KAUNO KOLEGIJA

TECHNOLOGIJŲ FAKULTETAS
INFORMATIKOS IR MEDIJŲ TECHNOLOGIJŲ KATEDRA

Žygimantas Žiūkas

GIMNAZIJOS KOMPIUTERIŲ TINKLO SAUGUMO DIDINIMO PROJEKTAS

Baigiamasis darbas

Kibernetinių sistemų ir saugos studijų programos
valstybinis kodas 6531BX024
Informatikos inžinerijos studijų krypties

Vadovas dr. Dangis Rimkus

Kaunas, 2024

TURINYS

ĮVADAS 9
1. ANALITINĖ DALIS 11
1.1. Organizacijos tinklo analizė 11
1.2. Tinklo konfigūracija 11
1.2.1. Įrangos prievadai ir jų paskirtis 11
1.2.2. Kibernetinių grėsmių tyrimo įrankių lyginamoji analizė 12
1.3. Esama saugumo politika 17
1.4. Darbo objekto atitikimas Nacionalinei kibernetinio saugumo strategijai 19
1.5. Esamos organizacijos darbuotojų pareigos ir atsakomybė 19
1.6. Esamos problemos 21
1.6.1. Galimos grėsmės darbuotojui 21
1.6.2. Galimos grėsmės organizacijai 21
1.7. Tinklo patikimumo skaičiavimai 22
1.8. Tinklo pažeidžiamumo vertinimas 23
1.9. Apibendrinimas 24
2. SPECIFIKACIJA 25
2.1. Projektuojamo objekto apibūdinimas 25
2.2. Projektuojamo objekto paskirtis 25
2.3. Projektuojamo objekto funkcijos 25
2.4. Reikalavimai projektuojamo objekto posistemėms 25
2.4.1. Reikalavimai aparatūros posistemei 25
2.4.2. Reikalavimai naudotojo sąsajai 25
3. PROJEKTINĖ DALIS 26
3.1. Projektuojamas objektas 26
3.1.1. Atnaujinta tinklo modelio struktūra 26
3.1.2. Naudojami prievadai 27
3.1.3. Tinklo IP adresai 27
3.1.4. Tinklo įrangos specifikacija 27
3.2. Problemos sprendimai 30
3.2.1. Turinio filtravimas 30
3.2.2. Ugniasienės sudarymas 30
3.2.3. Kibernetinių atakų įtakos analizė 31
3.2.4. Atnaujintos struktūros patikimumo skaičiavimai 32

3.2.5. Atnaujintos struktūros pažeidžiamumo vertinimas 33
3.3. Reorganizacijos plano sudarymas 33
3.4. Kibernetinių incidentų valdymo diagrama 34
4. PRAKTINĖ-EKSPERIMENTINĖ DALIS 35
4.1. Kibernetinio saugumo diegimo specifikacija 35
4.2. Techninis kibernetinio saugumo testavimas 35
4.3. Testavimo rezultatų analizė ir išvadų apibendrinimas 37
5. EKONOMINĖ DALIS 38
5.1. Projekto projektavimo sąmata 38
5.2. Projekto projektavimo darbo užmokesčio skaičiavimas 38
5.3. Projekto įgyvendinimo sąmata 39
5.4. Projekto įgyvendinimo darbo užmokesčio skaičiavimas 40
5.5. Įdiegto projekto palaikymo sąnaudos 40
5.6. Projekto sąmata 41
5.7. Ekonominės naudos nustatymas 41
IŠVADOS 42
LITERATŪRA IR KITI INFORMACIJOS ŠALTINIAI 43

LENTELIŲ IR PAVEIKSLŲ SĄRAŠAS

LENTELĖS

1 lentelė. Prievadų analizė 12
2 lentelė. „Nmap“ įrankio privalumų ir trūkumų lentelė 13
3 lentelė. „Wireshark“ įrankio privalumų ir trūkumų lentelė 14
4 lentelė. „Nagios“ įrankio privalumų ir trūkumų lentelė 15
5 lentelė. „Zabbix“ įrankio privalumų ir trūkumų lentelė 17
6 lentelė. Esamos saugumo politikos klausimynas 18
7 lentelė. Kibernetinio saugumo strategijos tikslai, pagal 818 nutarimą 19
8 lentelė. Tinklo patikimumas be rezervinių kompiuterių 23
9 lentelė. Tinkle naudojamų prievadų sąrašas 27
10 lentelė. IP adresai 27
11 lentelė. Maršrutizatoriaus „Fortigate 60F“ specifikacija 28
12 lentelė. Komutatoriaus „Cisco Catalyst C9300-24P-A“ specifikacija 29
13 lentelė. Kompiuterio „Lenovo ThinkCentre V35s“ specifikacija 29
14 lentelė. Kibernetinių atakų analizės lentelė 31
15 lentelė. Patikimumo skaičiavimai po rezervavimo 32
16 lentelė. Projektavimo darbo laiko nustatymas 38
17 lentelė. Ilgalaikio turto nusidėvėjimo ir programinės įrangos mokestis 38
18 lentelė. Projektavimo sąmata 39
19 lentelė. Įgyvendinimo darbo laiko skaičiavimas 39
20 lentelė. Įrangos pirkimo sąmata 39
21 lentelė. Ilgalaikio turto nusidėvėjimo ir programinės įrangos mokestis 40
22 lentelė. Projektavimo sąmata 40
23 lentelė. Įdiegto projekto atlyginimo skaičiavimas 40
24 lentelė. Įdiegto projekto palaikymo sąmata 40
25 lentelė. Projekto sąmata 41

PAVEIKSLAI

1.1 pav. Esama tinklo topologija 11
1.2 pav. „Nmap“ sąsajos langas 13
1.3 pav. „Wireshark“ sąsajos langas 14
1.4 pav. „Nagios“ sąsajos langas 16
1.5 pav. Zabbix sąsajos langas 17

1.6 pav. Tinklo pažeidžiamumo vertinimas prieš atnaujinimą 23
3.1 pav. Atnaujinta tinklo topologija 26
3.2 pav. Maršrutizatorius „FortiGate 60F“ 28
3.3 pav. Komutatorius „Cisco Catalyst C9300-24P-A“ 29
3.4 pav. Kompiuteris „Lenovo ThinkCentre V35s“ 29
3.5 pav. Tinklo pažeidžiamumo vertinimas po atnaujinimo 33
3.6 pav. Kibernetinių incidentų valdymo diagrama 34
4.1 pav. Paketų perdavimas iš Pedagogai3 į Biblioteka 35
4.2 pav. Paketų perdavimas iš Biblioteka į Pedagogai3 36
4.3 pav. Paketų perdavimas iš Administracija2 į Pedagogai3 36
5.1 pav. Projekto projektavimo darbų tvarkaraštis 38
5.2 pav. Projekto įgyvendinimo darbų tvarkaraštis 39

SĄVOKŲ SĄRAŠAS

Sąvoka	Aprašymas	Nuoroda į šaltinį
CVSS	Pažeidžiamumų vertinimo sistema	(first.org, 2024)
TCP	Protokolas, užtikrinantis patikimą apsikeitimą žinutėmis tinkle	(nmap.org, 2024)
SYN	Paketas, kurį klientas siunčia į serverį, kad inicijuotų ryšį ir tarp jų būtų sinchronizuojami eilės numeriai.	(nmap.org, 2024)
API	Taisyklių ir protokolų rinkinys, leidžiantis skirtingoms programinės įrangos programoms bendrauti ir sąveikauti viena su kita, palengvinant keitimąsi duomenimis ir funkcionalumu tarp sistemų.	(nagios.org, 2024)
VoIP	Technologija, leidžianti balso ir daugialypės terpės ryšius perduoti internetu, o ne tradicinėmis analoginėmis telefono linijomis.	(wireshark.org, 2024)
ICMP	Protokolas, naudojamas siųsti klaidų pranešimus ir operatyvinę informaciją, nurodant IP paketų pristatymo problemas, teikiant tinklo trikčių šalinimo galimybes ir tinklų diagnostiką.	(wireshark.org, 2024)
SNMP	Protokolas, leidžiantis tinklo įrenginiams, pvz., maršrutizatoriams, serveriams ir spausdintuvams, dalytis informacija	(zabbix.com, 2024)

SANTRAUKA

Autorius Žygimantas Žiūkas. *Gimnazijos kompiuterių tinklo saugumo didinimo projektas*. Baigiamasis darbas. Vadovas dr. Dangis Rimkus. Kauno kolegija, Technologijų fakultetas, Informatikos ir medijų technologijų katedra. Kaunas, 2024, 43 psl.

Reikšminiai žodžiai: Optinis tinklas, optiniai dalikliai, signalo slopinimas.

Darbe atliekama gimnazijos kompiuterių tinklo analizė. Pagal nustatytus trūkumus sudaromi žingsniai, kuriais pasiekiamas saugesnio tinklo tikslas. Esminiai trūkumai yra rezervinių kompiuterių stoka, ugniasienės konfigūravimo stoka, potinklių nebuvimas. Šie trūkumai yra tinklo pažeidžiamumo vertinime, atlikus tinklo pakeitimus paskaičiuotas naujas vertinimas. Atlikta eksperimentinė dalis parodo, jog šios priemonės veikia. Paskaičiuota projekto ekonominė sąmata ir padarytos viso projekto išvados.

SUMMARY

Author Žygimantas Žiūkas. *Project for Increasing the Security of the Gymnasium's Computer Network*. Graduation Thesis. Supervisor PhD Dangis Rimkus. Kauno kolegija HEI, Faculty of Technologies, Department of Informatics and Media Technologies. Kaunas, 2024, 43 pages.

Key words: Optical network, optical splitters, signal attenuation.

The analysis of the gymnasium's computer network is performed in the work. Based on the identified weaknesses, steps are taken to achieve a more secure network. The main disadvantages are the lack of spare computers, the lack of configuration of the firewall, the absence of subnets. These flaws are in the network vulnerability assessment, a new assessment is calculated after the network changes. The completed experimental part shows that these tools work. The economic estimate was calculated and the conclusions of the whole project were made.

ĮVADAS

Darbo aktualumas. Gimnazijų tinklo saugumo užtikrinimas yra vis aktualesnis klausimas švietimo sistemoje. Nors internetinės technologijos ir virtualios mokymosi platformos tapo neatskiriama mokyklos dalimi, kartu jos atveria naujas saugumo spragas, kurias kibernetiniai nusikaltėliai gali panaudoti savo veiklai. Remiantis pateikta statistika galime nustatyti, kad atakų kiekis yra ganėtinai aukštas (Nacionalinio kibernetinio saugumo ataskaita, 2022).

Nepakankamas gimnazijos tinklo saugumas gali turėti rimtų padarinių. Dėl blogos kibernetinės higienos, kurios dažnai stokoja net didelės organizacijos, gali įvykti įsilaužimų į elektronines mokyklos paslaugas ir jų veiklos sutrikdymas. Be to, nenuoseklus mokyklų tinklo saugumo didinimo plano įgyvendinimas gali neigiamai paveikti pačios įstaigos veiklą.

Atsižvelgiant į šias augančias kibernetinio saugumo grėsmes, yra svarbu ištirti gimnazijos tinklo saugumo didinimo priemones, kurios padėtų užtikrinti saugią mokymosi aplinką ir apsaugotų jos informaciją nuo kibernetinių atakų. Šio bakalauro darbo tikslas yra išanalizuoti galimas gimnazijos tinklo saugumo gerinimo priemones ir pateikti rekomendacijas, kurios galėtų būti pritaikytos praktikoje.

Darbo problema. Šio darbo pagrindinė problema yra gimnazijos tinklo saugumo užtikrinimas. Dažniausiai praktikoje pasitaikančios spragos nulemiančios kibernetinių paslaugų tiekimo trikdžius:

- Dėl pasenusios programinės įrangos ar jos komponentų.
- Dėl piktybinių įsilaužimų į sistemą
- Dėl neteisingos maršrutizatoriaus konfigūracijos, kuri yra pažeidžiama įsilaužėlių.

Dėl pasenusios technologijos, įskaitant pasenusią programinę ir aparatinę įrangą, gali padidėti kibernetinio saugumo pažeidžiamumas. Naudojant pasenusias sistemas atsiranda lengvai išnaudojamų saugumo spragų, atveriančių kelią kibernetinėms atakoms, pvz.: išpirkos reikalaujančioms programoms, kenkėjiškoms programoms ir duomenų pažeidimams.

Žmogaus klaidos yra svarbus saugumo pažeidimų veiksnys, o 95 % kibernetinių incidentų priskiriami žmonių klaidoms. Socialinės inžinerijos atakos, tokios kaip sukčiavimas, socialinės inžinerijos atakos, siekiant apgauti asmenis ir pakenkti saugumui. Šios dažnos spragos – silpni slaptažodžiai, pasenusi programinė įranga ir žmogaus klaidos – suteikia daugybę įėjimo taškų, kad užpuolikai galėtų neteisėtai pasiekti mokyklų tinklus, o tai lemia duomenų pažeidimus, kenkėjiškų programų užkrėtimą ir kitus kibernetinio saugumo incidentus.

Darbo objektas. Darbo objektas yra gimnazijos kompiuterių tinklo kibernetinė sauga.

Darbo tikslas – Pagerinti gimnazijos kompiuterinio tinklo saugumą.

Darbo uždaviniai:

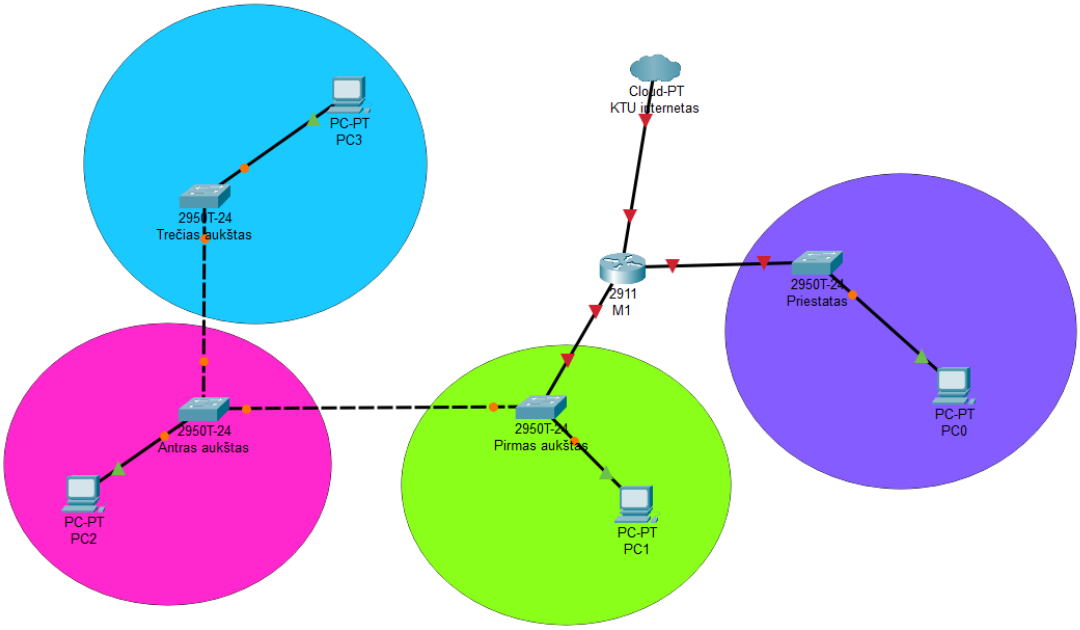
1. Atlikti gimnazijos tinklo saugumo analizę.
2. Naudojant programinius įrankius suprojektuoti saugesnį tinklą.
3. Atlikti patikimumo analizę.
4. Atlikti ekonominės naudos skaičiavimą.

Darbo struktūra. Analitinėje dalyje apžvelgiami kibernetinio saugumo įrankiai, atliekama objekto analizė, išskiriamos darbo objekto problemos, trūkumai. Projektinėje dalyje sprendžiama objekto problema, atliekami tinklo patikimumo skaičiavimai, tinklo saugumo vertinimas, numatomas reorganizavimo planas supaprastinantis tinklo perjungimo darbus, atliekama kibernetinių atakų analizė. Eksperimentinėje dalyje atliekami tinklo bandymai po pakeitimų, įsitikinama, kad sprendimas yra veikiantis ir paruoštas naudoti. Ekonominėje dalyje paskaičiuojama sąmata, nauda.

1. ANALITINĖ DALIS

1.1. Organizacijos tinklo analizė

Atliekant pirminę tinklo analizę buvo nustatyta, kad mokyklos tinklas veikia viename potinklyje ir tai sukelia aukšta tinklo pažeidžiamumo riziką. Naudojant vieną potinklį, tinklas tampa labiau pažeidžiamas neteisėtai prieigai, nes bet kuris kenkėjiškas veikėjas, gavęs prieigą prie potinklio, gali laisvai judėti tinkle. Taip yra todėl, kad nėra vidinių ribų ar segmentavimo, kuris apribotų užpuoliko judėjimą. Vienas iš efektyviausių būdų sumažinti saugumo riziką viename potinklyje yra tinklo segmentavimas. Tai apima tinklo padalijimą į kelis potinklius.



1.1 pav. Esama tinklo topologija

1.2. Tinklo konfigūracija

1.2.1. Įrangos prievadai ir jų paskirtis

Mokyklos naudoja įvairius tinklo prievadus interneto prieigai, vidiniam ryšiui ir konkrečioms programoms. 1 lentelėje pateikiamas naudojamų prievadų sąrašas.

1 lentelė. Prievadų analizė

Prievadas	Paskirtis	Būtina (+)	Nebūtina (-)
21	Failų perdavimo protokolas (FTP) yra taikomųjų programų lygmens protokolas, leidžiantis perkelti failus tarp vietinės ir nuotolinės failų sistemos per TCP tinklą.	+	
22	SSH (Secure Shell). SSH, taip pat žinomas kaip Secure Shell arba Secure Socket Shell, yra kriptografinis tinklo protokolas, leidžiantis saugiai nuotoliniu būdu prisijungti, užšifruoti ryšį ir saugiai perduoti failus neapsaugotu tinklu.	+	
25	SMTP (Simple Mail Transfer Protocol). SMTP yra esminis programos lygmens protokolas, naudojamas el. laiškams siųsti ir gauti.	+	
80	HTTP (Hyper Text Transport Protocol). Palengvina hiperteksto dokumentų perdavimą ir leidžia keistis informacija tarp klientų ir serverių hipertekstinių dokumentų pavidalu.	+	
110	POP3 (Post Office Protocol). Yra standartinis interneto protokolas, kurį naudoja el. pašto programos, kad gautų el. laiškus iš nuotolinio pašto serverio per TCP/IP ryšį.	+	
143	IMAP4 (Internet Message Access Protocol). Yra taikomųjų programų lygmens protokolas, skirtas el. paštui gauti, leidžiantis vartotojams pasiekti ir valdyti el. laiškus serveryje.		–
443	SSL (HTTP su Secure Socket Layer). Naudojamas saugiam ryšiui kompiuterių tinkle.	+	
587	Pranešimo pateikimo protokolas, naudojamas su SMTP		–
995	POP3S (POP3 + SSL). Naudojamas POP3 protokolui įgyvendinti per SSL/TLS ryšį, leidžiantį saugiai gauti el. paštą iš serverių.		–
3306	Prievadas naudojamas MySQL protokolui.		–

1.2.2. Kibernetinių grėsmių tyrimo įrankių lyginamoji analizė

„Nmap“, sutrumpintas iš „Network Mapper“, yra galingas ir universalus atvirojo kodo įrankis, plačiai naudojamas saugos specialistų, tinklo administratorių ir net kenkėjiškų veikėjų įvairioms tinklo aptikimo, žemėlapių sudarymo ir pažeidžiamumo nuskaitymo užduotims atlikti. Sukurtas Gordono Lyono (taip pat žinomo kaip „Fiodoras“), „Nmap“ bėgant metams įgijo didžiulį populiarumą dėl savo tvirto funkcijų rinkinio ir pritaikymo įvairioms tinklo aplinkoms.

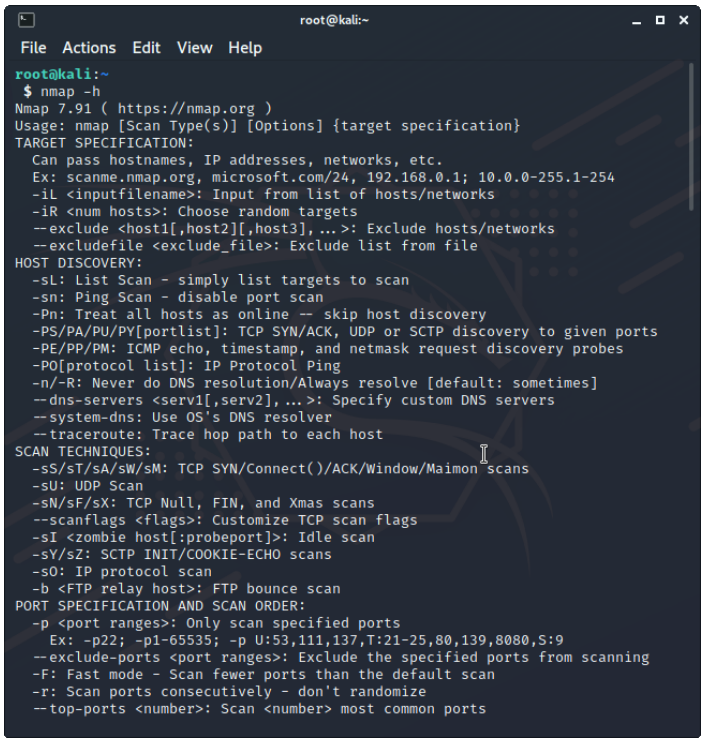
Iš esmės „Nmap“ leidžia vartotojams ištirti tinklo sistemas, identifikuoti aktyvius pagrindinius kompiuterius, atrasti atvirus prievadus ir veikiančias paslaugas bei aptikti operacinės sistemos detales. Dėl šių galimybių „Nmap“ yra esminis tinklo saugumo audito, pažeidžiamumo įvertinimo ir reagavimo į incidentus įrankis. „Nmap“ universalumą dar labiau padidina „Nmap Scripting Engine“ (NSE), leidžiantis vartotojams „Lua“ programoje rašyti pasirinktinius scenarijus, kad būtų galima automatizuoti įvairias tinklo užduotis, aptikti pažeidžiamumą ir netgi vykdyti tikslines atakas.

Vienas iš pagrindinių įrankio „Nmap“ pranašumų gebėjimas prisitaikyti prie įvairių tinklo sąlygų, įskaitant delsą ir perkrovą nuskaitymo metu. Tai leidžia pateikti tikslius ir patikimus rezultatus net sudėtingose tinklo aplinkose. Be to, „Nmap“ siūlo platų nuskaitymo tipų asortimentą – nuo pagrindinių nuskaitymų iki pažangesnių metodų, tokių kaip TCP SYN nuskaitymas, UDP nuskaitymas ir slaptas nuskaitymas, kurių kiekvienas turi savo privalumų ir naudojimo atvejų.

Išsamios „Nmap“ funkcijos taip pat apima OS aptikimą, versijos atpažinimą ir net galimybę suklastoti šaltinio adresus ir apeiti ugniasienes bei įsibrovimų aptikimo sistemas, kad būtų galima slaptai žvalgytis. Dėl šių pažangių galimybių „Nmap“ yra vertingas įrankis tiek saugos specialistų, tiek kenkėjiškų veikėjų rankose, pabrėžiant atsakingo ir etiško naudojimo svarbą (2 lentelė).

2 lentelė. „Nmap“ įrankio privalumų ir trūkumų lentelė

Įrankio privalumai	Įrankio trūkumai
• Atranda pagrindinius kompiuterius, paslaugas ir įrenginius tinkle, pateikdamas išsamų infrastruktūros žemėlapį. • Tiksliai aptinka operacines sistemas, versijas ir veikiančias paslaugas aptiktuose pagrindiniuose kompiuteriuose. • Identifikuoja ugniasienes, filtruotus / blokuojamus prievadus ir suteikia įžvalgų apie tinklo topologiją. • „Nmap Scripting Engine“ (NSE) leidžia rašyti pasirinktinius scenarijus, kad būtų galima automatizuoti užduotis ir aptikti pažeidžiamumą. • Žinomas dėl greito ir efektyvaus didelių tinklų nuskaitymo.	• Tam tikri „Nmap“ nuskaitymo būdai gali būti laikomi įkyriais ir gali suaktyvinti saugos įspėjimus arba sutrikdyti tinklo darbą. • „Nmap“ komandų eilutės sąsaja gali būti sudėtinga pradedantiesiems, todėl reikia šiek tiek mokytis ir eksperimentuoti. • „Nmap“ nuskaitymas kartais gali duoti klaidingai teigiamų rezultatų dėl tokių veiksnių kaip ugniasienės, NAT įrenginiai arba tinklo konfigūracijos.



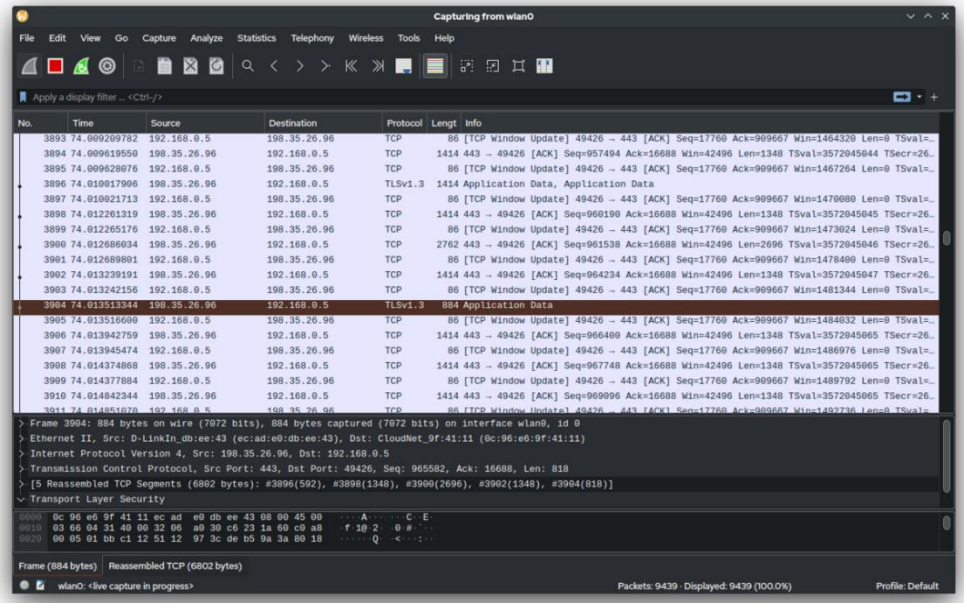
1.2 pav. „Nmap“ sąsajos langas

„Wireshark“ yra universalus ir plačiai naudojamas atvirojo kodo tinklo paketų analizatorius, kuris tapo nepakeičiamu įrankiu tinklo administratoriams, saugos specialistams ir IT entuziastams. Viena iš išskirtinių „Wireshark“ savybių yra galimybė iššifruoti ir interpretuoti daugybę tinklo protokolų – nuo visur esančio TCP/IP iki labiau specializuotų protokolų, tokių kaip VoIP ir ICMP. Ši protokolo išskaidymo galimybė leidžia vartotojams giliai ištirti tinklo srautą, atskleidžiant detalią informaciją apie kiekvieno paketo turinį ir struktūrą. Patogi „Wireshark“ grafinė sąsaja dar labiau pagerina jos naudojimo patogumą, todėl ji tampa prieinamesnė.

Nepaisant saugumo aspekto, „Wireshark“ yra neįkainojama tinklo trikčių šalinimo ir našumo optimizavimo srityje. Tinklo administratoriai gali naudoti „Wireshark“ diagnozuoti ir išspręsti našumo problemas, nustatyti kliūtis ir užtikrinti efektyvų tinklo išteklių naudojimą. Įrankio statistinės analizės ir vizualizavimo funkcijos suteikia vertingų įžvalgų apie tinklo srauto modelius, leidžiančius priimti pagrįstus sprendimus ir aktyviai valdyti tinklą (3 lentelė).

3 lentelė. „Wireshark“ įrankio privalumų ir trūkumų lentelė

Įrankio privalumai	Įrankio trūkumai
• „Wireshark“ fiksuoja ir išskaido tinklo srautą, suteikdama detalų tinkle tekančių duomenų vaizdą. • „Wireshark“ gali iššifruoti ir interpretuoti daugybę tinklo protokolų, todėl vartotojai gali ištirti srautą giliu lygmeniu. • „Wireshark“ padeda diagnozuoti ir išspręsti tinklo veikimo problemas, nustatyti kliūtis ir užtikrinti efektyvų išteklių panaudojimą. • „Wireshark“ yra atvirojo kodo įrankis su turtinga papildinių ir plėtinių ekosistema, leidžiančia tinkinti ir pritaikyti.	• „Wireshark“ galimybės analizuoti šifruoto tinklo srautą yra ribotos, nes vartotojai turi būti susipažinę su šifravimo ir iššifravimo metodais. • Išsamios „Wireshark“ paketų fiksavimo ir analizės galimybės gali turėti didelės įtakos pagrindinės sistemos veikimui. • „Wireshark“ pateikia tik vieno taško tinklo perspektyvą, o to gali nepakakti norint suprasti viso tinklo elgseną. • Dėl plataus „Wireshark“ funkcijų rinkinio ir jos teikiamos informacijos gylio pradedantiesiems vartotojams gali būti sudėtinga įsisavinti.



1.3 pav. „Wireshark“ sąsajos langas

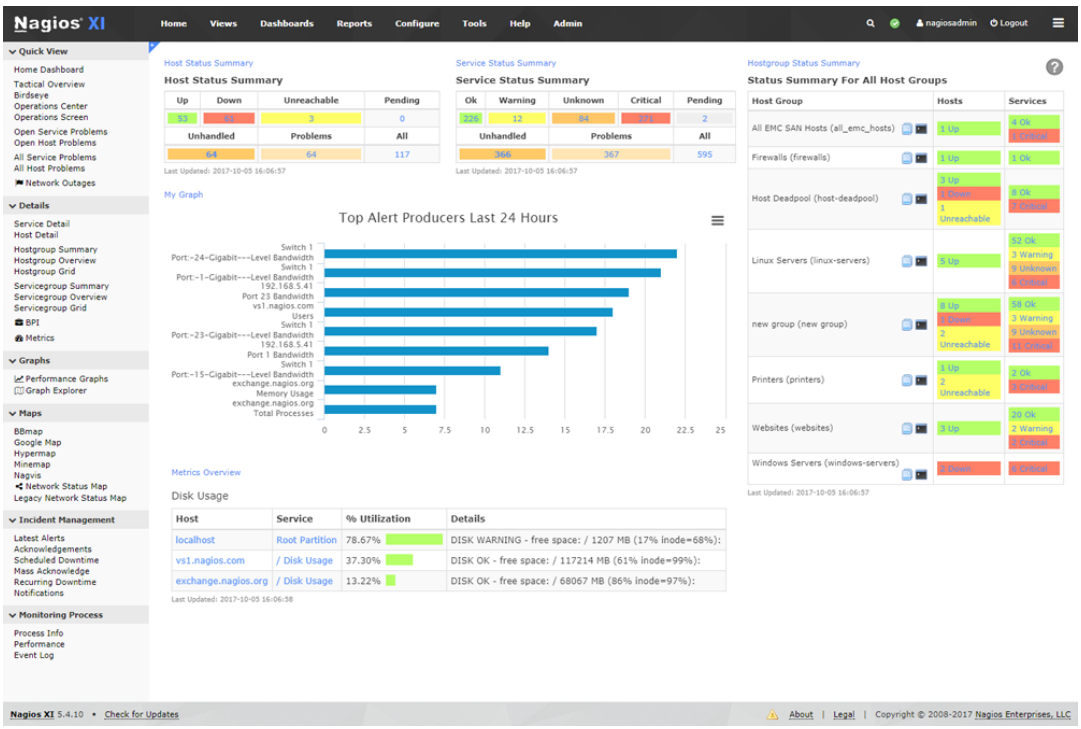
„Nagios“ yra plačiai naudojama atvirojo kodo stebėjimo sistema, leidžianti organizacijoms aktyviai nustatyti ir išspręsti IT infrastruktūros problemas, kol jos dar nepaveikė svarbių verslo procesų. Iš esmės „Nagios“ teikia išsamias stebėjimo galimybes, leidžiančias vartotojams stebėti daugybę komponentų, įskaitant programas, paslaugas, operacines sistemas, tinklo protokolus, sistemos metriką ir infrastruktūros elementus. Šį platų stebėjimo pasiekiamumą palengvina galingos „Nagios“ scenarijų API , kurios leidžia lengvai integruoti su individualiomis vidaus programomis ir sistemomis.

Viena iš pagrindinių „Nagios“ pranašumų yra galimybė keisti mastelį, kad būtų galima stebėti tūkstančius tinklo mazgų ir paslaugų įvairiose platformose ir protokoluose. Šis mastelio keitimas kartu su kelių nuomininkų galimybėmis leidžia „Nagios“ aptarnauti įvairaus dydžio organizacijų, nuo mažų įmonių iki didelių įmonių, stebėjimo poreikius. „Nagios“ taip pat gali pasigirti išplečiama architektūra, turinti turtingą aktyvios bendruomenės sukurtų priedų ir papildinių ekosistemą, leidžiančią vartotojams toliau tobulinti jos funkcionalumą ir pritaikyti prie konkrečių stebėjimo reikalavimų.

Gedimo ar problemos atveju „Nagios“ gali greitai įspėti atitinkamą techninį personalą įvairiais kanalais, pvz.: el. paštu, SMS žinutėmis ir kitais pranešimo būdais. Šiuos įspėjimus galima pritaikyti ir išplėsti atsižvelgiant į problemos sunkumą ir trukmę, greitas reagavimas į incidentus ir sprendimas. „Nagios“ taip pat teikia istorinių ataskaitų ir tendencijų teikimo galimybes, leidžiančias vartotojams analizuoti praeities incidentus, planuoti infrastruktūros atnaujinimus ir užtikrinti, kad būtų laikomasi susitarimų.

4 lentelė. „Nagios“ įrankio privalumų ir trūkumų lentelė

Įrankio privalumai	Įrankio trūkumai
• „Nagios“ gali stebėti daugybę komponentų, įskaitant programas, paslaugas, operacines sistemas, tinklo protokolus ir infrastruktūros elementus. • „Nagios“ gali stebėti tūkstančius tinklo mazgų ir paslaugų, taip pat palaiko kelių nuomininkų konfigūracijas įvairiems organizaciniams poreikiams. • „Nagios“ gali greitai įspėti darbuotojus apie problemas, todėl galima greitai reaguoti ir išspręsti problemą bei sumažinti prastovos laiką. • „Nagios“ suteikia ataskaitų teikimo ir tendencijų nustatymo galimybes, kad būtų galima analizuoti praeities saugos incidentus, planuoti infrastruktūros atnaujinimus ir užtikrinti atitiktį.	• Dėl sudėtingų konfigūracijos failų „Nagios“ gali būti sudėtinga konfigūruoti ir nustatyti, ypač naujiems įrankio naudotojams. • „Nagios“ labai priklauso nuo įskiepių, kuriuos gali būti sunku rasti, įdiegti ir prižiūrėti, ir jie gali būti ne visada patogūs vartotojui. • Nagios projekto aktyvios plėtros bei paramos trūkumas gali kelti susirūpinimą dėl jo ilgalaikio išlaikymo ir tvarumo.



1.4 pav. „Nagios“ sąsajos langas

„Zabbix“ yra galingas ir universalus atvirojo kodo stebėjimo įrankis, plačiai naudojamas visų dydžių organizacijose. Iš esmės „Zabbix“ teikia išsamias stebėjimo galimybes, leidžiančias vartotojams stebėti įvairius IT komponentus, įskaitant tinklus, serverius, virtualias mašinas, duomenų bazes ir debesies paslaugas. Modulinė įrankio architektūra ir įvairių duomenų rinkimo metodų, tokių kaip SNMP, IPMI ir pasirinktiniai scenarijai, palaikymas leidžia prisitaikyti prie įvairių stebėjimo reikalavimų.

Viena iš išskirtinių „Zabbix“ funkcijų yra galimybė automatiškai aptikti ir stebėti naujus įrenginius ir komponentus, įtrauktus į tinklą. Naudodama žemo lygio aptikimo funkciją, „Zabbix“ gali dinamiškai aptikti ir pradėti stebėti naujus tinklo įrenginius, serverius ir kitus išteklius, taip sumažindama administracines išlaidas, susijusias su rankiniu konfigūravimu. Be to, „Zabbix“ siūlo gausią iš anksto sukurtų šablonų biblioteką populiariems aparatinės ir programinės įrangos pardavėjams, todėl vartotojai gali greitai prisijungti ir pradėti stebėti savo IT infrastruktūrą.

„Zabbix“ įspėjimų ir pranešimų sistema yra dar vienas svarbus privalumas. Ji suteikia vartotojams galimybę apibrėžti lanksčias paleidimo sąlygas, pagrįstas įvairiomis našumo metrikomis, ir sukonfigūruoti pasirinktinius pranešimus, kurie būtų siunčiami el. paštu, SMS arba net integruojant su trečiųjų šalių įrankiais. Įspėjimo mechanizmai leidžia darbuotojams greitai nustatyti ir spręsti problemas, kol jos neperauga į didelius incidentus.

5 lentelė. „Zabbix“ įrankio privalumų ir trūkumų lentelė

Įrankio privalumai	Įrankio trūkumai
• „Zabbix“ palaiko įvairius duomenų rinkimo protokolus ir metodus, tokius kaip SNMP, IPMI ir pasirinktinius scenarijus, leidžiančius prisitaikyti prie įvairių stebėjimo reikalavimų. • „Zabbix“ gali automatiškai aptikti ir pradėti stebėti naujus įrenginius ir komponentus, įtrauktus į tinklą, sumažindama administracines išlaidas. • „Zabbix“ siūlo lanksčią įspėjimo sistemą su pritaikomomis paleidimo sąlygomis ir pranešimų kanalais, leidžiančiais aktyviai identifikuoti ir išspręsti problemas.	• „Zabbix“ sąrankos procesas gali būti sudėtingas, todėl norint efektyviai konfigūruoti ir valdyti, reikia tam tikro lygio techninių žinių. • Bendruomenės palaikymas „Zabbix“ gali būti ne toks stiprus kaip kai kurių kitų atvirojo kodo stebėjimo įrankių. • „Zabbix“ derinimo galimybės gali būti ne tokios pažangios, kaip norėtų kai kurie vartotojai, ypač sudėtingose aplinkose. • „Zabbix“ integruoti vizualizacijos įrankiai gali būti ne tokie lankstūs, kaip siūlomi kai kuriuose kituose stebėjimo sprendimuose.

1.5 pav. Zabbix sąsajos langas

1.3. Esama saugumo politika

Toliau pateikiama informacija apie 20 ypač svarbių efektyvios kibernetinės gynybos saugumo kontrolės priemonių, kurias rekomenduoja Nacionalinis kibernetinio saugumo centras (6 lentelė). Šios priemonės apima tinklo įrenginių ir programinės įrangos valdymą, saugią konfigūraciją, apsaugą nuo kenksmingos programinės įrangos, prieigos kontrolę, audito žurnalų stebėjimą, reagavimą į incidentus ir kitas svarbias saugumo sritis. Taip pat pateikiami patarimai mažoms organizacijoms, kaip pradėti rūpintis savo kibernetiniu saugumu. Dokumentas parengtas remiantis SANS instituto ir Kibernetinio saugumo tarybos gerąja praktika (NKSC Ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės).

Mažoms organizacijoms rekomenduojama pradėti nuo 4 pagrindinių veiksmų: 1) sudaryti leistinos naudoti programinės įrangos sąrašus, 2) naudoti saugias konfigūracijas, 3) laiku diegti programinės įrangos ir operacinių sistemų naujinimus, 4) griežtai riboti administratorių skaičių.

6 lentelė. Esamos saugumo politikos klausimynas

Eil.Nr.	Saugumą didinanti priemonė	Ar taikoma priemonė	
		Taip	Ne
1.	Tinklo įrenginių, kuriems leidžiama naudotis institucijos tinklo paslaugomis, identifikavimas.		X
2.	Leistinos ir neleistinos naudoti programinės įrangos identifikavimas.		X
3.	Techninės ir programinės įrangos saugios konfigūracijos mobiliuosiuose įrenginiuose, darbo vietos ar tarnybinėse stotyse numatymas.		X
4.	Nenutrūkstamas sistemų pažeidžiamumo vertinimas ir saugumo spragų taisymas.		X
5.	Naudojimosi administratoriaus teisėmis kontrolė.	X	
6.	Audito žurnalų įrašų stebėjimas, analizė ir saugojimas.		X
7.	Elektroninio pašto ir naršyklių apsauga.	X	
8.	Apsauga nuo kenkimo programų.	X	
9.	Tinklo prievadų, protokolų ir paslaugų naudojimo apribojimai.		X
10.	Duomenų atkūrimo pajėgumas.		X
11.	Saugios tinklo įrenginių, tokių kaip saugasienės, maršruto parinktuvai, komutatoriai, konfigūracijos numatymas.		X
12.	Tinklo perimetro apsauga.	X	
13.	Duomenų apsauga.	X	
14.	Prieigos kontrolė, paremta principu „būtina žinoti“.		X
15.	Belaidės prieigos kontrolė.		X
16.	Naudotojų paskyrų stebėjimas ir kontrolė.		X
17.	Saugumo srities gebėjimų vertinimas ir reikiamų mokymų numatymas.		X
18.	Taikomųjų programų saugumas.	X	
19.	Reagavimas į incidentus ir jų valdymas.	X	
20.	Bandymai įsilaužti ir „raudonųjų komandų“ pratybos.		X

1.4. Darbo objekto atitikimas Nacionalinei kibernetinio saugumo strategijai

Nacionalinė kibernetinio saugumo strategija yra skirta sustiprinti šalies kibernetinį saugumą ir gynybos pajėgumus. Jame nustatomi svarbiausi nacionalinės kibernetinio saugumo politikos tikslai ir kryptys viešajame bei privačiame sektoriuose penkeriems metams. Strategija taip pat įgyvendina Europos Sąjungos reikalavimus, nustatytus Tinklų ir informacinių sistemų saugumo direktyvoje. Darbo objekto atitikimas keliamiems uždaviniams yra aprašomas 7 lentelėje.

7 lentelė. Kibernetinio saugumo strategijos tikslai, pagal 818 nutarimą

Pirmasis Strategijos tikslas *– stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą.*	
Uždavinys	Stiprinti kibernetinį saugumą ir kibernetinių gynybos pajėgumus, kad būtų apsaugota jos informacinė infrastruktūra nuo kibernetinių grėsmių ir atakų.
Sprendimas	Gimnazija turėtų investuoti į modernias kibernetinio saugumo technologijas ir infrastruktūrą, įskaitant stiprius ugniasienės sistemas, duomenų šifravimą, atsarginių duomenų kopijų saugojimą ir duomenų atkūrimo planus. Gimnazija turi sukurti ir įgyvendinti išsamią kibernetinio saugumo politiką ir procedūras, kuriomis būtų apibrėžiamos saugumo standartai, atsakomybės ir procedūros kibernetinių incidentų atveju.
Antrasis Strategijos tikslas *– užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą.*	
Uždavinys	Užtikrinti veiksmingą nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą, siekiant apsaugoti gimnazijos duomenis bei infrastruktūrą nuo kibernetinių nusikaltėlių veiksmų.
Sprendimas	Stiprinti gimnazijos bendradarbiavimo su kitomis institucijomis kibernetinių nusikaltimų tyrimo pajėgumus. Tai apima mokymus informacijos technologijų srityje bei glaudesnį bendradarbiavimą su policija ir kitomis valstybinėmis institucijomis.
Trečiasis Strategijos tikslas *– skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą.*	
Uždavinys	Gimnazijai reikia skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, siekiant sukurti tinkamą požiūrį į kibernetinį saugumą ir skatinti naujoves, kurios padėtų stiprinti saugumą ir efektyviai reaguoti į kibernetines grėsmes.
Sprendimas	Organizuoti švietimo programas, mokymus ir seminarus, skirtus skatinti kibernetinio saugumo sąmoningumą ir suformuoti kibernetinio saugumo kultūrą gimnazijos darbuotojams. Tai gali apimti mokymus apie saugumo praktikas, mokymus apie naujausias kibernetines grėsmes ir būdus joms priešintis.
Ketvirtasis Strategijos tikslas *– stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą.*	
Uždavinys	Gerinti kibernetinį saugumą ir bendrai reaguoti į kibernetines grėsmes.
Sprendimas	Bendrai organizuoti kibernetinio saugumo mokymus, kuriose dalyvautų tiek viešojo, tiek privataus sektoriaus atstovai. Tokios programos galėtų būti skirtos informuoti apie naujausias grėsmes, mokytų veiksmingų saugumo priemonių ir skatintų bendradarbiavimą.
Penktasis Strategijos tikslas *– stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą.*	
Uždavinys	Stiprinti kibernetinį saugumą tarptautinėje kibernetinėje erdvėje
Sprendimas	Aktyviai dalyvauti kibernetinių grėsmių tyrimuose su kitomis tarptautinėmis institucijomis ir organizacijomis. Tai padėtų gauti svarbią informaciją apie naujausias grėsmes ir gerąją praktiką kibernetinio saugumo srityje.

1.5. Esamos organizacijos darbuotojų pareigos ir atsakomybė

Už elektroninės informacijos saugą pagal kompetenciją atsako informacinės sistemos valdytojas ir informacinės sistemos tvarkytojas (-ai). Informacinės sistemos tvarkytojas (-ai) atsako

už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir saugos politiką nustatytoje tvarkoje.

Saugos įgaliotiniu negali būti skiriamas asmuo, kuris turi neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, turi paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą. Jei asmuo turi tokią teistumą ar nuobaudą, jam negali būti suteikta saugos įgaliotinio pareigybė, nebent nuo jos paskyrimo praėję mažiau nei vieni metai. Saugos įgaliotiniui privaloma išmanyti ir taikyti elektroninės informacijos saugos užtikrinimo principus, nuolatos tobulinti kvalifikaciją elektroninės informacijos saugos srityje, atliekant darbus vadovautis Aprašo, kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis. Saugos įgaliotiniui yra pavesta atlikti šias funkcijas: teikti informacinės sistemos valdytojo vadovui pasiūlymus dėl administratoriaus paskyrimo bei reikalavimų sudarymo, institucijos informacinės saugos atitikties vertinimo, teikti informacinės sistemos valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo bei keitimo, koordinuoti kibernetinės saugos incidentų tyrimus įvykusius informacijos sistemoje, aktyviai bendradarbiauti su institucijomis tiriančiomis kibernetinio saugumo incidentus, neteisėtas veikas, susijusias su kibernetinio saugumo incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka kibernetinės saugos darbo grupės. Saugos įgaliotinis yra atsakingas už rizikos įvertinimo organizavimą, teikia administratoriui bei sistemos naudotojams privalomas vykti pareigas bei nurodymus, susijusius su saugos politika ir jos įgyvendinimu. Norint apsaugoti tinklą, saugos įgaliotinis turi aktyviai organizuoti kibernetines saugos mokymus, kurie informuoja apie galimas grėsmes ir būdus kaip apsisaugoti. Pabrėžiama, kad saugos įgaliotinis negali atlikti administratoriaus funkcijų (716 nutarimas, dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo, 2013).

Administratorius atlieka funkcijas, susijusias su informacinės sistemos naudotojų teisių valdymu, sistemos komponentais, taisyklinga šių komponentų sąranka, pažeidžiamumų nustatymu, saugos reikalavimų nustatymu ir priežiūra. Saugos įgaliotinis pateikia visus nurodymus susijusius su saugos užtikrinimu administratoriui ir nuolatos turi teikti saugos įgaliotiniui informaciją apie pagrindinių komponentų būklę. Atlikdamas sistemos konfigūracijos pakeitimus, administratorius turi laikytis pokyčių valdymo tvarkos, pokyčius privalo patikrinti ne rečiau kaip kartą per metus po sistemos pokyčio (716 nutarimas, dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo,

Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo, 2013).

1.6. Esamos problemos

1.6.1. Galimos grėsmės darbuotojui

Nacionalinis kibernetinio saugumo centras 2022 m. rengiamose saugumo pratybose pasinaudojo socialinės inžinerijos įrankį ir išsiuntė sukčius imituojančius el. laiškus ir nustatė, kad 13% darbuotojų arba 7,1 tūkst. asmenų neatpažino šio laiško ir atliko žalingus veiksmus. (Nacionalinio kibernetinio saugumo ataskaita, 2022). Šio tipo atakos yra labai populiarios ir atkartojamos. Socialinės inžinerijos atakos apima psichologinį žmonių manipuliavimą siekiant gauti prieigą prie jautrios informacijos ar sistemų. Šios atakos paprastai išnaudoja žmogaus elgesį ir emocijas, o ne techninius pažeidžiamumus. Mokyklos renka ir saugo daugybę asmeninių ir neskelbtinų duomenų apie mokinius ir darbuotojus, įskaitant pažymius, drausmės įrašus ir t.t. Sėkmingos socialinės inžinerijos atakos gali lemti šios neskelbtinos informacijos vagystę ir netinkamą jos naudojimą.

Darbuotojai tarp 18-41 amžiaus yra lengviau išnaudojami socialinės inžinerijos atakų. Siekdamos sumažinti socialinės inžinerijos atakų riziką, mokyklos turi įgyvendinti išsamią kibernetinio saugumo strategiją, apimančią darbuotojų mokymą, prieigos kontrolės politiką ir pažangias saugos technologijas. Spręsdamos žmogiškąjį kibernetinio saugumo aspektą, mokyklos gali padidinti savo bendrą atsparumą grėsmėms

1.6.2. Galimos grėsmės organizacijai

Mokykla kaupia didelį duomenų kiekį susijusi su mokiniais:

- Asmens kodas
- El. paštas
- Gyvenamoji vieta
- Telefono numeris

Dažnu atveju panaši informacija yra kaupiama ir apie šeimos narius. Ši informacija yra labai patrauklus taikinys kibernetiniams įsilaužėliams todėl privaloma laikytis normų ir įstatymų reglamentuotų „Lietuvos Respublikos asmens duomenų apsaugos įstatyme“ Šio įstatymo paskirtis yra apsaugoti žmogaus teises, asmens duomenų apsaugą ir užtikrinti, kad duomenų apsauga būtų

aukštame lygmenyje. Asmens kodą yra draudžiama skelbti viešai. (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 1996). Svarbu pasirūpinti, kad jautri informacija būtų kontroliuojama, nes už duomenų apsaugos pažeidimus yra taikomos administracinės baudos. (LR administracinių nusižengimų kodeksas, 2015).

1.7. Tinklo patikimumo skaičiavimai

Nagrinėjant tinklo patikimumą reikia žinoti, kiek prijungta kompiuterių prie kiekvieno komutatoriaus. Darbo vietoje nėra rezervinių kompiuterių.

Paskaičiavus kompiuterio patikimumą buvo gautas atsakymas P = 0,999. Žinant patikimumą ir kompiuterių skaičių galime bendrą neveikimo laiką metuose.

Toliau apskaičiuojamas antro aukšto patikimumas žinant, kad turima iš viso kompiuterių N = 10, ir iš jų naudojami visi n = 10. Vienos darbo vietos patikimumas yra P = 0,999.

Apskaičiuojamos šios formulės:

$$N! = 10! = 3628800 \tag{1.1}$$

$$n!\,(N-n)! = 10! * (10-1)! = 362880 \tag{1.2}$$

Apskaičiuojamas derinių skaičius:

$$C_n^N = \frac{N!}{n!(N-n)!} = C_1^{10} = \frac{10!}{10!*(10-1)!} = \frac{3628800}{362880} = 10 \tag{1.3}$$

Toliau atliekame skaičiavimą:

$$(1-P)^n = (1-0{,}999)^1 = 0{,}001 \tag{1.4}$$

Ši formulė naudojama, kai patikimumas yra arti vieneto:

$$C_n^N * (1-P)^n = 10 * 0{,}001 = 0{,}01 \tag{1.5}$$

Susumavus visas gautas reikšmės iš paskutinio skaičiavimo gauname 0,01005. Patikimumas gaunamas atimant šia reikšmę iš vieneto:

$$1 - 0{,}01005 = 0{,}98995 \tag{1.6}$$

Norint gauti bendrą neveikimo laiką padauginame patikimumą iš minučių metuose:

$$\Delta = 0{,}9899 * 525960 = 5283 \tag{1.7}$$

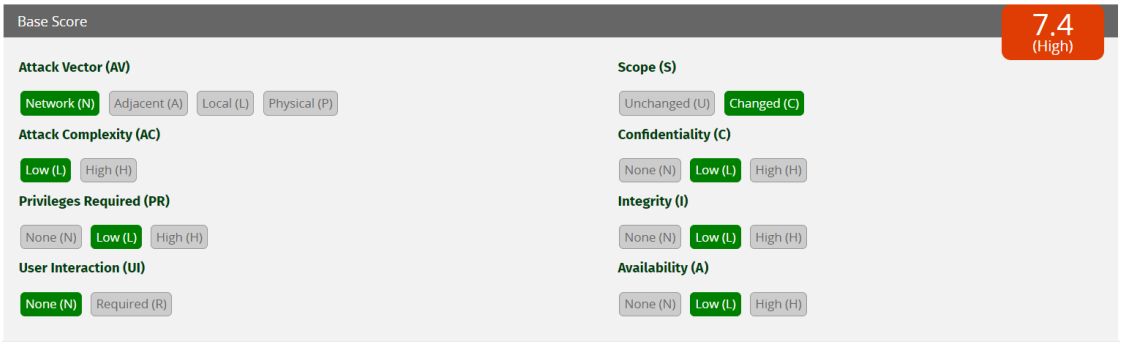
8 lentelė. Tinklo patikimumas be rezervinių kompiuterių

Pirmas aukštas			Antras aukštas			Trečias aukštas			Priestatas		
sk.	patik.	Δ, min.	sk.	patik.	Δ, min.	sk.	patik.	Δ, min.	sk.	patik.	Δ, min.
26	0,9736	13847	10	0,9899	5283	8	0,9919	4222	3	0,9969	1579

Atlikus lentelės analizę matome, kad pirmame aukšte esantys kompiuteriai turi didžiausią prastovą lyginant su kituose aukštuose esančiais kompiuteriais. Galime padaryti išvadą, kad kuo daugiau kompiuterių yra darbo vietoje, tuo didesnis prastovos laikas ir yra reikalingi pakeitimai šiai situacijai pagerinti.

1.8. Tinklo pažeidžiamumo vertinimas

Bendra pažeidžiamumo vertinimo sistema (CVSS) yra sistema, skirta kompiuterių sistemos saugumo spragų sunkumui įvertinti. CVSS naudoja metrikų rinkinį, kuris užfiksuoja esmines pažeidžiamumo savybes, įskaitant pagrindines, laiko ir aplinkos charakteristikas. Bazinis balas atspindi vidines pažeidžiamumo savybes, laikinas – esamą pažeidžiamumo būseną, o aplinkos balas – konkretaus vartotojo aplinką. Tada šie balai sujungiami, kad būtų gautas bendras pažeidžiamumo vertinimas, kuris svyruoja nuo 0 (žemo pažeidžiamumo) iki 10 (aukšto pažeidžiamumo) (Pažeidžiamumo vertinimo sistema CVSS).



1.6 pav. Tinklo pažeidžiamumo vertinimas prieš atnaujinimą

Atlikus vertinimą nustatyta, kad pažeidžiamumą gali nuotoliniu būdu išnaudoti užpuolikas, turintis žemo lygio privilegijas, nereikalaujant vartotojo sąveikos. Pažeidžiamumas turi poveikį paveikto komponento konfidencialumui, vientisumui ir prieinamumui, jis taip pat gali paveikti kitus komponentus, kurie nepatenka į pradinę taikymo sritį. Šio tipo pažeidžiamumas gali leisti užpuolikui gauti neteisėtą prieigą, modifikuoti duomenis arba sutrikdyti įprastą sistemos veikimą, o tai kelia riziką bendram tinklo saugumui.

1.9. Apibendrinimas

Viso mokyklų tinklo valdymas viename potinklyje žymiai padidina saugumo riziką ir neteisėtos prieigos galimybę. Neįgyvendinus tinklo segmentacijos, nėra vidinių ribų, kurie trukdytų judėjimui ir apribotų grėsmių plitimą tinkle.

Be to, tai, kad mokyklos tinkle nėra atsarginių kompiuterių tai padidina ilgalaikės prastovos riziką įrangos gedimų atveju. Neturint rezervinio kompiuterio, net vienas kompiuterio gedimas gali sutrikdyti svarbiausius švietimo išteklius ir programas, kuriomis naudojasi mokiniai, mokytojai ir darbuotojai.

Nors ugniasienės atlieka itin svarbų vaidmenį užtikrinant tinklo saugumą, jų veiksmingumas priklauso nuo tinkamos konfigūracijos ir integracijos su kitomis saugos priemonėmis. Pagrindinė ugniasienės funkcija yra stebėti ir valdyti gaunamą ir išeinantį srautą pagal iš anksto nustatytas taisykles leistinas srautas pasiekia numatytą tikslą, tuo pačiu atmesdamas arba blokuodamas potencialiai kenkėjiškus ar neteisėtos prieigos bandymus. Be to, ugniasienės padeda apsaugoti duomenis nuo neteisėtos prieigos stebėdamos srautą, aptikdamos įtartiną veiklą ir pranešdamos administratoriams apie galimas grėsmes.

Tačiau vien ugniasienės nėra visapusiškas tinklo saugumo sprendimas. Juos turi papildyti patikima saugumo praktika, pvz., tinklo segmentavimas, darbuotojų mokymas, mokinių prieigos apribojimai, išorinių grėsmių stebėjimas ir programinės įrangos atnaujinimai. Diegiant daugiasluoksnį saugos metodą, apimantį tinklo segmentavimą, rezervavimą ir tinkamai sukonfigūruotos ugniasienės, mokyklos gali žymiai pagerinti savo tinklo saugumą ir sumažinti neteisėtos prieigos, duomenų pažeidimų ir ilgos prastovos riziką.

2. SPECIFIKACIJA

2.1. Projektuojamo objekto apibūdinimas

Šio projekto tikslas – suprojektuoti saugų gimnazijos tinklą pasinaudojant saugius sprendimus. Atliekant šį projektą bus patobulintas vidinis tinklas.

2.2. Projektuojamo objekto paskirtis

Projekto tikslas – esamo tinklo atnaujinimas gimnazijoje padarant tinklą saugesniu.

2.3. Projektuojamo objekto funkcijos

- Atskirtas kompiuterių tinklas į atskirus potinklius.
- Kompiuterių rezervavimas padidina patikimumą.
- Išanalizuoti kibernetinių grėsmių tyrimo įrankiai.
- Sukonfigūruota ugniasienė

2.4. Reikalavimai projektuojamo objekto posistemėms

2.4.1. Reikalavimai aparatūros posistemei

Rezerviniai kompiuteriai su Windows 10 operacine sistema, su procesoriumi Ryzen 3 3250U, su 8 GB RAM operatyviąja atmintimi ir 256 GB SSD talpos.

2.4.2. Reikalavimai naudotojo sąsajai

Operacinės sistemos:

- Windows 10
- Windows 11

3. PROJEKTINĖ DALIS

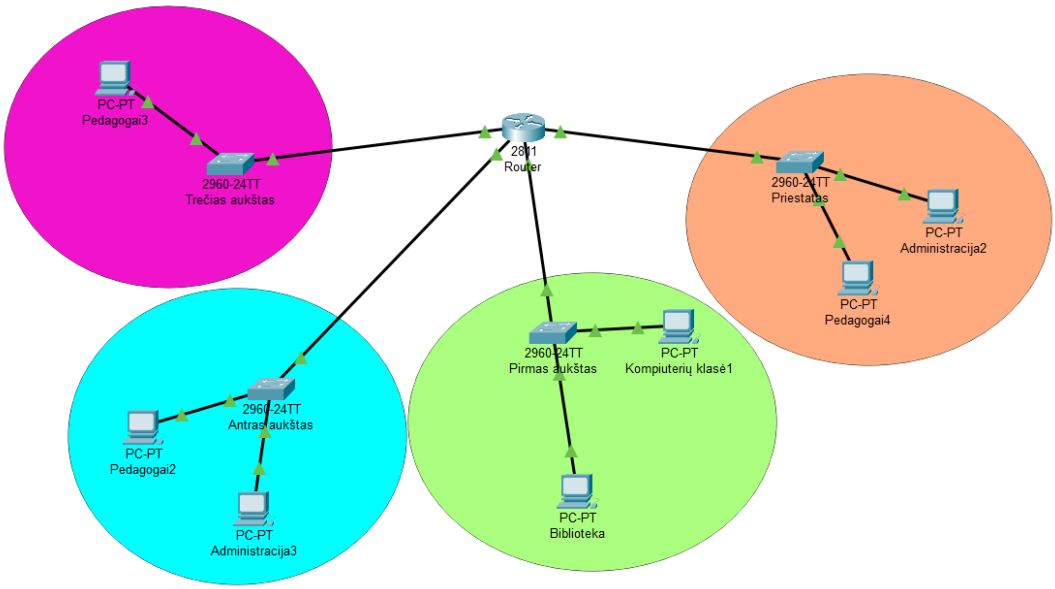
3.1. Projektuojamas objektas

3.1.1. Atnaujinta tinklo modelio struktūra

Siekiant padidinti bendrą tinklo infrastruktūros efektyvumą, saugumą ir patikimumą, gimnazijoje buvo atlikta pertvarka (3.1 pav.). Ši iniciatyva apėmė esamo tinklo padalijimą į keturis atskirus potinklius, kurių kiekvienas aptarnauja tam tikras funkcines sritis. Atskyrus tinklą į loginius segmentus, buvo pasiekta patobulinta prieigos ir srauto kontrolė, o tai galiausiai padidino našumą ir sumažino spūstis.

Be to, buvo priimtas sprendimas įtraukti rezervinius kompiuterius, taip padidinant bendrą tinklo patikimumą. Ši aktyvi priemonė padeda užtikrinti nepertraukiamą veiklą ir sumažina prastovos laiką net ir įvykus netikėtiems gedimams.

Siekiant sustiprinti tinklo saugumą, buvo įdiegtas prieigos kontrolės sąrašas (ACL). Šis ACL buvo sukonfigūruotas taip, kad būtų apribota neteisėta prieiga prie potinklio, kuriame yra biblioteka ir kompiuterių klasės kompiuteriai. Blokuojant prieigą prie šio potinklio, saugumo pažeidimų ir duomenų sugadinimo rizika buvo žymiai sumažinta, o vartotojams ir sistemoms vis tiek buvo suteikta prieiga prie reikiamų išteklių.



3.1 pav. Atnaujinta tinklo topologija

3.1.2. Naudojami prievadai

Kompiuterių tinklo paskirtis yra sujungti mazgus, tokius kaip kompiuteriai, maršrutizatoriai ir komutatoriai, kad įrenginiai galėtų bendrauti ir dalytis informacija bei ištekliais. Būtinos paslaugos, kad kompiuterių tinklas galėtų atlikti numatytas funkcijas, apima duomenų perdavimo ir ryšio tarp įrenginių palengvinimą, veiksmingo ir saugaus tinklo ryšio užtikrinimą, tinklo našumo didinimą ir srauto optimizavimą, grėsmių prevenciją. Atliekant analizę išskirti reikalingiausi prievadai (9 lentelė).

9 lentelė. Tinkle naudojamų prievadų sąrašas

Naudojami prievadai	Paskirtis
20 (FTP)	Failų perdavimo protokolas
22 (SSH)	Naudojamas saugiai ir šifruotai nuotolinei prieigai, failų perdavimui ir sistemos administravimui tarp klientų ir serverių nesaugiame tinkle sukurti.
23 (Telnet)	Naudojamas nuotolinei prieigai prie tinklo įrenginių, leidžiant administratoriams valdyti ir konfigūruoti įrangą, pvz., maršrutizatorius, komutatorius, serverius ir kitus tinklo infrastruktūros elementus iš nuotolinės vietos.
25 (SMTP)	Naudojamas, kad palengvintų el. pašto pranešimų siuntimą ir gavimą tarp pašto serverių.
53 (DNS)	Naudojamas žmonėms suprantamiems domenų pavadinimams išversti į atitinkamus IP adresus, kurių reikia įrenginiams palaikyti ryšį tinkle.
80 (HTTP)	Naudojamas nešifruotiems žiniatinklio duomenims perduoti tarp žiniatinklio serverių ir žiniatinklio klientų, kad vartotojai galėtų prisijungti ir pasiekti internete pasiekiamus tinklalapius.
161 (SNMP)	Naudojamas tinklo įrenginiuose, kad galėtų juos stebėti ir valdyti nuotoliniu būdu.

3.1.3. Tinklo IP adresai

Atlikus struktūros pakeitimus tinklas buvo padalintas į atskirus potinklius (10 lentelė).

10 lentelė. IP adresai

LAN (Po-tinklis)	Kompiute-rių skaičius	Kaukė	Adresų segmentas nuo - iki	Gateway (Maršrutizato-riaus jungties) adresas	Adresai kompiuteriams
Pirmas aukštas	26	255.255.255.224	192.168.10.0-31	192.168.10.1	192.168.10.2-31
Antras aukštas	10	255.255.255.224	192.168.10.32-63	192.168.10.33	192.168.10.34-63
Trečias aukštas	8	255.255.255.224	192.168.10.64-95	192.168.10.65	192.168.10.66-95
Priestatas	3	255.255.255.224	192.168.10.96-127	192.168.10.97	192.168.10.97-127

3.1.4. Tinklo įrangos specifikacija

„Fortigate 60F“ yra galingas tinklo saugos įrenginys, skirtas teikti pažangią apsaugą nuo įvairių kibernetinių grėsmių mažoms ir vidutinio dydžio įmonėms. Kaip pagrindinis tinklo

maršrutizatorius, „Fortigate 60F“ ir toliau atliks savo paskirtį, siūlydamas platų pagrindinių kibernetinio saugumo funkcijų spektrą.

„FortiGate 60F“ siūlo platų saugos funkcijų rinkinį, įskaitant ugniasienę, įsibrovimų prevencijos sistemą (IPS), virtualų privatų tinklą (VPN), apsaugą nuo kenkėjiškų programų, žiniatinklio filtravimą ir kt. Jis palaiko įvairius diegimo režimus, tokius kaip NAT.

11 lentelė. Maršrutizatoriaus „Fortigate 60F“ specifikacija

Maršrutizatorius „Fortigate 60F“ https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-fortiwifi-60f-series.pdf	
Specifikacija	**Aprašymas**
Operacinė sistema	„FortiOS“ („Fortinet“ patentuota operacinė sistema)
Aparatinės įrangos architektūra	64 bitų RISC pagrindu veikiantis procesorius
Tinklo sąsajos	14 x GbE RJ45 prievadų (įskaitant 12 x vidinius prievadus, 2x išorinius prievadus). 2 x Shared Media (SFP/SFP+) lizdai
Atmintis	4 GB
Maitinimo šaltinis	Du keičiami maitinimo šaltiniai
Svoris	4,5 kg.
Matmenys	4.4 x 43.2 x 27 cm

3.2 pav. Maršrutizatorius „FortiGate 60F“

Gimnazijos tinklo pertvarkymo projektui „Cisco Catalyst C9300-24P-A“ pasirodo kaip labai galingas ir universalus sprendimas. Šis tvirtas įrenginys turi 24 Gigabit Ethernet 10/100/1000 PoE+ prievadus, užtikrinančius platų ryšį įvairiems tinklo įrenginiams. 208 Gbps perjungimo sparta ir 154,76 Mpps persiuntimo sparta užtikrina sklandų pralaidumą ir mažą delsą net ir didelio pralaidumo aplinkoje. Be to, jame yra pažangių saugos funkcijų, tokių kaip šifravimas, prieigos kontrolės sąrašai (ACL) ir įvairių maršruto parinkimo protokolų palaikymas, užtikrinantis tvirtą tinklo apsaugą ir efektyvų srauto valdymą.

12 lentelė. Komutatoriaus „Cisco Catalyst C9300-24P-A“ specifikacija

Komutatorius „Cisco Catalyst C9300-24P-A“ https://www.router-switch.com/c9300-24p-a.html	
Specifikacija	**Aprašymas**
Prekės aprašymas	Catalyst 9300 24-port PoE+, Network Advantage
Numatytasis kintamosios srovės maitinimo šaltinis	715W AC
Bendras MAC adresų skaičius	32,000
Persiuntimo greitis	154.76 Mpps
Saugos sertifikatai	• UL 60950-1 • CAN/CSA-C222.2 No. 60950-1 • EN 60950-1 • IEC 60950-1 • AS/NZS 60950.1 • IEEE 802.3
Vidutinis laikas tarp gedimų (valandos)	299,000

3.3 pav. Komutatorius „Cisco Catalyst C9300-24P-A“

Norint pagerinti patikimumą buvo nuspręsta įsigyti „Lenovo ThinkCentre V35s“ rezervinių kompiuterių.

13 lentelė. Kompiuterio „Lenovo ThinkCentre V35s“ specifikacija

Kompiuteris „Lenovo ThinkCentre V35s“ https://www.varle.lt/stacionarus-kompiuteriai/stacionarus-kompiuteris-lenovo-thinkcentre-v35s-sff--32278044.html	
Specifikacija	**Aprašymas**
Procesoriaus tipas	AMD Ryzen 3 3250U
Operatyvioji atmintis (RAM)	8 GB
Procesoriaus dažnis, Ghz	2,6
Talpa	256 GB
Jungtys	1x VGA, 1x HDMI 1.4, 2x. 0 USB 7, 2x. -in-1 kortelių skaitytuvas / GBit LAN,

3.4 pav. Kompiuteris „Lenovo ThinkCentre V35s“

3.2. Problemos sprendimai

3.2.1. Turinio filtravimas

Turinio filtravimas yra esminis švietimo įstaigų kibernetinio saugumo aspektas, nes jis padeda apsaugoti mokinius nuo prieigos prie netinkamo ar žalingo internetinio turinio. Mokyklos tinklo kontekste turinio filtravimas paprastai įgyvendinamas skirtinguose potinkliuose, siekiant užtikrinti saugią mokymosi aplinką. Turinio filtravimas nėra privalomas administracijai ir pedagogams, tačiau jis yra privalomas bibliotekos ir kompiuterių klasėse, kad apsisaugoti nuo incidentų.

3.2.2. Ugniasienės sudarymas

Prieigos kontrolės sąrašas, dar žinomas kaip prieigos kontrolės sąrašas (ACL), yra pagrindinė ugniasienės ir tinklo įrenginių saugos funkcija. Tai taisyklių rinkinys, apibrėžiantis, kuriam srautui leidžiama praeiti arba kurią užkardą blokuoja. Prieigos kontrolės sąrašai yra labai svarbūs norint valdyti ir stebėti tinklo srauto srautą, nes jie leidžia tinklo administratoriams pasirinktinai leisti arba uždrausti prieigą prie konkrečių IP adresų, prievadų ar protokolų.

Negalima pervertinti prieigos kontrolės sąrašų svarbos. Ji atlieka svarbų vaidmenį užtikrinant tinklo saugumą, užkertant kelią neteisėtai prieigai, sumažinant kibernetinių atakų riziką ir užtikrinant, kad tik teisėtam srautui būtų leidžiama pereiti tinklą. Kruopščiai sudarydami prieigos kontrolės sąrašus, tinklo administratoriai gali įgyvendinti savo organizacijos saugos politiką ir apsaugoti svarbiausius išteklius nuo galimų grėsmių.

Kuriant prieigos kontrolės sąrašą, reikia atidžiai apsvarstyti konkrečius savo tinklo poreikius ir reikalavimus. Tai apima srauto, kurį reikėtų leisti arba uždrausti, tipų nustatymą, srauto šaltinius ir paskirties vietas bei atitinkamus veiksmus (leisti arba uždrausti). Prieigos kontrolės sąrašus galima sukonfigūruoti taip, kad būtų galima atlikti įvairius scenarijus, pvz., leisti prieigą prie konkrečių žiniatinklio serverių, blokuoti žinomus kenkėjiškus IP adresus arba apriboti tam tikrų protokolų naudojimą.

3.2.3. Kibernetinių atakų įtakos analizė

14 lentelė. Kibernetinių atakų analizės lentelė

Atakos pavadinimas	Įtaka mokyklai	Įtaka darbuotojams
Duomenų pažeidimas	• Prarandama jautri informacija apie studentus ir personalą. • Finansiniai nuostoliai. • Žala reputacijai.	• Tapatybės vagystės • Privatumo pažeidimai • Emocinis išgyvenimas
Išpirkos reikalaujančios programos	• Sistemos prastovos ir veiklos sutrikimai • Svarbių duomenų praradimas • Finansiniai nuostoliai dėl išpirkos mokėjimų	• Darbo sutrikimas • Emocinė žala dėl pasekmių
Paslaugos trikdymo ataka (angl., „DDoS“)	• Negalėjimas pasiekti mokyklų sistemų, svetainių ir internetinių paskyrų • Mokymo ir mokymosi proceso nesklandumai	• Nesugebėjimas pasiekti reikiamų sistemų ir išteklių • Produktyvumo nuostoliai
Sukčiavimo atakos	• Kenkėjiškų programų įdiegimas • Neteisėta prieiga prie mokyklų tinklų • Finansiniai nuostoliai	• Tapatybės vagystė • Finansiniai nuostoliai • Žala reputacijai

Sukčiavimo atakos kelia didelę grėsmę švietimo įstaigoms. Šios atakos, kai kibernetiniai nusikaltėliai apsimeta patikimais šaltiniais, kad apgautų vartotojus atskleisti neskelbtiną informaciją arba įdiegtų kenkėjiškas programas, gali turėti neigiamų padarinių mokykloms, jų mokiniams. Sukčiavimo atakų poveikis gali būti platus. Jie gali sukelti finansines vagystes, tapatybės sukčiavimą ir jautrių studentų ir darbuotojų duomenų, informacijos atskleidimą. Tai ne tik sukelia tiesioginius finansinius nuostolius ir daroma žala mokyklai reputacijai, bet ir sukelia emocinius išgyvenimus bei ilgalaikę žalą nukentėjusiems asmenims. Siekiant sumažinti sukčiavimo atakų grėsmę, labai svarbu, kad mokyklos pirmenybę teiktų kibernetinio saugumo supratimui ir mokinių, mokytojų ir darbuotojų švietimui. Tai apima mokymą, kaip atpažinti sukčiavimo bandymo požymius, pvz., įtartinus el. laiškų siuntėjus, kenkėjiškas nuorodas, ir skubūs raginimai imtis veiksmų. Mokyklos taip pat turėtų investuoti į patikimus kibernetinio saugumo sprendimus, pvz., el. pašto saugos įrankius, galinių taškų apsaugą ir tinklo ugniasienes, kad aptiktų ir užkirstų kelią sukčiavimo atakoms.

Paslaugos trikdymo ataka (angl., „DDoS“) atakos kelia didelę grėsmę švietimo įstaigoms. Per šias atakas kibernetiniai nusikaltėliai užvaldo tinklą ar serverį kenkėjišku srautu, todėl jis sugenda ir tampa neprieinamas teisėtiems vartotojams. DDoS atakų poveikis mokykloms gali būti nuostolingas. Dėl jų gali sutrikti mokymasis internetu ir patiriami finansiniai nuostoliai dėl taisymo išlaidų. Kad sumažinti DDoS atakų riziką, mokyklos turi įgyvendinti daugiasluoksnę gynybos strategiją. Tai apima grėsmių stebėjimą realiuoju laiku, kad būtų galima greitai aptikti įtartiną veiklą

ir į ją reaguoti, turinio transliavimo tinklų (CDN) naudojimą srautui sugerti ir paskirstyti bei greičio ribojimo metodus gaunamoms užklausoms valdyti. Be to, mokyklos turėtų užtikrinti, kad jų tinklai būtų saugūs su ugniasienėmis, įsibrovimų aptikimo sistemomis ir kitomis saugumo priemonėmis, kad būtų išvengta neteisėtos prieigos ir nustatytų galimas grėsmes. Investuojant į įmonės lygio DDoS apsaugos sprendimus taip pat galima užtikrinti pažangų grėsmių aptikimą.

Duomenų pažeidimo atakos yra dar viena dažnai pasitaikanti ataka mokyklose. Šios atakos, kai kibernetiniai nusikaltėliai neteisėtai gauna prieigą prie konfidencialios informacijos ir duomenų. Duomenų pažeidimo atakos gali sukelti finansinių nuostolių, neskelbtinų studentų ir darbuotojų duomenų, asmeninės informacijos atskleidimą ir didelę žalą mokyklos reputacijai. Siekiant sumažinti duomenų pažeidimo atakų grėsmę, labai svarbu, kad mokyklos pirmenybę teiktų mokinių, mokytojų ir darbuotojų informavimui apie kibernetinį saugumą. Tai apima mokymą, kaip atpažinti galimo duomenų pažeidimo požymius, pvz., įtartinus el. pašto siuntėjus, kenkėjiškas nuorodas ir neteisėtos prieigos bandymus. Mokyklos taip pat turėtų investuoti į patikimus kibernetinio saugumo sprendimus, tokius kaip duomenų šifravimas, prieigos kontrolė ir tinklo stebėjimo įrankiai, aptikti ir užkirsti kelią duomenų pažeidimo atakoms.

Išpirkos reikalaujančios atakos tapo nerimą keliančia grėsme švietimo įstaigoms, ypač mokykloms. Šios kenkėjiškos atakos užšifruoja svarbius duomenis ir sistemas, todėl jos tampa neprieinamos, kol nebus sumokėta išpirka. Mokyklos tapo pagrindiniais kibernetinių nusikaltėlių taikiniais dėl daugybės neskelbtinos asmeninės informacijos, kurią jos saugo, pavyzdžiui, mokinių įrašų, darbuotojų informacijos. Dėl šios atakos gali sutrikti mokyklos procesas ir gali būti patirta žala reputacijai. Siekdamos sumažinti išpirkos reikalaujančių programų atakų riziką, mokyklos turi teikti pirmenybę aktyvioms kibernetinio saugumo priemonėms. Tai apima reguliarų duomenų atsarginių kopijų kūrimą, programinės įrangos ir sistemų atnaujinimą, prieigos kontrolės sąrašų įgyvendinimą ir darbuotojų, ir mokinių saugos mokymą.

3.2.4. Atnaujintos struktūros patikimumo skaičiavimai

Atnaujintas tinklas turi po viena rezervinį kompiuterį kiekviename potinklyje, taip nuspręsta daryti nes senasis tinklas neturėjo rezervinių kompiuterių ir buvo nustatytos ilgos prastovos gedimų atveju. Naudojamas tik vienas rezervinis kompiuteris, nes mokyklos tinklas nėra didelis. Dideliame tinkle būtų siūloma diegti du ar daugiau rezervinių kompiuterių (15 lentelė).

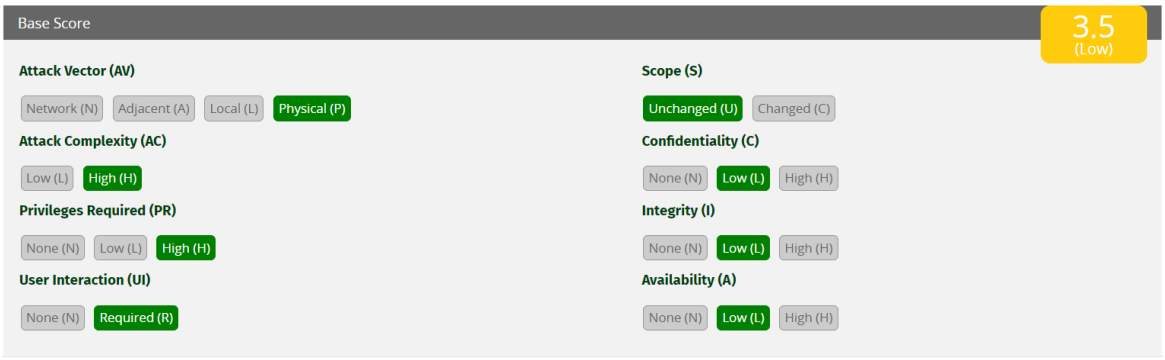
15 lentelė. Patikimumo skaičiavimai po rezervavimo

Pirmas aukštas			**Antras aukštas**			**Trečias aukštas**			**Priestatas**		
sk.	patik.	Δ, min.	sk.	patik.	Δ, min.	sk.	patik.	Δ, min.	sk.	patik.	Δ, min.
27	0,9996	182	11	0,9994	29	9	0,9999	19	3	0,9999	3

Atlikus patikimumo apskaičiavimus atnaujintame tinkle, galime daryti išvada, kad rezervavimas prisideda prie tinklo stabilumo. Tinklas tampa ženkliai patikimesnis ir stipriai sumažėja prastovų laikas.

3.2.5. Atnaujintos struktūros pažeidžiamumo vertinimas

Atlikus tinklo pakeitimus, tinklo struktūros pažeidžiamumas sumažėjo. Prieš atliekant pakeitimus buvo nustatytas aukštas balas (7,4), o pakoregavus tinklą šis balas nukrito iki (3,5). Pertvarkius gimnazijos tinklą, patobulintos fizinės saugos priemonės padeda sušvelninti riziką, susijusią su pažeidžiamumu, reikalaujančiu fizinės prieigos, taip pagerinant bendrą saugumo padėtį (3.5 pav.).



3.5 pav. Tinklo pažeidžiamumo vertinimas po atnaujinimo

Pažeidžiamumo vektorius - CVSS:3.1/AV:P/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L

3.3. Reorganizacijos plano sudarymas

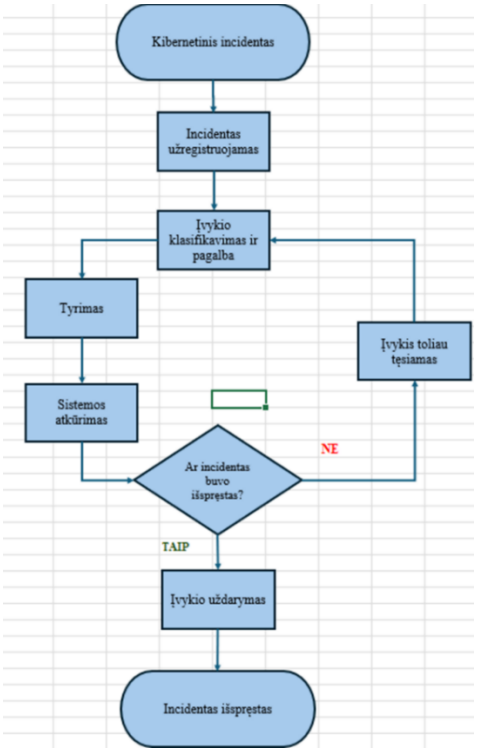
Modernizuojant mokyklų tinklus, siekiant kuo mažiau trikdyti ugdymo procesą, itin svarbu parengti išsamų reorganizavimo planą. Planas turėtų būti sutelktas į aiškių tikslų, prioritetų ir strategijų nustatymą esamoms kliūtims ir iššūkiams pašalinti. Pagrindinis prioritetas turėtų būti kuo labiau sumažinti švietimo veiklos trikdžius pertvarkant tinklą. Tai galima pasiekti taikant etapinį metodą, pvz., „nuskaityti, eiti, bėgti“ metodą (angl. crawl, walk, run), kuris apima koncepcijos patikrinimą ribotoje aplinkoje prieš įgyvendinimą. Perėjimas nuo senojo tinklo į naują turėtų būti organizuojamas palaipsniui, procesą aktyviai derinant su mokyklos administracija. Turėtų būti parengtas perėjimo grafikas, nurodant suplanuotą perjungimo laiką ir datas, taip pat pateikiama informacija apie paruoštą tinklo įrangą. Be to, išlaikant matomumą apie infrastruktūros būklę ir naudojant tinklo našumo stebėjimo ir diagnostikos priemones, galima išvengti bet kokių diegimo

klaidų ir jas greitai pašalinti. Tinklas gali būti sukonfigūruotas taip, kad vienu metu veiktų ir senos, ir naujos sistemos, užtikrinant sklandų perėjimą. Tai galima pasiekti tinkamai sukonfigūravus tinklo sąsajas, įskaitant IP adresų, potinklio kaukių informacijos priskyrimą. Šiuo požiūriu siekiama kuo labiau sumažinti poveikį ugdymo procesui ir užtikrinti sklandų mokyklos perėjimą į saugesnį tinklą.

3.4. Kibernetinių incidentų valdymo diagrama

Norint užtikrinti veiksmingą koordinavimą, labai svarbu turėti specialų asmenį, atsakingą už reagavimą į kibernetinius incidentus. Šis kontaktinis taškas supaprastina komunikaciją, sprendimų priėmimą ir priežiūrą incidento metu. Jo vaidmuo apima viso reagavimo proceso priežiūrą – nuo aptikimo iki koordinavimo su kitais pagrindiniais komandos nariais. Šis specialus vaidmuo atitinka geriausią praktiką ir pabrėžia organizacijos įsipareigojimą aktyviai valdyti kibernetinius incidentus.

Veiksmingam kibernetinių incidentų valdymui reikalinga gerai koordinuota komanda, turinti skirtingus vaidmenis. Darbuotojai, atsakingi už reagavimą į incidentus ir sistemos atkūrimą, supaprastina procesus, išvengia dubliavimosi ir užtikrina, kad nebūtų pamirštos svarbios užduotys. Aiškus vaidmenų priskyrimas palengvina komunikacija, todėl komanda gali greitai rasti sprendimus.



3.6 pav. Kibernetinių incidentų valdymo diagrama

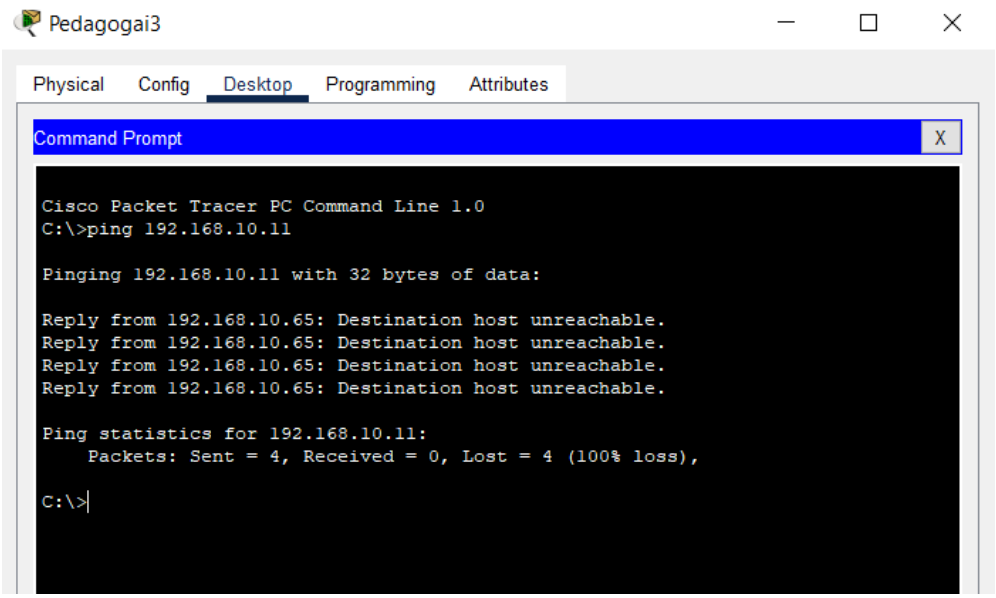
4. PRAKTINĖ-EKSPERIMENTINĖ DALIS

4.1. Kibernetinio saugumo diegimo specifikacija

Siekiant užtikrinti saugumą ir išvengti neteisėtos prieigos, mokyklų kompiuterių klasėse ir bibliotekose esantys kompiuteriai izoliuojami nuo pagrindinio tinklo, naudojant ugniasienę.

4.2. Techninis kibernetinio saugumo testavimas

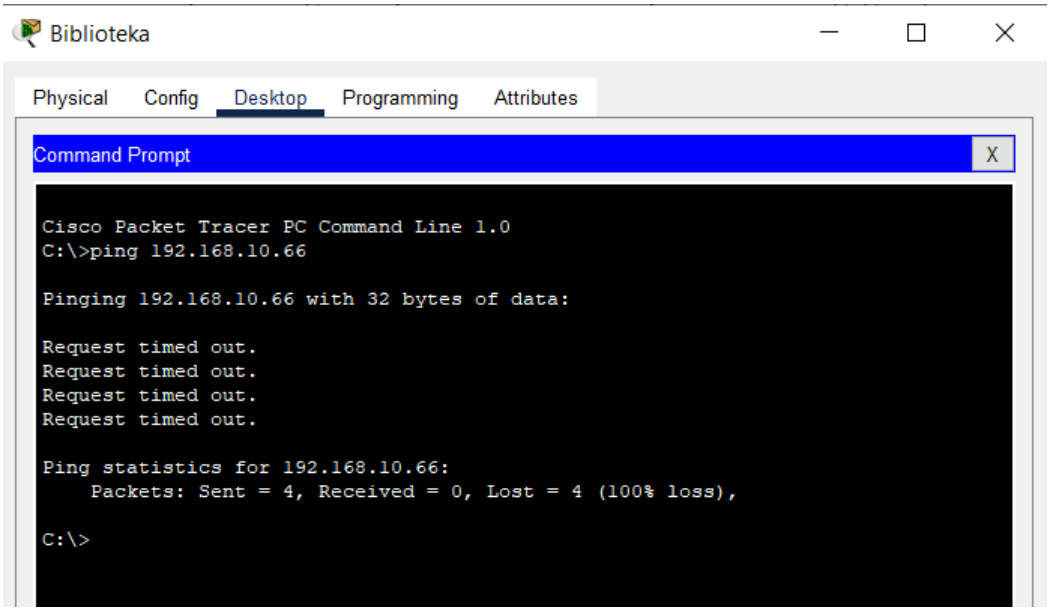
Saugumo testavimui patikrai bus naudojamas Pedagogai3 ir Biblioteka esantys kompiuteriai. Naudojant prieigos kontrolės sąrašus siekiamas tikslas atskirti šias darbo vietas, kad jos neturėtų jokios prieigos viena su kita. Ar šis tikslas pasiektas galime patikrinti išsiunčiant paketus iš Pedagogai3 į Biblioteka kompiuterį.



4.1 pav. Paketų perdavimas iš Pedagogai3 į Biblioteka

Atlikus pirmąjį testą matome, kad Pedagogai3 esantis kompiuteris neturi galimybės susisiekti su Biblioteka kompiuteriu.

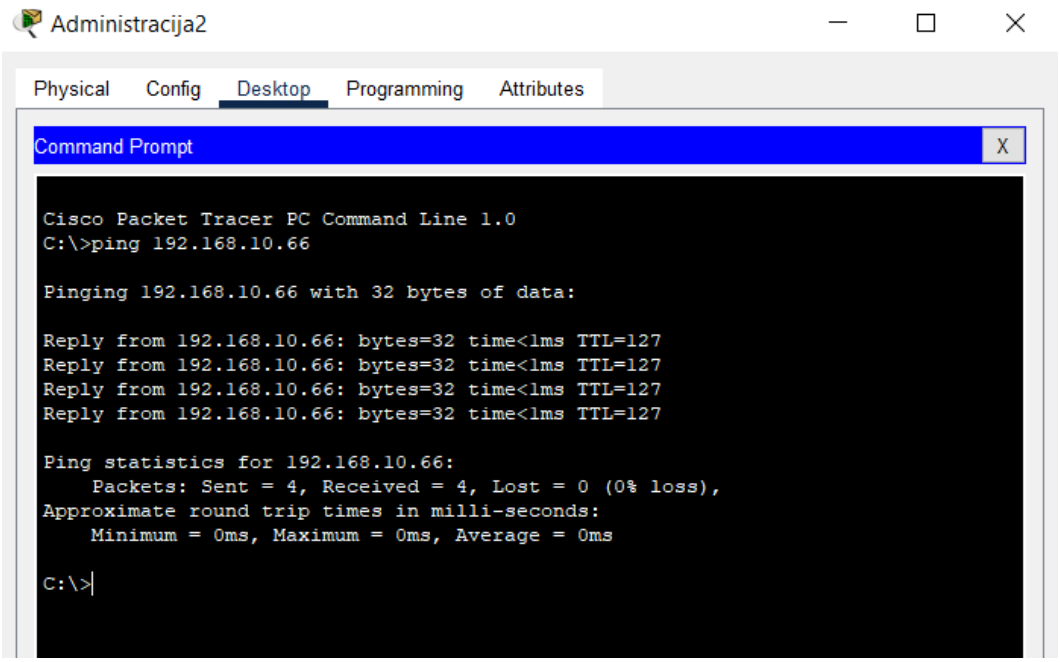
Taip pat turime nustatyti ar Biblioteka kompiuteris negali pasiekti Pedagogai3 kompiuterio išsiunčiant paketus.



4.2 pav. Paketų perdavimas iš Biblioteka į Pedagogai3

Paketai nepasiekė savo tikslo ir galime daryti išvadą, kad prieigos kontrolės sąrašų nustatymas veikia ir darbo vietos buvo atskirtos.

Pilnam bandymo užtikrinimui išsiunčiame paketus iš Administracija2 į Pedagogai3.



4.3 pav. Paketų perdavimas iš Administracija2 į Pedagogai3

Siunčiami paketai pasiekią tikslą ir matome, kad konfigūracija yra teisinga ir paketai yra praleidžiami tarp šių kompiuterių.

4.3. Testavimo rezultatų analizė ir išvadų apibendrinimas

Atliekant kibernetinio saugumo didinimą buvo skiriamas dėmesys kompiuterių klases ir bibliotekos kompiuterių atskyrimui nuo mokyklos tinklo. Šis tikslas buvo siekiamas naudojant prieigos kontrolės sąrašo taisykles. Atlikus reikiamus žingsnius, rezultatas buvo pasiektas ir šios darbo vietos buvo atskirtos.

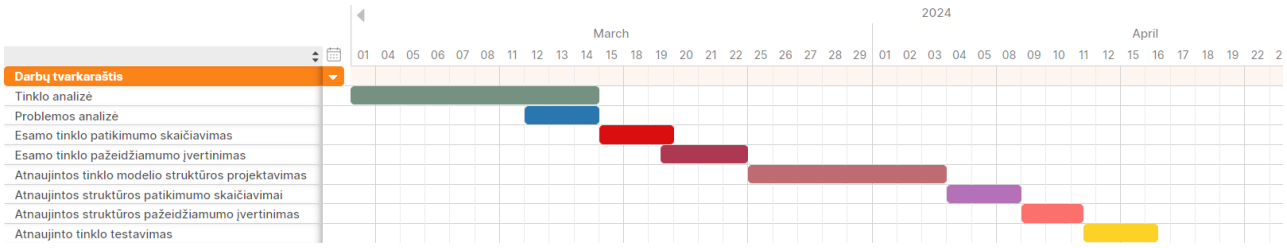
Galime teigti, kad uždaviniai atlikti ir tinklo saugumas yra pasiektas.

5. EKONOMINĖ DALIS

Ekonominio vertinimo atlikimas yra labai svarbus norint pagrįsti projekto ekonominę vertę ir pristatyti jį kaip perspektyvią investavimo galimybę.

5.1. Projekto projektavimo sąmata

Norint atlikti ekonominę dalį privalu pasiskirstyti atliktus darbus ir žinoti kiek laiko tie darbai buvo daromi.



5.1 pav. Projekto projektavimo darbų tvarkaraštis

16 lentelė. Projektavimo darbo laiko nustatymas

Darbai	Dirbta valandų
Tinklo analizė	25
Problemos analizė	10
Esamo tinklo patikimumo skaičiavimas	6
Esamo tinklo pažeidžiamumo įvertinimas	12
Atnaujintos tinklo modelio struktūros projektavimas	40
Atnaujintos struktūros patikimumo skaičiavimai	6
Atnaujintos struktūros pažeidžiamumo įvertinimas	10
Atnaujinto tinklo testavimas	10

17 lentelė. Ilgalaikio turto nusidėvėjimo ir programinės įrangos mokestis

Pavadinimas	1 mėn. vertė, eur.	Mėn. kiekis, vnt.	Iš viso, eur
Ilgalaikis turtas	-	-	-
1. Kompiuteris	21	3	63
2. Maršrutizatorius	2	3	6
3. Klaviatūra	1	3	3
Programinė įranga	-	-	-
1. Microsoft „Office“	7,5	3	22,5
2. Microsoft „Windows“	9,6	3	28,8
		Iš viso:	123,3

5.2. Projekto projektavimo darbo užmokesčio skaičiavimas

Skaičiuojant atlyginimą naudojamas vidutinis atlyginimas Lietuvoje – 2110 eurai, valandinis darbo užmokestis – 12,63 eur. Atliekant projektą išdirbta 119 valandų.

Bruto atlyginimo skaičiavimas:

12,63 * 119 = 1502,97 eur

VSD yra 1,77% tai – 1502,97 * 0,0177 = 26,60 eur

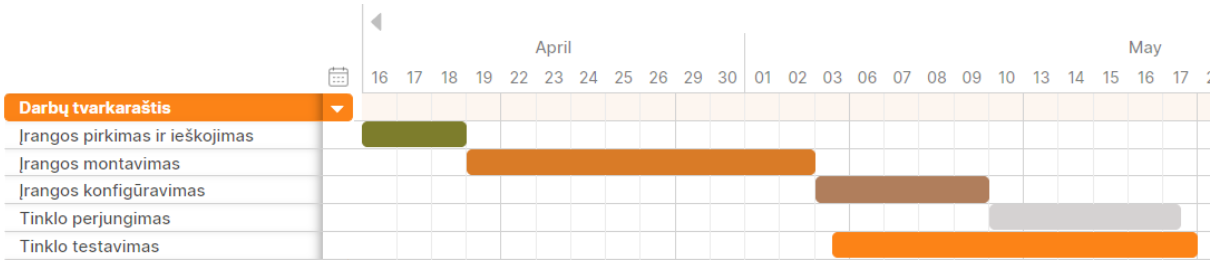
Gaunama alga: 1502,97 + 26,60 = 1529,57

18 lentelė. Projektavimo sąmata

Nr.	Pavadinimas	Suma, eur
1.	Ilgalaikio turto nusidėvėjimas ir programinė įranga	123,3
2.	Projektavimo atlyginimo sąnaudos	1529,57
	Iš viso:	1652,87

5.3. Projekto įgyvendinimo sąmata

Projekto įgyvendinimo sąmatoje aprašomi reikalingi darbai, išlaidos projekto įgyvendinimui.



5.2 pav. Projekto įgyvendinimo darbų tvarkaraštis

19 lentelė. Įgyvendinimo darbo laiko skaičiavimas

Darbai	Dirbta valandų
Įrangos pirkimas ir ieškojimas	15
Įrangos montavimas	50
Įrangos konfigūravimas	15
Tinklo perjungimas	20
Tinklo testavimas	40

20 lentelė. Įrangos pirkimo sąmata

Įrangos pavadinimas	Tiekėjo pavadinimas	Kaina, eur	Kiekis	Suma, eur
1. „Fortigate 60F“	Fortigate	600	1	600
2. „Cisco Catalyst C9300-24P-A“	Cisco	700	4	2800
3. „Lenovo ThinkCentre V35s“	Lenovo	236,99	6	1421,94
			Iš viso:	4821,94

21 lentelė. Ilgalaikio turto nusidėvėjimo ir programinės įrangos mokestis

Pavadinimas	1 mėn. vertė, eur.	Mėn. kiekis, vnt.	Iš viso, eur
Ilgalaikis turtas	-	-	-
1. „Fortigate 60F“	9,78	3	29,34
2. „Cisco Catalyst C9300-24P-A“	10,52	3	31,56
3. „Lenovo ThinkCentre V35s“	4,68	3	14,04
		Iš viso:	74,94

5.4. Projekto įgyvendinimo darbo užmokesčio skaičiavimas

Skaičiuojant atlyginimą naudojamas vidutinis atlyginimas Lietuvoje – 2110 eurai, valandinis darbo užmokestis – 12,63 eur. Atliekant projektą išdirbta 140 valandų.

Brutto atlyginimo skaičiavimas:

12,63 * 140 = 1768,2 eur

VSD yra 1,77% tai – 1768,2 * 0,0177 = 31,29 eur

Gaunama alga: 1768,2 + 31,29 = 1799,29 eur

22 lentelė. Projektavimo sąmata

Nr.	Pavadinimas	Suma, eur
1.	Naujos įrangos pirkimas	4821,94
2.	Ilgalaikio turto nusidėvėjimo ir programinės įrangos mokestis	74,94
3.	Projekto rengėjo atlyginimo sąnaudos	1799,29
	Iš viso:	6696,17

5.5. Įdiegto projekto palaikymo sąnaudos

Paskaičiuojamos reikalingos išlaidos projekto palaikymui.

23 lentelė. Įdiegto projekto atlyginimo skaičiavimas

Darbai	Dirbta valandų	Įdiegto projekto palaikymo rengėjo valandinis atlyginimas, eur	Iš viso, eur
Įrangos pirkimas ir ieškojimas	3	12,63	37,89
Įrangos montavimas ir konfigūravimas	10	12,63	126,3
Įrangos testavimas	5	12,63	63,15
		Iš viso:	227,34

24 lentelė. Įdiegto projekto palaikymo sąmata

Nr.	Pavadinimas	Suma, eur
1.	Įdiegto projekto palaikymo atlyginimo sąnaudos	223,34
	Iš viso:	223,34

5.6. Projekto sąmata

25 lentelė. Projekto sąmata

Nr.	Pavadinimas	Suma, eur
1.	Projekto projektavimo sąnaudos	1652,87
2.	Projekto įgyvendinimo sąnaudos	6696,17
3.	Įdiegto projekto palaikymo sąnaudos	223,34
	Iš viso:	8572,38
4.	Administracinės sąnaudos (10%)	857,23
	Iš viso:	9429,61

5.7. Ekonominės naudos nustatymas

Skaičiuojant ekonominę naudą sužinome per kiek laiko atsiperka projektas. Pagal NKSC nurodymus privaloma paskaičiuoti šiuos rodiklius.(Lietuvos Respublikos Vidaus reikalų ministerija, 2005):

- Pažeidžiamumo veiksniai (žala) (PV)
- Tikėtini vienkartiniai nuostoliai (TVN)
- Metinis dažnumo rodiklis (MDR)
- Tikėtinas metinis nuostolis (TMN)

Rizikos paskaičiavimas prieš projekto atnaujinimą:

PV = 50%;
TVN = turto vertė * PV =10143,73 * 50% = 5071,86 eur
MDR = 0,5;
TMN = TVN * MDR = 4026,07 * 0,5 = 2013,03 eur

Rizikos paskaičiavimas po projekto atnaujinimo:

PV = 20%;
TVN = turto vertė * PV =10143,73 * 20% = 2028,74 eur
MDR = 0,15;
TMN = TVN * MDR = 4026,07 * 0,15 = 603,91 eur

Atlikus ekonominės naudos skaičiavimus nustatyta, kad projektas atsipirktų per 6 metus.

IŠVADOS

1. Išanalizuotas gimnazijos tinklas ir surasti sprendimai kibernetinio saugumo gerinimui: darbo vietų atskyrimas, kompiuterių rezervavimas, prieigų sąrašo naudojimas.
2. Atlikus kibernetinio saugumo padidinimo įrankių analizę, buvo apžvelgiami įrankiai padėsiantys stebėti tinklą.
3. Atliekant tinklo pažeidžiamumo vertinimą ir remiantis vertinimo įrankiu, buvo nustatytas aukštas tinklo pažeidžiamumo lygis. Įgyvendinus projektą šis rodiklis sumažėjo nuo 7,4 iki 3,5.
4. Analizuojant tinklą nustatyta, kad nėra rezervuotų kompiuterių, tai reiškia aukštas prastovas gedimų atveju. Pasiūlyta kiekviename potinklyje turėti bent viena rezervinį kompiuterį taip apsisaugant nuo nenorimų prastovų.
5. Modeliavimo programoje sukurtas tinklas remiantis surastais kibernetinio saugumo didinimo sprendimais. Šis sprendimas buvo ištestuotas virtualioje aplinkoje.
6. Atlikti ekonominiai skaičiavimai pagrindžiantys projekto ekonominę vertę. Nustatyta, kad projektas atsipirks per 6 metus.

LITERATŪRA IR KITI INFORMACIJOS ŠALTINIAI

1. 716 Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo ir Saugos dokumentų turinio gairių aprašo patvirtinimo. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.454399?jfwid=
2. 818 Nutarimas dėl nacionalinės kibernetinio saugumo strategijos patvirtinimo. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595
3. Cisco Packet Tracer. https://www.netacad.com/courses/packet-tracer
4. Lietuvos Respublikos administracinių nusižengimų kodeksas. https://www.e-tar.lt/portal/lt/legalAct/4ebe66c0262311e5bf92d6af3f6a2e8b
5. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/bc0837f27f9511e89188e16a6495e98c
6. Lietuvos Respublikos Vidaus reikalų ministerija, (2005) https://www.nksc.lt/doc/rizikos_analize.pdf
7. Nacionalinė kibernetinio saugumo ataskaita 2022. https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf
8. Nagios. https://www.nagios.org/
9. NKSC Ypač svarbios efektyviai kibernetinei gynybai saugumo kontrolės priemonės. https://www.nksc.lt/doc/NKSC%20plakatas%20(20cc)_1.pdf
10. Nmap Network mapper https://nmap.org/
11. Pažeidžiamumo vertinimo sistema CVSS. https://www.first.org/cvss/calculator/3.1
12. Tom’s Planner. https://www.tomsplanner.com/
13. Višniakas I., Slivinkas K., (2005) Patikimumo teorija http://elibrary.lt/resursai/Mokslai/VGTU/Leidiniai/Leidinukai/10.pdf
14. Wireshark. https://www.wireshark.org/
15. Zabbix. https://www.zabbix.com/