6
Laikina (angl. temporal) metrika	
Pažaidas išnaudojančios programos	Egzistuoja
Pataisomumas	Neapibrėžta
Ataskaitos patikimumas	Patvirtintas
Laikinas rezultatas	7,2
Aplinkos metrikos	
Šalutinės grėsmės galimybė	Aukšta
Taikinio pasiskirtymas	Neapibrėžta
Prieinamumo poreikis	Vidutinis

Integralumo poreikis	Aukštas
Konfidencialumo poreikis	Aukštas
Aplinkos rezultatas	8,6
Bendras CVSS rezultatas	8,6

Nors pramonės sektorių kontrolės sistemų saugos sritis yra sąlyginai nauja, bet šaltiniuose publikuojami pakankamai išsamūs statistikos ir saugos tyrimų duomenys. JAV industrinių kontrolės sistemų saugos incidentų tyrimo tarnyba (angl. Industrial Control Systems Cyber Emergency Response Team - ICS-CERT) tiria kritinės infrastruktūros kontrolės sistemų saugos incidentus. Organizacijos praneša ICS-CERT apie kibernetinius incidentus ir reikalauja analizės duomenų, kuri suteikia išsamesnę informaciją apie incidentus, tame tarpe ir įsilaužėlių technikas ir strategijas. Tokia informacija padeda turto savininkams įvertinti jų padėtį saugos atžvilgiu ir imtis priemonių stiprinant sistemų kontrolę ir tinklo saugą [41]. ICS-CERT tarnyba akcentuoja tinklo architektūros svarbą pabrėždama, kad pirmasis atakos prieš kontrolės sistemas etapas yra prieigos prie lokalaus tinklo įgyjimas. Kitais etapais bandoma surinkti informaciją apie procesus ir juos kontroliuoti. Saugos problemos kategorizuojamos į tris sritis: taisykles ir procedūras, operacinių sistemų saugą ir tinklo saugą. Tam, kad saugos taisyklės būtų veiksmingos, jos turi būti realizuojamos praktinėmis priemonėmis. Akcentuojama tinklo segmentavimo svarba pasinaudojant užkardas ir sukuriant demilitarizuotas zonas kontrolės sistemų tinklo apsaugai. Esant poreikiui atskirti atskirus funkcionalumus ir prieigos privilegijas gali būti sukurta daug demilitarizuotų zonų. Visos jungtys su kontrolės sistemų LAN tinklu turi turėti maršrutą per užkardą nesistengiant išvengti šio reikalavimo. Užkardų taisyklių sudarymo klausimu atkreipiamas dėmesys, kad taisyklės turi būti kuriamas ne tik įeinančiam, bet ir išeinančiam srautui. Pavyzdžiui tam, kad nuotoliniu būdu galima būtų kontroliuoti pažaidų išnaudojimo kodą, paleistą kontrolės sistemos kompiuteryje, reikalingas grįžtamasis ryšys. Jeigu bus tvarkingai surašytos išeinančios taisyklės, įsibrovėlis neįgis išeinančio srauto kontrolės ir negalės toliau tyrinėti ir kontroliuoti įsilaužto įrenginio. Kuo daugiau prievadų ir paslaugų yra prieinama, tuo didesnė atakų tikimybė prieš egzistuojančias paslaugų pažaidas. Rekomenduojama tinklą stebėti dėl neįprastos ir neautorizuotos veiklos tam skirtomis priemonėmis: IDS, IPS, ARP tarpininko (angl. Man in the middle - MiTM) stebėjimo įrankiu ir kt. Pabrėžiama rizika naudoti atvirojo

teksto protokolus, tokius kaip Telnet, kai gali būti paprastomis šnipinėjimo priemonėmis perskaitytas prisijungimo vardai ir slaptažodžiai [22].

3.4.4 lentelė. ICT-CERT kibernetinių incidentų statistiniai duomenys pagal veiklos sektorių

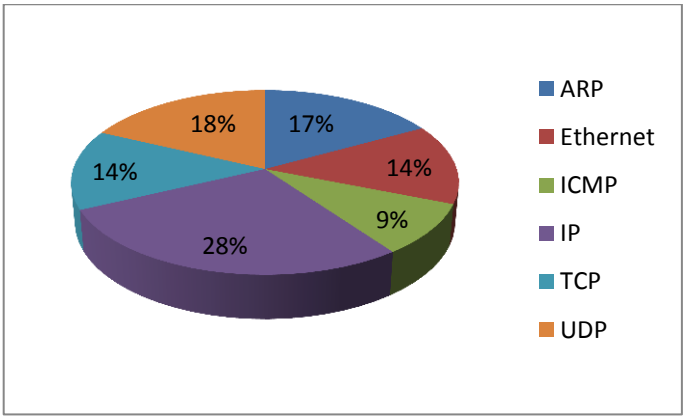
Veiklos sektorius	**Incidentų skaičius, %**	**Metai**
Energetikos	44	2010
	16	2011
	41	2012
	73	2013
Chemijos	7	2010
	5	2011
	4	2012
	0	2013
Vandens	10	2010
	41	2011
	15	2012
	7	2013
Vyriausybinės	5	2010
	6	2011
	4	2012
	5	2013
Sveikatos apsaugos	0	2010
	0	2011
	3	2012
	0,5	2013
Finansų	0	2010

	0	2011
	0,5	2012
	0,5	2013

3.4.5 lentelė. ICT-CERT kibernetinių incidentų statistinių duomenų vidurkiai pagal veiklos sektorių

Veiklos sektorius	**Incidentų skaičius (%)**
Energetikos	43,5
Chemijos	4
Vandens	18,25
Vyriausybinės	5
Sveikatos apsaugos	0,825
Finansų	0,25

Ištestavus industrinės infrastruktūros sistemas ir įrenginius ir susumavus pažaidų procentinį pasiskyrstymą L2, L3 ir L4 lygmenims, išryškėjo, kad daugiausia pažaidų rasta IP protokole, mažiausiai ICMP [26]. Net 17% pažaidų rasta ARP protokole. Tai pakankamai didelė dalis atsižvelgiant į protokolo paprastumą.



3.4.1 pav. Procentinis pažaidų pasiskirstymas L2, L3 ir L4 protokolams [26]

Tokie duomenys gauti iš „Achilles“ pažaidų duomenų bazės, kuri yra suprojektuota šiuolaikinės pramonės kontrolės sistemų pažaidų testavimui, centralizavimui ir efektyviam jų mažinimui. 3.5.6 lentelėje pateikti duomenys įrenginių ARP ir ICMP pažaidų, rastų su „Achilles“ platforma, kai rezultatai įvertinami CVSS v2 balu.

3.4.6 lentelė. „Achiles“ atliktų saugos pažeidimų testų skirtingiems pramonės sektoriams rezultatai [26]

Pažaidų protokolas	**CVSS balas**	**Pramonės šaka**
ICMP	3,1	Energetika
ICMP	3,1	Chemija
ARP	8,5	Energetika
ARP	8,5	Chemija
ICMP	5,3	Energetika
ARP	5,3	Chemija
ICMP	8,7	Vanduo
ARP	8,7	Maisto

Taip buvo atsižvelgta į įrenginių pažaidų pasiskirstymą pagal veiklos sektorių. Nustatyta, kad didelis skaičius pažaidų tenka naftos ir dujų sektoriams, darbe apibendrintai vadinamiems energetikos sektoriumi. Kiekvienas tyrimo metu testuotas įrenginys buvo susietas su atskiru industrijos sektoriumi. Tam tikras veiklos sektorius lemia CVSS v2 metrikos vertes arba CVSS v2 balo rezultato vertę.

Tokio pobūdžio tyrimai ir gauti duomenys būtų naudingi ne tik pramoninių sistemų tinklo valdymo saugai, bet ir įprastai infrastruktūrai, tačiau publikacijose ir kituose šaltiniuose retai pateikiami. Matoma, kad pramonės infrastruktūros valdymo sistemų saugos duomenų tyrimai yra išsamesni ir lengviau gali būti susisieti su konkretaus pramonės sektoriaus rizika.

Tokio pobūdžio ir išsamumo ataskaitų ir statistikų, kai duomenys skirstomi pagal tam tikro tipo tinklo ataką konkrečiam sektoriui vertinant CVSS v2 balais nėra dažnos, skirtos daugiausia pramonės sektoriams, tokiems kaip paminėtieji energetikos, chemijos, pramonės.

Remiantis šiuo metu pateikiamais rizikos skaičiavimus lemiančius duomenimis, reikia ieškoti būdų, kaip įvertinti riziką, sukeltas nerealizavus tam tikrų tinklo protokolų saugos priemonių, atsižvelgiant į organizacijų aplinkos duomenis, tokius kaip pramonės sektorius.

TOE (Target of Evaluation) (Humb 2007) arba vertinamas objektas gali būti bet kuri sistemos/tinklo dalis arba visa sistema/tinklas ir yra naudojamas tiesiog apibūdinti objektą. Šiame darbe TOE yra tinklo įrenginiai, kurių pažaidos yra išnaudojamos. Rizikos lygio matavimo modelis koncentruojamas į operacinio lygmens pažaidas. Pažaidos taip pat gali būti strateginio lygmens, tokie kaip saugos procesai. Pažaidų lygmeniui nustatyti yra naudojama CVSS skaičiavimo sistema.

HyunChul Joh ir Yashwant K. Malaiya publikacijoje apibrėžiama tam tikros pažaidos poveikio konfidencialumui (I_C), integralumui (I_I) ir prieinamumui (I_A) įvertinimas kartu su lemiančiais kiekvienos sistemos specifiniais faktoriais. Pateikiama poveikio išraiska:

Poveikis = $fc(I_C R_C, I_I R_I, I_A R_A)$

Formulėje f_c yra tinkamai parinkta funkcija. CVSS apibrėžia aplinkos metrikas vadinamas konfidencialumo, integralumo ir prieinamumo reikalavimais, kurios įvardijamos kaip R_C, R_I ir R_A. Funkcija f_c gali būti sudedamoji arba multiplikatyvi.[13].

Siv Hilde Houmb and Virginia N. L. Franqueira galimus nepageidaujamus įvykius (pažaidos išnaudojimo pasekmes) vadina piktnaudžiavimu (angl. misuse) ir pažymi šių piknaudžiavimų dažnį (angl. frequency) dydžiu MF, o poveikį (angl. impact) dydžiu MI. Rizikos lygmens skaičiavimui reikalingi dažnio ir poveikio duomenys gali būti apskaičiuojami iš CVSS v2 informacijos. MF turi būti intervale nuo 0 iki 1, tam kad tenkintų teigiamos tikimybės (dydis P) sąlygą ir nebūti didesnis nei 1. MF reikšmė lygi 0 reiškia, kad pažaidas niekada negali būti išnaudota, o reikšmė 1, kad jis tikrai bus išnaudotas. Vertė mažesnė intervale tarp 0 ir 0.5 autoriaus laikoma mažos tikimybės atakai, tuo tarpu intervale tarp 0.5 ir 1 didelės tikimybės.

Taigi autoriai TOE rizikos lygio matavimo modeliui panaudoja CVSS metrikų grupes ir apskaičiuoja piknaudžiavimo dažnį ir poveikį. Magistrinio darbe, skirtingai nuo minėtų autorių darbo, MF arba pažaidų dažniui skaičiuoti panaudojamos ne CVSS metrikos, o

statististika, pagal kurią skaičiuojama sėkmingo pažaidos išnaudojimo tikimybė. Tuo tarpu autoriai MF skaičiavimui naudoja bazines metrikas: reikalavimus prieinamumui (B_AR), atakos kompleksiškumas (B_AC) ir autentifikacijos pobūdį (B_Au). Toks dažnio skaičiavimas pagrindžiamas tuo, kad kuo lengviau išnaudoti pažaidą, tuo labiau tikėtina, kad tai bus padaryta, tuo turima didesnė tikimybė.

Darbe panaudojama trečioji komponentė – reikalavimai aplinkai, kuri susideda iš konfidencialumo (E_CR), integralumo (E_IR) ir prieinamumo (E_AR), kurios matuojamos pagal kokybinę skalę {žema, vidutinė, aukšta}. Nepaisant to, kad aplinkos atributai gali keistis bėgant laikui, bet jie nėra tokie dinamiški kaip laikinieji. Be jie yra specifiniai pagal tam tikrą TOE, kas atitinka darbo tikslus, nes pažaidų vertinimas atliekamas sudarytai tinklo saugos metodikai. Laikinieji atributai apibūdina tam tikrą pažaidą.

Kaip jau minėta, šiame darbe poveikiui apskaičiuoti naudojamos bazinės komponentės, vertinančios poveikį konfidencialumui, integralumui ir prieinamumui, ir aplinkos komponentės reikalavimams konfidencialumui, integralumui ir prieinamumui. Autorių naudojamos formulės:

$$Poveikis_B = \int_{N-1} P(B_C, B_I, B_A) \, (1)$$

$$Poveikis_E = \int_{N-1} P(E_{CR}, E_{IR}, E_{AR}) \, (2)$$

$$Poveikis = \int_{N-1} Poveikis_B \times Poveikis_E \, (3)$$

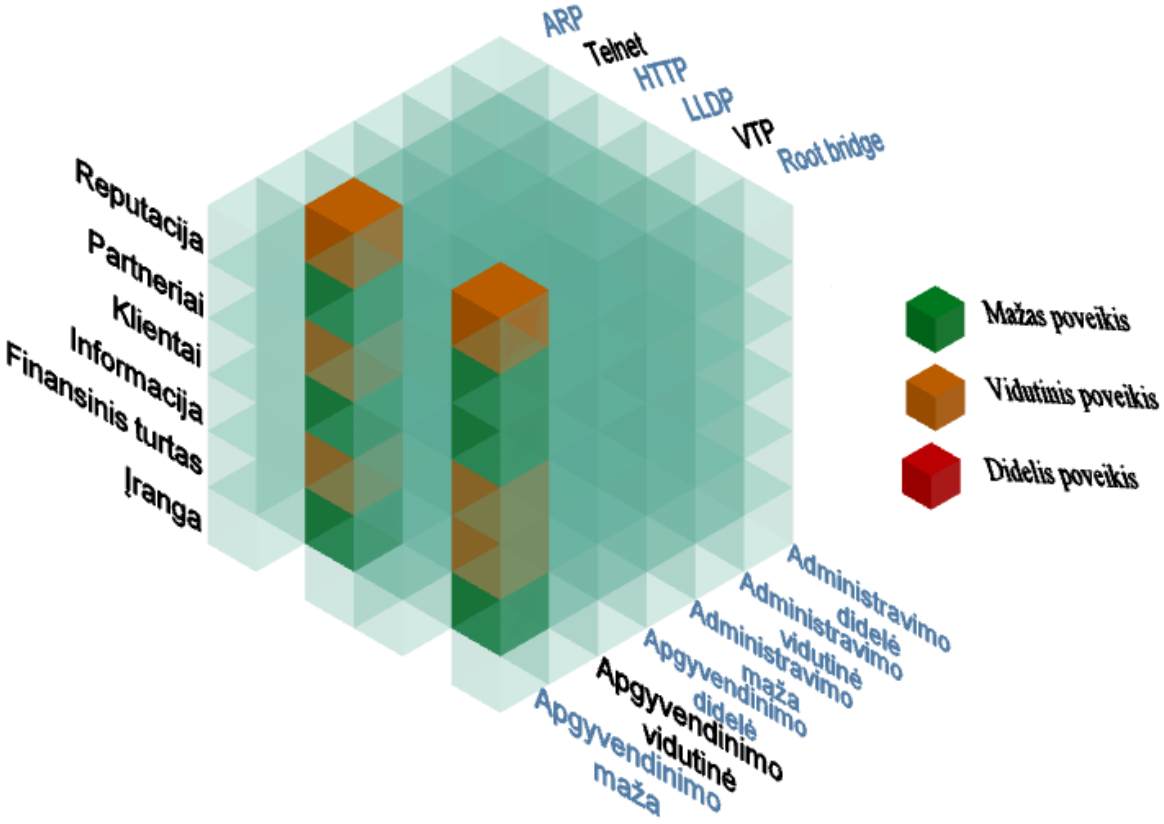
Bazinės poveikio vertės panaudojamos ir šiame darbe siekiant įtraukti sėkmingos atakos poveikį bazinių metrikų pagalba ir atspindėti taikinio specifiką, konkrečios veiklos sektoriaus įtaką, įtraukiant aplinkos atributus. CVSS aplinkos metrikos grupėje įtraukiami trys pažaidos aspektai: konfidencialumo, integralumo ir prieinamumo reikalavimai.

Šiame darbe incidento tikimybė yra skaičiuojama iš statistinių duomenų, kurie paimami iš metinės JAV *Verizone* telekomunikacijų kompanijos patvirtintų incidentų ataskaitos [5]:

3.4.7 lentelė. Tikimybei skaičiuoti naudojama metinė pažaidų statistika

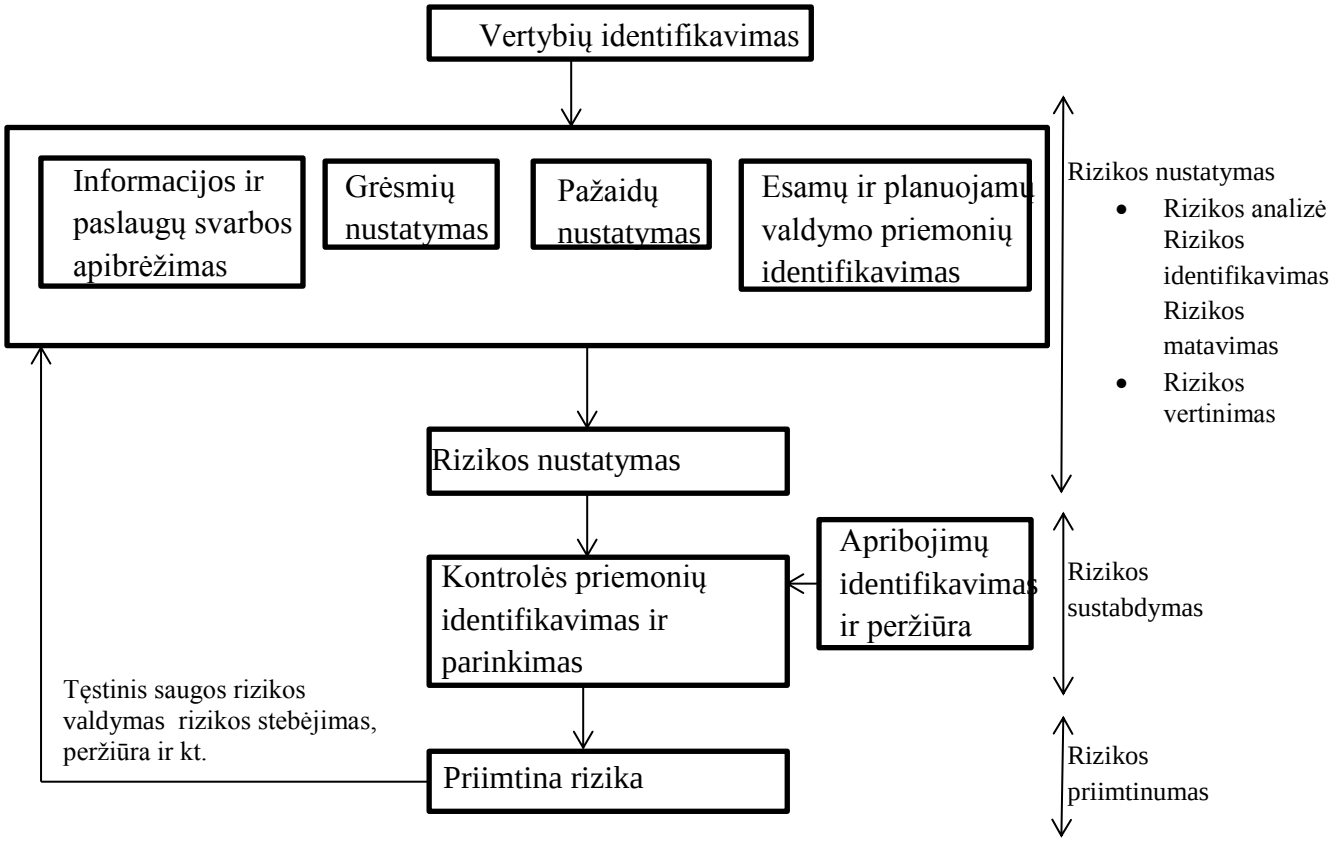
Pramonės sektorius	**Dalis**	**Mažos organizacijos**	**Didelės organizacijos**	**Nežinoma**
Apgyvendinimo	47	15	0,47	0,15
Administracijos	1	2	0,01	0,02
Statybos	0	0	0,00	0,00
Švietimo	0	6	0,00	0,06
Pramogų	1	1	0,01	0,01
Finansų	10	25	0,10	0,25
Sveikatos apsaugos	2	0	0,02	0,00
Informacijos	3	4	0,03	0,04
Vadybos	0	0	0,00	0,00
Gamybos	2	8	0,02	0,08
Iškasenų	0	5	0,00	0,05
Profesinių sąjungų	5	3	0,05	0,03
Viešojo sektoriaus	7	18	0,07	0,18
Nekilnojamo turto	1	0	0,01	0,00
Mažmeninės prekybos	14	8	0,14	0,08
Prekybos	1	0	0,01	0,00
Logistikos	1	3	0,01	0,03
Komunalinių įmonių	1	0	0,01	0,00
Kita	3	2	0,03	0,02

Kadangi trūksta L2, L3 tinklo lygmenų atakų duomenų, kuriuos turėtų pateikti atsakingos institucijos, tai poveikiui įvertinti pateikiami pavyzdiniai duomenys, kurių atvaizdavimui sudaromas informacijos kubas. Tinklų saugos užtikrinimo metodikai kaip rizikos valdymo praktinei priemonei konstruojamas informacijos kubas apjungia ir supaprastina anksčiau paveikslėlyje pavaizduoto rizikos nustatymo ir valdymo struktūrines dalis. Tai turimas konstrutyvus vaizdas, kuris formuojamas iš tinklo protokolų grėsmių (ARP, Telnet ir kt.), vertybių (reputacija, partneriai ir kt.), atsižvelgia į organizacijos unikalią aplinką (veiklos sritį ir dydį) ir atspindi kaip šių komponentų sąjunga nulemia poveikį.



3.4.2 pav. Tinklo saugos pažaidų išnaudojimo poveikio vertinimo informacijos kubas

Šiame darbe sudarytas ir pasiūlytas informacijos kubas formuojamas ir keičiamas, plečiant ar siaurinant, atitinkamai pagal apibrėžtų kraštinių elementų kiekį. Toks kubas suteikia paprastą būdą fiksuoti ištirtus incidentus organizacijoje ir įvertinti, koks poveikis buvo padarytas, integruojant organizacijos unikalią aplinką.



3.4.3 pav. Tinklo saugos rizikos nustatymo ir valdymo procesai [15]

Incidento tikimybę gerai perteikia ir minėtasis CVSS balas. Šio darbo tikslus atitinkančios komponentės pateiktos lentelėje.

3.4.8 lentelė. Pažaidų poveikiui skaičiuoti naudojami CVSS atributai

CVSS metrikų grupė	**CVSS atributai**	**Vertinimas**	**Vertė**
Bazinės metrikos	Poveikis konfidencialumui (B_C)	Nėra (N) Dalinis (P) Visiškas (C)	0.0 0.275 0.660
	Poveikis integralumui (B_I)	Nėra (N) Dalinis (P) Visiškas (C)	0.0 0.275 0.660
	Poveikis	Nėra (N)	0.0

	prieinamumui (B_A)	Dalinis (P) Visiškas (C)	0.275 0.660
Aplinkos metrikos	Konfidencialumo reikalavimas (E_CR)	Žemas (L) Vidutinis (M) Aukštas (H)	0.5 1.0 1.51
	Integralumo reikalavimas (E_IR)	Žemas (L) Vidutinis (M) Aukštas (H)	0.5 1.0 1.51
	Prieinamumo reikalavimas (EAR)	Žemas (L) Vidutinis (M) Aukštas (H)	0.5 1.0 1.51

Kad į pažaidos vertinimą įvesti unikalios aplinkos vertinimą, reikia užpildyti aplinkos vertinimo balus. Tai galima pasiekti turint reikalavimus konfidencialumui, integralumui ir preinamumui.

Vienintelis publikuojamas šaltinis pateikiantis saugos kategorizavimą pagal tam tikrą informacinės sitemos tipą, darbe įvardijamą kaip sektorių, atsižvelgiant į konfidencialumą, integralumą ir prieinamumą, yra NIST organizacijos FIP 199 dokumentas. Šiame dokumente pateikiama, kokį poveikį turėtų vieno iš CIA triados nario pažeidimas tam tikro sektoriaus informacinėje sistemoje. Tyrime tai įvardijama kaip poveikio apibrėžimas, bet savo prasme yra tapatus konfidencialumo, integralumo ir prieinamumo reikalavimui.

Informacinės sistemos, kurioje naudojama sutarčių informacija ir kasdieninė administravimo informacija saugos kategorija (angl. security category – SC), apibūdinama:

SC pirkimo sistema = {(konfidencialumas, vidutinis), (integralumas, vidutinis), (prieinamumas, žemas)}.

Toks rezultatas gaunamas įvertinant kelių tipų informaciją, su kuria dirbama:

SC sutarčių informacija = {(konfidencialumas, vidutinis), (integralumas, vidutinis), (prieinamumas, žemas)}

ir

SC administracinė informacija = {(konfidencialumas, žemas), (integralumas, žemas), (prieinamumas, žemas)}.

Bendrą CIA komponenčių įvertinimą nulemia aukštesnė poveikio vertė.

Organizacijos valdančios viešąją informaciją jų žiniatinklio serveriuose įvardija, kad jiems mažai svarus konfidencialumas, vidutiniškai svarbus integralumas ir prieinamumas. Rezultate saugos kategorija yra išreiškiama:

SC vieša informacija = {(konfidencialumas, nėra), (integralumas, vidutinis), (prieinamumas, vidutinis)}.

Tokiu pat būdu dokumente aptariamas galimas poveikis CIA triadai ir kito tipo informacinėms sistemoms. FIP 199 dokumente apibrėžti organizacijų reikalavimai pateikiami C priede.

Kadangi pažaidos vertinimas pagal tam tikrą sektorių CVSS balo skaičiavimo metu yra lemiamas įvykio tikimybės, tai yra koreguojamos CVSS balo konfidencialumo, integralumo ir prieinamumo poveikio metrikos. Tarkime, kad skaičiuojamas Telnet pažaidos CVE-2013-6979 CVSS balas mažai sveikatos apsaugos organizacijai, kurios veikla yra administravimas. Tokiam skaičiavimui atsižvelgiama į pagal statistiką apskaičiuotą tikimybę (3.5.7 lentelė) ir FIPS 199 dokumente nustatytus reikalavimus CIA triadai pagal organizacijos sektorių (C priedas). Poveikio vertės perskaičiuojamos pagal formules:

$P_K = I_C * P_x$.

$P_I = I_I * P_x$.

$P_P = I_A * P_x$.

(I_C, I_I, I_A – nepakeistos poveikio vertės).

Kai P_K, P_I ir P_P yra poveikio reikšmės, kurias įtakoja įvykio statistinės tikimybės.

Kintamasis P_x šiuo atveju yra lygus 0.02 (3.5.7 lentelė), taigi:

$P_K = 0.66 * 0.02 = 0.0132$.

$P_I = 0*0.02=0$.

$P_P = 0*0.02=0$.

Konstantos 0.66 ir 0 yra apribrėžtos CVSS skaičiavimo sistemoje ir reiškia visišką poveikį (0.66) arba poveikio nabuvimą (0).

3.4.9 lentelė. Pažaidų poveikiui skaičiuoti naudojami CVSS atributai

CVSS metrikų grupė	**CVSS atributai**	**Vertinimas**	**Vertė**
Bazinės metrikos	Poveikis konfidencialumui (B_C)	Visiškas (C)	0.66
	Poveikis integralumui (B_I)	Nėra (N)	0.0
	Poveikis prieinamumui (B_A)	Nėra (N)	0.0
Aplinkos metrikos	Konfidencialumo reikalavimas (E_CR)	Žemas (L)	0.5
	Integralumo reikalavimas (E_IR)	Vidutinis (M)	1.0
	Prieinamumo reikalavimas (EAR)	Žemas (L)	0.5

Bazinio CVSS balo poveikio vertė skaičiuojama pagal formulę:

Poveikis = 10.41 * (1 - (1 - PoveikisKonf) * (1 - PoveikisInteg) * (1 – PoveikisPriein)).

Prieš pakeitimus poveikio vertė būtų:

Poveikis = 10.41 * (1 - (1 – 0.66) * (1 - 0) * (1 -0)) = 6.87.

Po atliktų pakitimų skaičiavimui:

Poveikis = 10.41 * (1 - (1 – 0.0132) * (1 - 0) * (1 -0)) = 0,14.

Matoma, kad poveikio tikimybės balas sumažėjo apytiksliai 49 kartus.

Sekančiu etapu galima skaičiuoti poveikio vertę, kuri priklausoma nuo pavyzdinės organizacijos CIA triados reikalavimų.

PritaikytasPoveikis = Min(10, 10.41 * (1 - (1 - PoveikisKonf * ReikalavimasKonf) * (1 - PoveikisInteg * ReikalavimasInteg) * (1 - PoveikisPriein * ReikalavimasPriein))).

PritaikytasPoveikis = Min (10, 10.41 * (1 – (1 – 0,0132 * 0.5) (1 - 0 * 1) (1 – 0 * 0.5))) = 0.07.

Su pradine poveikio verte:

PritaikytasPoveikis = Min (10, 10.41 * (1 – (1 – 0,66 * 0.5) (1 - 0 * 1) (1 – 0 * 0.5))) = 3.44.

Skaičiuojant pagrindinį bazinį balą, kai buvo atsižvelgta į statistinę įvykio tikimybę ir aplinkos parametrus gauname:

BazinisBalas = round_to_1_decimal (((0.6 * Poveikis) + (0.4 * Išlaužiamumas) - 1.5) * f (Poveikis)).

f (Poveikis) = 0, jei Poveikis = 0; 1.176 kitu atveju.

BazinisBalas = round_to_1_decimal (((0.6 * 0.07) + (0.4 * 4.9) - 1.5) * 1.176)) = 0,6.

Bazinis balas, kai neatsižvelgta į statistinę įvykio tikimybę:

BazinisBalas = round_to_1_decimal (((0.6 * 3.44) + (0.4 * 4.9) - 1.5) * 1.176)) = 3.

Rezultatas rodo, kad pateiktas CVSS balas su papildytais aplinkos parametrais ir įvertinus incidento tikimybę yra daugiau nei 5 kartus mažesnis nei tas, kuris neatsižvelgia į incidento tikimybę. Tačiau balo skaičiavimo formulė neatsiejama nuo bazinių metrikų pažaidos išnaudojimo komponenčių (prieinamumumo vektoriaus, prieigos kompleksiškumo ir autentifikacijos):

BazinisBalas = round_to_1_decimal (((0.6 * Poveikis) + (0.4 * Išlaužiamumas) - 1.5) * f (Poveikis)).

Išlaužiamumas = 20 * PrieigosVektorius * PrieigosKompleksiškumas * Autentifikacija.

Toks skaičiavimas negali būti bendru modeliu dėl CVSS komponenčių, kurios negali būti atsietos nuo skaičiavimo, todėl darbe vertinant riziką naudojama tik tikimybė, gauta iš statistinių ataskaitų duomenų.

3.5. Sprendimų medžių realizacija su „WEKA“ programinė įranga.

Kiekvienai atakai, nuo kurios siekiama apsisaugoti aprašomi įvesties duomenys *.arff (Attribute-Relation File Format)* faile. Įvesties duomenys gali būti paimti iš reikiamą informaciją suteikiančių šaltinių: audito ataskaitų, rizikos vertinimo dokumentų. Atakos medžiais siekiama apimti kuo daugiau organizacijos savybių tam, kad kuo tiksliau išvesti, kokios yra labiausiai rekomenduotinos saugos priemonės. Jie yra aprašomi kaip atributai. Įvedami duomenys gali būti skaitiniai arba žodiniai. Įprastai šitie duomenys yra saugomi tam tikros formos lentelėje, tokioje kaip skaičiuoklės, duomenų bazės arba kitame lenteliniame failo formate, tokiame kaip šiame darbe pasirinktos programinės WEKA įrangos *.arff* formatas.

Įvestys:

relation saugospriemones

@attribute sritis {Statybos,Finansu,Sveikatos_apsaugos,Viesojo_sektoriaus,Nekilnojamo_turto,Logistikos}

@attribute dydis {maza,didele}

@attribute tikimybe {1,2,3}

@attribute poveikis {1,2,3}

@attribute rizika real

@attribute rekomendacija {n,v,r}

@data

Statybos,maza,1,1,1,n

Statybos,maza,1,1,1,n

Finansu,maza,1,2,2,n

Finansu,maza,1,3,3,r

Finansu,maza,1,3,3,r

Sveikatos_apsaugos,maza,1,2,2,v

Viesojo_sektoriaus,maza,1,1,1,n

Viesojo_sektoriaus,maza,1,1,1,n

Viesojo_sektoriaus,maza,1,2,2,v

Viesojo_sektoriaus,maza,1,1,1,n

Nekilnojamo_turto,maza,1,2,2,v

Statybos,didele,1,1,1,n

Finansu,didele,1,3,3,r

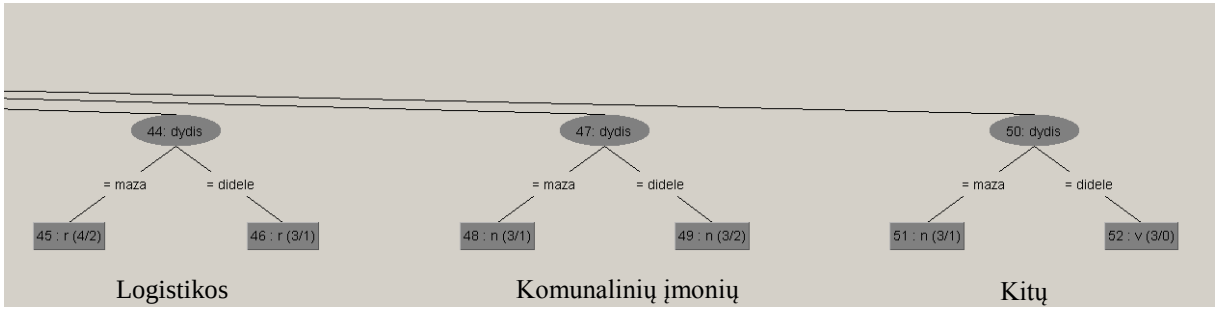
Finansu,didele,1,3,3,r

Finansu,didele,1,2,2,v

Finansu,didele,1,3,3,r

ir t.t.

Tokiu formatu yra pateikimas įrašų rinkinys. Kievienas įrašas turi panašią struktūrą, susidedančią iš atributo ir vertės porų. Sprendimų medžių išvestis – tinklo saugos priemonės rekomendacijos vertės, atspindinčios riziką, kurią turime neužtikrinus tam tikros tinklo technologijos saugos. Nubraižytas medis parodo, kaip vertinama su saugos priemone susijusi rizika kiekviename organizacijos sektoriuje. Taigi sprendimo medžio išdavos yra vyraujantis rizikos vertinimas arba rekomenduotinumas: jei daugiausiai nerekomenduotina, tai žymima raide „n“, jei vidutiniškai rekomenduotina raide „v“, o jei rekomenduotina – raide „r“.



3.5.1 pav. Sprendimo medžio dinaminės ARP inspekcijos rekomendacijai fragmentas

Tolesnis sprendimų medžių panaudojimas automatizuotuose įrankiuose, tokiuose kaip realaus laiko programos, nėra aptariamas. Sudaryti sprendimų medžiai yra pateikiami kaip pradiniai modeliai kurie gali būti plečiami ir pildomi.

4. Išvados

Publikuojamos metodikos per siaurai apžvelgia tinklo įrangos saugą: pateikiama arba rekomenduotina architektūra arba būtinos technologijos, dar kitu atveju atskirų įrenginių konfigūracijos, siekiant išvengti atitinkamų grėsmių. Platesnio pobūdžio saugos metodikos yra per plačios apimties tinklo saugos apžvalgos, kuriomis nepavyktų nuosekliai vadovautis tinklą prižiūrinties asmenims. Magistrinio darbe parengiama metodika, kuri paremta saugiu tinklo projektavimu, pavienių tinklo įrenginių sauga. Metodika yra suderinta su ISO/IEC 27002 ir ISO/IEC 27003:1 standartais.

Magistriniame darbe buvo pateiktas CVSS v2 balo modifikavimas, atsižvelgiant į unikalią organizacijos aplinką, kuri perteikiama įvedus į balo skaičiavimą incidento tikimybę konkrečiame organizacijos veiklos sektoriuje ir konfidencialumo, integralumo bei prieinamumo reikalavimus.

Darbe suformuotas informacijos kubas kaip konstruktyvus vaizdas poveikio, kuris panaudojamas rizikos skaičiavimui, vertinimui. Toks kubas suteikia paprastą būdą fiksuoti incidentus organizacijoje ir atspindi jos unikalius parametrus

Metodikoje pritaikyta sprendimo medžių koncepcija, gautas pagal pramonės sektorius suskirstytas tinklo saugos priemonių vertinimo modelis, kuris ateityje galėtų būti plečiamas ir pildomas. Sprendimų medžių technika buvo panaudota duomenų masyvo, skirto įvertinti riziką, apibendrinimui ir paprasto vaizdo, atspindinčio tinklo saugos priemonės rekomenduotinumą, kūrimui. Toks modelis yra greitas saugos priemonių poreikio įvertinimas.

Literatūra

1. Ahmad R., Sahib S. ir Azuwa M.P. Effective Measurement Requirements for Network, 2014.

2. Alabady S. Design and implementation of a network security model for cooperative network, 2008.

3. Antoine V., Bongiorni R., Borza A. ir kiti. Router security configuration guide. Principles and guidance for secure configuration of IP routers, with detailed intructions for Cisco Systems routers, 2005.

4. A practical guide to risk assessment, 2008, [žiūrėta 2014-05-01]. Prieiga per internetą:

http://www.pwc.com/en_us/us/issues/enterprise-risk management/assets/risk_assessment_guide.pdf

5. Baker, W. Data Breach Investigations Report, Verizon Business: 50, 2009.

6. Bhaiji Y. CCIE Professional development series network security technologies and solutions, 2008.

7. Cameron R., Woodberg B., Giecco P., Eberhard T., Quinn J. Junos security, 2010.

8. Computer Crime and Security Survey, 2010. Prieiga per internetą: http://www.ncxgroup.com/wp-content/uploads/2012/02/CSIsurvey2010.pdf.

9. Data Breach Investigations Report, 2014, [žiūrėta 2014-05-01]. Prieiga per internetą: http://ics-cert.us-cert.gov/Other-Reports.

10. Eronen P. and Zitting J. An expert system for analyzing firewall rules, 2001.

11. Garla E., Dubovskaja V. Kompiuterinių tinklų projektavimas, 2008.

12. Gerundino D., Hilb M. The ISO methodology. Assessing the economic benefit of standarts, 2010, [žiūrėta 2013-12-08]. Prieiga per internetą:

http://www.iso.org/sites/TC_Chairs_2011/assets/Gerudino_Hilb_ISO%20Focus%2010-06-E.pdf

13. HyunChul J. ir Yashwant K. Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics, 2011.

14. Houmb S.H. and Franqueira V. N. L.Estimating ToE Risk Level using CVSS Information Systems Group, 2009

15. ISO/IEC 27033-1:2009, Information technology — Security techniques — Network security.

16. ISO/IEC 27002-1:2005, Informacijos technologija — Saugos metodai — Informacijos saugos valdymo praktikos kodeksas.

17. Kube N. Testing the security of connected industrial infrastructure systems and devices, 2012, [žiūrėta 2014-05-01]. Prieiga per internetą: http://www.embedded.com/design/safety-and-security/4403458/Testing-the-security-of-connected-industrial-infrastructure-systems-and-devices.

18. Lindsey M.B. A Method for Estimating the Financial Impact of Cyber Information Security Breaches Utilizing the Common Vulnerability Scoring System and Annual Loss Expectancy, 2010.

19. Lipovac L. Expert System Based Network Testing, 2001.

20. Mandal. S., Chatterjee S., Neogi B. DIAGNOSIS AND TROUBLESHOOTING OF COMPUTER, 2003.

21. Mell P., Scarfone K. A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007, [žiūrėta 2014-03-09]. Prieiga per internetą: http://www.first.org/cvss/cvss-guide.html.

22. Mitigations for Security Vulnerabilities Found in Control System Networks, 2006, [žiūrėta 2014-03-09]. Prieiga per internetą: https://ics-cert.uscert.gov/sites/default/files/recommended_practices/MitigationsForVulnerabilitiesCSNetsISA.pdf.

23. National vulnerability database v2, [žiūrėta 2014-04-15]. Prieiga per internetą: http://nvd.nist.gov/.

24. Panko R.R.. Corporate computer and network security, Second Edition, 2010.

25. Paquet C. Network Security Concepts and Policies, 2013. Prieiga per internetą: http://www.ciscopress.com/articles/article.asp?p=1998559.

26. Peláez M. S. H. Measuring effectiveness in Information Security Controls, 2010.

27. PredictionWorks: Data Mining Glosarry. Interneto prieiga http://www.predictionworks.com/glossary/

28. Russell ir Norvig, Artificial Intelligence: A Modern Approach, 2003.

29. Odom W., R.Healy, Donohue D. CCIE Routing and Switching Certification Guide, Fourth Edition, 2010.

30. Safe: Best practices for securing routing protocols, 2004. Prieiga per internetą: http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/sfblp_wp.pdf

31. SANS Institute InfoSec Reading Room. Using decision tree analysis for intrusion detection: a how-to guide, 2011.

32. SANS Institute. „Using Decision Tree Analysis for Intrusion Detection: A How-To Guide“, 2011

33. Scarfone K., Souppaya M., Cody A., Orebaugh A. Recommendations of the National Institute of Standart and Technology, 2008.

34. Schneidewind N. Metrics for mitigating cybersecurity threats to Networks, 2010.

35. Securing Networks Systematically – the SkiP method, 2002.

36. SHAHRIARI H.M., GANJISAFFAR Y., JALILI R.ir HABIBI J. Topological Analysis of Multi-phase Attacks Using Expert Systems.

37. Stamp M. Information security principles and practice, 2006.

38. Tan P., Steinbach M., Kumar V. Introduction to data mining, 2005.

39. The CIS Security Metrics v1.1.0, 2010, [žiūrėta 2014-01-13]. Prieiga per internetą: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf.

40. Noran O.S.The Evolution of Expert Systems, Griffith University, School of computing

and Information Technology.

41. Tofan D. Information Security Standards. Journal of Mobile, Embedded and Distributed Systems, vol. III, no. 3, 2011.

42. Zanni C., Silva M. A methodology for secure network.

43. Wei-jia S., Hao C. Ethernet switch-based security risks and defense method research, 2011.

44. White D., Rea A. A paradigma of network security design: model for teaching network security, 2007.

PRIEDAI

A priedas

KOMPIUTERIŲ TINKLO SAUGOS UŽTIKRINIMO METODIKA

1. Vienas iš būdų sumažinti įvairias ARP paremtas tinklo atakas yra DHCP sąsajų naudojimas kartu su dinaminiu ARP tikrinimu (angl. Dynamic ARP Inspection – DAI). Ne DHCP aplinkoje ir neturint DHCP sąsajų bazės (angl. snooping binding database), DAI gali tikrinti ARP paketus pagal naudotojo statiškai apibrėžtus ARP prieigos sąrašus, nurodančius, kurie IP yra surišti su kuriais MAC adresais. Komutatoriai naudodami DAI egzaminuoja ARP žinutes, filtruodami netinkamas. DAI skirsto prievadus į patikimus ir nepatikimus. Būtent nepatikimų prievadų ARP užklausos ir atsakymai yra tikrinami, o netinkami ARP paketai yra nufiltruojami. DAI tikrinimas gali vykti naudojantis keliais būdais:

- DAI nusprendžia ARP paketo teisėtumą tikrindamas DHCP duomenų bazės lentelę, kurios įrašai yra IP adresai susieti su MAC adresais. Taip tinklo įrenginiai įvertina ARP paketus pagal nustatymą praleisdami, įrašydami arba atmesdami, jei MAC adreso sąsaja su IP adresu neleistina.
- DAI taip pat gali vertinti ARP paketus pagal naudotojo sukonfigūruotus prieigos sąrašus (angl. ACLs). Tokiu būdu ARP paketai tikrinamami pagal statiškai sukonfigūruotus IP adresus.
- DAI taip pat leidžia uždėti preigos sąrašus prievadui ir/arba virtualiam tinklui (angl. VLAN).

DAI tikrina gauto ARP atsakymo šaltinio MAC adresą eterneto antraštėje su šaltinio MAC adresu ARP žinutėje. Minėtieji MAC adresai įprastuose ARP atsakymuose turėtų būti vienodi, o jeigu ne, DAI nufiltruoja ARP žinutes. Panašiai kaip prieš tai minėtas būdas, tik tikrinama gavėjo MAC adresas antraštėje su ARP žinutės gavėjo MAC. Taip tikrinama neįprati ARP žinutei IP adresai, tokie kaip 0.0.0.0 255.255.255.255 ir kt.

2. Tam tikros MiM atakos, kurių metu vykdomas ARP užnuodijimas, generuojama dideli kiekiai ARP atsakymų. Komutatoriuose turi būti nustatomas tokių paketų dažnio limitas, ir jei jis pasiekiamas, generuojamas pranešimas arba prievadas nustatomas į klaidos būseną. Pagal nutylėjimą, įrenginiuose, kuriuose sukonfigūruotas ARP tikrininimas ARP paketų skaičius yra apribotas tam tikra verte. Taigi:

- Prievadui nustatomas ARP paketų limitas (pvz. 20).
- Prievadui nustatomas ARP tikrinimas.

3. Tam, kad apibrėžti MAC adresus susietus su prievadu galimi trys metodai:

- Statiškai konfigūruojami MAC adresai. Galima apibrėžti, kad tik tam tikri MAC adresai pasiekiami per tam tikrą prievadą.
- Prievadui nustatomas maksimalus išmokstamų adresų skaičius arba prievadui aprašomi tam tikri MAC adresai.
- Nustatomas sankcija jei viršijamas MAC adresų skaičius, pvz., išjungimo, apribojimo ir kt.
- Dinamiškai komutatoriaus įsirašomų MAC adresų skaičius.
- Dinamiškai įsirašomi MAC adresai, kurie išsaugomi ir komutatoriaus konfigūracijoje (angl. sticky learning).

4. Nepaisant to, kad tinklo įranga daugeliu atveju laikoma atskiroje fizinėje patalpoje, užrakintoje spintoje, reikalinga apsauga nuo galimybės prisijungti prie konsolės:

- Konsoliniam prisijungimui nustatomas slaptažodis.

5. Rekomenduotina prisijungti SSH v3 protokolu, o TELNET protokolo nenaudoti:

- Nustatyti SSH v3 protokolą.
- Išjungti TELNET protokolą nuotoliniam prisijungimui.
- Įjungti SSH v3 nuotoliniam prisijungimui.

6. Visada privaloma nuotolinio prisijungimo linijas apsaugoti nuo neteisėto prisijungimo prieigos sąrašais, del to konfigūracija papildoma:

- Sudaromas prieigos sąrašas SSH v3 prisijungimui.
- Prieigos sąrašas priskiriamas nuotolinio prisijungimo linijoms.

7. Įrenginių stebėjimui ir valdymui nerekomenduojama naudoti HTTP prievado, nes srautas nėra šifruojamas ir apsaugomas:

- Išjungiamas HTTP servisas.
- Įjungiamas HTTPS servisas (esant poreikiui).

8. Esant poreikiui žiniatinklio prisijungimui naudoti HTTPS, bet su prieigos sąrašais tam tikram IP:

- Sukuriamas prieigos sąrašas HTTPS prisijungimui.

9. Rekomenduojama tinkle išjungti L2 lygmens informacijos mainams su kaimynais protokolą LLDP (angl. Link Layer Discovery Protocol), standartizuotą IEEE 802.11ab, arba analogišką patentuotą tam tikro gamintojo protokolą. Informacija keliaujanti LLDP protokolo pagalba yra nešifruota ir neautentifikuojama. Protokolą reiktų palikti tik išimtiniais atvejais, pvz., prie prieigos komutatoriaus įjungti IP telefonai, arba mišrių gamintojų tinklo stebėjimo ir valdymo protokolui SNMP ir kitais atvejais reikalingas LLDP palaikymas.

- Globaliu lygmeniu išjungiame LLDP arba analogišką protokolą.

10. Esant poreikiui turėti LLDP arba analogišką protokolą turi būti apribojama prieiga iš išorinio tinklo arba iš potinklių, kurie netalpina valdymo serverio. Taigi protokolas turi būti paliekamas tik ant reikalingų prievadų:

- Prievado lygmeniu išjungiame LLDP arba analogišką protokolą.

11. IEEE 802.1x standartas apibrėžia klientas-serveris principu paremtą prieigos kontrolę ir autentifikacijos protokolą, kuris apriboja neautorizuotų įrenginių prijungimą prie LAN per viešai prieinamus prievadus. Taigi reikia nustatyti 802.1x prieigos komutatoriuose ir bevieliuose prieigos taškuose užtikrinant, kad bet kokia prieiga prie tinklo infrastruktūros reikalautų autentifikacijos:

- Įjungiamas AAA palaikymas.
- Nurodomas Radius serverio, suderinto se EAP, IP adresas.
- Nurodomas prievadas komunikacijai.

12. VTP yra L2 protokolas leidžiantis tinklo administratoriams centralizuotai valdyti virtualių tinklų pridėjimą, trynimą ir pervadinimą. VTP saugumui užtikrinti turi būti nustatytas slaptažodis, kuris įrašomas į komutatorių VTP duomenų bazę ir naudojamas VTP pranešimų autentifikacijai:

- Globaliame režime nurodome VTP slaptažodį.

13. Kompiuterių tinkle turi būti įjungtas STP protokas, kad tinkle būtų išvengta kilpų ir apsisaugoti nuo tinklo neveiksnumo.

Tam, kad būtų sumažintos manipuliacijų tinkle galimybės, pasinaudojant STP protokolu, tam tikrų priemonių pagalba fiksuojama svarbiausio komutatoriaus virtualiame tinkle vieta. Taip užtikrinama, kad kuo mažesnė tikimybė būtų jį perrinkti.

- Įjungiamas STP.
- Tam tikriems prievadams įjungiamas svarbiausio komutatoriaus virtualiame tinkle apsauga.

14. BPDU apsauga leidžia užtikrinti, kad tinkle neatsiras konkurencingas įrenginys, turintis svarbiausio komutatoriaus statusą. Taip būtų jei turėtų ne tik priorotetą lygų nuliui, bet ir žemesnį komutatoriaus ID ir perrinktų geriausią komutatorių. Tokia saugos priemonė itin tinkama tinklo įrangos prievadams, kurie skirti naudotojų pajungimui.

- Įjungiama STP apsauga nuo BPDU kadrų.

15. Komutatoriuose liekančius nenaudojamus prievadus reikia tinkamai sukonfigūruoti, kad būtų išvengta neteisėto kanalo, per kurį praleidžiami keli ir daugiau virtualių tinklų, suformavimo:

- Prievadas nustatomas preigos režime.
- Prievadas priskiriamas nenaudojamam virtualiam tinklui.
- Nenaudojamas virtualus tinklas ištrinamas iš kanalo, per kurį praleidžiami keli ir daugiau virtualių tinkle.

16. Virtualaus tinklo šokinėjimo ataka įvykdoma, kai atakuojantysis siunčia paketus gavėjui, esančiam kitame virtualiame tinkle, kurio įprastai neturėtų pasiekti. Perduodami kadrai pažymimi dvejomis 802.11q antraštėmis, tam kad pasiektų reikiamą virtualų tinklą, kuriame yra gavėjas. Pirmasis komutatorius gavęs tokį kadrą nuardo pirmąją žymę ir perduoda kitam komutatoriui, kuris perduoda kadrą pagal likusią klaidingą žymę antrajam gavėjui.

Kitas neteisėtas būdas bandant pasiekti gavėją yra apsimetimas komutatoriumi (angl. switch spoofing) sukuriant kelis arba daug virtualių tinklų praleidžiantį sujungimą su kitu komutatoriumi, ir tokioms salygoms esant siunčiant ir gaunant kitų virtualių tinklų srautą. Todėl ten, kur nereikalingas prievadui toks režimas:

- Prievadas nustatomas prieigos, nežymėtajam arba alternatyviam režimui, skirtam nepraleisti ryšio linija daugiau nei vieno virtualaus tinklo.

17. Įrenginiai, prijungti prie prieigos prievado gali suklastoti IP arba MAC adresus, užtvindydami komutatorių paketais su neteisingais adresais. Tokio pobūdžio atakos kaip ir TCP SYN užtvindymo atakos gali sukelti DoS tipo atakas. Įsibrovėlis gali suklastoti IP adresą būdamas tame pačiame arba kitame potinklyje.

IP šaltinio sargybinis leidžia įjungti srauto filtravimą pagal DHCP sąsajų duomenų bazę arba rankiniu būdu konfigūruotas IP ir MAC sąsajas tam, kad būtų apsisaugota nuo atakų, kai klastojamas kito įrenginio IP adresas. DHCP sąsajų duomenų bazėje saugoma informacija apie IP, MAC ir virtualių tinklų ryšius.

IP šaltinio sargybinis tikrina IP paketus siunčiamus iš nepatikimų prievadų pagal aprašytas sąsajas.

- Sukonfigūruojamos DHCP sąsajos reikiamiems virtualiems tinklams.
- Įjungiamas DHCP tikrinimas ant nepatikimo (angl. untrusted) prievado.
- Įjungiamas IP šaltinio sargybinis ant prievado, virtualaus tinklo/ų.

18. Netikri ryšio būklės pranešimai (angl. Link State Advertisement – LSA) sukelia SPF medžio perskaičiavimą, kuris pareikalauja procesoriaus resursų. Dėl tokios pat priežasties kenksminga, kai gaunamas ryšio būklės pranešimai su klaidingais MD5 slaptažodžiais ir įsijungia MD5 funkcija. OSPF autentifikacija yra aktuali saugiam maršruto parinkimo atnaujimų mainams. Bet kurie maršrutai, gauti iš šaltinio, kuris negali būti autentifikuotas, yra atmetami.

- Kaimynų poros prievadams nurodoma OSPF MD5 autentifikacija, rakto ID numeris ir slaptažodis.

19. Maršruto parinktuvai, esantys OSPF tinkle, bendrauja su kitais įrenginiais tik jei yra tinkamai konfigūruoti (pvz., teisingas srities numeris). Tokiam bendravimui užmegzti siuntinėjami grupinio transliavimo paketai. Išvengiant nereikalingų santykių užmezgimo maršruto parinktuvai konfigūruojami

- Nustatomi kaimynų IP adresai, su kuriais galima užmegzti kaimyninius santykius.

20. BGP maršruto parinkimo protokolo saugai užtikrinti kaimynai turi būti autentifikuojami:

Kaimynų poros prievadams nurodoma BGP MD5 autentifikacija, rakto ID numeris ir slaptažodis.

21. Viena iš BGP atakų yra paslaugos DoS ataka. Ji įvykdoma, kai kenkėjas siunčia netikėtą arba nepageidaujamą BGP srautą su tikslu išnaudoti prieinamus BGP arba CPU resursus, ko pasekoje resursų pritrūksta legaliam BGP srautui apdoroti. BGP TTL (Time

To Live) sauga yra tam, kad būtų apsaugotas BGP procesas nuo CPU išnaudojimo ir maršrutų manipuliavimo atakų.

BGP kaip ir OSPF reikia apriboti įrenginius su kuriais galima užmegzti kaimyninius santykius:

- Prieigos sąraše nurodoma reikiamo kaimyno IP, kad jis gali kreiptis TCP 179-uoju prievadu, kuriuo bendrauja BGP, link konfigūruojamo įrenginio IP.
- Prieigos sąraše nurodomas, kad konfigūruojamo įrenginio IP gali kreiptis 179-uoju TCP prievadu link reikiamo kaimyno.
- Priegos sąraše apibrėžiama, kad draudžiama kreiptis į kitus įrenginius 179-uoju prievadu.
- Prieigos sąraše nurodoma, kad kitiems įrenginiams draudžiama kreiptis 179-uoju prievadu link konfigūruojamo įrenginio IP.
- Prieigos sąrašas priskiriamas prievadui, prie kurio prijungtas reikiamas kaimynas.

22. Maršruto parinkimo kaimynų veiklos registravimas praverčia esant maršruto parinkimo proceso nesklandumams:

- Įrenginyje nustatoma vesti maršruto parinkimo kaimynų įvykių žurnalus.

23. Maršruto parinktuvai ir komutatoriai, esant tinkle tam tikroms valdymo ir stebėjimo sistemoms, konfigūruojami kaip SNMP klientai. Įjungus įrenginiuose SNMP paslaugas, tinklo valdymo ir stebėjimo įrankiai gali gauti informaciją apie konfigūraciją, maršruto parinkimo lenteles, ryšio linijų apkrovą ir kt. Tinklo įrangoje nustatyta vieša grupės (angl. community) eilutė suteikia neribotą prieigą administruoti komutatorių arba maršrutizatorių nuotoliniu būdu. Taigi turi būti apibrėžta, kas gali gauti tokio pobūdžio informaciją.

- Jei SNMP naudojamas pakeičiama numatytoji vieša grupės eilutė, jeigu nenaudojamas išjungiams SNMP agentas.
- Sukuriamas prieigos sąrašas nurodant praleidžiamo SNMP serverio

adresą.

- Kadangi SNMP v1 ir SNMP v2 nepalaiko saugios autentifikacijos, įrašymo ir skaitymo prieigai gauti siuntinėjami grupės vardai atviru tekstu, rekomenduotina naudoti SNMP v3

24. Kad būtų išvengta slaptažodžių nuskaitymo turint galimybę peržiūrėti įrenginio tekstinę kopiją, slaptažodis turi būti šifruojamas bet kokiu būdu peržiūrint konfigūraciją, taip apsaugant nuo jo panaudojimo kenkėjiškai veiklai:

- Įrenginiuose įjungiamas paslaugos slaptažodžio šifravimas.

Tokio funkcionalumo įjungimas yra taip pat reikšmingas ir visiems konfigūracijose saugomiems slaptažodžiams.

25. Saugos užtikrinimas yra dinaminis procesas. Dėl to įgyvendinus saugos užtikrinimo priemones, svarbu skirti dėmesio stebėjimui. Tinklo srautas turi būti stebimas tinklo stebėjimo programa, kad būtų laiku pastebėtos tinkle vykstančias anomalijas ir kuo greičiau bandyti rasti jų priežastis ir jas šalinti.

26. Prižiūrint tinklą, o taip pat ir nagrinėjant saugos incidentus, svarbu turėti išsaugojus žurnalo įrašus (angl. logs). Turint centralizuotą žurnalų įrašų serverį įrašai yra surinkinėjami iš skirtingų įrenginių, kurie siuntinėja pranešimus apie įvykius:

- Nurodyti įvykių žurnalo serverio, kuris gaus žinutes IP adresą.
- Nustatyti įvykių žunalo saugojimo detalumo lygį.
- Įjungti įvykių žurnalų saugojimą.

27. Įsibrovimų aptikimo sistema (angl. Intrusion Detection System – IDS), pralaidumo fiksavimas yra tinklo stebėjimo komponentės. Naudojantis IDS tinkle yra stebimi įvykiai ir analizuojami į kenkėjišką veiklą panašūs požymiai, pvz., autorizuoti naudotojai bandantys gauti jiems nepriklausančias privilegijas. Nagrinėjant IDS pranešimus rekomenduotina atsižvelgti į:

- Pranešimų skaičių iš vieno IP adreso.
- Atakų tipų skaičių iš vieno IP adreso.
- Vieno IP adreso atakuojamųjų skaičius.
- Naujų atakų tipus.
- Atakas, kurios retos arba kurių prieš tai nebuvo.
- Laiko periodą, per kurį įvyksta atakos.

Svarstant įsibrovimų prevencijos sistemos (angl. Intrusion Prevention System – IPS), kuri realiu laiku analizuoja L2-L5 TCP/IP srauto turinį apsaugodama tinklą nuo kenkėjiškos veiklos, reikia atsižvelgti, kad veikimo principas imlus įrangos resursams, taigi svarbu numatyti, ar IPS nelėtins tinklo darbo.

28. Siekiant užtikrinti saugų tinklų sujungimą arba saugią nuotolinę prieigą, konfigūruojamas VPN IPSec protokolas. Šiuo tuneliavimo protokolu užtikrinamas informacijos konfidencialumas, tapatumo nustatymas ir vientisumas. (Plačiau skaityti šiuolaikinių metodikų apžvalgos dalyje).

29. Tinklas turi būti dalinamas į saugos zonas: serveriams, naudotojams ir t.t. Atitinkamai pagal saugos zonas konfigūruojamos užkardos taisyklės įeinančiam ir išeinančiam srautui. Užkardos taisykles reikia sudaryti pagal individualių serverių poreikius. Kuriami atskiri virtualūs tinklai skirtingo funkcionalumo tinklo dalims. (Plačiau skaityti šiuolaikinių metodikų apžvalgos dalyje).

B priedas

PADUODAMI DUOMENYS SPRENDIMO MEDŽIUI „WEKA“ PROGRAMINĖJE ĮRANGOJE

relation saugospriemonesrekomendacija

@attribute sritis {Apgyvendinimo,Administracijos,Statybos,Svietimo,Pramogu,Finansu,Sveikatos_apsaugos,Informacijos,Vadybos,Gamybos,Iskasenu,Profesiniu_sajungu,Viesojo_sektoriaus,Nekilnojamo_turto,Mazmenines_prekybos,Prekybos,Logistikos,Komunaliniu_imoniu,Kita}

@attribute dydis {maza,didele}

@attribute tikimybe {1,2,3}

@attribute poveikis {1,2,3}

@attribute rizika real

@attribute rekomendacija {n,v,r}

@data

Apgyvendinimo,maza,1,1,1,n

Administracijos,maza,1,2,2,v

Statybos,maza,1,1,1,n

Statybos,maza,1,1,1,n

Svietimo,maza,1,2,2,v

Pramogu,maza,1,1,1,n

Finansu,maza,1,2,2,n

Finansu,maza,1,3,3,r

Finansu,maza,1,3,3,r

Sveikatos_apsaugos,maza,1,2,2,v

Informacijos,maza,1,3,3,r

Vadybos,maza,1,1,1,n

Gamybos,maza,1,1,1,n

Iskasenu,maza,1,1,1,n

Profesiniu_sajungu,maza,1,2,2,v

Viesojo_sektoriaus,maza,1,1,1,n

Viesojo_sektoriaus,maza,1,1,1,n

Viesojo_sektoriaus,maza,2,2,4,v

Viesojo_sektoriaus,maza,1,1,1,n

Nekilnojamo_turto,maza,1,2,2,v

Mazmenines_prekybos,maza,2,1,2,n

Prekybos,maza,1,1,1,n

Logistikos,maza,1,2,2,v

Komunaliniu_imoniu,maza,1,1,1,n

Kita,maza,1,1,1,n

Apgyvendinimo,didele,1,1,1,n

Administracijos,didele,1,2,2,v

Statybos,didele,1,1,1,n

Svietimo,didele,1,2,2,v

Pramogu,didele,1,1,1,n

Finansu,didele,1,3,3,r

Finansu,didele,1,3,3,r

Finansu,didele,1,2,2,v

Finansu,didele,1,3,3,r

Sveikatos_apsaugos,didele,1,1,1,n

Sveikatos_apsaugos,didele,1,2,2,v

Informacijos,didele,1,3,3,r

Vadybos,didele,1,2,2,v

Gamybos,didele,1,1,1,n

Iskasenu,didele,1,1,1,n

Profesiniu_sajungu,didele,1,2,2,v

Viesojo_sektoriaus,didele,1,2,2,v

Nekilnojamo_turto,didele,1,2,2,v

Nekilnojamo_turto,didele,1,1,1,n

Nekilnojamo_turto,didele,1,2,2,v

Mazmenines_prekybos,didele,1,3,3,r

Prekybos,didele,1,2,2,v

Prekybos,didele,1,2,2,v

Logistikos,didele,1,3,3,r

Komunaliniu_imoniu,didele,1,1,1,n

Kita,didele,1,2,2,v

Apgyvendinimo,maza,1,3,3,r

Administracijos,maza,1,2,2,v

Statybos,maza,1,2,2,v

Svietimo,maza,1,2,2,v

Pramogu,maza,1,3,3,r

Finansu,maza,1,1,1,n

Sveikatos_apsaugos,maza,1,2,2,v

Informacijos,maza,1,1,1,n

Vadybos,maza,1,2,2,v

Gamybos,maza,1,3,3,r

Iskasenu,maza,1,2,2,v

Profesiniu_sajungu,maza,1,2,2,v

Viesojo_sektoriaus,maza,1,3,3,r

Nekilnojamo_turto,maza,1,2,2,v

Mazmenines_prekybos,maza,2,2,4,v

Prekybos,maza,1,2,2,v

Logistikos,maza,1,3,3,r

Logistikos,maza,1,1,1,n

Komunaliniu_imoniu,maza,1,3,3,r

Kita,maza,1,1,1,n

Apgyvendinimo,didele,1,1,1,n

Administracijos,didele,1,1,1,n

Statybos,didele,1,1,1,n

Svietimo,didele,1,2,2,v

Pramogu,didele,1,3,3,r

Finansu,didele,1,1,1,n

Sveikatos_apsaugos,didele,1,1,1,n

Informacijos,didele,1,1,1,n

Vadybos,didele,1,2,2,v

Gamybos,didele,1,1,1,n

Iskasenu,didele,1,2,2,v

Profesiniu_sajungu,didele,1,2,2,v

Viesojo_sektoriaus,didele,1,2,2,v

Nekilnojamo_turto,didele,1,3,3,r

Mazmenines_prekybos,didele,2,1,2,n

Prekybos,didele,1,1,1,n

Logistikos,didele,1,1,1,n

Komunaliniu_imoniu,didele,1,3,3,r

Kita,didele,1,2,2,v

Apgyvendinimo,maza,1,2,2,v

Administracijos,maza,1,3,3,r

Statybos,maza,1,1,1,n

Svietimo,maza,1,1,1,n

Pramogu,maza,1,1,1,n

Finansu,maza,1,3,3,r

Sveikatos_apsaugos,maza,1,2,2,v

Informacijos,maza,1,2,2,v

Vadybos,maza,1,3,3,r

Gamybos,maza,1,2,2,v

Iskasenu,maza,1,1,1,n

Profesiniu_sajungu,maza,1,2,2,v

Viesojo_sektoriaus,maza,1,3,3,r

Nekilnojamo_turto,maza,1,2,2,v

Mazmenines_prekybos,maza,2,1,2,v

Prekybos,maza,1,2,2,v

Logistikos,maza,1,3,3,r

Komunaliniu_imoniu,maza,1,1,1,n

Kita,maza,1,3,3,r

Apgyvendinimo,didele,1,2,2,v

Administracijos,didele,1,3,3,r

Statybos,didele,1,2,2,v

Svietimo,didele,1,1,1,n

Pramogu,didele,1,1,1,n

Finansu,didele,2,3,6,r

Sveikatos_apsaugos,didele,1,2,2,v

Informacijos,didele,1,3,3,r

Vadybos,didele,1,2,2,v

Gamybos,didele,1,2,2,v

Iskasenu,didele,1,1,1,n

Profesiniu_sajungu,didele,1,3,3,r

Viesojo_sektoriaus,didele,1,3,3,r

Nekilnojamo_turto,didele,1,2,2,v

Mazmenines_prekybos,didele,1,3,3,r

Prekybos,didele,1,3,3,r

Logistikos,didele,1,3,3,r

Komunaliniu_imoniu,didele,1,2,2,v

Kita,didele,1,2,2,v

C priedas

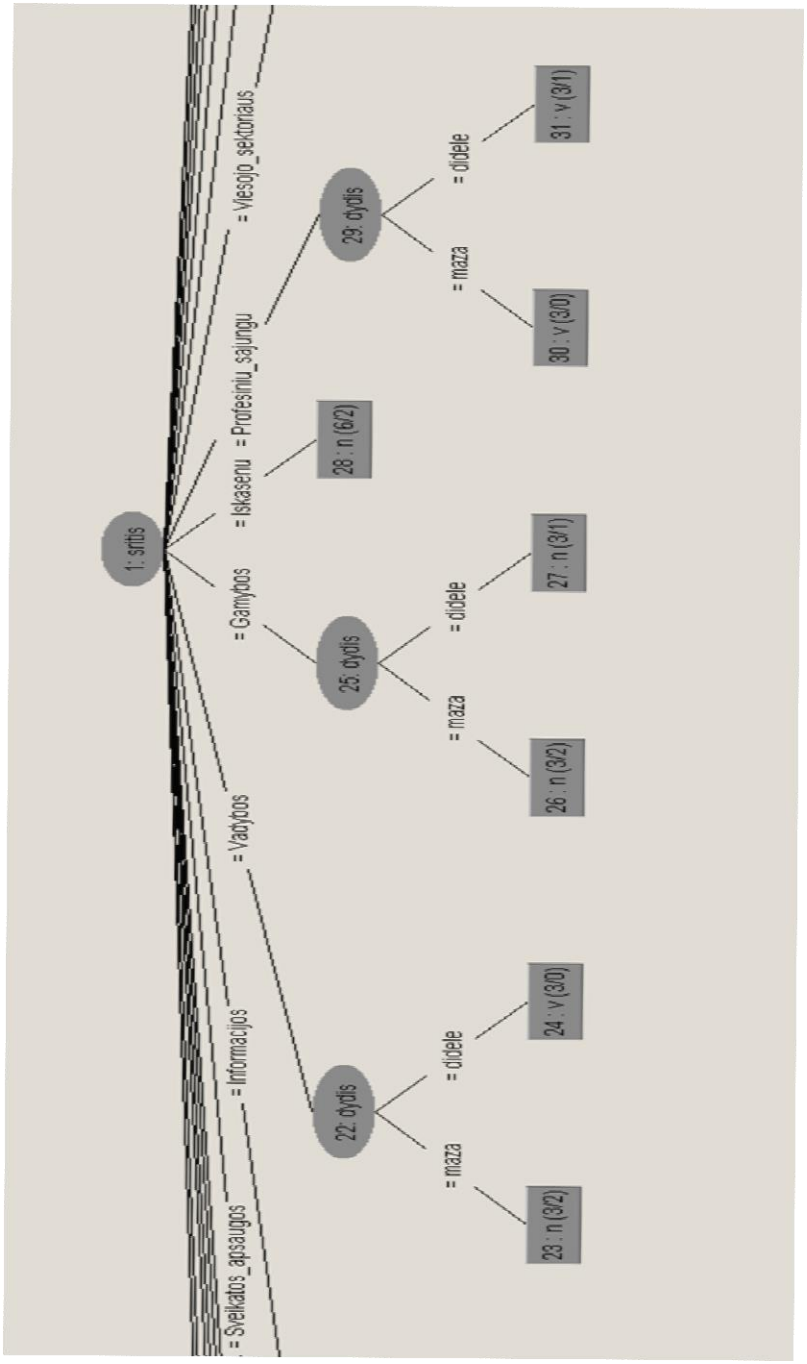
Saugos kategorizavimas pagal informacijos paskirtį (FIP 199)

Pramonės sektorius	**Konfidencialumas**	**Integralumas**	**Prieinamumas**
Žemės ūkio	Žemas	Žemas	Žemas
Statybos	Žemas	Žemas	Žemas
Švietimo			
Pradinis, vidurinis ir profesinis išsilavinimas	Žemas	Žemas	Žemas
Aukštasis išsilavinimas	Žemas	Žemas	Žemas
Kultūros ir istorijos išsaugojimas	Žemas	Žemas	Žemas
Kultūros ir istorijos viešinimas	Žemas	Žemas	Žemas
Finansų			
Dotacijos	Žemas	Žemas	Žemas
Perlaidos	Žemas	Žemas	Žemas
Subsidijos	Žemas	Žemas	Žemas
Mokesčių kreditai	Vidutinis	Žemas	Žemas
Sveikatos apsaugos			
Paslaugų suteikimas	Žemas	Vidutinis	Žemas
Gyventojų sveikatos vadyba ir vartotojų teisė	Žemas	Vidutinis	Žemas
Administravimas	Žemas	Vidutinis	Žemas

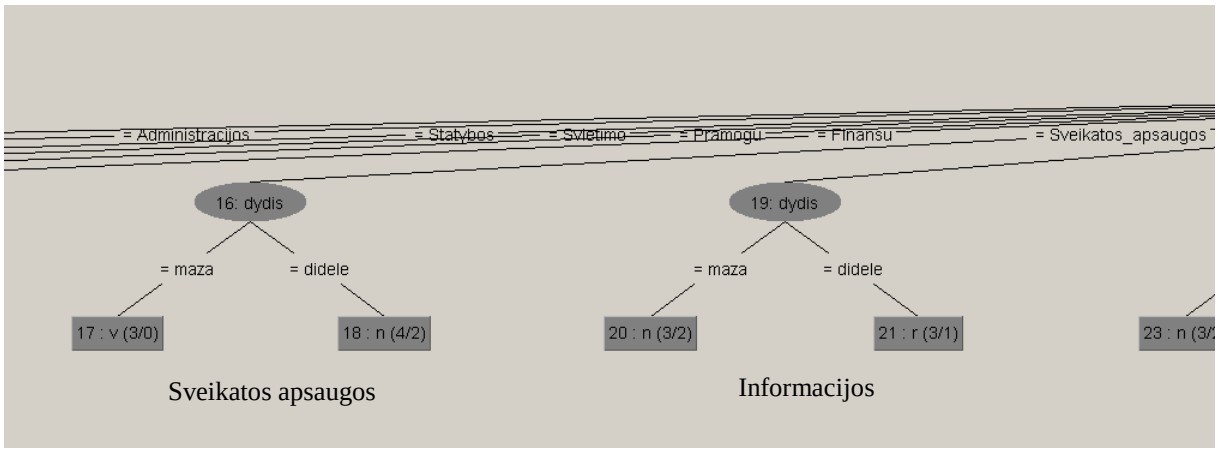
Perdavimo paslaugos	Žemas	Aukštas	Žemas
Tyrinėjimai ir praktinis mokymas	Žemas	Vidutinis	Žemas
Informacijos	Žemas	Žemas	Žemas
Gamybos	Žemas	Žemas	Žemas
Profesinių sąjungų			
Apmokymas ir įdarbinimas	Žemas	Žemas	Žemas
Darbuotojų tesių valdymas	Žemas	Žemas	Žemas
Darbuotojų sauga	Žemas	Žemas	Žemas
Viešojo sektoriaus	Žemas	Žemas	Žemas
Logistikos			
Žemės	Žemas	Žemas	Žemas
Vandens	Žemas	Žemas	Žemas
Oro	Žemas	Žemas	Žemas
Kosmoso	Žemas	Aukštas	Aukštas
Ir kt.			

D priedas

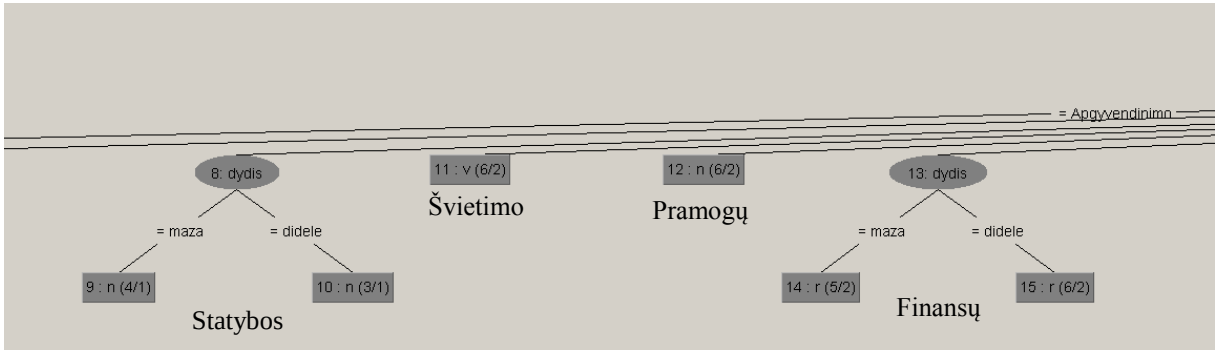
RIZIKOS VERTINIMO MODELIO DINAMINĖS ARP INSPEKCIJOS REKOMENDACIJAI SPRENDIMO MEDIS



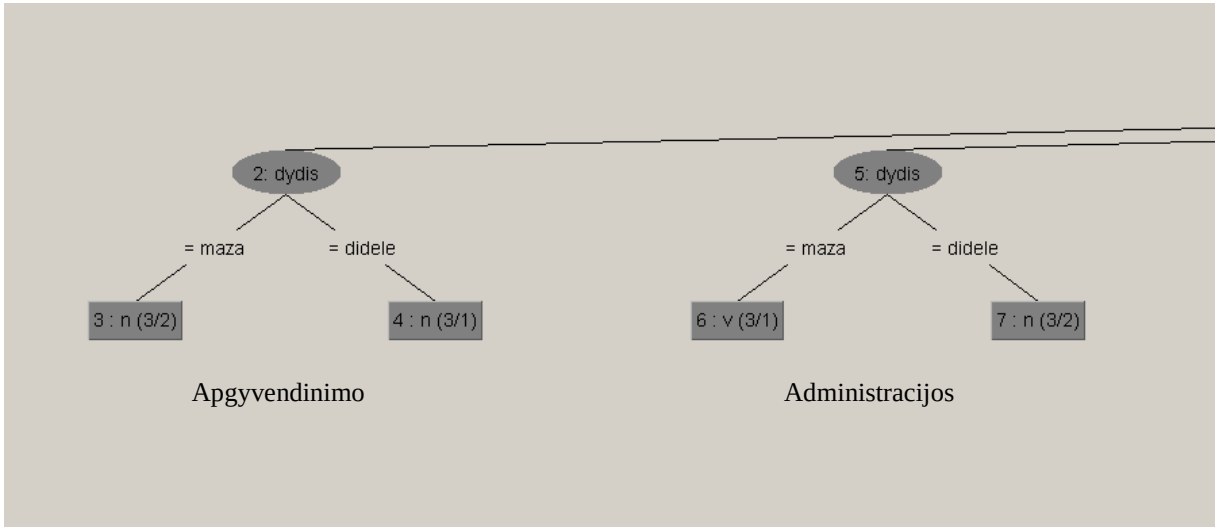
Sprendimo medžio dinaminės ARP inspekcijos naudojimo rekomendacijai viršūnė



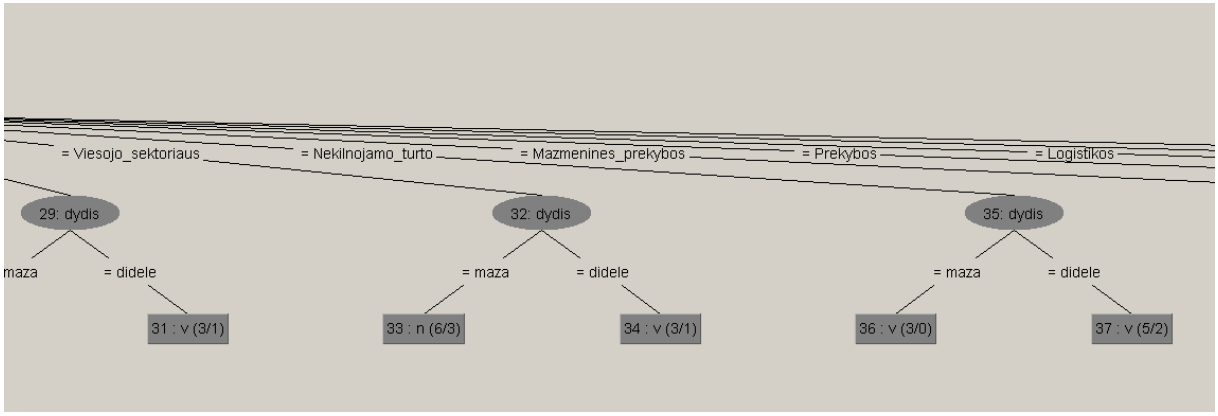
Sprendimo medžio šakos. Sveikatos apsaugos, informacijos sektoriai.



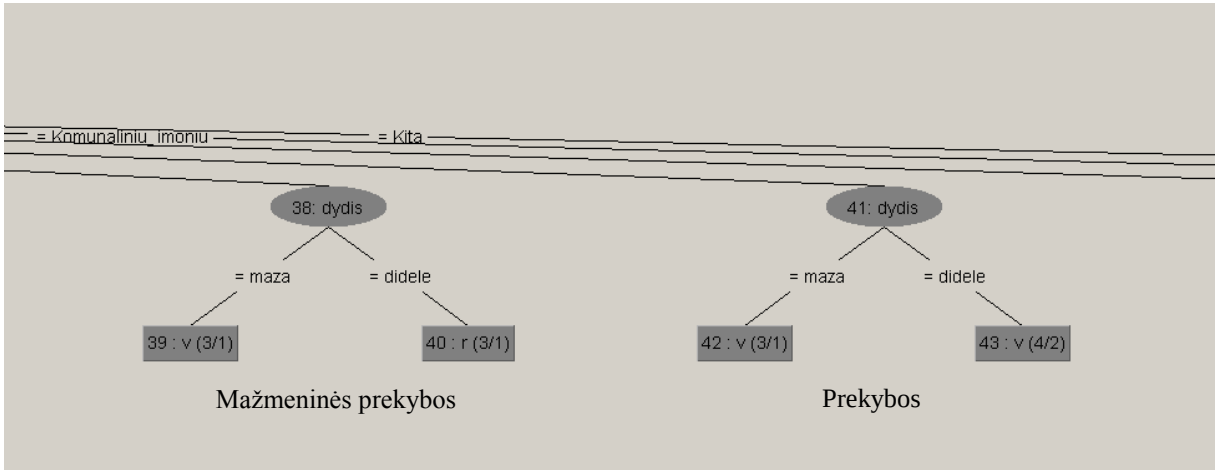
Sprendimo medžio šakos. Statybos, finansų sektoriai.



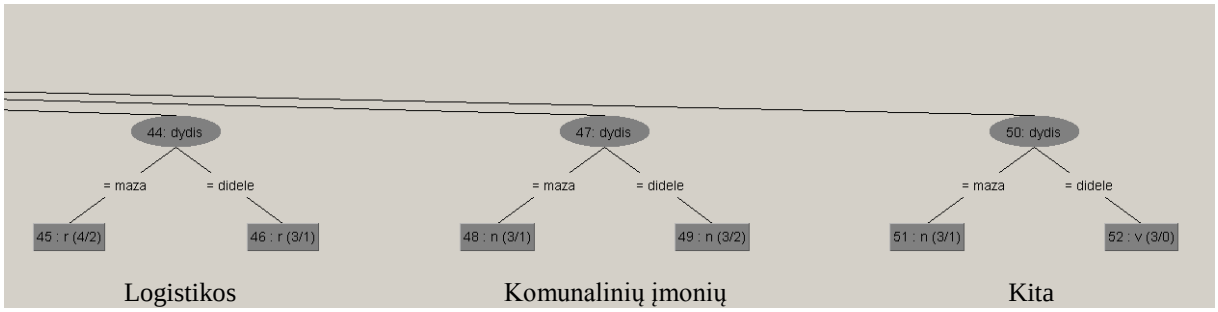
Sprendimo medžio šakos. Apgyvendinimo, administracijos sektoriai.



Sprendimo medžio šakos. Viešojo, nekilnojamo turto sektoriai.



Sprendimo medžio šakos. Mažmeninės prekybos, prekybos sektoriai.



Sprendimo medžio šakos. Logistikos, komunalinių, kitų sektorių.